[Nihar] and I affirm Resolved: The benefits of the United States federal government’s use of offensive cyber operations, or OCOs, outweigh the harms.

The ASPI defines offensive cyber operations, or OCOs, as:

Operations to harm targeted computers, information systems or networks.

## Contention 1 is Stopping Terrorism (2:15)

#### Thanks to the US’s efforts,

Michael S **Rogers 18**, April 11 2018, HOUSE COMMITTEE ON ARMED SERVICES, "EMERGING THREATS AND CAPABILITIES SUBCOMMITTEE", <https://docs.house.gov/meetings/AS/AS26/20180411/108076/HHRG-115-AS26-Wstate-RogersM-20180411.pdf>, Date Accessed 11-1-2019 WS

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.

#### ~~This is because ISIS uses the internet to maintain power~~**~~Dina Raston wrote for NPR in, 9/26/2019 that, NPR, “How The U.S. Hacked ISIS,”~~** [**~~https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis~~**](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~~ **~~us[ing] 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 operation [in response] in U.S. military history.~~** ~~Few details about Joint Task Force ARES and Operation Glowing Symphony have been made public.~~

#### US OCOs are crucial to stopping ISIS from exploiting cyberspace in four ways:

#### **First, we can disrupt their communications networks**

**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/> CCD

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 2017] in 2016 to cripple ISIS digitally by developing malware and other tools to knock out computer and communications equipment [and]. 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 [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**.

#### **These OCO’s can take down their entire global network**

Dina **Raston concludes for NPR that**, 9/26/2019, NPR, “How The U.S. Hacked ISIS,” <https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis> kegs

**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 inside ISIS'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[ing] 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."

#### **Second is by preventing online recruiting**

**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 den[ied] ISIS access to its own propaganda outlets and deleted 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[ing] down ISIS’s capacity for propaganda.**

#### ~~Online recruiting is critical for ISIS survival.~~

~~(Iftekharul~~ **~~Bashar 19,~~** ~~Associate Research Fellow at the International Centre for Political Violence and Terrorism Research, “Islamic State Ideology Continues to Resonate in Bangladesh”,~~ [~~https://www.mei.edu/publications/islamic-state-ideology-continues-resonate-bangladesh~~](https://www.mei.edu/publications/islamic-state-ideology-continues-resonate-bangladesh)~~, MEI)IEA~~

**~~(paraphrased)~~ ~~In Bangladesh, a hot-spot for ISIS recruitment, 82% of ISIS militants were recruited online.~~**

~~IS in Bangladesh has been able to recruit both from existing terrorist groups as well as youth with no prior record of engagement in violence. According to Bangladesh’s Counter Terrorism and Transnational Crime Uni~~**~~t, 82% of the operatives arrested were recruited online~~**~~. Though there has been a significant decline in the production of propaganda materials in the local language, the existing materials available in the cyber domain are substantial and being frequently read, referred to and shared by the group’s followers.~~

#### **Third is by supporting conventional forces**

Martelle 18 GWU https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil

More difficult to observe is the impact of cyber operations focusing in on Iraq and Syria, however isolated episodes have given a glimpse into the possibilities of **cyber [attacks] combined with kinetic counter-terror operations [allow]**. Conflicting reports suggest **ISI[S’s]** hacker Junaid Hussein’s **position [to be] pinpointed** when he either clicked on a malicious hyperlink or had his messages compromised before he was **[and then] killed by a US drone [forces]** as he left an internet café. More recently, US General Stephen Townsend described to military.com how **cyber capabilities were used to interfere with communications from an ISIL headquarters in Iraq, forcing ISIL leadership to move to and reveal their backup command posts before kinetic strikes were ordered.**

[~~Lamothe Washington Post~~](https://www.washingtonpost.com/news/checkpoint/wp/2017/12/16/how-the-pentagons-cyber-offensive-against-isis-could-shape-the-future-for-elite-u-s-forces/)

~~The~~ **~~U.S.~~** ~~military has conducted~~ **~~cyber attacks [have a]~~** ~~against the Islamic State for more than a year, and~~ **~~its record of success when those attacks are coordinated with elite Special Operations troops~~** ~~is such that the Pentagon is likely carry out similar operations with greater frequency, according to current and former U.S. defense officials. The cyber offensive against ISIS, an acronym for the Islamic State, was a first and included the creation of a unit named Joint Task Force Ares. It focused on destroying or disrupting computer networks used by the militant group to recruit fighters and communicate inside the organization. Such offensive weapons are more commonly associated with U.S. intelligence agencies, but they were brought into the open in 2016 after then-Defense Secretary Ashton B. Carter pressured U.S. Cyber Command to become more involved in the campaign to defeat the Islamic State. When combined with traditional military operations, Thomas said, the cyber strikes~~ **~~culminat[ing] in the “destruction of th[e] adversary on an epic scale.~~**~~” He argued that the military can “~~**~~only~~****~~achiev[able]~~** ~~exquisite effects like this”~~ **~~with~~** ~~a task force that combines a variety of capabilities, including~~ **~~cyber weapons.~~**

#### **Fourth is cutting off financing**

**Pomerleau Fifth Domain 17** <https://www.fifthdomain.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. 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 **includ[ing] 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 **mak[ing] 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.”

**Taking out finances is critical to stopping terrorist organizations.**

Nathan **Sales 19**, 5-6-2019, "ISIS has suffered defeats, but the fight isn't over. Here's how we keep up the pressure.," USA TODAY, <https://www.usatoday.com/story/opinion/2019/05/06/fight-against-isis-strategies-keep-global-terrorist-network-bay-column/1112549001/>

Finances. **We need to cut off the flow of money to ISIS affiliates around the world [and].** It isn’t enough just to stop the gunmen. We also need to stop **the moneymen who pay for the[ir] guns.** One of our most effective financial weapons is terrorist designations, which freeze terrorist assets. Last year, the State Department designated 19 ISIS-linked individuals and organizations, and the Treasury Department designated 14 more. Our partner countries need to develop the necessary laws and capabilities, and push for stronger enforcement of international counterterrorism financing standards. This is especially true in light of UN Security Council Resolution 2462, which obligates all nations to criminalize terrorist financing, even when there’s no direct link to a terrorist attack.

### Impact is a stopping a global threat

#### While ISIS is weaker now, a failure to finish the fight will allow them to bounce back

**Brands 19 Stanford Uni** <https://www.hoover.org/research/why-america-cant-quit-middle-east>

This has happened before

Second, however, it is a fantasy to think that the United States can disengage from the Middle East without consequence. This is because America still has pressing interests in that region—and because those interests are as unlikely to protect themselves today as they ever have been in the past. Growing Russian influence, Iran’s hegemonic ambitions, the potential resurgence of key terrorist organizations, and the massive political instability and violence that plagues large swaths of the region are real problems that demand competent management. America’s partners in the region can do more to manage those problems than they have done to date, but they remain manifestly incapable of doing so without significant U.S. support.

Third, hasty withdrawals are likely to be followed by hasty re-engagements**. After the United States left Iraq in 2011,** the state nearly collapsed, **ISIS surged to prominence**, and an emergency military intervention—which has now lasted nearly five years—was needed to repair the damage. If the United States disengages from Syria and Afghanistan today and the result is a significant terrorist attack, the pressure to get back into the region and take decisive military action will be strong indeed—even if that means shortchanging other geopolitical priorities. If America goes home from the Middle East, it will sooner or later face pressures to go big.

**Reporter Alastair Jamieson wrote that,** ISIS Death Toll: 18,800 Killed in Iraq in 2 Years, U.N. Says, 1/19/2016, 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 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[ing to] “crimes against humanity, and possibly genocide.”**

#### ~~ISIS can and will go global~~

~~Reporter Tim~~ **~~Lister~~** ~~noted in~~ **~~2018~~** ~~that~~**~~,~~** ~~By Tim Lister, Ray Sanchez, Mark Bixler, Sean O'Key, Michael Hogenmiller and Mohammed Tawfeeq, CNN, Updated 11:24 AM ET, Mon February 12, 2018, https://www.cnn.com/2015/12/17/world/mapping-isis-attacks-around-the-world/index.html~~

~~Since declaring its caliphate in June 2014, the self-proclaimed~~ **~~Islamic State has conducted or inspired more than 140 terrorist attacks in 29 countries other than Iraq and Syria,~~** ~~where its carnage has taken a much deadlier toll. Those attacks have killed at least 2,043 people and injured thousands more.~~

**ISIS’s ability to launch and inspire global attacks create catastrophic damage**

**Kah '17,** Henry Kam Kah, "‘Boko Haram is Losing, But so is Food Production’: Conflict and Food Insecurity in Nigeria and Cameroon", Africa Development, Africa Development, Volume XLII, No. 3, 2017, pp. 177-196 © Council for the Development of Social Science Research in Africa, 2017 PM

Many of the internally displaced people in the north-eastern part of Nigeria face enormous difficulties in meeting their food and non-food needs. Assessments in late 2014 alone, following interviews with key informants in Gombe, Yobe and Adamawa states, revealed that vast areas of southern Yobe and Borno and northern Adamawa were under-cultivated and/or not harvested during the May to December main farming season as a result of attacks and conflict-related fears orchestrated by the Boko Haram insurgency in the area. **Many of the internally displaced persons in northeastern Nigeria can only secure a single meal a day. They have abandoned their farms, agricultural activities and homes due to insecurity. Internally displaced families have exhausted their food stocks and have turned to consuming grain reserved as seedlings for the next planting season.** Offseason farming and fishing activities in the first half of 2015 were lower than before, thereby affecting agriculture and fish farming activities. As a result, many households in the affected areas in Bornu, Yobe and Adamawa were left with significantly below-average food stocks in 2015. Income from agricultural wage labour for both the main and off-season periods were down due to decreased labour participation. As insurgents attacked livestock holdings and disrupted markets, incomes from livestock sales were also down.1 **Statistics for 2015 show that due to the Boko Haram insurgency [which is a Nigerian branch of ISIS, farming and food supplies have been disrupted and]  more than 5.2 million people in north-eastern Nigeria suffered from severe food insecurity and some 54,000 faced famine.** The current food insecurity crisis is massive in this conflict prone region of Nigeria. **over 15 million people are now food insecure** of whom over 5.2 million are severely food insecure (Nigeria – Complex Emergency 2015:2; Imaseun 2015:289). This is a problem that is likely to last for a long time considering the level of destruction to the flora and fauna of this area

## C2 is Breaking Down Botnets

#### OCOs are key to stopping cybercrime by hunting down criminals and preventing attacks from occurring

**Rosenbach 18** (Eric Rosenbach, Co-Director of the Belfer Center for Science and International Affairs at **Harvard** Kennedy School, 24 April 2018, “America, Democracy, and Cyber Risk: Time to Act”, <https://www.hsgac.senate.gov/imo/media/doc/Testimony-Rosenbach-2018-04-24.pdf> DOA 10/24/19)KJR

**Even with improved cyber defenses, we will of course not be immune from attack.** To complement the work that DHS does, **the US Government, l**ed by the Department of Defense, **must bolster real capabilities to disrupt and degrade cyber[attacks] and information operations at their source [by].** In particular, there is a need to • Strengthen indications and warning of cyber and information attacks. The Intelligence Community, and the National Security Agency in particular, need to bolster the “early warning” system for information operations which target US democratic institutions  **• Bolster Cyber Command’s capability to address information operations**. The US military lacks the structure and capability necessary to defend the nation from future attacks. Special Operations Command has historically led Department of Defense efforts in information operations, but the lead must now shift to Cyber Command in order to strengthen the nexus of cyber and information operations capabilities necessary for the information age. That said, the Department of Defense’s recent efforts to combat ISIS through a joint SOCOM-CYBERCOM effort, known as Task Force Ares, represents an outstanding model for future operations.  **• Take a leading role in building international capacity to disrupt the proliferation of black-market destructive malware.** The Proliferation Security Initiative for weapons of mass destruction—supported by over 100 countries—provides an analogous model for action. **• Take a more active role in disrupting and dismantling botnets used by criminals and foreign adversaries. Law enforcement organizations, led by the FBI and Department of Justice, alongside the Department of Defense when needed, should work very closely with telecommunications companies and international partners to neutralize botnets**

**Thankfully,**

**Fazzini 18 CNBC**

<https://www.cnbc.com/2018/09/21/trump-cybersecurity-policy-offensive-hacking-nsa-russia-china.html>

**The new White House cybersecurity strategy** was released today, outlining a high-level plan that includes **giv[es] government agencies more powers to pro-actively fight cybercrime.** The document calls several times for increasing participation by private companies, a complicated task for multinationals that do business in countries involved with cyber-related disputes in the U.S. The White House released a new cybersecurity strategy today, with several important changes in direction meant to give government agencies and law enforcement partners a greater ability to respond to cybercrime and nation-state attacks. The 40-page document mostly stays the course for past initiatives -- like working to strengthen the organizations that make up the country’s “critical infrastructure” industries, including electrical operators and financial institutions. Hacking back But some of the changes emphasize a shift toward a more offensive cybersecurity posture, a longtime request fromm the National Security Agency and cybersecurity branches of the U.S. Armed Forces. The strategy codifies the ability of agencies aligned with the Department of Defense, like the NSA and military branches, to **[and] conduct offensive actions in cyberspace.** This means these agencies will be able **to go after** the overseas sources of attacks more proactively. These activities can be risky, as **cybercriminals.** may position their attacks from a neutral third party or a non-hostile country, making it more complicated for the U.S. to engage in cyber battles. **These** back-and-forth **attacks can** also cause damage to the infrastructure that supports the internet, particularly telecommunications providers. This strategy gets the agency and law enforcement partners closer than ever to being allowed to make these offensive bids, which could include **dismantl[e] “botnets” — which are collections of compromised computers** and devices **used to attack [companies] corporate** or government **targets — [and also can take down] underground cyber black markets,** or other sources of cyberattacks.

**Jack Goldsmith, Law professor at Harvard** wrote in **2012** that [Jack, Henry L. Shattuck Professor @ Harvard Law School, where he teaches and writes about national security law, presidential power, cybersecurity, international law, internet law, foreign relations law, and conflict of laws, served as Assistant Attorney General, Office of Legal Counsel from 2003–2004, and Special Counsel to the Department of Defense from 2002–2003, member of the Hoover Institution Task Force on National Security and Law, 10/15, “The Significance of Panetta’s Cyber Speech and the Persistent Difficulty of Deterring Cyberattacks,” Lawfare, <http://www.lawfareblog.com/2012/10/the-significance-of-panettas-cyber-speech-and-the-persistent-difficulty-of-deterring-cyberattacks/>]

Secretary of Defense Leon Panetta’s speech last week on cyber is more significant than has been reported. Most of the coverage focused on Panetta’s grave warnings about cyber threats facing the nation, but the speech’s real significance, I think, concerns DOD’s evolving deterrence posture. (The speech has other significant elements, but I focus here on deterrence.) Panetta had two main messages related to deterrence. First, because the USG’s attribution skills have improved, “[p]otential aggressors should be aware that the United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America.” Second, “If we detect an imminent threat of attack that will cause significant, physical destruction in the United States or kill American citizens,” then on **the** orders of the President, DOD **[Department of Defense] can “conduct effective operations to counter threats to our national interests in cyberspace [by]**.” (This second point echoes earlier USG statements, including one made earlier this month by DRNSA Keith Alexander, who said, somewhat less cautiously than Panetta, that DOD must be able to “stop [an attack] before it happens. . . . **Part of our defense has to consider offensive measures like that to stop it from happening.**”) Here is what I think is significant about Panetta’s speech.¶ First, DOD has previously said that it is trying to improve is attribution capabilities, and in conversation officials have noted some success. Panetta goes further, saying concretely and definitively that DOD has “made significant advances in solving” the attribution problem, presumably through a combination of **tracing** back the source of a cyber attack **and identifying the attacker[s] through “behavior-based algorithms**” and human and electronic intelligence. Panetta does not tell us how good or fast DOD is at attribution, and he may to some unknown degree be puffing. Nonetheless, **this is a potentially big deal for cyber deterrence.** Second, Panetta was more aggressive than DOD has been in the past about the trigger for a **self-defensive cyberattack** by the United States. Previously, DOD has stated that adversaries would face a “grave risk” if they launched a “crippling” or “significant” cyberattack on the ho~~meland. Panetta’s speech changes this posture in two ways. He is less definitive about the high threshold of a “significant” or “crippling” attack as a trigger for a USG response, and indeed implies that the threshold is (or can be) lower. And more importantly, he makes plain that the [Pentagon] DOD has the~~ **~~capability and desire~~** ~~to engag~~**~~e in preemptive attacks against~~ [to destroy] imminent cyber threats.** ~~This possibility has been hinted at before (most recently, in Alexander’s comment above and in Harold Koh’s NSA Cyber Command legal conference speech last month). But Panetta was more definitive about DOD’s capacity and desire to engage in such attacks. (Herb Lin, chief scientist at the National Research Council’s Computer Science and Telecommunications Board, noted to me that Panetta referred to the need to “take action” with “effective operations” against imminent cybe~~rthreats, and pointedly did not state that such actions or operations would necessarily involve cyber means or cyber targets. This is consistent with DOD’s prior claims that it would use “cyber and/or kinetic capabilities” to redress large-scale cyberattacks.) Panetta was ambiguous, however, about whether DOD currently has the authorities to engage in such preemptive attacks (by cyber means or other means) in the face of cyber threats. He said that “we need to have the option to take action against those who would attack us to defend this nation when directed by the president” (emphasis added), and he emphasized DOD capabilities while several times calling for more DOD authorities. I have previously criticized DOD’s announced deterrence policy, so I should say that Panetta’s speech takes steps in the right direction. Panetta noted improvement in attribution (which is potentially huge), he warned that the USG would hold attackers responsible, he appeared to eliminate unjustifiably super-high thresholds for a self-defensive responses to cyberattacks, and he noted DOD’s capacity and need for preemptive attacks in the face of imminent cyberattacks. That said, Panetta made these points in an after-dinner speech, not an official declaratory policy. And many questions remain, such as: How much better (in terms of speed and accuracy) is our attribution capacity? How do adversaries know whether the USG’s supposed attribution advances are not a bluff? What exactly is the threshold for a self-defensive offensive operation in response to a cyber attack? What counts as an imminent threat of cyberattack that would warrant a preemptive attack by the USG? The effectiveness of any deterrence posture depends on the answers to these (and related) questions, and (very importantly) on our adversaries’ beliefs about the answers to these questions. Ambiguity about the answers might over-deter (as vague criminal law often does), but it might also under-deter (because the adversary misperceives where the red lines are). The effectiveness of deterrence also depends, crucially, on the credibility of our threat to attack in the face of actual or imminent attacks. Several obstacles prevent our threats from being entirely credible. Panetta’s speech and other DOD pronouncements, as well as news reports, indicate that DOD does not think it has adequate legal authorities to engage in offensive operations related to defense, and that USG lawyers are currently putting up affirmative obstacles to such operations. To the extent that the USG is and appears to be legally constrained from acting as it says it needs to, its threats to act are not credible. In addition, even if our attribution skills are fast and accurate (which they won’t always be), any responsive cyberattack that has public effects must be accompanied by public evidence that the attack was warranted – something very hard to do when attribution is based on sophisticated and fragile intelligence tools. To the extent the USG cannot prove attribution publicly, its threats of a cyberattack are diminished. This point implies that self-defensive cyberattacks are (all things equal) more likely to be unattributable than attributable. But that conclusion in turn presents two problems. First, how to convince the adversary that we have hit it in response to a cyberattack when we cannot take public credit for the attack? (This is potentially difficult, not impossible; Iran certainly suspected the USG even before the public revelations about Stuxnet/Olympic Games.)\* Second, an unattributable self-defensive cyberattack is more likely in response to a relative small actual or threatened cyberattack on the nation. If we suffer a crippling blow, we will need to respond with large public fire, in cyber or kinetic space, or both. The worry is that the difficulties of public proof of attribution will slow the needed public response, or weaken it, or make it seem less legitimate ex post – all of which weakens the credibility of a responsive attack ex ante, and thus weakens deterrence. Finally, some thoughts about Stuxnet/Olympic Games, the cyber operation(s) against the Iranian nuclear facilities. While many in the USG are no doubt genuinely angry that the USG hand in Stuxnet was revealed, this revelation probably has the happy effect of enhancing U.S. cyber deterrence. For it demonstrates that the USG has sophisticated cyberweapons that – despite legal and other obstacles – it is willing to deploy, even in a preemptive fashion. For many reasons that I lack time explain (having to do with the nature of the Iranian threat, which did not present an attribution problem, and the nature of the cyber attack on the Iranian facilities), I think the legal and policy hurdles to the Iranian operation were less significant than ones that would arise with a self-defensive USG attack in response to an actual or threatened cyberattack.  Nonetheless, the Stuxnet/Olympic Games revelations probably enhance U.S. cyber deterrence overall.  (And no, the Iranian cyberattacks [in the news yesterday](http://www.nytimes.com/2012/10/14/world/middleeast/us-suspects-iranians-were-behind-a-wave-of-cyberattacks.html), which reportedly inflicted “modest damage,” do not by themselves belie this claim.)

**These operations have proved to be highly effective**

**Marks 19 Seattle Times** <https://www.seattletimes.com/nation-world/shutdown-hits-fbi-cyber-investigations-hard-agents-say/>

**FBI [alone] has disrupted, dismantled, and deterred 7400 cybercrimes in 2018** That slowdown could be particularly damaging because the FBI is trying to meet an ambitious goal of “deterring, detecting, disrupting, and dismantling,” 8,400 computer crimes during the 2019 fiscal year. That’s about 1,000 more crimes than the bureau dealt with in 2018 — a year that didn’t include a weekslong slowdown in operations.

**Impact: Preventing attacks on financial infrastructure**

**Shuermann 18 Harvard Business Review.**

(Paul Mee is a partner at consulting firm Oliver Wyman and leads its cyber risk practice. Til Schumer manyn is a partner in Oliver Wyman’s financial services practice and was a senior vice president at the Federal Reserve Bank of New York during the financial crisis. September 14th, 2018. “How a Cyber Attack Could Cause the Next Financial Crisis.” Harvard Business Review. <https://hbr.org/2018/09/how-a-cyber-attack-could-cause-the-next-financial-crisis> DOA 10/25/19) GSH

How might a financial crisis triggered by a cyber attack unfold? A likely scenario would be **an attack by a rogue nation or terrorist group on financial institutions** or major infrastructure. Inside **North Korea,** for example, the Lazarus Group, also known as Hidden Cobra, routinely looks for ways to compromise banks and exploit crypto currencies. **An attack on a bank, investment fund, custodian firm, ATM network, the interbank messaging networks known as SWIFT, or the Federal Reserve itself would represent a direct hit on the financial services system.**Another possibility would be if a so-called hacktivist or “script kiddy” amateur were to use malicious programs to launch a cyber attack without due consideration of the consequences**[it]. Such an attack could [cause] have a chain reaction,** causing damage way beyond the original intent, because rules, battle norms, and principles that are conventional wisdom in most warfare situations but don’t exist in a meaningful way in the digital arena. For example, in 2016 a script kiddie sparked a broad denial-of-service attack impacting Twitter, Spotify, and other well-known internet services as amateurs joined in for mischief purposes. Whether a major cyber attack is deliberate or somewhat accidental, the damage could be substantial. **Most of the ATM networks across North America could freeze. Credit card and other [and banking and] payment systems could fail across entire nations, as happened to the VISA network in the UK in June. Online banking could become inaccessible: no cash, no payments, no reliable information about bank accounts. Banks could lose the ability to transact with one another during a critical period of uncertainty. There could be widespread panic, albeit temporary.** Such an outcome might not cause the sort of long-simmering financial crisis that sparked the Great Recession, because money would likely be restored to banks and payments providers once systems were back online. At the same time, it isn’t clear how a central bank, the traditional financial crisis firefighter, could respond to this type of crisis on short notice. After the problem is fixed and the crisis halted, a daunting task of recovery would loom. It would be even more difficult if data were corrupted, manipulated or rendered inaccessible.

**Which is they conclude that**

Ever since the forced bankruptcy of the investment bank Lehman Brothers triggered the financial crisis 10 years ago, regulators, risk managers, and central bankers around the globe have focused on shoring up banks’ ability to withstand financial shocks. **But the next [financial] crisis might not come from a financial shock at all. The more likely culprit: a cyber attack that causes disruptions to financial services capabilities, especially payments systems, around the world.**

**Criminals have always sought ways to infiltrate financial technology systems. Now, the financial system faces the added risk of becoming collateral damage in a wider attack on critical national infrastructure. Such an attack could shake confidence in the global financial services system, causing banks, businesses and consumers to be stymied, confused or panicked, which in turn could have a major negative impact on economic activity.**

**Cybercrime alone costs nations more than $1 trillion [each year and is] and is] globally,** far more than the record $300 billion of damage due to natural disasters in 2017, according to a recent analysis our firm performed. **We ranked cyber attacks as the [single] biggest threat facing the business world today — ahead of terrorism, asset bubbles, and other risks.**

#### ~~Most companies aren’t prepared~~

[**~~https://www.inc.com/adam-levin/more-than-70-percent-of-businesses-admit-theyre-unprepared-for-a-cyberattack.html~~**](https://www.inc.com/adam-levin/more-than-70-percent-of-businesses-admit-theyre-unprepared-for-a-cyberattack.html) **~~Levin 18~~**

**~~How Can 73 Percent of Companies Not Be Prepared for [cyberattacks] Hackers? Most organizations admit to having inadequate defenses, even as cyberattacks continue to intensify~~**

#### These attacks could collapse the global economy

**Kempe Atlantic Council 2014**, Fred Kempe and Axel Lehmann, “Risk Nexus: Beyond data breaches: global interconnections of cyber risk,” https://www.files.ethz.ch/isn/182163/Zurich\_Cyber\_Risk\_April\_2014.pdf kegs

Prior to the financial crisis, risks were assessed by financial institutions individually. For example, a bank with significant exposure to certain risks – such as those associated with a large portfolio of sub-prime mortgages – might have had to set aside a reserve and perhaps expect to have a bad quarter or two if the underlying risk led to a meltdown. There was little assessment by either regulators or the market participants themselves of the **complex interconnections among the financial risks of different institutions. The resulting shock started with those who [make the riskiest decisions, but soon cascaded to everyone, even those who had invested wisely and conservatively. Not only were the chances for [can cause] a cascading catastrophe** widely ignored, but many experts insisted at the time that the system was sufficiently diversified so that linkages between risks were impossible. The system’s very complexity allowed risk to be spread to those most willing and able to deal with it. But it was this complexity, magnified by attendant lack of transparency and limited understanding, which contributed to the ultimate crash of 2008. **A failure in one small part of the U.S. mortgage market thus could lead to a global recession**, the collapse of governments, a sovereign debt crisis requiring bailouts, and even fears for the future of the euro and European Union. Unfortunately, cybersecurity professionals often approach risks in a similar fashion, relying on a reductionist analysis of risks, while assuming that the risk posed to the system as a whole is merely the sum of all the point risks. They analyze cyber vulnerabilities looking at one technology, one organization or one nation at a time, paying little attention to how risk[s] might emerge from the interaction of those organizations or technologies. Just as sound, internally-focused risk management failed to protect companies from the collapse of the financial system, s**trong internal computer security controls won’t shield even the best-protected companies from a ‘cyber sub-prime’ failure.** The similarities between the financial and cyber risk management methodologies go well beyond simple analogy. In the financial crisis, banks, corporations, individuals and even nations became vulnerable because they were highly leveraged, taking on incredible financial debts. The same is true in cybersecurity, where modern economies and societies are perhaps even more heavily leveraged, but their leverage involves information technologies (IT), not borrowed dollars, yen or euros. Companies are feeling the pressure to increase their IT leverage for the same reason that banks and other companies once increased their financial leverage: to keep pace with rivals that are all doing the same. IT leverage has just as much complexity, lack of transparency with regard to the risks, and lack of understanding of the underlying fundamentals as financial leverage. Few people truly understand their own computers or the internet, or the cloud to which they connect, just as few before the crisis truly understood the financial system as a whole or the parts to which they were most directly exposed. **A significant chain of disruptions to an interconnected system that only a few, if any, fully understand, could bring it all crashing down.**

#### **Because this results in a devastating recession**

**IMF** , 04/05/**13,** (Former Associate Business Editor, The Huffington Post,) “Economic Shock Could Throw 900 Million People Into Poverty, IMF Study Warns,” *Huffington Post*, <https://www.huffpost.com/entry/global-poverty-900-million-economic-shock_n_3022420> dpet

Hundreds of millions of people worldwide are on the brink of poverty. A recent study by the International Monetary Fund warns that as many as **900 million people could fall back into poverty in the event of an economic shock like the Great Recession**. That figure is three times the size of the U.S. population. According to the World Bank, 1.2 billion people are currently living on less than $1.25 a day. While the report acknowledges that progress has been to made to reduce global poverty and strengthen the world economy following the financial crisis, the world is still in a vulnerable situation. Global unemployment, for example, is the highest it’s been in two decades with 40 percent of the world’s population out of work, according to the report. And things could get much worse in the event of a macroeconomic shock, of which the Europe and U.S. are dangerously close. The recent bailout of Cyprus threw the eurozone into chaos, igniting fears that the situation could lead to the next financial crisis. Here in the U.S., a series of automatic spending cuts know as the sequester could cost the economy hundreds of thousands of jobs. The cuts have already threatened the stability of safety nets designed to aid the nation’s poorest.. The U.S. continues to fail to sustain a robust job market, adding only 88,000 jobs in March.

**around the world**.

**Thus we affirm.**

# Framing

1. **We are in a constant state of attacks - need offensive**
2. **Prefer empirics over hypotheticals - hard to tell what’s true in cyberspace**
3. **Probability outweighs magnitude---large but low probability impacts lock us into counter-effective apocalyptic rhetoric**

**Boisvert 15-** [Will, journalist for The Breakthrough, writes on energy, environmental, and urban policy for The New York Observer, Dissent, and other publications, “Fear and Time: Risk Culture and the Broken Doomsday Clock” web 7.8.2017, https://thebreakthrough.org/index.php/journal/past-issues/issue-5/fear-and-time] Fall 2015//ad

But there are problems with apocalyptic dread as a framework for dealing with the issues the Bulletin has taken up. **The doomsday metaphor** fits nuclear war, suggesting a simple, stark, overwhelming peril that merits moral revulsion and abolition. But climate change and other issues of sustainability and development pose complex, ambiguous risks, for which a simple eliminationist program may be neither feasible nor desirable. Apocalypticism **can systematically distort our understanding of risk, mesmerizing us with sensational scenarios that distract us from mundane risks that are objectively large**r. Worse, it can block rather than galvanize efforts to solve global problems. By treating risks as infinite, **doom-saying makes it harder to take their measure — to prioritize them, balance them against benefits, or countenance smaller ones to mitigate larger ones**. The result can be paralysis, as initiatives get tangled in conflicting anxieties that yield incoherent policies — a muddle that’s amply reflected in the Bulletin’s pages. **The Doomsday Clock demands that we avoid every risk at any cost.** But addressing global crises will require us to do something very different: **to embrace the risks that are most worth taking**.

# Lay Rhetoric

benefits O/W harms

Lay Strats: Ballot looks like/2 reasons one reason

Cheese Frontline strats: We account, directionality, no warrant, not a turn

# Frontlines

## C1: Terrorism

### Case Extension

Vote on contention 1 about taking down ISIS with OCOs

Rogers ev - OCOs have been critical to taking 98% of ISISs territory

1. Varvra and raston- surgical strikes knock down their entire communications network so fighters can’t coordinate attacks
2. ASP - destroy propaganda so they can’t recruit new fighters anymore
3. GWU - support conventional troops and airstrikes by pinpointing terrorist positions
4. Pomerleau and Sales - find people who fund terrorists to cut off the group’s money flow - ISIS can no longer afford to fight

Impact: We need to finish the fight against ISIS to prevent resurgence like what happened in 2011 - otherwise we see genocide and global attacks putting 15 million lives at risk

### Weighing

O/W probability - empirics guarantee solvency in stopping ISIS -

O/W magnitude - ISIS is committing genocide - 15 mil lives at risk in africa

Prereq dev countries - Al-Shabab destabilizes states

Prereq social spending:

1. Without OCOs it would cost more money to fight terror - [harrington](https://www.csis.org/analysis/arab-gulf-states-and-iran-military-spending-modernization-and-shifting-military-balance) CSIS says ME nations spend over 10% of economy on military and counterterror
2. Terror destabilizes gov - Iraq syria - obv cant provide since infra is destroyed and no govt

### FL: TOPICALITY

#### FL: Surveillance not OCO

1. Uren 18- it is
2. Bulter 13 - it is
3. Kosseff 19 - Defend forward says it is

### FL: ALT SOLVENCY

#### FL: ISIS collapsing now

1. GiIlsinan 19 - past precedent for resurgence - 2014, conditions are ripe: power vacuum, recruiting, poor governance, weak KDF

#### FL: Drones Solve

1. It helps drones find targets - in case
2. It makes drones more accurate in tracking ppl- Bramlette 19

#### FL: The US will combat ISIS without OCO’s

1. Troops depends on cyberintel - only way to know who to attack and where terrorists are - 2017 pinpointed the location of terrorists and their secret bases
2. Only way to stop digital propaganda and recruitment - conventional methods fail since they don’t operate in cyberspace
3. Trump wants to back out of Syria -- more ground troops isn’t an option

#### FL: hacktivists solve

1. Only the Pentagon has a bunch of special military-grade algorithms not internet trolls
2. Uncoordinated - taking down a few twitter posts is not enough - Raston - US can take down the whole network

#### FL: Australia/other nations solve

1. Part of the US-Led coalition - reliant on our leadership and can’t do it all themselves
   1. not a single example where they stopped *ISIS* themselves
   2. We show only the US is proven to work - our cyber is #1 in the world
   3. Greer 17 Foreign Affairs - lack of global coop makes it way harder to stop terrorists - can share info/techniques between forces

### FL: NO SOLVENCY

#### FL: OCO’s don’t take down ISIS/Will resurge

1. Empirics prove success - this postdates their [xxxx] evidence - Vavra 19 and NPR 19 - lose their ability to recruit online, took down their communication and control systems - we’ve seen a significant decrease in threat level - ISIS only doing isolated attacks vs a full scale war
2. Raston - Surgical strikes take down their whole network - no new fighters either
3. Brands 19 in case- only resurge if we prematurely stop OCOs and quit

#### F2: Launching gets delayed

1. Raston 19 NPR - spent months planning but carried out the attack in just 5 hours - shut down all isis control nodes
2. Empirically successful+ Varva and Martelle give tons of examples

#### FL: Don’t quant recruitment

1. Wired 16 - 30k ppl joined bc online propaganda

#### F2: Recruit domestically now

1. Barely anyone left- refugees flee from war zones
2. Klor 16 - Thats why recruited 30k foreign fighters in the past to replenish support

#### AT: ISIS Membership is still growing

1. Not true - Rogers says ISIS territory down by 98%
2. Neff NYT December - lost 90% of fighters only 300 now
3. Full OCO deployment solves

#### FL: Encryption stops us from beating them

1. Empirics prove its effective - o/w’s hypotheticals
2. Khandelwal 16 - The NSA cracked the encryption system used
3. Just cut off their internet

#### FL: ISIS gets around attacks

1. NPR - empirically they can’t recover, almost impossible to buy new servers and domain addresses from Syria

#### FL: Org Decapitation Bad

1. Not the arg - it’s generic

### FL: NO IMPACT/“TURNS”

#### FL: Terrorism is inevitable

1. Even if terrorism is inevitable, ISIS is one very dangerous terrorist organization globally that has used the internet as a recruitment and communication tool successfully.

#### AT: ISIS Reverse Engineers our OCO’s

1. No examples of this happening
2. Don’t have capacity if they’re computers are getting destroyed/losing their internet connections (Raston)
3. Yeah that’s because our defense is weak not our offense
4. Turn: if we don’t stop ISIS they could try to steal them

#### FL: US intervention increases anti-American sentiment

1. ~~There is no impact of an increase anti-American sentiment.~~
2. No warrant or UQ- card not about OCOs which are targeted attacks that dont harm civilians
3. Nobody in Syria likes ISIS due to the damage they created and Sharia law oppressive - US eliminating ISIS increases positive sentiment instead
4. Getting rid of propaganda prevents ISIS from spinning the story and recruiting
5. No quant
6. Turn: Don’t have capacity if their computers are getting destroyed

#### FL: Terrorists get more angry/more attacks

1. NUQ: They angry now - always trying to inflict maximum damage
2. Turn: Don’t have capacity if their computers are getting destroyed

#### FL: Lose Surveillance Capability

1. Berger 16 Brookings - can pick and choose - weigh which ones to keep and which ones to take down - concludes loss is minimal

F2: Splintering

1. Doesn’t matter since no capacity to attack anymore
2. Turn - Rand 19 and barber 15- conclude that fractured terrorists groups become weaker
   1. Lose a coherent ideological message so can’t gain followers
   2. No leadership so splintered groups start fighting each other
   3. They conclude this happened to both al qaeda and ISIS now - that’s why dec 98%

### FL Cards

Klor 16 - https://www.nber.org/digest/jun16/w22190.html

As of December 2015, approximately 30,000 fighters from at least 85 countries had joined the Islamic State of Iraq and Syria (ISIS). Although the great majority of ISIS recruits come from the Middle East and the Arab world, there are also many from Western nations, including most member-states of the European Union, as well as the United States, Canada, Australia, and New Zealand. Thousands of fighters from Russia and hundreds from Indonesia and Tajikistan also have joined. ISIS's recruitment of foreign fighters is a global phenomenon that provides the organization with the human capital needed to operate outside the Middle East.

Raston 19 NPR - spent months planning but carried out the attack in just 5 hours - shut down all isis control nodes

<https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis>

**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. "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."

Barber 15 - <http://www.terrorismanalysts.com/pt/index.php/pot/article/view/469/html>

The true breakdown in Al Qaeda Core’s control came during the 2006-2010 interval, where it was not yet ousted as the sole source of information and direction within the network, but its affiliates were clearly poised to take active leadership roles. Even more damaging, it abandoned efforts to maintain ties with ideologically similar groups altogether. There could be any number of logistical or tactical motivations for this, but the ultimate implication is that the ideology of the group is not as important. For an ideologically motivated organization like **Al Qaeda, this represents a dangerous departure from its rhetoric and the loss of control over its overall message.**

The final interval, although incomplete, is important in that it represents both the increasing regionalization of the network, and **the introduction of competition between Al Qaeda Core and its regional branch**. Al Qaeda Core had previously been insulated from such negative ties, implying that this new period marks the end of Al Qaeda’s unquestioned leadership. It also seems to point to the end of a global network, as groups increasingly focus on regional conflicts and objectives. The ultimate function of Al Qaeda Core was to inspire the rise of militant organizations and then connect them to each other. As the network grew and Al **Qaeda Core’s power waned,** rather than prop up its creator, the movement fractured into regional networks. Given the ongoing regionally focused conflicts in which many of these groups operate today, the trend towards regionalism is unlikely to change. However, without additional data, it would be unwise to draw firm conclusions from this interval.

<https://www.rand.org/blog/2017/01/is-isis-breaking-apart.html>

To gain a sense of how splintering has affected ISIS, we analyzed the group's media output—the propaganda it releases—over time. An examination of productivity, provenance, and quality can offer clues to how its metanarrative is shifting, how well its brand coheres, and, by default, how easily the group can communicate with its audience. In our pursuit, few insurgent movements have offered better opportunities for research. ISIS, after all, has been inundating the Internet with propaganda for years.

In recent months, the geographic scope of ISIS' media has narrowed.

Although ISIS' overall media output is ebbing, as a recent study by the Combating Terrorism Center at West Point shows, the issue of overall productivity is less important in this context than is where the messages are actually being produced. With this in mind, relying on a comprehensive archive of ISIS propaganda collected over the last six months, we systematically went through each of the organization's 57 media production units to assess dormancy levels, noting when a given unit last released a piece of media and what that product was. An unambiguous trend emerged: the ISIS brand is contracting. Indeed, in recent months, the geographic scope of ISIS' media has narrowed, with dormancy levels the highest at the periphery. At its height in 2015, no fewer than 40 individual propaganda “offices” were producing media. As of mid-January 2017, just 19 outlets were active. These days, the caliphate brand is associated almost entirely with Iraq and Syria, and regional affiliates appear to be becoming even more distant and disconnected from the core.

**Berger 16 Brookings**

**https://www.brookings.edu/wp-content/uploads/2016/06/isis\_twitter\_census\_berger\_morgan.pdf**

Our anecdotal observation indicates that **the most valuable intelligence tends to emanate from the least obvious vectors, such as accounts with very small numbers of followers.** The most active and visible ac-counts contain more noise, and their content is more carefully stage-managed by ISIS and its adherents. Based on both anecdotal observation and ISIS social media strategy documents, original information tends to flow from more obscure accounts to more visible accounts such the mujtahidun, the core group of ISIS supporters devoted to disseminating information that originates elsewhere.

**The ability to accurately identify tens of thousands of ISIS supporters on Twitter provides ample room for the suspension of accounts that have strong op-erational, recruitment, or propaganda value, with little or no functional loss of intelligence**

If every single ISIS supporter disappeared from Twitter tomorrow, it would represent a stagger-ing loss of intelligence—assuming that intelli-gence is in fact being mined effectively by some-one somewhere.  **However, many thousands of accounts can likely be removed from the ecosys-tem without having a dramatic negative impact on the potential intelligence yield**

GiIlsinan 19 <https://www.theatlantic.com/politics/archive/2019/11/evolution-of-isis/602293/>

**After the US declared ISIS defeated in 2014 and withdrew, ISIS resurged**

It was the summer of 2014 when most Americans took notice of the Islamic State, but the group had been around in different forms for about a decade. Many of its fighters were the same people who’d fought U.S. troops under the name of al-Qaeda in Iraq, until a massive U.S. military effort suppressed them. Then the American people and their government decided that the war was done. What came next was a renewed militant group with even greater international ambitions, asISIS **captur[ing] territory across Iraq and Syria and declar[ing]** it **a caliphate**. Now, with the U.S. government once again trying to wind down a war following the so-called caliphate’s collapse, the question is whether ISIS can repeat its history of survival, and what it might morph into next. In the past year, its leader has died and it has lost the last of its territory, which at its peak was roughly the size of Britain. Much like after the Iraq War, though, both ISIS and the conditions that fostered it remain—and in some ways, the environment is even more promising for its survival now**. ISIS may be weaker,** but it retains thousands of members across Iraq and Syria. The Obama administration’s management of the U.S. withdrawal from Iraq had its own problems, but Trump’s abrupt and unilateral decision to pull U.S. troops from northeastern Syria has been a picture of chaos. U.S. efforts to rebuild and provide humanitarian relief and security in former ISIS strongholds in the country are in jeopardy, as is the Kurdish-led Syrian Democratic Forces, which served as America’s main partner. In Iraq, many areas have not been adequately rebuilt, and the country’s political and economic morass has spurred weeks of demonstrations, to which the government has responded with brutal crackdowns. An entire generation across both Iraq and Syria has been traumatized by extremism and war, and tens of thousands of suspected ISIS members and their families languish in the limbo of poorly resourced camps in Syria. The international community has made little effort to help the masses of children whom ISIS made a concerted effort to radicalize.

So what’s next? Aaron Zelin, a veteran researcher of jihadist groups, told us that another ISIS surge and land grab is unlikely in the near term. Instead, ISIS will probably retain its core in Iraq especially, but in Syria as well—as Zelin noted, the group is comfortable underground in its territory and has survived this way before—with connections to supporters and affiliates around the globe. From there, it can bide its time, pursuing a long-term vision that its leaders have called a “generational strategy,” Zelin said. “They see this as a battle of attrition, and that eventually they’re going to wear everyone out. They’re not rigid in their thinking, and they’re **willing to evolve.”**

Neff NYT dec 19

<https://www.nytimes.com/2019/12/02/world/asia/ISIS-afghanistan-baghdadi.html>

Western and Afghan officials see a combination of factors that led to the Islamic State’s losses in the east, forcing many of the fighters to either move or surrender. One Western official estimated that the group’s strength was now reduced to around 300 fighters in Afghanistan, from an estimated 3,000 earlier this year.

Kosseff 19 <https://ccdcoe.org/uploads/2019/06/Art_17_The-Contours-of-Defend-Forward.pdf>

In 2018, United States Cyber Command announced a new operational

concept to “defend forward” against other states whose cyber operations against

the United States have been hostile, but short of an armed attack. Defend Forward

supports the U.S. strategy of persistent engagement, which recognizes the need to

continuously engage to inhibit incessant adversarial cyber operations against the

United States. Although the public Defend Forward description was short on details, it

consists of three general components: (1) positioning to degrade cyber operations; (2)

warning to gather information about threats and inform defenses; and (3) influencing

adversaries to discourage them from deploying cyber operations against the United

States.

Bramlette 19 <https://apps.dtic.mil/dtic/tr/fulltext/u2/1074625.pdf.>

(can cut more} This research succeeds in proving the hypothesis that a functional cyber-attack drone

payload could be built under $500, under 1 kg, and within four months. One of the four

data sets shows that geolocation via radiolocation of Wi-Fi targets can be accurate below

the hypothesized 15% of distance from the targets at 600 m using less than 90° of angular

coverage and full channel hopping, however the other three data sets failed to reach that

degree of accuracy. Geolocation efforts with larger coverage angles, targeted single-channel

sweeps, and intelligent filtering are recommended to increase accuracy.

Greer 17 https://www.foreignaffairs.com/articles/middle-east/2017-04-10/defeat-isis-cooperation-key

Despite politically driven rhetoric touting the virtues of “going it alone” in foreign policy, **cooperation with other nations in its various forms remains essential to countering terrorism.** The Islamic State (also known as ISIS) may be on the run within Iraq and Syria, but its affiliates and other terrorist groups such as al Qaeda still represent a significant threat to international security. Because such groups span countries, communities, and borders, international cooperation to defeat them has been critical.

In a recent report, we used game theory and related methods to assess the likelihood of ISIS’ defeat. **We found that if the international trend toward isolationism continues, ISIS’ destruction will become less likely—and as terrorism continues from al Qaeda and other groups, international cooperation will be just as relevant to ISIS’ successor. However, if countries and firms band together and share resources, they can succeed.**

**The benefits of multilateral cooperation against terrorism are readily apparent.** The Coalition to Counter ISIS, for example, comprises 68 countries and institutions that have come together around core principles such as military cooperation, disrupting the flow of foreign recruits to and from Iraq and Syria, cutting off ISIS’ access to the international financial system, addressing humanitarian crises, and countering the ISIS brand. Such cooperation is critical to ISIS’ defeat.

#### **OCO’s include spying and info-gathering**

Alan **BUTLER**, Appellate Advocacy Counsel, Electronic Privacy Information Center (EPIC); J.D. UCLA School of Law, **13** [June, 2013, “When Cyberweapons End Up on Private Networks: Third Amendment Implications for Cybersecurity Policy,” American University Law Review, 62 Am. U.L. Rev. 1203, Lexis]

Offensive cyberoperations include "actions taken against an adversary's computer systems or networks that **harm the adversary's interests**." n55 Many military cyberoperations are not intended to cause physical destruction. n56 For example, cyberexploitations are used to facilitate quiet and undetectable information-gathering. n57 These operations take advantage of the same vulnerabilities and access [\*1213] paths as targeted cyberattacks. n58 The viruses used in cyberexploits can infect computers and systems across the globe, and these viruses can remain dormant for years without detection. n59 Recently uncovered cyberexploitation attacks used sophisticated malware to gather troves of confidential data from a broad range of computers and devices. n60

**Uren,** Tom (Senior Analyst at the ASPI), Bart Hogeveen (Analyst at the ASPI) and Fergus Hanson (Director of the International Cyber Policy Centre of the ASPI). “Defining offensive cyber capabilities.” Australian Strategic Policy Institute, 4 June 2018,<https://www.aspi.org.au/report/defining-offensive-cyber-capabilities>. DG

In both UK and US military doctrine, **offensive operations are a distinct subset of cyberspace operations that also include defensive actions; intelligence surveillance and reconnaissance** and operational preparation of the environment—non-intelligence enabling activities conducted to plan and prepare for potential follow-on military operations.

Wired 16 <https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/>

Among these is the group’s use of narrowcasting—creating varied content that caters to niche audiences. (Think of those BuzzFeed listicles aimed at groups like Army brats or Florida natives.) Only a fraction of the Islamic State’s online output depicts the kind of sadism for which the group is notorious: Far more common are portrayals of public-works projects, economic development, and military triumphs, frequently aimed at specific Muslim enclaves throughout the world. This content is meant to convince prospective recruits of the veracity of the organization’s core narrative: that its empire is both stable and inexorably growing. (The Islamic State’s slogan is “Baqiya wa Tatamaddad”—Remaining and Expanding.) **So far, digital propaganda of this sort has helped motivate more than 30,000 people to turn their backs on everything they’ve ever known and journey thousands of miles into dangerous lands, where they’ve been told a paradise awaits.**

Khandelwal 16 <https://thehackernews.com/2016/10/nsa-crack-encryption.html>

In the year 2014, we came to know about the NSA's ability to break Trillions of encrypted connections by exploiting common implementations of the Diffie-Hellman key exchange algorithm – thanks to classified documents leaked by ex-NSA employee Edward Snowden.

<https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis>

**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.** 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."**

<https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis>

"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.

## C2: Botnets

### Case Extension

Defense alone is insufficient- Fazzini Goldsmith ev - OCOs stop cybercriminals by hacking into and shutting down botnets, which are collections of compromised computers used by hackers to launch their most powerful attacks - this prevents them from doing damage and deters criminals from future attacks

Marks 19 - empirically very successful - we stopped and deterred 7400 attacks last year

The impact is preventing a financial crisis:

Shuermann and Kempe - attacks on interbank networks could cause a global chain reaction where all payment systems fail - that causes 1T in damage and collapses the global economy. IMF says that pushes 900 mil into poverty

### Weighing

1. O/W Mag - recession puts 900 mil into poverty - most impacts the global poor- that comes first - [comparison]
2. O/W Prob - 100% empirical proof of success and will work- [comparison]
3. Prereq - Econ collapse
   1. Decrease tax revenue for govt services
   2. prevents cyber **defense** spending - magnifies risk for all other impacts since we cant protect ourselves

### FL: TOPICALITY

#### FL: FBI Not OCOs

1. Gellman Washpo - usually an interagency joint effort involving FBI and other agencies
2. Marks 19 (and Rubino) - FBI does cyberops
3. FBI is just one example not the only agency

### FL: ALT SOLVENCY

#### FL: Companies can stop it themselves

1. Obv not true or we wouldn’t be seeing so many attacks
2. Bhatik 18 Forbes - financial firms are 300x as vulnerable to cyberattacks compare to other biz
3. Always reactive not proactive - criminals are 1 step ahead
4. Ringel 2019 The Next Web - Very expensive and often cant afford

#### FL: Defense alone Stops Attacks

1. Offense vs Defense card: defense alone fails, too many vulnerabilities
2. Goldsmith - offensive cyber operations can deter and prevent attacks from occurring

### FL: NO SOLVENCY

#### FL: Not Effective -- Generic

1. This statistic is misleading - the gvmt focuses on stopping the biggest and most damaging attacks
   1. Still stopped 7k+ attacks
   2. Hawkins 18 WashPo - Stopped FIN7 biz which attacked 100+ businesses

#### FL: 350% increase under Trump administration

1. Our impact is scalar. Under the Obama administration, our offensive cyber attacks were considered non-existent, and for the first time in a decade Trump has increases OCO’s. Even if there is a temporary short term spike in OCO’s against the US, our argument is the more money and effect the administration puts into OCO’s, the more legitimacy our attacks gain thus deterring foreign attackers.
2. Kramer 12 (in case) - Legitimacy of OCO’s is the way to future cyber attacks

#### FL: OCO’s don’t deter

1. Not reading anymore

### FL: DUM DUM RESPONSES

#### FL: Escalation

1. It’s targeting criminals, this doesn’t apply
2. Arms race already happening no

### FL: NO IMPACT

#### FL: No risk of cyber catastrophe

1. Shuermann - #1 threat - already cost trillions and risk is high - single major attack triggers chain reaction
   1. Increasing interconnectedness
   2. Increasingly advanced cybercriminals

### FL Cards

#### **The risk now is higher than ever**

**Bhatik 18 Forbes**

https://www.google.com/amp/s/www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/amp/

The risk of cyberattack on financial services firms cannot be overstated. Cyberattacks cost financial services firms more to address than firms in any other industry at $18 million per firm (vs. $12 million for firms across industries). **Financial services firms also fall victim to cybersecurity attacks 300 times more frequently than [other] businesses in other industries.** In other words, while the typical American business is attacked 4 million times per year, the typical American financial services firm is attacked a staggering 1 billion times per year.

Rubino 18 [**https://www.frankrubino.com/Legal-Articles/FBI-Cracks-Down-On-Cyber-Crimes.shtml**](https://www.frankrubino.com/Legal-Articles/FBI-Cracks-Down-On-Cyber-Crimes.shtml)

**The Federal Bureau of Investigation (FBI) is cracking down on cyber crimes.** The bureau's assistant director of the Criminal, Cyber, Response and Services Branch recently announced that cyber criminals would be held accountable for their actions and that the agency was **gearing up to tak[ng] a "much more offensive side" in its cyber program.** It is no surprise that the FBI is putting forward a strong effort **to catch those who commit cyber crimes and deter future violations.** Cyber crimes appear to be on the rise, with Wired magazine calling these offenses the "next entrepreneurial growth business." In fact, the magazine reports that cyber crimes are estimated to cost the global economy over $400 billion every year. However, a strong push to prosecute those who violate these laws will likely lead to

**Hawkins 18 Washington Post** <https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/08/02/the-cybersecurity-202-feds-arrest-three-in-global-cybercrime-ring-linked-to-hacks-on-chipotle-arby-s-and-other-u-s-chains/5b61e2331b326b0207955ea6/>

**The Justice Department [stopped]** appears to have put a dent in **the global cybercrime ring known as FIN7**, or Carbanak Group. Prosecutors said yesterday they **arrested three senior members** of the organization, **which has targeted more than 100 U.S. businesses and stolen about 15 million credit card numbers** in a long-running hacking campaign, as my colleague Devlin Barrett reported. The FBI arranged the arrests of the three suspects, all Ukrainian nationals, as they traveled outside their home country. They’re charged with more than two dozen counts including conspiracy, wire fraud, computer hacking, fraud and aggravated identity theft. The case has been a heavy lift for U.S. authorities. Tabb, of the FBI, said the agency’s Seattle field office had devoted half of its “cyber resources” to the investigation. He added that it was “among the top three criminal computer intrusion cases that the FBI is working right now, in terms of loss, the number of victims, the global reach of it, and the size of the organization.” And there’s still more work to do.

Gellman WashPo <https://cyber-peace.org/wp-content/uploads/2013/06/%E2%80%98Black-budget%E2%80%99-summary-details-U.S-Part2.pdf>

**When it comes time to fight the cyberwar against the best of the NSA’s global competitors, t**he TAO calls in its elite operators, who work at the agency’s Fort Meade headquarters and in regional operations centers in Georgia, Texas, Colorado and Hawaii. The NSA’s organizational chart has the main office as S321. Nearly everyone calls it “the ROC,” pronounced “rock”: the Remote Operations Center. “To the NSA as a whole, the ROC is where the hackers live,” said a former operator from another section who has worked closely with the exploitation teams. “It’s basically the one­stop shop for any kind of active operation that’s not defensive.” **Once the hackers find a hole in an adversary’s defense, “[t]argeted systems are compromised electronically, typically providing access to system functions as well as data. System logs and processes are modified to cloak the intrusion, facilitate future access, and accomplish other operational goals,”** according to a 570­page budget blueprint for what the government calls its Consolidated Cryptologic Program, which includes the NSA. **Teams from the FBI, the CIA and U.S. Cyber Command work alongside the ROC,** with overlapping missions and legal authorities. So do the operators from the NSA’s National Threat Operations Center, whose mission is focused primarily on cyberdefense. That was Snowden’s job as a Booz Allen Hamilton contractor, and it required him to learn the NSA’s best hacking techniques.

Marks 19 https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/01/23/the-cybersecurity-202-fbi-cyber-investigations-hit-hard-by-shutdown/5c475f7c1b326b29c3778c68/

The bureau will also face significant difficulty resuming cyber operations after weeks in limbo, says Anthony Ferrante, former chief of staff for the FBI’s cyber division. After the October 2014 shutdown, Ferrante told me in an email, it took months before the bureau was processing cases at normal speed again.

**Franklin Kramer,** adistinguished research fellow in the **Center for Technology and National Security Policy** at the National Defense University, wrote **in 2012** [Franklin D. Kramer is a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He served as the assistant secretary of defense for international security affairs from 1996 to 2001. Stuart H. Starr is also a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He concurrently serves as the president of the Barcroft Research Institute. Larry Wentz is a senior research fellow in the Center for Technology and National Security Policy at the National Defense University., “Cyberpower and National Security”, p. 318]

No cyber deterrence strategy can hope to be airtight to prevent all minor attacks. However, a strategy **can increase the chances that major cyber attacks can be prevented**; this could protect the United States and its allies not only from a single major attack but also from serial cyber aggressions and resulting damage. A worthwhile goal of a cyber deterrence strategy would be to transform medium-sized attacks into low-probability events and to provide practically 100 percent deterrence of major attacks. A cyber deterrence strategy could contribute to other key defense activities and goals, including **assurance of allies, dissuasion, and readiness to defeat adversaries in the event of actual combat**. The goal of dissuading adversaries is crucially important. Thus far, the United States has not been noticeably forceful in **stating its intentions to deter major cyber attacks** and, if necessary, **to respond to them with decisive force employing multiple instruments of power**. Meanwhile, several countries and terrorist groups are reportedly developing cyber attack capabilities. Dissuasion of such activities is not an easy task: it **requires investment in technical capabilities as well as building an internal consensus to employ these capabilities.** If some of these actors can be dissuaded from entering into cyber competition with the United States and its allies, t**he dangers of actual cyber aggression will diminish.** How would a cyber deterrence strategy operate, and how can its potential effectiveness be judged? Deterrence depends on the capacity of the United States **to project an image of resolve, willpower, and capability in sufficient strength** to convince a potential adversary to refrain from activities that threaten U.S. and allied interests. As recent experience shows, deterrence can be especially difficult in the face of adversaries who are inclined to challenge the United States and otherwise take dangerous risks. In cases of failure, deterrence might well have been sound in theory but not carried out effectively enough to work. The aggressions of Saddam Hussein, Slobodan Milosevic, and al Qaeda might not have been carried out had these actors been convinced that the United States would respond with massive military force. These aggressions resulted because of a failure to communicate U.S. willpower and resolve, not because the attackers were wholly oblivious to any sense of restraint or self-preservation, nor because the logic of deterrence had lost its relevance.

Ringel 2019 The Next Web

<https://thenextweb.com/podium/2019/10/26/modern-cybersecurity-is-inaccessible-to-smaller-companies-and-thats-bad-for-you/>

With so much data flying around, hackers have more opportunities to steal and exploit it for identity theft, creating a measurable phenomenon that regularly drains billions each year from the economy. Keeping the data tabs open yet segregated from fraudsters, unfortunately, begs an equally high price tag. While high-profile hacks motivate the largest companies to form robust cybersecurity departments, mobilize their multinational-size budgets, and orchestrate the integration of multiple cybersecurity products, small-and-medium-sized businesses can’t afford these solutions yet suffer more for not having them. The best cyber solutions are too expensive for many to afford, which unintentionally makes these consumers an easier target for hackers. That’s not to say large companies don’t get hacked; they do, but rarely and with more fanfare.

# Extra Cards

### Extra REcruiting

https://www.voxpol.eu/download/article/Halting-Boko-Haram-Islamic-States-West-Africa-Province-Propaganda-in-Cyberspace-with-Cybersecurity-Technologies.pdf

It is known that terrorist organizations are using online tactics to spread fear, panic,and present situations of uncertainty to the public.Social media is an efficient and convenient tool for terrorist groups because it has the capability of spreading short messages with blends of image, voice, and text.Every device such as laptop computers, desktop computers, mobile phones, and digital watches have Internet access capability and network to reinforce ideological beliefs and spin messages. Young people have been encouraged via social media to take terrorist action against their homelands. **Several examples of the last few years indicate that ISIS mobilized young people via social media to travel and join jihadists in the war in Syria. Most fatawiissues by terrorist leaders are communicated to the public via social media**

[AFF Terrorism (moved to case)](https://docs.google.com/document/d/1JnJrpjAOlxKvCBNcRYciUyOC_A0X6qAAFW4s9bCzAPU/edit)[AFF Cybercrime (Done)](https://docs.google.com/document/d/1YRkixfFhHyrWWrrHda7eSqryXClbKVKeK4RqB8GxFvo/edit#heading=h.419qeyvnw3fm)

<https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html>

The goal of the new campaign is to disrupt the ability of the Islamic State to spread its message, attract new adherents, circulate orders from commanders and carry out day-to-day functions, like paying its fighters. A benefit of the administration’s exceedingly rare public discussion of the campaign, officials said, is to rattle the Islamic State’s commanders, who have begun to realize that sophisticated hacking efforts are manipulating their data. Potential recruits may also be deterred if they come to worry about the security of their communications with the militant group.

**https://www.cyberscoop.com/john-bolton-offensive-cybersecurity-not-limited-election-security/**

The U.S. is beginning use offensive cyber measures in response to commercial espionage, President Trump’s national security adviser, John Bolton, said Tuesday.

“We’re now looking at — beyond the electoral context — a whole range of other activities to prevent this other kind of cyber interference … in the economic space, as well,” Bolton said while speaking at The Wall Street Journal’s CFO Network annual meeting.

#### ~~Second, deterrence can solve future cyber attacks~~

**~~Franklin Kramer,~~**~~a~~~~distinguished research fellow in the~~**~~Center for Technology and National Security Policy~~** ~~at the National Defense University, wrote~~ **~~in 2012~~** ~~[Franklin D. Kramer is a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He served as the assistant secretary of defense for international security affairs from 1996 to 2001. Stuart H. Starr is also a distinguished research fellow in the Center for Technology and National Security Policy at the National Defense University. He concurrently serves as the president of the Barcroft Research Institute. Larry Wentz is a senior research fellow in the Center for Technology and National Security Policy at the National Defense University., “Cyberpower and National Security”, p. 318]~~

~~No cyber deterrence strategy can hope to be airtight to prevent all minor attacks. However, a strategy~~ **~~can increase the chances that major~~ ~~cyber attacks can be prevented~~**~~;~~ ~~this could protect the United States and its allies not only from a single major attack but also from serial cyber aggressions and resulting damage. A worthwhile goal of a cyber deterrence strategy would be to transform medium-sized attacks into low-probability events and to provide practically 100 percent deterrence of major attacks.~~**~~A cyber deterrence strategy could contribute to~~** ~~other key defense activities and goals, including~~**~~assurance of allies, dissuasion, and readiness to defeat adversaries~~ ~~in the event of actual combat~~**~~. The goal of dissuading adversaries is crucially important. Thus far, the United States has not been noticeably forceful in~~ **~~stating its intentions to deter major cyber attacks~~** ~~and, if necessary,~~ **~~to respond to them with decisive force employing multiple instruments of power~~**~~. Meanwhile, several countries and terrorist groups are reportedly developing cyber attack capabilities. Dissuasion of such activities is not an easy task: it~~ **~~requires investment in technical capabilities as well as building an internal consensus to employ these capabilities.~~** ~~If some of these actors can be dissuaded from entering into cyber competition with the United States and its allies~~~~,~~ **~~the dangers of~~ ~~actual~~ ~~cyber aggression~~ ~~will~~ ~~diminish.~~** ~~How would a cyber deterrence strategy operate, and how can its potential effectiveness be judged?~~**~~Deterrence depends on the capacity of the U~~**~~nited~~ **~~S~~**~~tates~~ **~~to project an image of~~ ~~resolve, willpower, and~~ ~~capability in sufficient strength~~**~~to convince a potential adversary to refrain from activities that threaten U.S. and allied interests. As recent experience shows, deterrence can be especially difficult in the face of adversaries who are inclined to challenge the United States and otherwise take dangerous risks. In cases of failure, deterrence might well have been sound in theory but not carried out effectively enough to work. The aggressions of Saddam Hussein, Slobodan Milosevic, and al Qaeda might not have been carried out had these actors been convinced that the United States would respond with massive military force. These aggressions resulted because of a failure to communicate U.S. willpower and resolve, not because the attackers were wholly oblivious to any sense of restraint or self-preservation, nor because the logic of deterrence had lost its relevance.~~

#### 

#### **Economic downturn causes great power war, turns every impact.**

**Green and Schrage 9 –** Michael, Senior Advisor and Japan Chair at CSIS and Associate Professor at Georgetown, Steven, CSIS Scholl Chair in International Business and a former senior official with the US Trade Representative's Office, State Department and Ways & Means Committee, “It's not just the economy”, Asia Times, 3/26, http://www.atimes.com/atimes/Asian\_Economy/KC26Dk01.html

Facing the worst economic crisis since the Great Depression, analysts at the World Bank and the US Central Intelligence Agency are just beginning to contemplate the ramifications for international stability if there is not a recovery in the next year. For the most part, the focus has been on fragile states such as some in Eastern Europe. However, **the Great Depression taught us that a downward global economic spiral can even have jarring impacts on great powers. It is no mere coincidence that the last great global economic downturn was followed by the most destructive war in human history**. In the 1930s, **economic desperation helped fuel autocratic regimes and protectionism in a downward economic-security death spiral that engulfed the world in conflict. This spiral was aided by the preoccupation of the United States and other leading nations with economic troubles at home and insufficient attention to working with other powers to maintain stability abroad.** Today's challenges are different, yet 1933's London Economic Conference, which failed to stop the drift toward deeper depression and world war, should be a cautionary tale for leaders heading to next month's London Group of 20 (G-20) meeting. There is no question the US must urgently act to address banking issues and to restart its economy. But the lessons of the past suggest that we will also have to keep an eye on those fragile threads in the international system that could begin to unravel if the financial crisis is not reversed early in the Barack Obama administration and realize that economics and security are intertwined in most of the critical challenges we face. A disillusioned rising power? Four areas in Asia merit particular attention, although so far the current financial crisis has not changed Asia's fundamental strategic picture. China is not replacing the US as regional hegemon, since the leadership in Beijing is too nervous about the political implications of the financial crisis at home to actually play a leading role in solving it internationally. Predictions that the US will be brought to its knees because China is the leading holder of US debt often miss key points. China's currency controls and full employment/export-oriented growth strategy give Beijing few choices other than buying US Treasury bills or harming its own economy. Rather than creating new rules or institutions in international finance, or reorienting the Chinese economy to generate greater long-term consumer demand at home, Chinese leaders are desperately clinging to the status quo (though Beijing deserves credit for short-term efforts to stimulate economic growth). **The greater danger with China is not an eclipsing of US leadership, but instead the kind of shift in strategic orientation that happened to Japan after the Great Depression.** Japan was arguably not a revisionist power before 1932 and sought instead to converge with the global economy through open trade and adoption of the gold standard. The worldwide depression and protectionism of the 1930s devastated the newly exposed Japanese economy and contributed directly to militaristic and autarkic policies in Asia as the Japanese people reacted against what counted for globalization at the time. China today is similarly converging with the global economy, and many experts believe China needs at least 8% annual growth to sustain social stability. Realistic growth predictions for 2009 are closer to 5%. Veteran China hands were watching closely when millions of migrant workers returned to work after the Lunar New Year holiday last month to find factories closed and jobs gone. There were pockets of protests, but nationwide unrest seems unlikely this year, and Chinese leaders are working around the clock to ensure that it does not happen next year either. However, the economic slowdown has only just begun and nobody is certain how it will impact the social contract in China between the ruling communist party and the 1.3 billion Chinese who have come to see President Hu Jintao's call for "harmonious society" as inextricably linked to his promise of "peaceful development". If the Japanese example is any precedent, a sustained **economic slowdown has the potential to open a dangerous path from economic nationalism to strategic revisionism in China too**. Dangerous states It is noteworthy that **North Korea, Myanmar and Iran have all intensified their defiance in the wake of the financial crisis, which has distracted the world's leading nations, limited their moral authority and sown potential discord.**