# NOVDEC AC – Conflict/Terror

We affirm

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

## Contention One is Avoiding Direct Conflict.

**Ali & Stewart** of Reuters explains in **2019** that cyber strikes are seen as a less-provocative option below the threshold of war, as you can do damage without killing people. It is an important option in the toolkit.

This alternative is crucial to keeping the US out of war. **Groll** of Foreign Policy explains in **2019** that already twice this year, the US government has canceled military strikes on Iran in favor of offensive cyberattacks, once after Iran shot down a US drone and again after Iran attacked Saudi oil facilities. Crucially, **Rasidi** of Citizen Truth explains in **2019** that these cyberattacks successfully hijacked computers Iran had used to launch missiles and it crippled the Iranian military for months without any casualties being reported.

However, without the option for offensive cyber operations, the US would have been forced to conduct conventional military strikes in response to Iranian provocations.

A conventional strike could be devastating as **Dilanian** from NBC writes in **2019** that just a **LIMITED** US strike on Iran could prompt a potent Iranian reaction that would spark a much larger military conflict, as the US hasn’t authorized a strike on Iran since the 1980s. This could result in a full-scale war that costs trillions of dollars and untold American lives.

## Contention Two is Countering ISIS.

Admiral Michael **Rogers** writes in **2018** that ISIS’ so-called caliphate is crumbling as it has lost 98% of its territory. US cyber operations have played a crucial role in this campaign.

This is for 3 reasons.

First, is by Controlling Recruiting Networks.

**Work** of the Atlantic Council explains in **2017** that ISIS is the product of utterly modern global communication networks. Internal communications, foreign recruitment, and the promotion of its global brand are operations crucial to its survival. ISIS had turned the web into a weapon.

This is important because **Bate** of the American Security Project finds in **2017** that the US has used offensive cyber operations to inhibit communication between ISIS members and bring down media platforms that are critical to recruiting. Because of this ISIS’ international recruitment rate has collapsed. That is why **Temple-Raston** of NPR concludes in **2019** that 6 months after this operation, ISIS’ media operations were a shadow of its former self.

Second, is by Cutting Off Their Funding.

**Windrem & Arkin** write for NBC in **2019** that the cyber efforts against ISIS financial network have been critical in upending ISIS, as they have a constant need for hard currency to pay their fighters and feed their population. Through cyber war, the US is tracking, manipulating, and destroying the financial assets of these terrorists.

Even more, these cyber operations have complemented military operations as by gaining critical intelligence on ISIS financial transactions through offensive cyber operations the US military has been able to find and physically destroy ISIS financial centers in air strikes, thus turning millions of dollars into confetti.

Third, is by aiding Kinetic Military Strikes.

**Pomerlau** explains in **2018** that US Cyber Command has been heavily involved in using offensive cyber operations against ISIS to provide US agencies with intelligence and thus aid kinetic operations to rid the group from Iraq and Syria. This has helped provide battlefield options to military commanders.

In addition, **Duffy** of cyberscoop writes in **2018** that through offensive cyber operations, we were able to find ISIS command posts and launch cyberattacks against their computer systems, forcing them to leave these command posts and exposing them to attack with kinetic weapons. Even more, this forced ISIS to reveal alternate command posts in Iraq and Syria that the US was able to destroy to finally rid them from the region.

The impact is stability in the Middle East.

**Jamieson** writes for NBC News in **2016** that between 2014 and 2016, the UN recorded 55,000 casualties due to ISIS violence and **Crowcroft** finds in **2015** that in Iraq alone 3.3 million people have been displaced with millions more in Syria. Fortunately, thanks to US offensive cyber operations, **Rogers** reports that ISIS has lost 98% of its territory, thus saving lives and promoting stability.

**Vavra** continues that going forward, the US will be poised to rely more heavily on offensive cyber capabilities to target the dispersed but continually active membership of ISIS. She finds that as ISIS gains momentum in other areas like Afghanistan, cyber operations will play a critical role in controlling their growth.

Thus, to ensure a peaceful future, we affirm.

# CARDS

## C1 Direct Conflict

Freiburger ’19, Kevin Freiburger, 27 August 2019, GCN, <https://gcn.com/articles/2019/08/27/cybersecurity-offense.aspx>

The U.S. currently deploys offensive cybersecurity strategies [with Russia](https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html). In what is a more aggressive strategy for the U.S., officials confirmed that they have placed the equivalent of digital land mines into Russia’s electric power grid to serve as a warning to President Vladimir Putin and as a demonstration of Cyber Command’s power. This particular effort adds to a previous cyber strategy already in place meant to overwhelm the computer systems at Russia’s Internet Research Agency -- the entity responsible for the 2016 election meddling. Offensive cyberattacks are conducted remotely, shortening the time for deployment and costing less than conventional weaponry and military infrastructure. And in some ways, offensive cyber strategy has the potential to save lives. In June of this year, the U.S. called off a conventional weapons [counterattack on Iran](https://news.yahoo.com/pentagon-secretly-struck-back-against-iranian-cyber-spies-targeting-us-ships-234520824.html) due to the high potential of human casualties. The DOD chose to instead move forward with an unnamed cyberattack.

Ali & Stewart ’19, 16 October 2019, Idrees Ali & Phil Stewart, Reuters, <https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-idUSKBN1WV0EK>

The impact of the attack, if any, could take months to determine, but cyber strikes are seen as a less-provocative option below the threshold of war. “You can do damage without killing people or blowing things up; it adds an option to the toolkit that we didn’t have before and our willingness to use it is important,” said James Lewis, a cyber expert with the Washington-based Center for Strategic and International Studies.

Rasidi ’19, Yasmeen Rasidi, 23 October 2019, Citizen Truth, <https://citizentruth.org/has-the-us-already-declared-a-cyber-war-on-iran/>

Conventional battlefields have been replaced by cyber warfare and the U.S. has already conducted two cyber attacks on Iran in 2019. The U.S. is believed to have launched at least two secretive cyber attacks on Iran in the last six months, the most recent came following two drone attacks on Saudi Arabian oil facilities on September 14. To the best of public knowledge, Iran has not conducted any cyber attacks on the U.S in recent months. But given the growing tensions between the two countries and their shared desire to avoid firing bullets, cyberspace could be emerging as the new alternative battlefield of choice. The ongoing U.S.-Iran tension was triggered by Washington’s withdrawal from the Iran Nuclear Deal, known as the Joint Comprehension Plan of Action (JCPOA). The U.S. under President Trump claimed the deal was not adequate in halting Iran’s nuclear ambitions despite [repeated assurances by an international monitoring agency](https://citizentruth.org/israel-accuses-iran-of-lying-about-nuclear-weapons-programs-while-iaea-un-say-otherwise/) that Iran was in compliance with the deal. President Trump then also reimposed sanctions on Tehran after withdrawing from the JCPOA. The rift escalated after Iran announced it would reduce its compliance to the JCPOA by enriching uranium exceeding the level allowed in the JCPOA. That announcement was followed by a series of attacks on oil tankers crossing the Strait of Hormuz which the U.S. blames on Iran despite a lack of evidence supporting the U.S. claims. The September 14 cyber attack was reported by two unidentified American officials to [Reuters](https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-say-idUSKBN1WV0EK) who claimed the operation was aimed at crippling Iran’s ability to spread propaganda. The U.S. attack came in retaliation for the drone strikes on Saudi oil facilities which the U.S. believes Iran carried out despite Houthi rebels in Yemen claiming responsibility. The American officials told Reuters the attack affected “physical hardware” without specifying more detail. The Pentagon refused to comment on the Reuters report, [stating](https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html), “As a matter of policy and for operational security, we do not discuss cyberspace operations, intelligence, or planning.” Iran also denied the Reuters report with Iran’s Minister of Communications and Information Technology Mohammad Javad Azari-Jahromi telling Reuters: “They must have dreamt it.” It’s possible but unknown whether Washington has carried out any other cyber attacks on Iran since the end of September. However, one thing is clear, the September attack on Iran was not a first and suggests cyber warfare may be increasingly favored by U.S. administrations intent on avoiding actual military confrontations. The U.S. Army conducted a previous cyber attack targeting Tehran last June as retaliation following U.S. allegations that Iran shot down American surveillance drones in international airspace, but which Iran claims were in Iranian airspace. [According to The Washington Post,](https://www.washingtonpost.com/national-security/us-military-carried-out-secret-cyber-strike-on-iran-to-prevent-it-from-interfering-with-shipping/2019/08/28/36202a4e-c9db-11e9-a1fe-ca46e8d573c0_story.html) President Trump himself ordered the U.S. Cyber Command to carry out the Iran cyber attack following the drone shooting and recent attacks on oil tankers. The order for the attack reportedly came the same day that Trump called off airstrikes targeting Iran. The attack hit computers used to control the launching of rockets and missiles, but no casualties were reported, according to The Post. U.S. officials claimed the June cyber attack hit 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,” [as the N.Y. Times reported](https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html). Officials also brandished the attacks a widespread success, claiming the attacks crippled Iran for months.

Groll ’19, Elias Groll, Foreign Policy, 27 September 2019, <https://foreignpolicy.com/2019/09/27/the-u-s-iran-standoff-is-militarizing-cyberspace/>

That fact has heightened the appeal of cyberweapons to Trump; hesitant to inflict casualties, he canceled at the last minute a retaliatory military strike against Iran after the downing of a U.S. drone in June. Instead, Trump launched cyberattacks against Iranian computer systems that were used in organizing the seizure of tankers. Once again, this time in retaliation for an attack earlier this month on Saudi oil facilities, Trump is reportedly mulling the use of cyberweapons.

Dilanian ’19, Ken Dilanian, NBC News, 21 June 2019, <https://www.nbcnews.com/news/world/if-u-s-strikes-iran-what-might-happen-next-n1020451>

A limited U.S. strike on Iran of the sort President Donald Trump says [he canceled](https://www.nbcnews.com/politics/politics-news/trump-says-he-did-not-given-final-approval-iran-strikes-n1020386) Thursday night could prompt a potent [Iranian reaction](https://www.nbcnews.com/news/world/tensions-high-iran-mideast-after-trump-calls-strikes-n1020136) that in turn might spark a much larger military conflict, current and former U.S. officials and experts tell NBC News. Iran could do enormous damage to the global economy by mining the Strait of Hormuz, the waterway off its coast through which flows 40 percent of the crude oil traded internationally. That action, even if quickly countered by the U.S. Navy, would cause oil prices to spike. But that may not be Iran's first move in response to a limited American bomb and missile attack, experts say. Iran would likely turn first to [its proxies](https://www.nbcnews.com/politics/national-security/iran-uses-proxies-punch-above-its-weight-middle-east-experts-n1008731), who could inflict major damage on American allies, experts say. Houthi rebels in Yemen could step up attacks against Saudi Arabian infrastructure with missiles and drones. Shiite militias could destabilize Iraq. Hezbollah, the Iran-backed terrorist organization, could attack Israel or other American interests anywhere in the world. And if Iran wanted to kill Americans, any of those groups could do that on its behalf, with some deniability, said the experts. Shiite militias could overrun the U.S. Embassy in Baghdad and seize hostages. Hezbollah, which, before 9/11, had killed more Americans than any other terror group, could strike in places as far flung as Latin America, where the group has a strong presence. "Traditionally, when faced with this sort of American action, Iran doesn't tend to respond directly and immediately, but they do so asymmetrically and over a period of time," said Ray Takeyh, a former State Department official and Iran expert at the Council on Foreign Relations. Trump said in a tweet Friday that he stopped a U.S. attack on Iran that would have targeted three sites. He told NBC's Chuck Todd in an exclusive interview Friday that, after being told the attack could cost 150 Iranian lives, he decided it was not proportional to the downing of an unmanned spy drone. The U.S. and Iran have been attacking one another covertly for decades. President Barack Obama is believed to have ordered a cyberattack that employed malware known as Stuxnet to set back Iran's nuclear program by causing centrifuges to malfunction, for example. Iran built powerful bombs that killed American troops in Iraq. But the last time an American president authorized a military strike on Iranian forces was in the 1980s, when Iran was fighting a war against Iraq and attacking tanker traffic in the Persian Gulf. In April 1988, an Iranian mine wounded 10 sailors on the USS Samuel B. Roberts. American forces responded by destroying much of Iran's small navy and taking out two oil platforms used by the Islamic Revolutionary Guard Corps. After a U.S. guided missile cruiser accidentally shot down an Iranian passenger airliner in July 1988, killing 290 civilians, Iran capitulated, believing the shootdown was not an accident. But analysts say Iran's capacity to inflict pain on the U.S. and its allies is much greater than in the 1980s, experts say. In addition to its extensive proxy forces, Iran has a potent cyber capability that could, in theory, take down networks and harm the American economy. Iran is believed to be responsible for a cyberattack that wiped out 35,000 computers at the Saudi oil company Aramco in 2012. The U.S., of course, could inflict massive damage on Iran. American forces could obliterate Iran's entire navy in two days, according to a recent Pentagon analysis, described by multiple U.S. officials. But Iran's clerical regime, which cares most about its survival, may respond to that in unpredictable ways. "Very quickly we could end with miscalculation as both sides fear offensive action by the other or tit for tat that escalates into a much more significant conflict," said Ilan Goldenberg, director of the Middle East Security Program at the Center for New American Security, on Twitter. The U.S. might believe it was sending Iran a message of deterrence by punishing it with limited air strikes. But Iran could interpret those strikes as a precursor to an invasion, and act accordingly. The result could be full-scale war. An all-out effort by the U.S. to depose the Iranian regime could cost trillions of dollars and untold American lives, Goldenberg wrote in a recent analysis. "Even short of such worst-case scenarios, any war with Iran would tie down the United States in yet another Middle Eastern conflict for years to come. The war and its aftermath would likely cost hundreds of billions of dollars and hobble not just Trump but future U.S. presidents. Such a commitment would mean the end of the United States' purported shift to great-power competition with Russia and China," he wrote. Trump has said he doesn't want that. The president told NBC News he is inviting Iran's senior leaders to talk. "I'm not looking for war," Trump said to Todd. "And if there is, it will be obliteration like you've never seen before. But I'm not looking to do that. But you cannot have a nuclear weapon. You want to talk — good. Otherwise you're going to have a bad economy for the next three years."

## C2 ISIS

### Intro

Rogers ’18, Michael S Rogers, <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 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. I should emphasize that this campaign was a coalition fight, with key international partners conducting and supporting both kinetic and cyberspace operations against ISIS.

We believe we may also face a further evolution of the cyberspace threat from violent extremist elements. Since its inception, ISIS leaders and their technical experts have maintained a robust online presence, and we assess that they will seek to increase their efforts in and through cyberspace. They and other groups, such as al Qaeda and its affiliates, still use the Internet to market their versions of terrorism, garner financial and material support, and inspire followers. ISIS, like al Qaeda before it, has worked hard to target susceptible individuals and inspire them to commit attacks in the West. That is why USCYBERCOM works with law enforcement, intelligence, and liaison partners to find and destroy the key nodes in ISIS online infrastructure and media operations (along with the analogous infrastructures of other violent extremists).

### 1 – Recruiting

Temple Raston ’19 ,https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis

In August 2015, **the NSA and U.S. Cyber Command, the military's main cyber arm, were at a crossroads about how to respond to a new terrorist group that had burst on the scene with unrivaled ferocity and violence**. The one thing on which everyone seemed to agree is that **ISIS had found a way to do something other terrorist organizations had not: It had turned the Web into a weapon. ISIS routinely used encrypted apps, social media and splashy online magazines and videos to spread its message, find recruits and launch attacks.**

A response to ISIS required a new kind of warfare, and so the NSA and U.S. Cyber Command created a secret task force, a special mission, and an operation that would become one of the largest and longest offensive cyber operations in U.S. military history. Few details about Joint Task Force ARES and Operation Glowing Symphony have been made public.

"It was a house of cards"

Steve Donald, a captain in the Naval Reserve, specializes in something called cryptologic and cyber operations, and when he is not in uniform, he is launching cybersecurity startups outside Washington, D.C. He's pale, bespectacled and has the slightly shy demeanor of a computer geek. In the spring of 2016 he received a phone call from the leader of his reserve unit. He needed Donald to come in.

"I said, well, I'm not in uniform [and he said] it doesn't matter — if you have a badge come on in," Donald said. "I can't believe I can actually say this but they were building a task force to conduct offensive cyber operations against ISIS."

Donald had to find a team of specialists to do something that had never been done before — hack into a terrorist organization's media operation and bring it down. Most of the forces flowed in from Joint Forces Headquarters, an Army cyber operation in Georgia. Donald also brought in experts in counterterrorism who understood ISIS and had watched it evolve from a ragtag team of Iraqi Islamists to something bigger. There were operators — the people who would be at the keyboards finding key servers in ISIS's network and disabling them — and digital forensics specialists who had a deep understanding of computer operating systems.

"They can say this is good, this is bad, this is where the files are located that we're interested in," he said. He found analysts, malware experts, behaviorialists and people who had spent years studying the smallest habits of key ISIS players. The mission, he explained to them, was to support the defeat of ISIS — to deny, degrade and disrupt them in cyberspace.

This was more complicated than it sounded.

The battle against the group had been episodic to that point. U.S. Cyber Command had been mounting computer network attacks against the group, but almost as soon as a server would go down, communications hubs would reappear. The ISIS target was always moving and the group had good operational security. Just physically taking down the ISIS servers wasn't going to be enough. There needed to be a psychological component to any operation against the group as well.

"This cyber environment involves people," Neil said. "It involves their habits. The way that they operate; the way that they name their accounts. When they come in during the day, when they leave, what types of apps they have on their phone. Do they click everything that comes into their inbox? Or are they very tight and restrictive in what they use? All those pieces are what we look at, not just the code."

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.

"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. The cyber equivalent of a surgical strike

The spring and summer of 2016 were spent preparing for attack. And while members of Task Force ARES didn't reveal everything they did to crack into ISIS's network, one thing they used early on was a hacking standby: a phishing email. ISIS members "clicked on something or they did something that then allowed us to gain control and then start to move," said Gen. Edward Cardon, the first commander of Task Force ARES.

Almost every hack starts with hacking a human, cracking a password or finding some low-level unpatched vulnerability in software. "The first thing you do when you get in there is you've got to get some persistence and spread out," Cardon said, adding that the ideal thing is to get an administrator's account. "You can operate freely inside the network because you look like a normal IT person." (ISIS didn't just have IT people; it had an entire IT department.) Once ARES operators were inside the ISIS network, they began opening back doors and dropping malware on servers while looking for folders that contained things that might be helpful later, like encryption keys or folders with passwords. The deeper ARES got insideISIS's network, the more it looked like the theory about the 10 nodes was correct. But there was a problem. Those nodes weren't in Syria and Iraq. They were everywhere — on servers around the world, sitting right next to civilian content. And that complicated things. "On every server there might be things from other commercial entities," said Air Force Gen. Tim Haugh, the first deputy commander of JTF ARES working under Cardon. "We were only going to touch that little sliver of the adversary space and not perturb anyone else." If ISIS had stored something in the cloud or on a server sitting in, say, France, ARES had to show Defense Department officials and members of Congress that U.S. cyber operators had the skill to do the cyber equivalent of a surgical strike: attack the ISIS material on a server without taking down the civilian material sitting right next to it. They spent months launching small missions that showed they could attack ISIS content on a server that also contained something vital like hospital records. Being able to do that meant they could target ISIS material outside Syria and Iraq. "And I looked at this young Marine and said, 'How big can we go?' and he said, 'Sir, we can do global.' I said, 'That's it — write it down, we're going to take it to Gen. Cardon.' " That Marine was Neil. He began peppering the leadership with ideas. He talked to them about not just hacking one person ... or ISIS in Syria and Iraq, but how to take down the media operation's entire global network. "That's how these attacks work," Neil said. "They start very simple and they become more complex." There was something else about Task Force ARES that was different: Young operators like Neil were briefing generals directly. "A lot of [ideas] come up that way, like somebody says, 'Well, we could gain access and do this to the files.' Really? You can do that? 'Oh yeah.' Would anyone notice? 'Well, maybe, but the chances are low.' It's like, hmmm, that's interesting, put that on the list." Cardon said young operators on Joint Task Force ARES understood hacking in a visceral way and, in many respects, understood what was possible in cyberspace better than commanding officers did, so having a direct line to the people making the decisions was key.

"An incredible rush" By the fall of 2016 there was a team, Joint Task Force ARES; there was a plan called Operation Glowing Symphony, and there were briefings — that had gone right up to the president. It was only then that there was finally a go. This account of the first night of Operation Glowing Symphony is based on interviews with half a dozen people directly involved. After months of looking at static webpages and picking their way through ISIS's networks, **the task force starting logging in as the enemy. They deleted files. Changed passwords.** "Click there," a digital forensic expert would say. "We're in," the operator would respond. There were some unintentionally comical moments. Six minutes in there was very little happening, Neil recalls. "The Internet was a little slow," he said without irony. "And then you know minute seven, eight, nine, 10, it started to flow in, and my heart started beating again." They began moving through the ISIS networks they had mapped for months. Participants describe it like watching a raid team clearing a house, except it was all online. Logging into accounts they had followed. Using passwords they discovered. Then, just as their move through targets started to accelerate, a roadblock: a security question. A standard, "what was your high school mascot"-type security question. The question: "What is the name of your pet?"The room quieted down. "And we're stuck dead in our tracks," Neil said. "We all look to each other and we're like, what can we do? There's no way we're going to get in. This is going to stop the 20 or 30 targets after this." Then an analyst stood up in the back of the room. "Sir, 1-2-5-7," he said. "We're like, what?" Neil says. "Sir, 1-2-5-7." "How do you know that? [And he said] 'I've been looking at this guy for a year. He does it for everything.' And we're like, all right ... your favorite pet. 1-2-5-7. "And boom, we're in." After that, the momentum started to build. One team would take screenshots to gather intelligence for later; another would lock ISIS videographers out of their own accounts. "Reset Successful" one screen would say. "Folder directory deleted," said another. The screens they were seeing on the Ops floor on the NSA campus were the same ones someone in Syria might have been looking at in real time, until someone in Syria hit refresh. Once he did that, he would see: 404 error: Destination unreadable. "Target 5 is done," someone would yell. Someone else would walk across the room and cross the number off the big target sheet on the wall. "We're crossing names off the list. We're crossing accounts off the list. We're crossing IPs off the list," said Neil. And every time a number went down they would yell one word: "Jackpot!" "We'd draw the line out and I had stacks of paper coming up on the corner of my desk," Neil said. "I knew in about the first 15 minutes that we were on pace to accomplish exactly what we need to accomplish." Once they had taken control of the 10 nodes, and had locked key people out of their accounts, ARES operators just kept chewing their way through the target list. "We spent the next five or six hours just shooting fish in a barrel," Neil said. "We'd been waiting a long time to do that and we had seen a lot of bad things happen and we were happy to see them go away." And there was something else that Neil said was hard to describe. "When you reach through the computer and on the other side is a terrorist organization, and you're that close, and you're touching something that's theirs, that they possess, that they put a lot of time and effort in to to hurt you, that is an incredible rush," he said. "You have the control to take that away." Enough to drive you nuts Brig. Gen. Jennifer Buckner was one of the people who took the reins of Task Force ARES afterGlowing Symphony had started. And after that first night, **the mission shifted into a second phase, one aimed at keeping pressure on ISIS with essentially five lines of effort: Keep the media operation under pressure, make it difficult for ISIS to operate on the Web more generally, use cyber to help forces on the ground fighting ISIS, hobble its ability to raise money, and work with other agencies in the U.S. and allies abroad.** Once the distribution hubs were hamstrung, the second phase of the mission was more creative. Joint Task Force ARES operators started making all those things that drive you crazy about today's technology — slow downloads, dropped connections, access denied, program glitches — and made it start happening to ISIS fighters. "Some of these are not sophisticated effects, but they don't need to be," Buckner said. "The idea that yesterday I could get into my Instagram account and today I can't is confusing." And potentially enraging. When you can't get into an email account, what do you do? You think: Maybe I mistyped the login or password. So you put it in again and it still doesn't work. Then you type it in more deliberately. And every time you type it, press enter, and are denied, you get a little more frustrated. If you're at work, you call the IT department, you explain the issue and then they ask you if you're sure you typed your login and password in correctly. It is enough to drive you nuts. It might never occur to you, or to ISIS, that this might be part of a cyberattack. 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.

Temple-Raston ’19, Dina Temple-Raston, NPR, 26 September 2016, NPR Interview, <https://www.npr.org/2019/09/26/764548436/how-a-classified-u-s-military-operation-hacked-isis>

TEMPLE-RASTON: Well, Operation Glowing Symphony was launched in November 2016. We'd heard a little bit about it before now. But what we know now because of our reporting is that it's thought to be the largest and longest offensive cyber operation ever in U.S. history, that the military has ever launched. Cyber operators behind it, Task Force ARES, were using, like, these incredibly ordinary hacks to do it. Now, we hear about zero days or we hear about exploits or tools that NSA builds to get into cyber operations or in networks. In this case, they just used the kinds of things that hackers use, phishing emails and backdoor exploits and that sort of thing, to get inside of ISIS' network. This is how a commander named Neil, who we talked to, talked about the operation. NEIL: And we're crossing names off the list. We're crossing accounts off the list. We're crossing IPs off the list. They were running back and forth on scratch pieces of yellow paper, and I had stacks of paper coming up on the corner of my desk. I knew in about the first 15 minutes that we were on pace to accomplish exactly what we needed to accomplish. TEMPLE-RASTON: And what they accomplished was, basically, they took over these 10 core accounts that these administrators for ISIS were using to basically send out everything - their videos, their tweets, their financial transactions. And once they took those over, ISIS had no access to them. They were frozen in cyberspace. INSKEEP: Why concentrate on their media operation? TEMPLE-RASTON: Well, the media operation - basically, ISIS had been able to weaponize the Internet like no other terrorist group ever had. They had videos. They had tweets. They even had a streaming radio station, and all this was incredibly popular with young Muslims around the world. And it was so effective in 2015 and 2016 that recruits were literally lining up at the Turkish border trying to get into Syria to join the group. So what Glowing Symphony decided to do was to stop that and basically do that by taking down their system. And we got a rare interview with NSA Director General Paul Nakasone. And he told us that, even today, the U.S. is still inside ISIS' networks. This is what he said. PAUL NAKASONE: 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.

Work ’19, JD Work, Atlantic Council, 17 September 2019, <https://www.atlanticcouncil.org/blogs/new-atlanticist/the-american-way-of-cyber-warfare-and-the-case-of-isis/>

There is no mistaking: this is combat between organizations. The Islamic State of Iraq and al-Sham (ISIS) is a product of utterly modern global communications networks welded to an ideologically twisted variant of a medieval governance model. The systematic nature of the group’s activities in cyberspace comes through clearly in the Operation Glowing Symphony (OGS) declassified concept of operations (CONOPS) and associated briefings. These are functions essential to ISIS’s survival as an organization—internal communications, foreign fighter recruitment, fanatic lone wolves, and the promotion of its global brand for fundraising and material support. The documents make notable reference to the underexplored role of ISIS cadres in acquiring and administering the group’s technology infrastructure, as well as brief mention of the group’s aspirational cyber espionage and attack capabilities. These ISIS members would naturally be a target for operations intended to disrupt and degrade key terrorist activities. The distribution of the ISIS’s online presence also illustrates the importance of global relationships in contemporary cyber conflict. No fight can be pursued without support from allies and partners—particularly when targets cut across traditionally segmented law enforcement or diplomatic instruments. While coalition members may approach operations in different ways, it is apparent that these relationships—including processes for notification and coordination—are featured prominently in these operations.

Bate ’17, American Security Project, Laura Bate, 16 June 2017, <https://www.americansecurityproject.org/fighting-isis-in-cyberspace/>

A strong defense is always important, but particularly given ISIS’s limited cyber capacity, offensive tools are available as well. Offensive Cyber Operations 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](https://www.defense.gov/News/Transcripts/Transcript-View/Article/682341/department-of-defense-press-briefing-by-secretary-carter-and-gen-dunford-in-the/) 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](https://www.us-cert.gov/ncas/tips/ST04-015) (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](https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.d32f43a988ef), 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](https://www.foreignaffairs.com/articles/2017-01-31/isis-breaking-apart) 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.

### 2 – Funding

Windrem & Arkin ’19, Robert Windrem & William Arkin, 1 May 2016, NBC News, <https://www.nbcnews.com/storyline/isis-terror/how-beat-isis-blow-money-n564956>

The U.S. has quietly turned to a new strategy in fighting ISIS — follow the money, then blow it up, U.S. officials tell NBC News. At least four times in the past four months, U.S. military jets have targeted [major] ISIS financial centers, destroying them in strikes that have turned millions of U.S. dollars into confetti. The U.S. has also killed ISIS financial leaders — its "oil minister" in 2015 and its "finance minister" in March. The strikes are the fruit of a secret cyber war in which the U.S. is tracking, manipulating and even stealing or destroying the financial assets of terrorists. Five years after the SEAL raid that killed Osama bin Laden on May 1, 2011, it's a subtle shift from the U.S. strategy against al Qaeda in which degrading the operational leadership was the priority. Just as unraveling the courier network was critical to tracking bin Laden, the cyber efforts against the ISIS financial network are critical to upending ISIS, say U.S. officials. Unlike al Qaeda, ISIS is trying to run a government and control a big chunk of land, and it has a constant need for hard currency to pay its fighters and bureaucrats and feed its population. The war is not just about tracing the movement of money but the movement of individuals linked to the cash. It's part of what CIA Director John Brennan calls a broader cyber effort against ISIS. "They are murderers and we need to be able to change this narrative — including in the cyber environment, the digital domain, in social media," said Brennan. "It is a question of what type of activities might take place in that cyber environment that we would be able to carry out destructive actions against." Financial transactions, one senior intelligence official tells NBC News, have become one of the most lucrative forms of intelligence on personal relations, foreign fighter movements, and sources of supply. The intelligence community tracks ISIS financial transactions through data collection programs with such secret code names as "Kaching" (CIA), "TRACKFIN" (NSA) and FINO (the National Clandestine Service). Newly created electronic portals for the processing of what is now called financial intelligence (or FININT) — Swordfish, QLIX/HYDRA and Sentry, among others — fuse together conventional banking, transaction and intercepted data. But the most visible actions against ISIS came earlier this year. Starting in January, after a series of strikes on ISIS oil production and distribution assets, the U.S. began targeting financial facilities. On January 11, a coalition airstrike destroyed an ISIS "cash and finance distribution center" in a nondescript building in Mosul, the Northern Iraqi city of 2 million controlled by the group. Video shows missiles hitting the building in the middle of the night, sending a plume of shredded U.S. cash, mostly $100 bills, hundreds of feet into the air. The senior intelligence official said as much as $50 million in financial assets was destroyed in that attack, including $35 million in U.S. paper currency and Euros. The amount is equal to about one-fifth of what the U.S. estimates ISIS looted from Iraqi banks when they ransacked Mosul in June 2014. “You can bet that (ISIS) is feeling the strain on its checkbook,” said CENTCOM commander Gen. Lloyd J. Austin III, describing the first “money bomb.” “We estimate that it served to deprive ISIL (ISIS) of millions of dollars.” U.S. officials say it was no coincidence that a few days later, President Obama referred indirectly to the targeting of money in his State of the Union speech. While describing (and defending) progress against ISIS, he mentioned going after financing first on his list of successes, before airstrikes on fighters, plot disruptions, even before efforts to stop the flow of foreign volunteers.

### 3 – Kinetic Strikes

Cox ’18, Matthew Cox, military.com, 25 May 2018, <https://www.military.com/dodbuzz/2018/05/25/us-coalition-forces-used-cyberattacks-hunt-down-isis-command-posts.html>

U.S. and coalition forces launched cyberattacks last year to help identify and destroy several command posts of Islamic State leaders, according to the former head of the task force to defeat ISIS in Iraq and Syria. "This is a vignette that actually played out during and after the battle of Mosul and after the battle of Raqqa," said Gen. Stephen Townsend, who commanded Combined Joint Task Force-Operation Inherent Resolve in 2017. Townsend, who now commands [Army](http://www.military.com/army) Training and Doctrine Command, described the multi-domain operation to an audience at the Association of the United States Army's LANPAC Symposium and Exposition in Hawaii. U.S. and coalition forces were scouring the middle Euphrates River Valley, between Al Qa'im in Iraq and Raqqa in Syria, in search of command posts used by ISIS leaders, Townsend said. Friendly forces had located the enemy's primary command post in the area but couldn't find the enemy's alternate sites. "We knew that the enemy had alternate command posts, but we didn't know where they were," Townsend said. "So rather than strike the primary command post and then have the enemy be unknown to us for a while while we reacquired where he went to, one of the subordinate units proposed that we use ... capabilities from space and cyber to deny the enemy's primary command post, forcing him to move to and unveil his alternate command posts," he explained. The plan worked, Townsend said. When the enemy moved, "we struck the alternate command posts kinetically with lethal fires once we identified them, and we worked our way backward to the primary command post." The coordinated strikes were a clear example of multi-domain operations, formally known as multi-domain battle, a strategy U.S. military leaders stress as the key to surviving future wars with near-peer adversaries such as Russia and China.

Vavra ‘19, Shannon “US cyber-offensve use against ISIS continues, and eyes are now on Afghanistan” Cyberscoop. 09/17/19. <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, 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 cyber attacks were used 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 for two years, forcing ISIS to reveal alternate command posts in Iraq and Syria. This whichallowed 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 withdraws troops from the region. “When we don’t have drones or … we don’t have an actual task force or any other 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. “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.

Duffy ’18, Ryan Duffy, Dyberscoop, 29 May 2018, <https://www.cyberscoop.com/u-s-official-reveals-military-combined-cyber-kinetic-operations-hunt-isis/>

U.S. Cyber Command, the country’s [leading cyberwarfare force](https://www.cyberscoop.com/us-cyber-command-nsa-government-hacking-operations-fight/), 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 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](https://www.military.com/dodbuzz/2018/05/25/us-coalition-forces-used-cyberattacks-hunt-down-isis-command-posts.html?utm_source=Mike%27s+Daily+Blast&utm_campaign=8d4307f510-EMAIL_CAMPAIGN_2018_04_27_COPY_02&utm_medium=email&utm_term=0_beae3dbeb1-8d4307f510-51475081). 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 general — who commanded Combined Joint Task Force-Operation Inherent Resolve in 2017 — told an audience of Hawaii conference-goers via teleconference that the coalition cyberattacks leveled against ISIS were part of “a multi-domain operation [that] unfolded in air, land, sea, cyberspace and space.” As United States-led forces rebuffed ISIS advances, overtook its territorial holdings and prepared to mount a final offensive, they determined that the Euphrates River Valley was where the terrorist group would make a last stand. Coalition forces combed through a wide swath of land, from Al Qa’im, Iraq to Raqqa, Syria, for ISIS outposts. Though they located the primary command, they couldn’t find other subcommand posts in the area. “We knew [they existed], but we didn’t know where they were,” Townsend said. Instead of hitting the primary command post with a missile or special forces raid and risk not finding the other hidden outposts, the task force enlisted “capabilities from space and cyber to deny the enemy’s primary command post, forcing him to move and unveil his alternate command posts,” said Townsend. As ISIS militants scattered to peripheral posts, they unmasked the locations. From there, the task force moved in and struck. ‘Evolutionary not revolutionary’ Since the operation dovetailed into a larger campaign that included intelligence gathering, special forces, overhead surveillance and boots on the ground, it can be best described as an instance of “cyber in warfare” rather than outright cyberwarfare, said Rick Forno, assistant director of the Center for Cybersecurity at University of Maryland, Baltimore County. “Instead of blowing up [an outpost] with a bomb or missile, maybe we’re able to go in and disrupt the operations with a less lethal way of doing it. That’s not revolutionary, that’s evolutionary – using a new tool to achieve the same outcome,” Forno told CyberScoop. But in many ways, the ongoing cyber campaign against ISIS represents a first. U.S. leaders have publicly touted similar operations in the past, which is especially rare for these types of covert activities. “We are dropping cyber bombs,” Robert Work, then-deputy secretary of defense, [told](https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html) the New York Times in 2016. “We have never done that before.” And former President Barrack Obama [referenced](https://www.defense.gov/News/Article/Article/721148/obama-counter-isil-campaign-accelerates/) the attacks in one public speech in 2016. “The role of cyber-capabilities in joint military operations is something that’s been talked about for a long time. The campaign against the Islamic State probably represents one of the more visible examples of those capabilities in action,” said Ben Buchanan, a postdoctoral fellow at Harvard’s Belfer Center. For some time, the DOD has sought to combine cyber-operations with its more conventional military capabilities, planning and strategy. It has integrated cyber teams — both deployed and stateside — [with regional commands](https://www.cyberscoop.com/us-cyber-command-nsa-government-hacking-operations-fight/) over the last 12 months. “Historically, cyberspace operations have been stovepiped and executed independently. As the domain has matured, we have started integrating cyber-operations into all of our planning efforts,” Gen. Joseph Votel, commander of U.S. Central Command, which covers parts of the Middle East and Central Asia, [said](http://www.centcom.mil/MEDIA/VIDEO-AND-IMAGERY/VIDEOS/videoid/554527/) in September 2017. More broadly, the ISIS vignette also sheds light on the Pentagon’s push to ready its forces for so-called “multi-domain operations.”

Pomerlau ’19, Mark Pomerlau, 17 September 2019, <https://www.c4isrnet.com/dod/cybercom/2019/09/17/how-cyber-command-can-limit-the-reach-of-isis/>

The U.S. military’s digital team tasked with targeting ISIS is now focused on providing agencies intelligence that will help identify specific individuals and that will limit the group’s financing. “About 90 percent of what we do is intelligence,” Brig. Gen. Len Anderson, deputy commander of Joint Task Force-Ares, said Sept. 16. 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](https://www.fifthdomain.com/dod/cybercom/2018/11/30/cyber-commands-anti-isis-offensive-undergoes-a-change/). 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. In regards to other terrorist organizations, Anderson said while they are “studying” what al-Qaeda is doing, Ares has to prioritize threats given its resources. “Right now, as far as threats to the West or external operations, it’s going to be primarily ISIS focused. They’re the ones that are most dangerous to us now,” he said. “Due to our broad partnership across the counterterrorism industry and not only that but with the National Counterterrorism Center we are aware and will be prepared to act with al-Qaeda or al-Qaeda operatives.”

### Impacts

Kirkpatrick & Schmitt ’19, David D Kirkpatrick & Eric Schmitt, New York Times, <https://www.nytimes.com/2019/10/21/world/middleeast/isis-syria-us.html>

Now, analysts say that Mr. Trump’s pullout has handed the Islamic State its biggest win in more than four years and greatly improved its prospects. With American forces rushing for the exits, in fact, American officials said last week that they were already losing their ability to collect critical intelligence about the group’s operations on the ground. “There is no question that ISIS is one of the big winners in what is happening in Syria,” said Lina Khatib, director of the Middle East and North Africa Program at Chatham House, a research center in London.

Jamieson ’16, Alastair Jamieson, 19 January 2016, NBC News, <https://www.nbcnews.com/storyline/isis-terror/isis-death-toll-18-800-killed-iraq-2-years-u-n499426>

At least 18,802 civilians have been killed in Iraq in [ISIS](http://www.nbcnews.com/storyline/isis-uncovered)-linked violence in under two years, a United Nations report said Tuesday — with millions of others forced 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](http://www.ohchr.org/Documents/Countries/IQ/UNAMIReport1May31October2015.pdf)]. 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.” 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](http://www.nbcnews.com/storyline/isis-uncovered/yazidi-women-tell-rape-enslavement-hands-isis-n462091)

Vavra ‘19, Shannon “US cyber-offensve use against ISIS continues, and eyes are now on Afghanistan” Cyberscoop. 09/17/19. <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, 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 cyber attacks were used 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 for two years, forcing ISIS to reveal alternate command posts in Iraq and Syria. This which 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 withdraws troops from the region. “When we don’t have drones or … we don’t have an actual task force or any other 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. “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.

Crowcroft ’15, 17 June 2015, <https://www.ibtimes.co.uk/isis-worst-refugee-crisis-generation-millions-flee-islamic-state-iraq-syria-1506613>

The rise of Islamic State (Isis) has displaced over 3.3 million people in Iraq alone, with millions more fleeing Syria for Lebanon, Turkey and the Gulf, and many of them risking perilous journeys to Europe via Egypt, Libya and the Mediterranean. It [was reported in 2015](http://www.economist.com/blogs/graphicdetail/2015/03/asylum-seekers) that asylum applications to rich countries reached their highest level for over two decades in 2014, with 866,000 applications lodged, an increase of 45% on 2013 and two-thirds of those in the European Union.

# FRONTLINES

### F/L Iran Cyber Retaliation

1) Iran doesn’t have the cyber capabilities to compete with the US and they know they are outmatched.

Rasidi ’19, Yasmeen Rasidi, 23 October 2019, Citizen Truth, <https://citizentruth.org/has-the-us-already-declared-a-cyber-war-on-iran/>

[A June 2019 assessment](https://nationalinterest.org/blog/buzz/how-iran-would-wage-cyber-war-against-united-states-85841) of Iran’s cyber capabilities by the Center for Strategic & International Studies (CSIS) described Iran as having “rapidly improved its cyber capabilities” though “it is still not in the top rank of cyber powers.”

Iran, most likely, does not want a cyber war with the U.S. knowing it is outmatched, but Iran may already be trapped in just that.

2) Our case ev is explicit in saying that after the US cyberattack in September, Iran did not retaliate.

### F/L ISIS Recruitment Hasn’t Decreased

1) Sure but ISIS has been growing rapidly since they were founded but we were able to slow the growth rate.

2) Not specific to Iraq and Syria – we were able to control their growth in these regions uniquely, thus decreasing their territory. We would agree that globally ISIS has seen increased membership such as in areas like Afghanistan, which is why OCOs are more critical than ever so we can continue to keep them at bay in these areas as well.

### F/L ISIS Resurging

Their ev is from August when Trump pulled out troop from Syria – it’s really outdated. Since then we’ve resumed large scale military operations in Syria to keep ISIS at bay. The combined use of OCOs and military operations will be crucial to keeping ISIS from resurging further in the future.

Tucker ’19, Emma Tucker, 25 November 2019, The Daily Beast, <https://www.thedailybeast.com/us-resumes-operations-against-isis-in-northern-syria-after-trumps-withdrawal-order>

United States troops have resumed large-scale counterterrorism missions against the Islamic State in northern Syria, military officials say, almost two months after President Trump’s ordered a withdrawal of American forces in the region, allowing a Turkish offensive. Trump’s decision in October was at odds with the advice of top officials in the Pentagon and the State Department who had sought to keep a small troop presence in northeast Syria to continue fighting ISIS alongside Kurdish forces. On Friday, American soldiers and hundreds of Syrian Kurdish fighters reunited to conduct a mission to kill and capture ISIS fighters in Deir al-Zour province, the Pentagon said. The Kurdish fighters, which are part of the Syrian Democratic Forces, have been crucial allies to the U.S. in counterterrorism efforts targeting the Islamic State. The local allies were abandoned by the Trump administration when U.S. troops were withdrawn.

# EXTRA

Vavra ’19, Shannon Vavra, Cyber Scoop, 17 September 2019, <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, 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](https://media.defense.gov/2019/Aug/06/2002167167/-1/-1/1/Q3FY2019_LEADIG_OIR_REPORT.PDF) 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](https://www.ft.com/content/ae7cd2c2-ce26-11e9-99a4-b5ded7a7fe3f). 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.](https://www.cyberscoop.com/u-s-official-reveals-military-combined-cyber-kinetic-operations-hunt-isis/) This allowed the Department of Defense to launch traditional military attacks against the outposts. Other capabilities include obtaining terrorists’ [credentials](https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html), 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](https://www.cnn.com/2019/09/16/politics/us-service-member-killed-afghanistan/index.html) 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 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](https://www.nytimes.com/2019/09/02/world/asia/us-withdrawal-afghanistan-taliban.html) 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](https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil) 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](https://cisac.fsi.stanford.edu/mappingmilitants/profiles/islamic-state-khorasan-province#highlight_text_9306), 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.

### C1 ! Extension

Even if Iran doesn’t retaliate, avoiding direct conflict is still a reason to vote for us. Because even if they don’t retaliate, the fact that the US does not conduct a direct attack on them saves lives by itself. When the United States uses cyber-attacks instead of missile launches civilian and military lives are saved because the attacks only target specific critical infrastructure.

## Funding Extension

Gutteridge ’17, Nick Gutteridge, Experess News, 5 January 2017, <https://www.express.co.uk/news/world/750783/Islamic-State-ISIS-stops-paying-fighters-Mosul-running-out-of-money>

ISIS ON THE BRINK: Terror group COMPLETELY runs out of cash to pay jihadis defending Mosul ISLAMIC STATE (ISIS) is running so short of money that it has stopped paying the salaries of its fighters in besieged Mosul, locals still living in the city claimed today. According to the Telegraph, some fighters in Mosul are so broke they are now effectively going rogue and smuggling families out of the city and to safety in return for bribes of as little as £15. A resident still living in the city, who posts anonymously under the moniker Mosul Eye, said: “The only food left for people living on the western bank is potatoes. They boil them for breakfast, lunch and dinner."