# Todo

Dulles aff: Norms

Dulles Neg:

Cant locate res es[c](https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/11/26/the-cybersecurity-202-u-s-officials-fret-about-hacking-by-a-new-generation-of-nations/5ddc808588e0fa652bbbda37/)

Sanctions not deter

T- <https://www.justsecurity.org/64875/u-s-offensive-cyber-operations-against-economic-cyber-intrusions-an-international-law-analysis-part-i/>

GBX Stuff

EMP

IP theft but better

Every hocka prepout

OVWs

~~Reverse engineering~~

China

Russia

~~Iran~~

~~ISIS~~

NK

~~Iran aff - stop proli~~f

CP

OCO is alt to traditional

~~Saudi PS def~~

~~Strait of hormuz~~

**Alliances**

 Aff - be norm setting?

 Neg - don’t piss off enemies?

Virus Plague

Docs to cut

[~~AT: Trump/Saudi attacks iran~~](https://docs.google.com/document/d/1rkeDKTka-jJbnF9389soOIchZtaxv-ujiO492sqGKCA/edit)

[~~AT: Businesses being hacked~~](https://docs.google.com/document/d/1BHfLILbSlVzdB2pxat1TJBlYSQpchLU4iS8_G1SVhoU/edit)

[~~AT: ISIS~~](https://docs.google.com/document/d/1xQepFmi9pNv-2yQSgOZxrSc7hMOqa5vtfhBhx3h_u58/edit#heading=h.y6xrxy92cmib)

[~~AT: Iran (extra)~~](https://docs.google.com/document/d/1S1AJb4nIpnQUViouCe__UwGbHwJ5Z3wT4Is6dA_0an8/edit#heading=h.2u4ipry7xpq0)

[~~AT: China Neg~~](https://docs.google.com/document/d/1JfbL6hKgHDg-Ww8FE5bfZvKYOr-3tD11jIhfDGGX8D0/edit)

[**AT: Child Porn/Dark Web**](https://docs.google.com/document/d/1abwronEkKvAQPgjN_9kcARDqV2ZqoTE2HlO_QRt4GdU/edit#heading=h.s498pza9sjtx)

[~~Westwood KS Aff Brandon~~](https://docs.google.com/document/d/1u72QTLJ7skhU84Zr35LtgwAsBQ4YzfTZN3UO95NTNyA/edit)

[~~westwood KS aff~~](https://docs.google.com/document/d/1VEkihprUvcSTi7LUp1j_OZUl06qTg5xOAHSxSQhBfq0/edit)

[~~Westwood FG AFF~~](https://docs.google.com/document/d/1ZN42Eriw_aSQwqF2qZ8WXbCGYoHDQMSAd3CF0OXvdo0/edit)

[~~New Coppell BC Aff~~](https://docs.google.com/document/d/19NnCDT2CQtRhIWFhh-0ynfdiJPwLJWmbNOwphB3if7A/edit)

[~~coppell bc neg~~](https://docs.google.com/document/d/1Hvo2PLxsHMmRJyweHMBmjlXdVZPb1RLxWMOFHyLu5a8/edit)

[~~Colley LW AFF~~](https://docs.google.com/document/d/1Ryx1ipCbmeM-9PH8sRUPScAeCDa3SIPW2C6q8nD6H1s/edit)

[~~AT:Colleyville LS~~](https://docs.google.com/document/d/1oZhXum6s2yyCF0nzrJ1RFsk-d4RE3_MfK9kAk29IKT0/edit)

[~~A2:Westwood FG Neg~~](https://docs.google.com/document/d/151HejnTxexTwpCoz34RN6s6JQBfPY-CRDHNG75316oE/edit#heading=h.rssy6jfmehmp)

[~~A2 Colley LW Af~~f](https://docs.google.com/document/d/1BWwKDZLiqq5KSlMy9Xb-93PKFJ7h9lYoC9TdRtXNAeA/edit)

# A2: NEG

## A2: Norm setting global alliances

<https://www.wired.com/story/paris-call-cybersecurity-united-states-microsoft/>

During a speech at the annual UNESCO Internet Governance Forum in Paris Monday, French President Emmanuel Macron announced the “**Paris Call for Trust and Security in Cyberspace,” a new initiative designed to establish international norms for the internet, including good digital hygiene and the coordinated disclosure of technical vulnerabilities.** The document outlines nine goals, like helping to ensure foreign actors don’t interfere with elections and working to prevent private companies from “hacking back,” or retaliating for a cybercrime. **It’s endorsed by more than 50 nations, 90 nonprofits and universities, and 130 private corporations and groups. The United States is not one of them.**

[Hoojidonk](https://richardvanhooijdonk.com/blog/en/the-future-of-war-will-be-digital/) 19:

**As the world’s governments become increasingly aware of the dangers posed by cyber-attacks, they’re stepping up their efforts to improve their cyber capabilities**, not only to defend themselves from such attacks, but also to use them against their enemies if necessary. **In fact, many countries now consider cyber capabilities as an essential part of their operational military capability and their strategic toolbox.** In a joint statement, US intelligence chiefs recently revealed that more than 30 countries of the world, including Russia, China, Iran, and North Korea, are currently building offensive cyber-attack capabilities. The US government aims to spend $15 billion on cybersecurity in 2019, which serves to illustrate just how seriously they take this threat. Similarly, the UK government revealed plans to invest $2.5 billion in cybersecurity as a part of its National Cyber Security Strategy 2016-2021.

[Carroll Independent 19](https://www.independent.co.uk/news/world/europe/us-cyber-attack-russia-power-grid-war-kremlin-a8964506.html)June 2019

**Cyber tensions between Russia and the West are not new. The first act of cyberwar assigned to Russia can be traced back to at least 2007,** whena decision by Estonian authorities to move a Soviet war memorial provoked weeks of DDOS attacks.Then, Estonian banks, governmental bodies and the media were all targeted. The systems weren’t penetrated, but authorities were forced to disengage from the external internet to free traffic. For several days, those accessing the Estonian web from outside received 404 messages. Russia’s guilt was never conclusively proven but Toomas Hendrik Ilves, President of Estonia at the time, was far from the only one to put the blame at the Kremlin’s door. The incident was “a massive annoyance” rather than an emergency, he told The Independent. But the lack of an international response laid the foundations for more serious operations later. **These operations, it is alleged, included hacking power grids in Ukraine from 2015 onwards**, attempts to infiltrate US civilian infrastructure and the operation to disrupt the 2016 US presidential elections.Under pressure to take action in response to these alleged attacks, in 2017 Barack Obamamade an unusual move by of announcing he had ordered retaliatory cyber operations against Russia. The operations were part of a broaderset of measures that included diplomatic expulsions, he said, but the cyber part would be kept secret.By that point, US active capability in cyber was already well-known —as early as 2009 it successfully planted malware into Iranian nuclear centrifuges,described as by a former CIA director as a game-changer equivalent to Hiroshima —but never before had the cyber capacity been so openly publicised. It is unclear to what extent these retaliatory operations were ever completed, or how the power grid operation described by the newspaper on Saturday offered any new intelligence capacity. **As the New York Times article admitted, power grids have been "low-intensity battleground for years."**

[Valeriano and Jensen 2019](https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint)(DS)

In moving to the new framework, the Trump administration appears to be changing the rules of the game in cyberspace. North Korea, Iran, **Russia**, and China have **[has] long been exploiting the digital connectivity of our world for covert operations to gain a position of advantage. They have exhibited less restraint or concern for the consequences of militarizing cyberspace than the United States. Yet, what the cyber hegemon (the United States) does defines the character of cyber operations much more than these secondary actors.21 Despite increasingly sophisticated operations**, between 2000 and 2016 cyberspace was a domain defined by political warfare and covert signaling to control escalation more than it was an arena of decisive action.22 **Taking a more offensive posture and preempting threats at their source**, an action implied by the Cyber Command Vision Statement, **has the potential to change the character of cyber operations, and through it, 21st-century great-power competition**.

## A2: Reverse Engineering

1. [Ranum 4-17-17] Code obfuscation is used to mask to the code and make it difficult, if not impossible, to reverse engineer and figure out what the code is actually doing. The NSA’s obfuscation is particularly good since they can afford the best experts. Obfuscation happens in 3 ways
	1. Encryption: [Wired 2-2015] New encryption trick for software makes reverse engineering basically impossible
	2. Kernel Rootkits: [Nachreiner 8/30/2017] Malware can get into the highest level part of the computer that controls all user interactions, allowing it to hide itself from people searching for it
	3. DLL Injection: [Nachreiner 8/30/2017] Hacks can pretend to be a different, normal process (like Notepad), masking activity and traffic from victims.
	4. Because of this, [Patel GIT 2/2010] Code Obfuscation effectively prevents reverse-engineering attacks and other similar attacks.
2. [Varmazis 4-19-18] NSA hasn’t been hit by a major/technical cyberattack in 2 years - enemies prefer using simpler hacking methods like taking advantage of human error bc its easier and cheaper

**A2: stuxnet**

1. [Szoldra and Leydan 12] In 2006, Bush wanted to deter Iran prolif but the only option was military strikes since diplo/sanctions were expected to fail - Stuxnet gave an alt mechanism to checkback Iran, prevent war
2. [Hackett Fortune 8-16] Cyberattacks are masked as general network traffic - if people don't know where or how they’re being attack, you cant reverse engineer it

<https://www.theregister.co.uk/2012/06/01/stuxnet_joint_us_israeli_op/>

By John Leyden 1 Jun 2012

The NYT teaser piece reports that Operation Olympic Games was devised as a means to throw sand in the works of Iran's

controversial nuclear program. **It was initially embarked upon in 2006 without much enthusiasm, as a preferable alternative to withdrawing objections against an Israeli air strike against Iran's nuclear facilities. There was little faith that either diplomacy or tougher economic sanction would work,** especially since the international community might be expected to regard warning about another country developing weapons of mass destruction with extreme scepticism after the Iraq War debacle.

<https://www.businessinsider.com/zero-days-stuxnet-cyber-weapon-2016-7>

Paul Szoldra Jul 7, 2016,

In 2006, then-President George W. Bush was increasingly worried about Iranian efforts at enriching uranium, and ultimately, its hopes to build an atomic bomb.

But he was mired in the Iraq war, and **had few options beyond air strikes or another full-scale war in the Middle East, which Israel was pushing for. So, his military leaders gave him a third option: a weapon that could potentially set back Iran's nuclear ambitions, while leaving no trace of the attacker.**

Sellin, Lawrence. “The US is unprepared for space cyberwarfare” Military Times. September 4, 2019 <https://www.militarytimes.com/opinion/commentary/2019/09/04/the-us-is-unprepared-for-space-cyberwarfare/>

In 2016, China delivered a second “Sputnik” shock to the U.S. when it launched the world’s first quantum communications-enabled satellite. Nowhere is the cyberthreat more urgent than in the code-cracking ability of quantum computing for everything from routine public key e-commerce transactions to the most sophisticated American terrestrial, maritime and space-based defense encryption systems. China is building the world’s largest and most advanced quantum research facility to develop “revolutionary” forms of technology that can be used by the military for cryptology, stealthy submarine navigation and “unhackable” quantum communication systems. **America’s answer to China’s quantum computing threat resides in lattice-based cryptography, which can provide algorithms that are secure from quantum-computing attacks. It is also the only post-quantum encryption option that is also fully homomorphic; that is, allowing computation on encrypted data without ever exposing that data. That feature is especially important when large data sets are involved, such as efforts to advance machine learning and artificial intelligence**. In 2018, the Pentagon elevated United States Cyber Command to the status of a full and independent unified combatant command, recognizing that cyberwarfare constitutes a unique theater of combat. Last week, President Donald Trump launched U.S. Space Command, acknowledging the importance and the centrality of space communications and infrastructure to America’s security and defense. It will be the responsibility of Congress to bridge the technological investment gap, while United States Cyber Command, U.S. Space Command and an engaged commercial sector must integrate space-cyber defense activities to meet the challenges posed by America’s 21st century technological adversaries.

Patel GIT

<https://www.researchgate.net/publication/269694315_A_WAY_TO_PROTECT_SOFTWARE_SECRETS_FROM_REVERSE_ENGINEERING_USING_CODE_OBFUSCATION_TECHNIQUES?enrichId=rgreq-0fbe74cc0f12e8182ef5143d6687f496-XXX&enrichSource=Y292ZXJQYWdlOzI2OTY5NDMxNTtBUzoxNzYzNTI0MDE1Njc3NDRAMTQxOTA1NzA5NzA0OA%3D%3D&el=1_x_3&_esc=publicationCoverPdf>

Obfuscation

As the Internet evolves rapidly, software piracy is rampant in the world; as a result, software protection becomes a vital issue in current computer industry and a hot research topic [1], [2], [3]. Software piracy has been causing enormous losses for software vendors [4]. Given enough time and resources, even a protected program can eventually be reverse-engineered. As a result, having gained physical access to the application, the reverse engineer can decompile it (using disassemblers / decompilers) and then analyze its data structures and control flow. This can either be done manually or with the aid of reverse engineering tools. For example, commercial software frequently includes a license verification that an illegal user of the software may wish to circumvent. The user may attempt to alter the program’s code to remove or bypass the license check [5]. To discourage reverse-engineering, developers use a variety of static software protections to obfuscate programs [6]. Three techniques have been used for software copyright protection [4], [7]: code obfuscation, software watermarking and code tamper-proofing. Code obfuscation is the process of transforming byte code to a less human-readable format; making it hard to be decompiled or analyzed even it is decompiled. It includes stripping all unnecessary information, such as line numbers, local variable names and source file names used by debuggers from the classes, and renaming classes, interfaces, fields and method identifiers to make them meaningless. Software watermarking is to embed watermarks into an executable program and these watermarks can be retrieved at a later stage by inputting a predefined key. Tamper-proofing mechanism puts a guard in the software to check authorization and to prevent the program from operating properly if a change is made to it. Software protection is a promising technology to cope with malicious or illegal access to mission critical servers. Besides attestation, code obfuscation and encryption are important techniques for trusted computing [8]. **Code obfuscation has been proposed as the solution to problems such as protection of transient secrets in programs, protection of algorithms, license management for software, protection of digital watermarks in programs, software-based tamper resistance, and protection of mobile agents [9], [10]. This effectively prevents reverse-engineering attacks and other similar attacks.**

 Marcus Ranum April 17, 2017 (literally a netsec god)

Marcus J. Ranum is a world-renowned expert on security system design and implementation. He is recognized as an early innovator in firewall technology, and the implementer of the first commercial firewall product. Since the late 1980's, he has designed a number of groundbreaking security products including the DEC SEAL, the TIS firewall toolkit, the Gauntlet firewall, and NFR's Network Flight Recorder intrusion detection system. He has been involved in every level of operations of a security product business, from developer, to founder and CEO of NFR. Marcus has served as a consultant to many FORTUNE 500 firms and national governments, as well as serving as a guest lecturer and instructor at numerous high-tech conferences. In 2001, he was awarded the TISC “Clue” award for service to the security community, and the ISSA Lifetime Achievement Award. Marcus is Chief Of Security for Tenable Network Security, where he is responsible for research in open source logging tools and product training. He serves as a technology advisor to a number of start-ups, established concerns, and venture capital groups.

<https://freethoughtblogs.com/stderr/2017/04/17/stories-about-code-obfuscation/>

**There are oodles of tools like this out there for a variety of programming languages, especially the scripted languages, where someone might want to obscure the purpose of their code.**

**And, if you’re an intelligence agency like NSA or CIA you’re going to want your own, too. The NSA’s obfuscation is particularly good (because they can afford the very best!)**  [ixia] But, like the “Romanian” hacker we dealt with in 2007, nobody with any understanding of the tools that are available is going to assume that Romanian variable names means the hacker is Romanian. It’s particularly interesting when you see something like Kaspersky’s report on NSA/”Equation Group” malware,[kaspersky] which appears to use the same obfuscation techniques as other pieces of NSA code. The obvious conclusion is that outgoing code is ‘sanitized’ with some kind of tool that automatically does certain obscuring transformations. **The intent is not to hide the fact that it’s malware. It’s not to hide what the malware does. It’s to make it harder to figure out what the malware does, and it’s also to make it harder to figure out who wrote the malware.** Imagine if Programmer Jane tends to use a particular indentation style and variable naming: if you can identify ‘signatures’ in Programmer Jane’s code, you might be able to search online for other code with the same techniques – it’s basically the same idea as identifying whether Bacon wrote Shakespeare through word frequency ‘signature’ comparison. The government agencies that are developing malware are absolutely aware of those techniques, because they invented them.

<https://blog.cryptographyengineering.com/2014/02/21/cryptographic-obfuscation-and/>

The Wired article deals with the subject of ‘program obfuscation‘, which is a term that software developers and cryptographers have long been interested in. T**he motivation here is pretty simple: find a way that we can give people programs they can run — without letting them figure out how the programs work.**

**In real world software systems, ‘obfuscation’ usually refers to a collection of ad-hoc techniques that turn nice, sensible programs into a morass of GOTOs and spaghetti code. Sometimes important constants are chopped up and distributed around the code. Some portions of the code may even be encrypted — though only temporarily, since decryption keys must ship with the program so it can actually be run. Malware authors and DRM folks love this kind of obfuscation.**

<https://www.darkreading.com/attacks-breaches/how-hackers-hide-their-malware-advanced-obfuscation/a/d-id/1329723>

Corey Nachreiner, 8/30/2017

Recognized as a thought leader in IT security, Nachreiner spearheads WatchGuard's technology vision and direction. Previously, he was the director of strategy and research at WatchGuard. Nachreiner has operated at the frontline of cyber security for 16 years, and for nearly a decade has been evaluating and making accurate predictions about information security trends. As an authority on network security and internationally quoted commentator, Nachreiner's expertise and ability to dissect complex security topics make him a sought-after speaker at forums such as Gartner, Infosec and RSA. He is also a regular contributor to leading publications including CNET, Dark Reading, eWeek, Help Net Security, Information Week and Infosecurity, and delivers WatchGuard's "Daily Security Byte" video on Facebook.

**How Hackers Hide Their Malware: Advanced Obfuscation**

Hackers use some basic techniques to hide their malware from antivirus (AV) software (See the first part of this two-part post). But here I'll explain **the more advanced obfuscation methods and showcase new tactics and technologies you can use to detect evasive malware.**

At the highest level, **rootkits are a combination of tools or techniques that allow malware to burrow into a system and hide from your operating system.** Computer processors have various privilege levels of execution (ring 0-3), and attackers can exploit these levels of privilege to trick programs that run at higher levels. For instance, operating systems like Windows and Linux have user space and kernel space**. At the highest level, you just need to know the kernel space (ring0) has higher privileges than user space (ring3)**. If you had a program that needed to list the files in a directory, you could call a user space function to do it, but you could also call a kernel function to do it.

**If a malicious program can get kernel privileges, it can actually "lie" to programs that run in user space**. So if you have a program using a user space function call to scan a file system, **a kernel rootkit can trick that program when it parses files. When the user space function gets to malicious file, the rootkit can say, "These are not the files you are looking for" or, more specifically, simply pass over those files and not return them as results to the user space program.** To make matters worse, virtualization adds a new layer to rootkit tricks because its hypervisor runs below (with higher privileges than) the kernel.

In short, malware can sometimes use rootkit functionality to hide from local AV, by hiding files, network connections, or other things from the operating system itself. That said, most AV now runs with its own kernel-mode driver and protections to avoid common rootkit tricks.

3. Code, Process, and DLL Injection

Process or **dynamic-link library (DLL) injection** represents**a variety of techniques a program can use to run code under the context of another process**. Malware authors often leverage these techniques to get their malware code to run through a necessary and required Windows process. For instance, they might inject explorer.exe, svchost.exe, notepad.exe, or another legitimate Windows executable. By picking a process Windows requires, the malware can make itself more difficult for AV software to find and kill. **Malware can also hook processes with known network capabilities to help mask any malicious traffic.** Over time, Microsoft has patched many of the process or code injection techniques criminals have exploited**, but researchers and attackers constantly find new techniques, such as the recently discovered AtomBombing.**

[Greenberg Wired](https://www.wired.com/2015/02/crypto-trick-makes-software-nearly-impossible-reverse-engineer/)

SOFTWARE REVERSE ENGINEERING, the art of pulling programs apart to figure out how they work, is what makes it possible for sophisticated hackers to scour code for exploitable bugs. It's also what allows those same hackers' dangerous malware to be deconstructed and neutered. **Now a new encryption trick could make both those tasks much, much harder.**

At the SyScan conference next month in Singapore, security researcher **Jacob Torrey plans to present a new scheme he calls Hardened Anti-Reverse Engineering System, or HARES. Torrey's method encrypts software code such that it's only decrypted by the computer's processor at the last possible moment before the code is executed. This prevents reverse engineering tools from reading the decrypted code as it's being run. The result is tough-to-crack protection** from any hacker who would pirate the software, suss out security flaws that could compromise users, and even in some cases understand its basic functions.

"This makes an application completely opaque," says Torrey, who works as a researcher for the New York State-based security firm Assured Information Security. "**It protects software algorithms from reverse engineering, and it prevents software from being mined for vulnerabilities that can be turned into exploits."**

##### **We can hide our tracks so nobody finds out we attacked them in the first place**

<https://fortune.com/2016/08/12/how-hackers-hide-tracks-cyberattacks/>

Hackett

The vast majority of cyberattacks use spoofed email messages or bogus websites to try to dupe unsuspecting employees into downloading malicious software or giving up login credentials. Such ploys are designed to trick their victims—but they don’t go very far when the booby-trapped messages arrive from addresses handled by known bad actors. That tends to raise an alarm.

**So the attackers disguise themselves, burrowing into seemingly innocuous networks. Computer security experts call this approach a “stepping stone attack,” given all the intermediary hops involved.**

**“They want to have a mechanism to hide their activity, and to make their attacks and traffic blend with general network behavior,” Falkowitz, an NSA alum, says.**

<https://www.publictechnology.net/articles/features/nsa-%E2%80%98we-have-not-responded-zero-day-two-years-%E2%80%93-our-adversaries-are-hitting-known>

13 April 2018 Sam Trendall

**The US National Security Agency has revealed that its cybersecurity unit has not had to deal with a zero-day cyberattack in two years, as adversarial states have been able to exploit bad practice and human error to cause harm.**

<https://nakedsecurity.sophos.com/2018/04/19/nsa-reveals-how-it-beats-0-days/>

Varmazis

This discipline has paid off for the **NSA**, as [Hogue says](https://twitter.com/RSAConference/status/986356214014492673) they **have not had any intrusions via a 0-day exploit in the last 24 months.** So, while the bad news may be that attackers are moving faster than ever – or at least the ones targeting the NSA are – **the good news is that attackers mostly still rely on their old tricks, simply because they’re easier to deploy and usually work.**

## A2: Tradeoff

1. What the heck how does that even make sense
2. [Lyngaas 2-16] When the DOD wants more offensive cyber operations they request more money from the federal gov, its not a rebalancing act - look to 2017 budget.
3. [Humayed 1-17 arxiv] Practically impossible for systems to have 0 vulnerabilities - purely defensive never perfect, hacks on healthcare devices, power grids, etc. can still happen

<https://outline.com/6BdHFF>

Humayed 1-17-17

<https://arxiv.org/pdf/1701.04525.pdf>

**In recent years, we have witnessed an exponential growth in the development and deployment of various types of Cyber-Physical Systems (CPS). They have brought impacts to almost all aspects of our daily life, for instance, in electrical power grids, oil and natural gas distribution, transportation systems, health-care devices, household appliances, and many more. Many of such systems are deployed in the critical infrastructure, life support devices, or are essential to our daily lives. Therefore, they are expected to be free of vulnerabilities and immune to all types of attacks, which, unfortunately, is practically impossible for all real-world systems.**

[Lyngaas FCW 2-2-16](https://fcw.com/articles/2016/02/02/dod-budget-cyber.aspx) (MM)

**Leaders of the U.S. Department of Defense (DOD) plan to increase spending for cyber security and cyber warfare operations next year by 15 percent -- or nearly a billion dollars** -- over current-year levels, according to Pentagon budget documents.

The fiscal 2017 DOD budget calls for spending $6.7 billion for cyber operations, which represents an increase of about $900 million over fiscal 2016 enacted levels **for the Pentagon's defensive and offensive cyberspace operations capabilities and cyber strategy,** according to the 2017 Defense Budget Overview. The DOD submitted its 2017 budget request earlier this month.

## A2: Iran angry

1. [Kennedy Natl Interest 10-19] No escalation: Iran cyber retal so far has been calculated to make sure it doesn’t go too far
	1. Iran understands that attacking major targets in U.S. would be escalatory, is avoiding doing that
	2. Understands that attacks on power grids and pipelines is too far - no meaningful harm manifests
2. [Barnes NYT 8-19] U.S. cyberattacks stop Iran aggression in Persian Gulf (war outweighs)
	1. U.S. cyberops calculated to create policy change without encouraging escalation
	2. Iran hasn’t escalated in response to those ops, gray zone clearly working
3. Cyber Warfare causes kinetic response - us conventional military always prevents
4. [Horowitz wpo 19] iran no war:
	1. Econ harms + human harms = political backlash and maybe change
	2. Iran parli elections coming up
	3. Iran cares about regime survival
5. [Hannah 5-19 FoPo] Iran has no interest in getting into a conflict - regime survival first
6. US never mili strike
	1. [Meierding FP 9-18-19] Strikes on iran raise oil prices, undermine Trump's election chances
	2. [Pollack 5-19] Trump goal is to end American wars in the Middle East - thats why he pulled troops from Syria
	3. [Ioanes Business Insider 6-19] Trump uncomfortable with mili escalation (literally ran on anti-intervention policies), the dialogue is just empty rhetoric - twitter diplo

<https://foreignpolicy.com/2019/05/31/iran-might-not-be-able-to-wait-trump-out/>

JOHN HANNAH | MAY 31, 2019

The risks of a broader conflagration must of course be taken seriously and guarded against. But it should be said that war is far from inevitable should the United States need to respond militarily to Iranian provocations. Israel has attacked hundreds of Iranian targets in Syria over the past two years, probably killing scores of Iranian troops in the process—all without triggering a wider war. **It’s clear that Iran’s regime has no interest in getting into a major conflict** with Israel, much less **with the United States**, which has the most powerful military in the world. **Should a conventional conflict start, the U.S. ability to retaliate would be overwhelming. Iran’s leaders know it and almost certainly want no part of it.** Trump’s jarring tweet that war would be “the official end of Iran” may have been inartfully crafted, but the basic equation it put forward—that such a conflict would inflict infinitely higher risks and costs on the stability and security of **Iran than of the United States—is surely not lost on those responsible for the Iranian regime’s survival.**

**Horowitz and Saunders 19** (Michael C. Horowitz (1) and Elizabeth N. Saunders (2) – (1) Professor of political science and the associate director of Perry World House at the University of Pennsylvania – (2) Associate professor in the School of Foreign Service at Georgetown University, and a nonresident senior fellow at the Brookings Institution – “War with Iran is probably less likely than you think” – The Washington Post – 6/17/19 - https://www.washingtonpost.com/politics/2019/06/17/war-with-iran-is-probably-less-likely-than-you-think///Gavsie)

Why war with Iran might be less likely than you think. Last week, an attack on two tankers in the Gulf of Oman raised tensions between the United States and Iran — on the heels of a similar attack in May. Though Iran denied responsibility, Secretary of State Mike Pompeo said intelligence evidence showed Iran was to blame, and President Trump concurred that “Iran did do it.” Although questions remain in some quarters about the attack’s nature and source, on Sunday on CBS’s “Face the Nation,” Rep. Adam Schiff (D-Calif.) said the evidence Iran was responsible is “very strong and compelling.” As was true when the United States and North Korea exchanged bellicose rhetoric in 2017 and early 2018, many are now worried that the U.S. and Iran are heading for war. When Trump was warning that North Korea faced “fire and fury” if it threatened the United States, we wrote about why, despite the rhetoric, war was unlikely. This time, some factors are indeed pushing the two sides toward conflict. But forces of restraint are also reducing the likelihood of war. Tensions can lead to a “spiral” of escalation. Both the United States and Iran say that they do not want a war, but that they are prepared to fight if the other side starts one. What’s worrisome is what political scientists call the spiral model of conflict escalation. Sometimes, when countries take measures they think will improve their own security, potential opponents can perceive that as threatening — a classic security dilemma. Those potential opponents then take measures to improve their own security — which the first country sees as threatening. And so on. When countries do not trust each other, and perhaps even fear that the other side wants war, they are unlikely to believe conciliatory signals from the other side, and nobody wants to appear weak. The result is a spiral of conflict. The past few weeks’ events have certainly ratcheted up tensions. The recent tanker attack and America’s decision to quickly blame Iran only raises them further. And as Tyler Jost and Rob Schub wrote here at TMC last month, the Trump administration’s decision-making process could make it even more difficult to navigate the tricky problem of reading and responding to signals in a crisis like this. War would be very costly in this case. A conflict between Iran and the United States could be very costly. For instance, in such a war, Iran might use mines to keep ships from traveling through traffic in the Strait of Hormuz — a crucial, narrow passage for world energy supplies. If that happened, the U.S. options for clearing the mines would be complicated and costly, as Caitlin Talmadge argues. Such an operation might require hitting targets inside Iran or risk Iranian retaliation from coastal positions given the narrow geographic chokepoint — all pointing toward further escalation. Knowing this, the United States might instead choose to go straight to a bombing campaign. But coercive bombing might also lead to escalation. Despite these dangers, there are still important constraints on both sides. Misperception rarely causes war. The spiral model may not be the right way to think about how conflicts escalate. Missed signals and miscalculation can indeed generate tension. But leaders have many ways to avoid conflicts that they do not want to fight. The historical record suggests that misperception and accidental escalation rarely lead to war — as Dan Reiter noted here at TMC during the height of North Korea tensions in 2018. Domestic political pressures don’t seem to be pushing toward war. The United States and Iran also face domestic pressures that may make both sides hesitate before escalating. Iran’s economy has suffered under the Trump administration’s renewed sanctions, and parliamentary elections are coming up. Although the country’s president, Hassan Rouhani, has used tough rhetoric recently, **a costly war might not benefit Iran’s leaders, since it could inflict further economic and human costs, or even lead to regime change or collapse.** Likewise, after nearly two decades of war in the Middle East and Afghanistan, Americans are unlikely to welcome another major conflict. Neither Trump’s own party nor the opposition Democrats has rallied the U.S. public to pressure Trump to escalate. As TMC’s Michael Tesler noted in December, although Trump’s base supporters tend to have hawkish views, they supported his decision to withdraw troops from Syria. If Trump does not want war with Iran, his base would likely follow. The president doesn’t seem eager for war. There has been much talk about a replay of the Iraq War, with the United States using possibly flawed intelligence to justify war. But although Trump has used limited military force in Syria, he seems generally opposed to costly wars in the Middle East, and unlikely to embrace a new one. Both Pompeo and national security adviser John Bolton are much more hawkish on Iran, but Trump has distanced himself from his advisers’ hawkish rhetoric, particularly the most costly option: regime change. [Designating an Iranian military unit a terrorist organization will make relations with Iran more difficult. Here's how.] Here’s what to watch for. So which will win out: the risks of escalation or the pressures for restraint? Amid all the tension, Iran wants its regime to survive, and Trump probably does not want to absorb a costly war. In the coming days and weeks, it will be telling to see if there is further daylight between Trump and his advisers. Here’s one more risk: if Trump’s hawkish advisers present an option that seems like it could be kept limited, but actually carries a strong likelihood of escalation. Trump has embraced limited displays of force, such as airstrikes in Syria in 2017 and 2018, and he issued a threatening tweet on Iran in May. But he has also pivoted away quickly from harsh rhetoric to diplomacy before — as he did toward North Korea — and has already achieved his campaign goal of pulling out of the nuclear deal he disdained. [Would Iran welcome a new nuclear deal? Think again.] The bottom line: Despite rising tension, powerful factors reduce the likelihood of war between the U.S. and Iran. That’s [is] unlikely to change anytime soon.

Amid all the tension, **Iran wants its regime to survive,** and Trump probably does not want to absorb a costly war. In the coming days and weeks, it will be telling to see if there is further daylight between Trump and his advisers.

[Barnes](https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html)  NYT 8-28-19

WASHINGTON — **A secret cyberattack against Iran in June wiped out a critical database used by Iran’s paramilitary arm to plot attacks against oil tankers and degraded Tehran’s ability to covertly target shipping traffic in the Persian Gulf**, at least temporarily, according to senior American officials. Iran is still trying to recover information destroyed in the June 20 attack and restart some of the computer systems — including military communications networks — taken offline, the officials said. Senior officials discussed the results of the strike in part to quell doubts within the Trump administration about whether the benefits of the operation outweighed the cost — lost intelligence and lost access to a critical network used by the Islamic Revolutionary Guards Corps, Iran’s paramilitary forces. **The United States and Iran have long been involved in an undeclared cyberconflict, one carefully calibrated to remain in the gray zone between war and peace.** The June 20 strike was a critical attack in that ongoing battle, officials said, and it went forward even after President Trump called off a retaliatory airstrike that day after Iran shot down an American drone. **Iran has not escalated its attacks in response, continuing its cyberoperations against the United States government and American corporations at a steady rate**, according to American government officials**. American cyberoperations are designed to change Iran’s behavior without initiating a broader conflict or prompting retaliation,** said Norman Roule, a former senior intelligence official. Because they are rarely acknowledged publicly, cyberstrikes are much like covert operations, he said.

[Lewis 6-25-19 CSIS](https://www.csis.org/analysis/iran-and-cyber-power)

How likely is an attack against the United States? A decision for a cyberattack on the United States will depend on Iranian calculations of the risk of a damaging U.S. response. **While the Iranians may appear hotheaded, they are shrewd and calculating in covert action and will consider how to punish the United States without triggering a violent response.** If we look at Iranian cyber actions against U.S. targets—the actions against major banks or the more damaging attack on the Sands Casino—**Iranian attacks are likely to be retaliatory, intending to make the point that the United States is not invulnerable but without going too far. Attacking major targets in the American homeland would be escalatory, something Iran wishes to avoid**. It wants to push back on U.S. presence in the region and demonstrate, to both its own citizens and its Gulf neighbors, that the United States can be challenged. If Iran does act in the United States, crippling a casino makes a point. **Blacking out the power grid or destroying a pipeline risks crossing the line.**

## A2: Russia angry

1. [Jensen CATO 1-19] Russia seeking cyberattack/espionage in squo, they always have an incentive to do if unchecked. OCO preempt attacks at the source and give the U.S. the upper hand
	1. the aff is the only side with any chance of solvency
	2. [Carrol Independent 6-19] US/Russia cyber tensions/attack started in 2007 - impacts should have manifested
2. [Blank Carnegie Endowment Nov 2017] Russia believes it is in a permanent state of cyberwar due to suspicions of global enemies wanting to undermine its interests - funding and incentive to dev weps always exists

[Carroll Independent 19](https://www.independent.co.uk/news/world/europe/us-cyber-attack-russia-power-grid-war-kremlin-a8964506.html)June 2019

**Cyber tensions between Russia and the West are not new. The first act of cyberwar assigned to Russia can be traced back to at least 2007,** whena decision by Estonian authorities to move a Soviet war memorial provoked weeks of DDOS attacks.Then, Estonian banks, governmental bodies and the media were all targeted. The systems weren’t penetrated, but authorities were forced to disengage from the external internet to free traffic. For several days, those accessing the Estonian web from outside received 404 messages. Russia’s guilt was never conclusively proven but Toomas Hendrik Ilves, President of Estonia at the time, was far from the only one to put the blame at the Kremlin’s door. The incident was “a massive annoyance” rather than an emergency, he told The Independent. But the lack of an international response laid the foundations for more serious operations later. **These operations, it is alleged, included hacking power grids in Ukraine from 2015 onwards**, attempts to infiltrate US civilian infrastructure and the operation to disrupt the 2016 US presidential elections.Under pressure to take action in response to these alleged attacks, in 2017 Barack Obamamade an unusual move by of announcing he had ordered retaliatory cyber operations against Russia. The operations were part of a broaderset of measures that included diplomatic expulsions, he said, but the cyber part would be kept secret.By that point, US active capability in cyber was already well-known —as early as 2009 it successfully planted malware into Iranian nuclear centrifuges,described as by a former CIA director as a game-changer equivalent to Hiroshima —but never before had the cyber capacity been so openly publicised. It is unclear to what extent these retaliatory operations were ever completed, or how the power grid operation described by the newspaper on Saturday offered any new intelligence capacity. **As the New York Times article admitted, power grids have been "low-intensity battleground for years."**

[Valeriano and Jensen 2019](https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint)(DS)

In moving to the new framework, the Trump administration appears to be changing the rules of the game in cyberspace. North Korea, Iran, **Russia**, and China have **[has] long been exploiting the digital connectivity of our world for covert operations to gain a position of advantage. They have exhibited less restraint or concern for the consequences of militarizing cyberspace than the United States**. Yet, what the cyber hegemon (the United States) does defines the character of cyber operations much more than these secondary actors.21 Despite increasingly sophisticated operations, between 2000 and 2016 cyberspace was a domain defined by political warfare and covert signaling to control escalation more than it was an arena of decisive action.22 **Taking a more offensive posture and preempting threats at their source**, an action implied by the Cyber Command Vision Statement, **has the potential to change the character of cyber operations, and through it, 21st-century great-power competition**.

[Blank from the Carnegie Endowment Nov 2017](https://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_Ch5.pdf)

**The Russian** deep**state clearly has incorporated cyber strikes and information operations into information warfare,** as it defi nes the term. **IW** assumes growing importance as a war **[is a] winning strategy that avoids attribution, inhibits enemy reactions, and minimizesexpenses—all crucial strategic issues for Russia.**

**“All authoritarian regimes, since they regard opposition as fundamentally illegitimate, tend to see their opponents engaged in subversive conspiracy.** In Russia, there is no hard-and-fast distinction between peace and war as there is in American strategic thinking. The US military has a concept of “phase zero,” or the stage antecedent to war. Rather, **given its perception of permanent** and protracted **conflict**, **Russia is every day preparing for war by deploying all the instruments of state power globally to enhance its security and interests.**Observing the operations of Russian state and associated criminal actors on a day- to- day basis demonstrates that the entire Russian state participates in polit-ical warfare, IW, and actual military operations. Russian official documents on national security since 2009 have all been plans for mobilizing the entire state for conflict.9 If one reads the 2009 document and the 2015 national security strat-egy and tracks behavior of the regime since 2009, then it becomes clear that the entire state is being put on a mobilization footing. Not only do they systemati-cally reinforce the message that Russia is under attack from both US- led IW and military threats but also the regime has allocated massive resources to spend on information operations like Russia Today and “troll factories” in Russia.10 Defense spending and the industry it supports are portrayed as locomotives of economic growth as well as security measures.

## A2: China angry

1. [Buchanan Lawfare 10-18] China cyberattacks are to increase its own power image. Regardless if U.S. cyber if offensive or defensive, China still is incentivised to hack U.S. to disrupt power order: China doesn’t care if U.S. is limiting aggression or not.
2. [Demchak 4-26-19 BAS] China is chasing global dominance in cyber
	1. [SACKS 6-18 Atlantic] Xi’s vision to define global cyber norms - involves giving China access to all the data/tech - meaning that IP theft is literally part of China’s future econ vision - nothing changes tha

[Jinghua 2019](https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734)

The overall defensive perspective of the government is ultimately in line with China’s strategic guidelines and its understanding of the general characteristics of cyber warfare. **China has consistently said that it adheres to the strategic guideline of Active Defense**, as elaborated in the 2015 defense paper. **Guided by these principles, the primary stated goal in cyber warfare is to enhance defense capabilities in order to survive and counter after suffering an offensive cyber strike.**

[Buchanan Lawfare 10-14-18](https://www.lawfareblog.com/deepening-us-china-cybersecurity-dilemma)

**China is also not satisfied with the status quo**, as Lyu’s piece suggests. There can be little doubt that the U.S. intelligence community also hacks Chinese targets for reasons that go beyond defense and disruption. **China likely sees U.S. cyber activities—whether intended to be defensive or offensive—as intrusive and threatening. It may well launch hacking operations to attempt to disrupt American efforts**; despite Lyu’s assertion that China’s concept of “active defense” is a “military strategic guideline … rather than an operational concept,” **we would be surprised if the Chinese government did not pursue efforts that aim to disrupt other nations’ hacking capabilities.**

Indeed, China’s 2015 National Defense White Paper characterizes the PLA’s approach to “active defense” as, among other things, “adherence to the unity of strategic defense and operational and tactical offense.” Given this doctrinal context, **Lyu’s attempt to distinguish “preemption” from “retaliation” fails to recognize the structural blurriness of such distinctions in the cyber domain.** American policymakers are likely to find the distinction meaningless, **just as Chinese policymakers will probably fail to appreciate areas in which the United States thinks it limits its aggressiveness.**

##

## A2: NoKo angry

1. Hacking fails
	1. [Melendez 8-17 Fast Company]
		1. Limited intelligence bc closed off from the rest of the world
		2. North Korea has dozens of missile launch sites (some of them hidden), which means its unlikely for the US to be able to disable every single one of them to prevent launches.
		3. They can literally just work around a lot of the hacks
	2. [Greenberg 10-19 Wired]
		1. Vast majority of infra disconnected - nothing to hack
		2. Missile Systems are likely not connected to the internet/intranet - can’t be hacked
		3. qualifies that because of this, hacking North Korea’s nuclear capabilities would be nearly impossible
	3. [Barnes NYT 6-19] The effects of cyberattacks can be reversed given time/work - NK always restores ability to launch missiles after US OCOs
	4. [Sanger 3-17 NYT] US doesn’t have the ability to effectively counter NK nuke/missile program
2. No reason for the U.S. to attack = no reason for nk to be scared
	1. [Wallcott Time OCt-19] Trump still continuing talks even tho nk increasing dev, no fear
	2. Trump doesn’t want war - anti intervention
	3. Trump doesn't want war - literally an election platform
3. Kim won’t attack
4. [Belfer Center 2017] Kim is rational actor [Bell CBC 16] any aggressive action will lead to its own destruction since [Bando Cato 09] US Naval/Air forces can instantly take it down
5. [Mckinney 38 North 2017] Kim nuke dev is used to compel concession, not attack

[Melendez](https://www.fastcompany.com/40451399/using-cyberattacks-to-stop-north-korean-nukes-not-easy-experts-warn) 8-10-17 Fast Company:

**“North Korea’s very limited exposure to the outside world, particularly by people who have knowledge of their systems, makes it very difficult,” he says**

**“Even gathering the kind of intel you need to do a successful cyberattack is tough, because we don’t know what we don’t know,”** says Steven Bucci, a visiting fellow at the Heritage Foundation who studies cybersecurity issues Would-be digital attackers looking to do significant damage to the North Korean weapons program would also have to strike more sites than the Stuxnet creators, who primarily targeted one enrichment facility in Iran. **Hampering one or two facilities likely wouldn’t be enough to prevent North Korea from launching an attack. “What we see in North Korea is that the program is actually fairly diversified in terms of weaponry that can be launched from different launch sites around the country,**” says Tim Maurer, co-director of the Cyber Policy Initiative at the Carnegie Endowment for International Peace. “All of this make**s the use of offensive cyber operations more difficult to accomplish the military objective.” North Korea might also have the capacity to simply work around parts or software hobbled by malware and hacks**, even if they don’t realize why they’re not working properly, suggests Chris Finan, a White House cybersecurity aide in the Obama administration.

[Greenberg of WIRED in 10-10-2017](https://www.wired.com/story/cyberattack-north-korea-nukes/)

But even that successful RGB strike appears to have been a denial of service attack—in which junk traffic overwhelms a system—rather than a penetrating breach of North Korea's computers. **And the vast majority of North Korea's overall infrastructure still remains disconnected, vastly reducing any footholds for hackers—and making the prospect of compromising its locked-down and air-gapped nuclear weapons systems all the more daunting.**

But North Korea's government is careful not to offer any easy connection to that intranet from the outside world, says Will Scott, a security researcher at the University of Michigan who spent several months-long stints in North Korea teaching at one of its universities. He says he's observed Red Star running on infrastructure ranging from computers at the country's Science and Technology Exhibition Center to the library at Pyongyang's Kim Il Sung University. But he found that organizations in North Korea were always careful to connect computers to either the country's intranet or the internet—never both. **Scott believes the most sensitive targets, like missile systems, likely aren't connected to either the internet or the intranet, and run custom software built by foreign suppliers.**

But **despite the US government's dominating powers in the digital realm**, security experts and former intelligence **officials believe that battlefield favors North Korea**. **US hackers can take** bites out of **the edges of North Korea's infrastructure**. **But** getting to its core—and **anywhere close to disrupting or even delaying its nuclear capabilities—will be extremely difficult,** they say, **if not impossible**.

[Wallcott of Time 19](https://time.com/5692361/trump-north-korea-missile-threat/)

In a briefing on Tuesday Oct. 1, Trump showed no interest when aides detailed North Korea’s new efforts to develop missiles that can be fired from a submarine, two U.S. officials who participated in the White House briefing tell TIME. **Trump decided talks with North Korea should continue despite thoat country’s evident intention to develop the new military capability, the two officials say.**

[Belfer Center 2017](https://www.belfercenter.org/publication/keeping-kim-how-north-koreas-regime-stays-power)

In contrast to **the media, which persist in portraying Kim Jong-il as a madman** or an incompetent playboy, this analysis shows him to be a shrewd, if reprehensible, leader. His meticulous use of the authoritarian toolbox reveals him to be a skilled strategic player. **Kim shows every sign of being rational**—and thus deterrable..

[Bando, Cato Institute 09](http://www.campaignforliberty.org/index.php?view=100)

It is even more obvious that Pyongyang poses no meaningful danger to America. The North has no ability to project military power. If it attempted to do so, **U.S. air and naval power would make quick work of North Korea's forces.**

[Bell, 2016, CBC](http://www.cbc.ca/news/world/north-korea-weapons-explainer-1.3439164)

"What's pretty clear is that they now have a long history of experimenting with both nuclear weapons and ballistic missiles. And so any estimate of this threat is going to depend upon your conclusions about how quickly they're developing these technologies. And the truth is, we just don't know​." Baker doesn't think North Korea poses much direct risk, because **"it's a regime that understands that any truly aggressive action ultimately will lead to its own destruction​."**

[Sharpio, Geopolitical Features, February 2017](https://geopoliticalfutures.com/the-meaninglessness-of-missile-defense-in-south-korea/)

. It is possible that the North Korean leadership is crazy enough to launch such an attack, but it is far more likely that **Pyongyang is using its nuclear program to ensure its survival and** not invite its own annihilation. That involves appearing to be deranged while **possessing enough nuclear capability to frighten its enemies, without actually using it.**

[Foreign Policy](http://foreignpolicy.com/2017/04/26/kim-jong-un-is-a-survivor-not-a-madman/)

“**Kim Jong Un sees the nuclear program as purely defensive.** Conquering the South would be nice in theory, but this task is completely beyond his reach, both due to the U.S. commitment to protecting South Korea and Seoul’s own huge advantage in economic and technological power. **He knows that any** unprovoked **North Korean attack against South Korea** or the United States **will end** badly,perhaps **in his death, and he is certainly not suicidal.** However, he also presumes that no great power would risk attacking a nuclear state or sticking a hand into its internal strife — especially if it has delivery systems and a second-strike capability.”

**Mckinney** [38 North 2017](http://www.38north.org/2017/03/understanding-north-koreas-nuclear-coercion-strategy/)

 Changing the dynamics of security talks. **North Korea sees improvements in its nuclear weapons capability as a way to** shift the format and dynamics of regional security talks in its favor.Instead of five countries arrayed against it in the Six-Party Talks, Pyongyang hopes to leverage its nuclear status to gain a more equal footing with the United States. Further, the North uses its relationships with China and Russia to strengthen its negotiating position vis-à-vis Washington. Finally, and maybe most importantly, acknowledging North Korean membership in the “nuclear club” serves to marginalize the ROK and Japan among 6PT participants. Elevating its status. Possession of nuclear weapons strengthens North Korea’s hand in Northeast Asia and elevates its status in the world as one of a handful of countries that possesses nuclear weapons and ballistic missile capabilities. While many see the North as a rogue nation because it continues to violate UN Security Council resolutions and flouts the Nuclear Nonproliferation Treaty (NPT) in the face of strong opposition from the international community, numerous other states either openly or quietly admire it for such independence. Leveraging greater security and economic benefits*.* Past North Korean brinkmanship has led to offers of engagement and assistance from countries that want to bolster regional stability. **North Korea has seen that its threatening actions can compel concessions from its opponents as well as extract diplomatic and monetary gains. It appears that Kim Jong Un is continuing this pattern of coercive diplomacy.**

## A2: Zero Days/NSA Leaks

<https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong>

1. [Kelly 3-17] 90% of cyber attacks bc of human error

[Ross Kelly - March 3, 2017](https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/)

But all too often CEOs confronted with cyber attacks tend to do the opposite: they fret about possible weaknesses in their technology defenses, rather than taking a hard look at the people in their organization.

**Evidence shows that many cyber attacks**—estimated to cost the average American company more than $15 million per year—**could be prevented with better people-management protocols.**

**Employee negligence or malicious acts accounted for two-thirds of cyber breaches**, according to historical claim data analyzed by London-based consultancy Willis Towers Watson. Just 18% were directly driven by an external threat, and extortion accounted for a measly 2%.

Overall, the research found that about**90% of all cyber claims stemmed from some type of human error or behavior.**

**“The simple truth is that a data compromise is more likely to come from an employee leaving a laptop on the train than from a malicious criminal hack,”** said Anthony Dagostino, the company’s head of global cyber risk.

Addressing the problem could be a simple matter of conducting training sessions that advise employees to use approved software and apply strong passwords—or applying common sense practices around technology access. For example, perhaps it’s not such a great idea to allow staff to take their laptops home on a Friday evening, should they happen to be drop by the local bar to unwind after a hard week’s work.

**Many hacks and extortion attempts occur when criminals impersonate senior executives at a company:** a problem that can be dealt with by instructing staff to reply to senior executives in a fresh email, rather than clicking reply.

<https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF>

In the course of carrying out USG missions, the USG may identify vulnerabilities that cyber actors could exploit. **In the vast majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest.** However, there are legitimate advantages and disadvantages to disclosing vulnerabilities, and the trade-offs between prompt disclosure and withholding knowledge of some vulnerabilities for a limited time or adopting a mitigation strategy short of full disclosure can have significant consequence

It is also important to recognize that the USG has not created these vulnerabilities. Information systems will continue to have vulnerabilities and **efforts to discover and disclose these flaws is an ongoing need.** Contributions by the Intelligence Community (IC) have been significant in securing modern information technology. **If the USG were to adopt a policy of immediate disclosure, there would still be vulnerabilities present that would be discovered and potentially exploited by other cyber actors.** For years,the USG’s process to robustly consider and disclose vulnerabilities was the only such process known amongst both our peers and our adversaries

Vulnerabilities are also used in the course of authorized military, intelligence,and law enforcement activities. At times, **intelligence and evidence discovered through judicious exploitation of a vulnerability are the only means to understand a much bigger threat. Often taking a considered risk to restrict knowledge of a vulnerability is the only way to discover significant intrusions that are compromising security and privacy**

<https://www.fedscoop.com/nsa-no-zero-days-were-used-in-any-high-profile-breaches-over-last-24-months/>

**Over the last 24 months, the National Security Agency has been involved in incident response and mitigation efforts for “all the high profile incidents** you’ve read about in the Washington Post and New York Times,” said Curtis Dukes, deputy national manager of security systems within the NSA.

**The one common characteristic shared between these incidents, said Dukes, was hackers were using relatively simply techniques — like spear phishing, water-holing and USB drive delivery — rather than zero day exploits to launch successful attacks.**

**“In the last 24 months, not one zero day has been used in these high profile intrusions,”** Dukes said Thursday during the Federal Cybersecurity Summit presented by Hewlett Packard Enterprise and produced by FedScoop.

<https://www.wired.com/story/meltdown-spectre-bug-collision-intel-chip-flaw-discovery/>

So when the NSA finds a so-called zero-day vulnerability—a previously unknown hackable flaw in software or hardware—Schneier argues that tendency for rediscovery needs to factor into whether the agency stealthily exploits the bug for espionage, or instead reports it to whatever party can fix it. Schneier argues bug collisions like Spectre and Meltdown mean they should err on the side of disclosure**: According to rough estimates in the Harvard study he co-authored , as many as one third of all zero-days used in a given year may have first been discovered by the NSA.**

## A2: Taiwan sad

1. Incentive to OCO always exists
	1. Part of china grand plan
	2. Russia/Iran and others also

## A2: Climate Satellites

**General**

1. [Sellin 9-4-19] [Their evi] U.S. has developed lattice based cryptography in response to China quantum hacking capabilities, no way to hack now?
2. China always has vested interest in devolping OCO
3. If anyone wanted to do this they wouldve alerady

**China**

1. doesn't want CC
	1. Inkstone/Shanghai rising sea levels threaten it
	2. [Khan MPDI 18]/Enviromental consequences (water shortage, unseasonal monsoons, floods) necessitate global commitment to sustainable enviro
	3. weforum/china mandate only seling green tech abroad
	4. Ballard 19/ 2016->2019, top 20 cities for emissions went 16->4 chinese cities
		1. Also per capita emissions less than U.S
			1. FL: Rising emissions just bc huge population increase
		2. Investment in green tech way higher
		3. Successful implementation of carbon cap policies that encourage companies to go green financially

Sellin, Lawrence. “The US is unprepared for space cyberwarfare” Military Times. September 4, 2019 <https://www.militarytimes.com/opinion/commentary/2019/09/04/the-us-is-unprepared-for-space-cyberwarfare/>

In 2016, China delivered a second “Sputnik” shock to the U.S. when it launched the world’s first quantum communications-enabled satellite. Nowhere is the cyberthreat more urgent than in the code-cracking ability of quantum computing for everything from routine public key e-commerce transactions to the most sophisticated American terrestrial, maritime and space-based defense encryption systems. China is building the world’s largest and most advanced quantum research facility to develop “revolutionary” forms of technology that can be used by the military for cryptology, stealthy submarine navigation and “unhackable” quantum communication systems. **America’s answer to China’s quantum computing threat resides in lattice-based cryptography, which can provide algorithms that are secure from quantum-computing attacks. It is also the only post-quantum encryption option that is also fully homomorphic; that is, allowing computation on encrypted data without ever exposing that data. That feature is especially important when large data sets are involved, such as efforts to advance machine learning and artificial intelligence**. In 2018, the Pentagon elevated United States Cyber Command to the status of a full and independent unified combatant command, recognizing that cyberwarfare constitutes a unique theater of combat. Last week, President Donald Trump launched U.S. Space Command, acknowledging the importance and the centrality of space communications and infrastructure to America’s security and defense. It will be the responsibility of Congress to bridge the technological investment gap, while United States Cyber Command, U.S. Space Command and an engaged commercial sector must integrate space-cyber defense activities to meet the challenges posed by America’s 21st century technological adversaries.

####

####

#### **Chinese hegemony is key to avert extinction due to climate change – Chinese climate leadership is significantly better than Trump’s**

**Ballard 19** [Eden Ballard, staff writer @ the UCLA International Institute, “Climate Change and Economic Hegemony,” 4/29/19, <http://the-generation.net/climate-change-and-economic-hegemony/>] sg

Since the Industrial Revolution in the late 1800s, the world has already warmed by one degree Celsius and human activity continues to raise average global temperatures. Every degree above pre-anthropocene levels has dire consequences that are felt around the world. A report by the United Nations Intergovernmental Panel on Climate Change (IPCC)1 released in October of 2018, which corroborated 6,000 independent studies on the issue, confirmed that climate change demands immediate global attention. The scientific community agrees that **left unchecked, the temperature will continue to rise and lead to increasingly frequent climate-related catastrophes.** A special coverage article by The New York Times, “Losing Earth: The Decade We Almost Stopped Climate Change”2, outlines the increasing levels of irreparable destruction prescribed with each degree the climate warms. An increase as small as two degrees means **the extinction of the world’s tropical reefs, sea-level rise of several meters and the forced abandonment of the Persian Gulf** due to uninhabitable temperatures. The consequences of each degree are increasingly severe until ultimately, **at five degrees, scientists warn about the end of human civilization.** With so much at stake, it is vital that the international community take action. The Paris Agreement3, a multilateral agreement facilitated by the United Nations that focuses on actions that can be taken to mitigate the effects of climate change, was signed by 175 nations4 on Earth day in 2016. Although it is one of the most comprehensive attempts at combating climate change to date, the Paris Agreement was designed to function primarily through the promotion of voluntary action by individual nations. It is not difficult to imagine then, that some countries have chosen not to take action as their economies are closely tied with some of the practices that are most responsible for pollution. Among them is the United States. President Donald Trump justified abandoning the agreement5 because of the “draconian financial and economic burdens the agreement imposes on our country.” Part of Trump’s campaign platform was rooted in protecting the jobs in the coal industry and a buzzword for him became “clean coal”6 meaning an effort to reduce pollution as a result of coal production. This short-sighted vision overlooks the fact that attempting to limit the environmental effects of coal is largely ineffective and equally as expensive as investing in alternative energy sources which would help the US be a leader in climate activism. The World Bank emphasizes that when it comes to climate change, “the costs of inaction are far higher”7 than those associated with investing in positive change. **Where the US is stepping down, China is stepping up.** One reason **China is motivated to take action** when the US is not lies in the fact that China, infamous for its unbreathable air, has already paid dearly for its dependency on coal. The International Energy Agency in Paris reports that fossil fuel emissions in China have close to tripled since 2000. This is mainly a reflection of China’s large population as per person emissions are lower than those in the US. In 2009, 16 of the world’s 20 most polluted cities8 were in China. **Today only the bottom four cities on the top 20 list are in China because the government has been investing in sustainable technology such as electric cars, wind and solar energy, as well as implementing emission reducing legislation.** In 2013 and 2014, **the Chinese government encouraged several pilot cap and trade programs** that generated close to $680 million in the 2017 fiscal year. In December of 2017 China announced a new plan9 for an even more comprehensive nationwide market focusing on their power generation sector to trade emissions credits that allow businesses to buy and sell the credits that allow them to emit planet-warming greenhouse gases. **Cap and trade programs10 are one of the most talked about ways to combat climate change using the free market.** They incentivize business that use clean energy by limiting the total amount of emissions allowed to all companies and then allowing those that have not used all of the emissions they are allotted to sell them to companies that continue to pollute. Hypothetically, **this incentivizes companies to go green by ensuring that eco-friendly policies save them money**. The challenge with a cap and trade program is closing the loopholes so that heavy polluters cannot skirt around the issue and do, in fact, take initiative to limit emissions. Though there is room for some refinement, **the existing measures are indicative of China’s awareness and sense of urgency around the issue of climate change.** China’s shift away from coal is not only environmentally responsible, it is also economically shrewd as **they are** setting themselves up for financial success for decades to come and **effectively leaving the United States to wallow in what remains of their 20th century glory**. **The W**orld **H**ealth **O**rganization **has acknowledged China’s efforts in curbing pollution and hopes that other nations will take a cue from their actions**. In order to stay economically relevant, nations need to invest in sustainable energy sources. The Visual Capitalist cites the “the Green Revolution” as on

<https://www.mdpi.com/2071-1050/10/11/4234/htm>

Khan 2018

The West, which, for decades, remained a proponent and a champion of free trade and globalization, has shown skepticism toward major cross-border military, political, and economic alliances [26]. It has always maintained a one-way road for exploitation and monopolization of the Third World, its cheap labor, and its financial markets. Thus, it is easy for the developed West to engage in a campaign against immigrants, blaming them for upstaging indigenous labor, and contributing to crime and terrorism. The U.S.’s recent unilateral withdrawal from UNESCO and President Trump’s decision to withdraw the U.S. from the Paris Climate Agreement left the world in a precarious position. The U.S. is steadily moving away from globalizing practices toward a more nationalist, protectionist approach**. On the other hand, China stood firm on its international commitments such as the Paris Climate Agreement, insisting on the need for a sustainable environment for future generations. There are severe environmental consequences of climate change, water shortage, unseasonal torrential rainfall patterns, and floods, necessitating national and global commitments to the future of a sustainable environment.**

[Zhou of Inkstone Sept 4 18](https://www.inkstonenews.com/china-translated/china-translated-where-does-china-stand-climate-change/article/2162728)

**As for China – no, the Chinese government is not selfless. China actually has a lot to benefit from in the fight against climate change.**

**In the long term, rising temperatures could be disastrous by causing glaciers to melt, sea levels to rise and other severe weather events.** Inkstone will explore some of these scenarios over the next two weeks.

For example, **coastal regions in eastern China are the country’s growth engines. Some of its most developed cities, including Shanghai, are located in low-lying areas that could disappear due to sea levels rising.**

## A2: Retal/Escalation

1. [Simon CSIS 10-12-17] Retal decided proportionally based on nature, duration, scope of initial attack - retal can be made limit escalation, only have temp effects, and not spiral out into other industries, i.e. trade - if we don’t escalate they won’t, and there's no reason why we would
	1. [Jensen CATO 1-19] Only 33% of cyber operations saw retaliation, of them, most are proportional response, mostly low level responses

Impact level

1. t/[Valeriano WPo 6-19] Cyber Op’s are used as retal in replacement of physical attacks / mili confrontation - less likely to escalate compared to conventional military bc less perm/less physical damage
	1. Trump switch from mili strike to cyber attack to attack Iran - avoided war

<https://www.theguardian.com/world/2019/jun/23/us-launched-cyber-attack-on-iranian-rockets-and-missiles-reports>

The US military launched a cyber-attack on Iranian weapons systems on Thursday, according to sources, as President Donald Trump backed away from plans for a more conventional strike in response to Iran’s downing of a US surveillance drone.

[Valeriano of the Washington Post 6-25-2019](https://www.washingtonpost.com/politics/2019/06/25/how-cyber-operations-can-help-manage-crisis-escalation-with-iran) (AS)

**Signaling restraint**, President **Trump opted not to escalate the ongoing crisis with Iran** by ordering precision airstrikes that would have resulted in civilian casualties. The discussion of potential responses to Iran’s aggression, however, presents a false choice between conflict that results in death and backing down completely. Instead, the United States chose to disrupt Iranian military targets **with two distinct covert cyber operations.** The United States appears to have sought to disable Iranian missile sites and eliminate the Iranian military’s command and control capabilities. The case illustrates the new character of strategy in a connected era. **In times of crisis, countries increasingly opt for non-military coercive instruments of power, including cyberattacks** and economic sanctions, **to control escalation risk**. As we note in a recent Cato Institute foreign policy analysis article, “rather than escalate with conventional military options, cyber operations offer rivals a way to respond to provocations without significantly increasing tension in a crisis.” **Cyber operations are more political warfare** than decisive battle instruments. **They provide decision-makers valuable intelligence** and potentially coercive options **that help avoid direct military confrontation and can reduce the severity of the response**

[Valeriano 15](https://books.google.com/books?id=HuWkBwAAQBAJ&pg=PA212&lpg=PA212&dq=%22we+developed+our+theory+of+cyber+engagement%22&source=bl&ots=g9btDljYyS&sig=ACfU3U1d7FpxkBX5R1ToJGKbFkq1BQnUoQ&hl=en&sa=X&ved=2ahUKEwi21dawjcflAhUEPK0KHeftCNgQ6AEwAHoECAkQAQ#v=onepage&q&f=false)(SS)

We developed our theory of cyber engagement fully in Chapter 3. The argument considers that **cyber restraint is expected to dominate cyber interactions and should be predictive of future cyber operations. States will restrain themselves from crossing the “red lines” of cyber conﬂict because of the high operational and normative cost associated with these operations.** They will not shut down military networks, knock out power grids, or black out Wall Street; the fear of blowback and retaliation not only in cyberspace,but by conventional means as well,is too great. States will also avoid these actions because of fears of collateral damage and infecting the rest of the Internet. Actions taken in cyberspace tend to invade all aspects of cyberspace. Even when states take actions to keep operations in the realm of cyber,the operations tend to spread and proliferate in ways not predicted.

**Measured escalation possible**

**Simon, Oct 12 2017**

[**https://www.csis.org/analysis/raising-consequences-hacking-american-companies**](https://www.csis.org/analysis/raising-consequences-hacking-american-companies)

**Taken together, these variables—nature, duration, and scope—should inform which elements of a sliding scale of potential responses the United States ultimately chooses to employ in defense of U.S. government and U.S. private-sector entities**. The possible response options should not only include digital or kinetic measures, but all the tools at America’s disposal, from economic sanctions to “naming and shaming” perpetrators. **This flexible approach will allow the United States to tailor its response to reflect the severity of any given cyber attack** and to hit the offending country where it is the most vulnerable, **while reducing the possibility for escalation and avoiding categorical issue linkages across domains, such as trade and cyber.**24 **In particular, when responding to cyber hacks on the less intense end of the spectrum, the U.S. response should incorporate reversible and temporary measures directed against our adversaries corresponding in magnitude to the initial attack against the U.S. private sector**. These measures might include, for instance, vigorous bot-takedown efforts that degrade the ability of our foreign adversaries to engage in malicious digital activity.

[Jenson 1-15-19 of CATO](https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint)

It is thus not surprising that **given the limited objectives of most cyber operations, to date rival states have tended to respond proportionally or not at all**. Returning to the data, **between 2000 and 2016, only 89 operations (32.72 percent) saw a retaliatory cyber response within one year. Of those, 54 (60.7 percent) were at a low-level response severity** (e.g., website defacements, limited denial of service attacks, etc.). Table 1 in the appendix compares the severity scores for cyber operations between rival states between 2000 and 2016.37 **When rival states do retaliate, the responses tend to be proportional**: that is, they tend to match the severity of the initial attack.38

Low-level responses beget low-level counter­responses as states constantly engage in a limited manner consistent with the ebbs and flows of what famed Cold War nuclear theorist Herman Kahn called “subcrisis maneuvering.”39 Rarely does a response include an increase in severity. **Instead, we witness counterresponses of a similar or lower level than the original intrusion or a response outside the cyber domain (for example, economic sanctions or legal indictment of specific individuals). The engagement is persistent but managed, and often occurs beneath an escalatory threshold.**40 As seen in Table 2 in the appendix, this behavior appears to apply equally to each possible cyber strategy: disruption, espionage, and degradation. **Espionage saw little retaliatory escalation, while disruption and degradation both exhibited more low-level responses.**

# A2: AFF

## OVWS:

## A2: CP

1. [Trigger Warning Theory](https://docs.google.com/document/d/1AqnSAHLBpZ8va8b8QHxdjLz6kQ3KNhXPsfRfBB7hMXQ/edit) (bank on them not reading a tw cus i wanna read this so badly(

#### **Tech companies solves**

<https://www.pbs.org/newshour/show/how-the-fbi-tracks-down-child-pornography-predators>

PBS19

Here is how it works: **Internet service providers like Google, Yahoo, and others monitor the billions of uploads and downloads of material with algorithms that search for possible child pornography.** When it is detected, the providers review them and contact NCMEC, sending a sample image, as well as information about the Web server and address. It is then passed along to the FBI for possible investigation.

December 7, 2018 Anderson Duff, REvision Legal

**Search engines, such as Google and Bing, are also blocking searches for restricted material, and are working to tackle peer-to-peer sharing of these images. A study analyzing data between 2011 and 2014 showed that these efforts reduced this type of search traffic by 70%.**

##

## A2: Strait of Hormuz

1. [Stratfor 7-18**]** Iran wont block
2. Iran/GCC war (bc GCC needs free/open shipping for power/econ) and Iran/US war
3. Iran own econ rely on trade in straight - wont risk econ collapse
4. Risks alienating trade allies (China, EU, India) and increasing sanctions from US - econ fails

<https://worldview.stratfor.com/article/why-iran-threatening-close-strait-hormuz>

Jul 5, 2018

Despite the rhetoric, actually blocking the Strait of Hormuz represents perhaps Iran's most extreme option. First and foremost, **attempting to close the strait would result in a devastating war for Iran against the United States and the Gulf Cooperation Council,**as the latter seeks to preserve the freedom of shipping and naval passage through the critical strait. Meanwhile **Iran's own economy and naval activity also depend on the free passage of goods and vessels through the strait**. Finally, cutting off the Strait of Hormuz **would be counterproductive to Iran's current goal of trying to stave off further U.S. sanctions and keep the European Union and other allies such as China and India in its good graces**. The move would be incredibly disruptive to global shipping and oil markets, spoiling the well with allies that Iran needs now more than ever.

## A2: Iran nuke prolif PS

1. Cyberattacks historically fail and create diminishing returns. [JNS 11-8-19] Iran sees 10 major cyberweapons attacks a year, prevented every one of them - defense exists
	1. Stuxnet caused Iran to pay more attention to cyber defence - any increase in OCO increases Iran cyber defence, meaning OCO have diminishing returns
2. [Keck 2-9-15 ] Israel never preemptive strikes:
	1. Israel historically strikes within months of discovering any nuclear research: Syria, Saddam. Iran has a working reactor and has been working since 2002 - should've happened already
	2. Israel attack just rallies domestic support for nuclear program and gives a legit reason to leave NPT - more likely prolif happens
	3. Iran would use attack to gain popularity with the globe: greater middle east support and less sanctions due to intl sympathy
	4. Israel/US relations break, plus blowback from EU/Asia - not worth it
	5. Israel mili action req approval of cabinet - IDF (Israel defence force) leadership opposes hardline policy on Iran
3. [Bernstein 11-5-19 NBC] (prob post-date) Iran never prolifs:
	1. Iran still following international monitoring/verification/inspection, meaning they aren’t able to dev a nuke without globe knowing
	2. Post JCPOA violations are a cry for help - need investment/econ after U.S. sanctions, starting nuclear tech to try to recreate deal with Asia/EU
4. [Glaser 8-17] Stuxnet resulted in, at best, a temp slowdown, and most likely no significant effect on Iran nuke dev

[NOVEMBER 6, 2019, JNS](https://www.algemeiner.com/2019/11/06/stuxnet-attack-made-us-pay-attention-to-cyber-security-says-senior-iranian-general/)

Iranian Islamic Revolutionary Guard Corps General Gholamreza Jalali told Iran’s Channel 5 TV in September that **the 2010 Stuxnet cyber attack had the positive effect of “causing us to pay attention” to the cyber security of its nuclear installations.**

These sites, said Jalali, who heads Iran’s Civil Defense Organization, experience as many as 50,000 cyber attacks per day, ranging from unimportant viruses that are automatically taken care of by security systems to what he referred to as “**cyber weapons.”** These, Jalali said, **are advanced viruses with several encrypted layers, and which hide in, gather intelligence on and sabotage computer systems**.

**There are fewer than 10 cyber-weapon attacks per year, said Jalali, adding that Iran has thus far successfully defended itself from such attacks.**

1. [National Interest](https://nationalinterest.org/feature/can-israel-still-count-the-begin-doctrine-stop-nuclear-25448) 18 - 3 reasons why Israel can’t pull a pre-emptive strike on Iran. If they know they can’t, they won’t
	1. Iran has multiple nuclear facilities unlike Iraq and Syria
	2. Iran has underground bunkers and defense systems against Israel
	3. They lack the intel to do so

[Glaser 8-21-17](https://www.cato.org/publications/commentary/cyberwar-iran-wont-work-heres-why) Cato

**“At best,” according to the University of Toronto’s Jon Lindsay, “Stuxnet thus produced only a temporary slow-down in the enrichment rate itself.” Other experts are even more skeptical. Ivanka Barzashka, Research Associate at King’s College London and a Fellow at Stanford, argues that “evidence of the worm’s impact is circumstantial and inconclusive.” Brandon Valeriano and Ryan Maness, in their book Cyber War Versus Cyber Realities contend, “It is wholly unclear if the Stuxnet worm actually had a significant impact on Iran.”**

<https://nbcmontana.com/news/nation-world/iran-violates-nuclear-deal-uranium-enrichment-not-a-breakout>

11-5-19 Bernstein

According to experts, **Iran's sequential breaches of the 2015 agreement are significant but there are strong indications that Iran's moves are not necessarily aimed at a nuclear breakout.** Heather Williams, a senior policy researcher at the RAND Corporation and former intelligence officer at the National Intelligence Council, noted that the advanced enrichment capability does not, in itself, signal an intent to rapidly develop a nuclear bomb. **Despite the U.S. withdrawal from the deal and Iran's violations, there are still mechanisms in place that would alert the international community if Iran were to race to a nuclear weapon** and Tehran has indicated it is willing to return to compliance, under certain conditions Kelsey Davenport, the director of nonproliferation policy at the Arms Control Association, explained that the risk posed by Iran's nuclear program has increased with its new violations. "But they are quickly reversible and **Iran is taking these steps under international monitoring and verification," she said. "So if Iran were to sprint to a nuclear weapon, inspectors would quickly realize Tehran was going down that path."**

In his televised statement Tuesday, **Iranian President Rouhani said that International Atomic Energy Agency (IAEA) inspectors "will continue to supervise" the activity at Fordo.** Rouhani further noted that Iran could quickly reverse the four violations and snap back into compliance if the remaining parties of the nuclear deal—China, France, Russia, the United Kingdom and Germany—provide Iran with sanctions relief, as agreed to under the JCPOA.

Over the past five months, **Iran's violations have largely been part of an appeal to Europe and Asia to find a way around U.S. sanctions. America's strict sanctions regime has made it untenable for foreign firms and countries to do business with Iran a**nd also have access to the U.S. financial system and market. Last month, the International Monetary Fund projected the Iranian economy would shrink by 9.5% in 2019, largely as a result of the sanctions.

Alex Vatanka, a senior fellow at the Middle East Institute with a focus on Iran and Middle East security, said **Iran's nuclear violations are a "scream for help" from the international community. "What they're doing right now is basically trying to get the world's attention and create some leverage," Vatanka said. "This is clearly not a dash for a nuclear bomb. This is a plea for the world to come back to the nuclear deal of 2015."**

[Keck 2-9-15 , The National Interest,](https://nationalinterest.org/commentary/five-reasons-israel-wont-attack-iran-9469)

Although the interim deal does further reduce Israel’s propensity to attack, the truth is that **the likelihood of an Israeli strike on Iran’s nuclear facilities has always been greatly exaggerated.** There are at least five reasons why Israel isn’t likely to attack Iran.

First, **if Israel was going to strike Iran’s nuclear facilities, it would have done so a long time ago**. Since getting caught off-guard at the beginning of the Yom Kippur War in 1973, **Israel has generally acted proactively to thwart security threats.** On no issue has this been truer than with nuclear-weapon programs. For example, **Israel bombed Saddam Hussein’s program when it consisted of just a single nuclear reactor. A**ccording to ABC News, **Israel struck Syria’s lone nuclear reactor just months after discovering it**. The IAEA had been completely in the dark about the reactor, and took years to confirm the building was in fact housing one.

Contrast this with Israel’s policy toward Iran’s nuclear program. **The uranium-enrichment facility in Natanz** and the heavy-water reactor at Arak first **became public knowledge in 2002**. **For more than a decade now, Tel Aviv has watched as the program has expanded into two fully operational nuclear facilities, a budding nuclear-research reactor, and countless other well-protected and -dispersed sites.**Furthermore, America’s extreme reluctance to initiate strikes on Iran was made clear to Israel at least as far back as 2008. It would be completely at odds with how Israel operates for it to standby until the last minute when faced with what it views as an existential threat.

2. Bombing Iran Makes an Iranian Bomb More Likely

Much like a U.S. strike, only with much less tactical impact, **an Israeli air strike against Iran’s nuclear facilities would only increase the likelihood that Iran would build the bomb**. At home, Supreme Leader Ali Khamenei could use the attack to justify rescinding his fatwa against possessing a nuclear-weapons program, while using the **greater domestic support for the regime and the nuclear program to mobilize greater resources for the country’s nuclear efforts.**

**Israel’s attack would also give the Iranian regime a legitimate** (in much of the world’s eyes) **reason to withdraw from the Nuclear Non-Proliferation Treaty** (NPT) **and kick out international inspectors**. If Tehran’s membership didn’t even prevent it from being attacked, how could it justify staying in the regime? Finally, support for international sanctions will crumble in the aftermath of an Israeli attack, giving Iran more resources with which to rebuild its nuclear facilities.

3. Helps Iran, Hurts Israel

Relatedly, *an Israeli strike on Iran’s nuclear program would be a net gain for Iran and a huge loss for Tel Aviv.* **Iran could use the strike to regain its popularity with the Arab street** and increase the pressure against Arab rulers. As noted above,**it would also lead to international sanctions collapsing, and an outpouring of sympathy for Iran** in many countries around the world.

Meanwhile, a strike on Iran’s nuclear facilities would leave Israel in a far worse-off position. Were Iran to respond by attacking U.S. regional assets, ***this could greatly hurt Israel’s ties with the United States*** at both the elite and mass levels. Indeed, a war-weary American public is adamantly opposed to its own leaders dragging it into another conflict in the Middle East. Americans would be even more hostile to an ally taking actions that they fully understood would put the U.S. in danger.

Furthermore, **the quiet but growing cooperation Israel is enjoying with Sunni Arab nations against Iran would evaporate overnight**. Even though many of the political elites in these countries would secretly support Israel’s action, their explosive domestic situations would force them to distance themselves from Tel Aviv for an extended period of time. **Israel’s reputation would also take a further blow in Europe and Asia, neither of which would soon forgive Tel Aviv.**

4. Israel’s Veto Players

Although Netanyahu may be ready to attack Iran’s nuclear facilities, he operates within a democracy with a strong elite structure, particularly in the field of national security. It seems unlikely that he would have enough elite support for him to seriously consider such a daring and risky operation.

For one thing, **Israel has strong institutional checks on using military force.** As then vice prime minister and current defense minister Moshe Yaalon explained last year: “**In the State of Israel, any process of a military operation, and any military move, undergoes the approval of the security cabinet and in certain cases, the full cabinet**… the decision is not made by two people, nor three, nor eight.” It’s far from clear Netanyahu, a fairly divisive figure in Israeli politics, could gain this support. In fact, Menachem Begin struggled to gain sufficient support for the 1981 attack on Iraq even though Baghdad presented a more clear and present danger to Israel than Iran does today.

What is clearer is that *Netanyahu lacks the support of much of Israel’s highly respected national security establishment.* Many former top intelligence and military o**fficials have spoken out publicly against Netanyahu’s hardline Iran policy,** with at least one of them questioning whether Iran is actually seeking a nuclear weapon. Another former chief of staff of the Israeli Defense Forces told The Independent that, “It is quite clear tha**t much if not all of the IDF [Israeli Defence Forces] leadership do not support military action at this point**…. In the past the advice of the head of the IDF and the head of Mossad had led to military action being stopped.”

## A2: Cybercrime

1. [U.S. Chamber of Commerce 18] FBI is the primary fed agency for responding to cybercrime
	1. [Gallagher May 2019] Don’t stop cybercrime - FBI is arresting the perpetrators in less than 1 percent of malicious cyberattacks.
	2. [Gallagher May 2019] Problem is getting worse bc cyber brain drain - literally losing the ability entirely
2. [Hoffman 6-17 Carnegie Endowment] Companies are dev their own tech to preempt, interfere and mitigate cyberattacks - FBI’s role is shifting to private companies
3. [Roseen 3-20-18] 88-90% of cyberattacks aren’t even reported/counted, criminals have nothing to fear
4. [McKenzie USAF 11-17]: stopping cyber crimes is basically impossible:
	1. Hard to track online activity
	2. Hackers move to places where govt policies make it difficult to catch/convict
	3. Too many cases to stop every one: 2010: 300,000 cybercrimes, 6 convictions
	4. Unreported: only 17% of companies report cybercrime losses
	5. Hackers weigh the possibility of getting caught with potential benefits: the US’s current ability is not enough to outweigh the benefits or serve as a deterrent

[McKenzie-](https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF) USAF Jan 17

**Cyber-criminal activity is** the largest group of cyber threats and **one of the most difficult to effectively deter.** This group of hackers ranges in sophistication from low ability (i.e., script kiddies) to elite-level hackers motivated by financial gain.  **Our ability to punish and deter** this group **is** sometimes  **limited** and largely dependent on law enforcement and effective cooperation from foreign nations. **Sophisticated hackers will seek out places where governance and policy conditions facilitate masking their identities.**20 **Punishing this group can be complex** for several reasons. **First, as discussed, accurately attributing the source of cyber attacks is problematic and sometimes time-consuming.** **Second, the sheer volume of activity makes prosecuting all cases impractical**. According to a 2013 US Government Accountability Office report on cyber-security, the number of computer security incidents that federal agencies reported to the United States Computer Emergency Readiness Team (US-CERT) over a six-year period increased from 5,503 in 2006 to 48,562 in 2012 (a 782 percent increase).21 **According to the Internet Crime Complaint Center’s 2010 Internet Crime Report, the Federal Bureau of Investigation received 303,809 Internet crime complaints resulting in 1,420 prepared criminal cases—which led to a mere six convictions**.22 In addition to the low conviction rate, **cybercrimes are among the most underreported forms of criminality. One estimate suggests that only 17 percent of companies report cybercrime-related losses to law enforce-ment**.23 **Hackers with criminal or financial intent have to weigh the possibility of being caught and prosecuted for their crimes against the potential profits**. **Skilled hackers** who know how to hide their identities and locations **will continue to conduct these crimes until identification, attribution, and prosecution of cybercrimes increase.** Our ability to deter political hacktivist groups is low for all the same reasons.

[By Dillon Roseen March 20, 2018](https://www.newamerica.org/millennials/dm/improving-cyber-crime-data-protect-vulnerable-communities/) New America

In the meantime, according to Donna Gregory’s estimate, **we know that approximately 88-90 percent of the cyber crimes that are being perpetrated remain uncounted.**The fact that we don’t have a perfectly clear picture of the scope of cyber crimes affecting specific populations should not stop us from pursuing the important work of protecting the communities that are likely to be most targeted online. As detailed throughout this piece, media reports and advocacy organizations have documented countless instances where certain populations are indeed more vulnerable to becoming victims of cyber crime than others. It is important to understand these existing efforts to protect against and respond to cyber crimes perpetrated against vulnerable online communities, especially since these victims are typically least equipped to receive justice through formal mechanisms.

[Grimes](https://www.csoonline.com/article/2618598/why-internet-crime-goes-unpunished.html)

**The conviction rate in 2010 was even worse. According to FBI's 2010 Internet Crime Report, from 303,809 complaints, 1,420 prepared criminal cases resulted in a mere six convictions. That's one jailed cyber criminal for every 50,635 victims, and these are just the cases significant enough to be reported to the FBI.**

1. [Lewis CSIS Jan 18] Literally no one wants to cybercrime:
	1. Non-state actors don’t have the resources and knowledge for large scale damaging attacks
	2. State actors fear any retal and avoid actions that would provoke damaging response in the form of armed conflict - incentive to not cyberattack always exists
	3. Terrorists have no interest in econ harm: doesn't serve a purpose and way too difficult
	4. China is focused on its growth rathering than undermine U.S. econ: OCO’s = nukes in china’s POV
	5. Russia is focused on disruption and showing its strength, not creating actual damage
	6. Iran and NK want political coercion, not destruction - nothing large scale since it will create retal

[Galaghar 5-20-19](https://www.kroll.com/en/insights/publications/cyber/identity-crisis-fbi-cyberthreats) Kroll

While the bureau has a history of being run by agents with guns, more funding and priority is now being funneled into behind-the-scenes digital experts who can watch network traffic and unravel digital trails back to hackers, and who can explain online activity to judges and secure subpoenas for tech companies. The Department of Justice budget request to Congress for 2019 asks for $370 million to fund the FBI’s cyber investigations and related work.

Yet even as the FBI’s need for cyber experts is increasing, its ability to retain agents and employees with the needed technical expertise is under threat. According to interviews with over a dozen former FBI cyber employees as well as other national security experts, **a cyber “brain drain” is taking place at the bureau that could hamper its ability to stem the constant flow of digital threats.**

While the bureau’s major arrests in cyber cases often make headlines, **the numbers are too small to make a significant dent in cyber crime,**according to analysis from national security think tank Thirdway, which determined that **the FBI is arresting the perpetrators in less than 1 percent of malicious cyberattacks.**

[U.S. Chamber of Commerce 2018](https://www.uschamber.com/file/22049/download)

**The FBI is the primary federal agency responsible for investigating cybercrime.** The agency leads threat response efforts as outlined in PPD-41 and is tasked with investigating cyberattacks on U.S. entities and providing attribution. Through its Cyber Division at headquarters in Washington, D.C. the FBI investigates computer intrusion cases involving counterterrorism, counterintelligence, or other criminal matters with national security implications

[Hoffman 6-14-17 Carnegie Endowment for Human Peace](https://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236)

A principles-based approach. To fill the vacuum in the cyber domain,**companies are engaging attackers within and outside of the defender’s network to preempt, interfere with, or mitigate the consequences of cyberattacks.** Rather than trying to enforce ineffectual laws and regulations, governments and stakeholders should seek to develop guiding principles for a spectrum of ACD, excluding “hacking back.” Such principles could be embedded in a range of mechanisms, for example a voluntary code of conduct for employing ACD.

<https://www.motherjones.com/politics/2019/07/the-us-government-has-done-almost-nothing-to-stop-cyber-attacks/>

Clarke and Knake have just published a new book—The Fifth Domain: Defending our Country, our Companies, and Ourselves in the Age of Cyber Threat—arguing that **the nation’s susceptibility to computer warfare is no longer a failure of technology but instead a failure of political will.** Cyber defense, they write, once bordered on the impossible, but now it’s much more achievable—if only our leaders take the right approach

Richard Clarke: What we’re saying is**, over the course of at least the last five years, major US corporations have proven that you can achieve cyber security.** Ten years ago, when we wrote the book Cyber War, we said no one can defend themselves, that defense was impossible. Now, we say**there have been changes in the defensive technology that allow major corporations to fight back—if they spend enough money and if they have enough skilled people to achieve cyber resilience—and that there are a large number of those companies.** That’s, that’s good news.

But if we survey where the government has come, and where military activity and intelligence activity have come during those 10 years, it’s not good news.**Now the major threat actors are governments and military organizations. The major cyber attacks now are being done by the Chinese People’s Liberation Army cyber unit, by the Russian GRU cyber unit, by North Korea’s army, by Iran’s army.**

<https://www.justsecurity.org/64875/u-s-offensive-cyber-operations-against-economic-cyber-intrusions-an-international-law-analysis-part-i/>

[James Andrew Lewis CSIS January 2018](https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/180108_Lewis_ReconsideringCybersecurity_Web.pdf)

**The most dangerous and damaging attacks required resources and engineering knowledge that are beyond the capabilities of nonstate actors,** and those who possess such capabilities consider their use in the context of some larger strategy to achieve national goals. Precision and predictability—always desirable in offensive operations in order to provide assured effect and economy of force—suggest that the risk of collateral damage is smaller than we assume,and with this, so is therisk of indiscriminate or mass effect. State Use of Cyber Attack Is Consistent with Larger Strategic Aims Based on a review of state actions to date, cyber operations give countries a new way to implement existing policies rather than leading them to adopt new policy or strategies

**Cyber operations** provide unparalleled access to targets, and **the only constraint on attackers is the risk of retaliation—a risk they manage by avoiding actions that would provoke damaging response. This is done by staying below an implicit threshold on what can be considered the use of force in cyberspace.**The reality of cyber attack differs greatly from our fears. Analysts place a range of hypothetical threats, often accompanied by extreme consequences, before the public without considering the probability of occurrence or the likelihood that opponents will choose a course of action that does not advance their strategic aims and creates grave risk of damaging escalation. **Our opponents' goals are not to carry out a cyber 9/11**. While there have been many opponent probes of critical infrastructure facilities in numerous countries, the number of malicious cyber actions that caused physical damage can be counted on one hand. While opponents have probed critical infrastructure networks, there is no indication that they are for the purposes of the kind of crippling strategic attacks against critical infrastructurethat dominated planning in the Second World War or the Cold War. Similarly, the popular idea that opponents use cyber techniques to inflict cumulative economic harm is not supported by evidence. Economic warfare has always been part of conflict, but there are no examples of a country seeking to imperceptibly harm the economy of an opponent. **The United States engaged in economic warfare during the Cold War, and still uses sanctions as a tool of foreign power, but few if any other nations do the same.** The intent of cyber espionage is to gain market or technological advantage. Coercive actions against government agencies or companies are intended to intimidate**. Terrorists do not seek to inflict economic damage. The difficulty of wreaking real harm on large, interconnected economies is usually ignored**. Economic warfare in cyberspace is ascribed to China, butChina's cyber doctrine has three elements:control of cyberspace to preserve party rule and political stability, espionage (both commercial and military), and preparation for disruptive acts to damage an opponent's weapons, military information systems, and commandand control. **"Strategic" uses, such as striking civilian infrastructure in the opponent's homeland, appear to be a lower priority and are an adjunct to nuclear strikes as part of China's strategic deterrence.Chinese officials seem more concerned about accelerating China's growth rather than some long-term effort to undermine the American economy**.6 The 2015 agreement with the United States served Chinese interests by centralizing tasking authority in Beijing and endingPeople's Liberation Army (PLA) "freelancing" against commercial targets. The Russians specialize in coercion, financial crime, and creating harmful cognitive effect—the ability to manipulate emotions and decisionmaking. Under their 2010 military doctrine on disruptive information operations (part of what they call "New Generation Warfare"). **Russians want confusion, not physical damage. Iran and North Korea use cyber actions against American banks or entertainment companies like Sony or the Sands Casino, but their goal is political coercion, not destruction**.None of these countries talk about death by 1000 cuts or attacking critical infrastructureto produce a cyber Pearl Harbor or any of the other scenarios that dominate the media

Major financial institutions face a high degree of risk but in most cases, the attackers' intent is to extract money. There have been cases of service disruption and data erasure, but these have been limitedin scope. **Denial-of-service attacks against banks impede services and may be costly to the targeted bank, but do not have a major effect on the national economy.** In all of these actions, there is a line that countries have been unwilling to cross. When our opponents decided to challenge American "hegemony," they developed strategies to circumvent the risks of retaliation or escalation by ensuring that their actions stayed below the use-of-force threshold—an imprecise threshold, roughly defined by international law, but usually considered to involve actions that produce destruction or casualties. Almost all cyber attacks fall below this threshold, including, crime, espionage, and politically coercive acts. This explains why the decades-long quest to rebuild Cold War deterrence in cyberspace has been fruitless. It also explains why we have not seen the dreaded cyber Pearl Harbor or other predicted catastrophes**.Opponents are keenly aware that launching catastrophe brings with it immense risk of receiving catastrophe in return. States are the onlyactors who can carry out catastrophic cyber attacks and they are very unlikely to do so in a strategic environment that seeks to gain advantage without engaging in armed conflict.**

## A2: Non-State Cyberattacks

Turn ---offensive cyber code can get out and be accessed by terrorists

[Yosef Harash,, June 6, 2019](https://www.haaretz.com/us-news/.premium-what-a-future-cyberwar-will-look-like-1.7441901),

**Another danger is that terror groups could get their hands on cyberwarfare tools. “As soon as a malicious tool of this kind is out in the world it may be exploited by everyone, including the sort of people it was never meant for**,” Giller says. “Private hacker groups could damage any type of physical infrastructure –on a countrywide or company-wide scale, to affect energy, water and oil companies, and others.”**Two years ago, tools for cyberwarfare leaked from the NSA to the internet**. This May, the city of Baltimorebattled a cyberattack from an unknown source that shut down thousands of computers, prevented email from being sent and disrupted real estate deals, payment of water bills, health warnings and many other services. It was determined that the attack was being carried out with the NSA’s EternalBlue software program

##

## A2: Boko Haram

1. [A2: Strake] The card about the threat Boko Haram poses in cyberspace is literally from 2015

**A2: Cyberattacks**

1. [Chelin 3-15-19] Boko Haram has not been able to carry out advanced cyberattacks or cybercrime
	1. Lack good Internet infrastructure
	2. Lack other resources
	3. Don’t want to face Nigeria army military retal

**A2: Recruiting/Prop**

1. [Ogunlana 4-19, strakes solvency evi] New AI methods allow social media companies to take down terror propaganda faster than humans can (private companies solve back better than the govt)
2. [Ogunlana 4-19, strakes solvency evi] Nigeria is working with other Western countries as well for cyber training/tools/tech
3. [SWG 9-18] IBM is working with Nigeria Cyber Warfare command to attack online presence of terrorists

Also the sick turns in ISIS

<https://enactafrica.org/research/trend-reports/should-africa-worry-about-cyber-attacks-from-extremists>

15 Mar 2019, Chelin from Enact Africa

**The chances of Boko Haram launching a cyber-attack are low,** but members who could launch such an attack could be recruited

For example, when Boko Haram pledged its allegiance to ISIS in early 2015, its presence on social media increased – as did its distribution of propaganda. **But Boko Haram has not apparently been able to carry out more advanced examples of cybercrime** other than so-called ‘419 fraud’ [literally nigerian king scams lmfao]. The group reportedly hacked a Nigeria State Security Service database in 2012, but did not claim responsibility for the attack.

**It appears, then, that the prospect of Boko Haram launching a cyber-attack in the near future is low.** However, the possibility of recruiting potential members who could launch such an attack exists. **Launching a cyber-attack would, however, mean overcoming practical challenges such as poor Internet infrastructure, lack of resources and the need to regroup following sustained counter-insurgency measures by the Nigerian army.**

<https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1707&context=jss>

Ogunlana, Sunday “Halting Boko Haram” Walden University. April 2019, Journal of Strategic Security https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1707&context=jss CCD

^^^ their solvency evi

Key findings of this study are as follows: that technology is useful in fighting the expansion and coordination of terrorism in cyberspace when properly integrated with other strategies. There has been little progress in countering the threat presented by terrorists’ propaganda in Nigerian cyberspace; a need exists to train and produce more experts with the requisite technical skills to dismantle terrorists’ websites and counter their messaging on social media platforms; and the government’s counter-narrative efforts on social media are ineffective. Cybersecurity technologies are useful and cost-effective tools to combat terrorist propagandas and networking in cyberspace. **New artificial intelligence and machine learning tools enable prominent social media organizations to take down terrorist content faster than human moderators do.** Nigeria constitution guarantees no protection for people spreading violence and hate speech in cyberspace. Law enforcement and intelligence agencies have inherent powers to listen to citizens’ communications, break offenders’ privacy, and collect evidence that can stop potential terrorist acts. **The government of Nigeria is coordinating with** the United States **and other western allies in the areas of training and technology transfer**

Meanwhile, **a coalition of top technology companies in the United States is making effortsto curb terrorists’use of social media technology with the use of Artificial Intelligence (AI).** Korolov explained that AI-based security applications can read and understand security —they can analyze every incident, identify causes, methods, and trends,and predict the next pattern even before it happens.48For instance, IBM developed Watson, which has been taught to readvast quantities of information online.49Watson provides smart data analysis and visualization services, which makes it easy to detect patterns. It has an inbuilt capability that enables the user to interact with data in a conversation with a response the user can easily understand. In some countries of Global North, the Law Enforcement and intelligence agencies are using AI and machine learning to detect and respond to different kinds of cyber threats, including cyberterrorism. There are different kinds of cybersecurity tools available, but the user or organizations must know how to apply them and integrate them into the broader cybersecurity strategy. Isaac found that there is an ongoing project to create a shared digital database which includes “fingerprinting”or patterns of all suspicious terrorist content that raise red flags.50This inter-company collaboration will ensure that contentthat has been flagged on Twitter will not appear on Facebook or another social media platform

<https://spacewatch.global/2018/09/nigerian-army-to-create-cyber-warfare-command-to-combat-online-terrorism-and-crime/>

Vanguard also reports that Lt. Gen. Buratai’s decision to create **Cyber Warfare Command** has been long in gestation, as he first proposed the creation of such an organisation in November 2016 **as part of the Nigerian government’s response to the threat posed by Boko Haram.**

**It is believed that the Cyber Warfare Command is being set up with technology and expertise provided by U.S. technology company IBM.** According to the Vanguard report, **IBM is providing the resources for** Cyber Warfare Command to carry out distributed denial-of-service (DDOS) **attacks against the online presence of terrorists, criminal groups, and other threats.**

## A2: ISIS

1. Any alt source of cyberattacks checksback:
	1. [CSIS 19] March 2019, Australia launched cyber attacks to disrupt communications
	2. [Bloomberg 4-18] UK cyberattacks in 2017 disrupted communication/propaganda infra for much of the year, making it almost impossible to recruit
	3. [Brookings FoPo 11-15] Non-state hacktivists organized to stop ISIS: take down 100k+ twitter accounts and 150 ISIS-linked websites
2. [Ash Carter (former def sec) 10-17 Belfor Center] U.S. cyberops had no meaningful effect on ISIS
	1. Rarely produced useful cybertools
	2. Intel agencies block cyberattack use, fear of interfering with intel gathering
	3. State Dep diplo issues in interfering with another countries internet
3. **A2: Recruitment**
	1. [Huber 11-6-19] Recruitment from refugee camps - Syria, Lebanon, etc
	2. [Brookings FoPo 11-15] Non-state hacktivists organized to stop ISIS: take down 100k+ twitter accounts and 150 ISIS-linked websites
	3. TURN [Berger March 2015 Brookings] Significant number of ISIS accounts provided GPS locations of ISIS strongholds (geotagging)
	4. TURN: ISIS doesn’t just lay down and die when their online recruiting, which is literally their lifeblood, is shut down. Rather, [Berger March 2015 Brookings] finds that Removal of propaganda outlets has historically resulted in more aggressive account promotion and social media presence by ISIS - recruitment and recruitment rate both increase
		1. After takedowns, ISIS members began working much harder to promote their own accounts, resulting in average follower count doubling
		2. Larger and more active social media presence increases the rate of radicalization by increasing the visibility of biased and manufactured information to manipulate followers
		3. [Nakashima (WaPo) 2017] ISIS persistent - when media is taken down, they just restore content or move to new servers - always adapt
4. **A2: Funding**
	1. [Dep of Treasury 4-19] US launched sanctions to cut off terror funding for ISIS
	2. [Taie 4-19] Iraqi forces capture financiers/money transfers for ISIS - literally their top priority
	3. [UNSC report 2-19] ISIS bulk stores cash - cyber no solve
5. **A2: Communication**
	1. [CSIS 19] March 2019, Australia launched cyber attacks to disrupt communications
6. **A2: Bases**
	1. [Calimachhi 4-4-18 NYT] ISIS controls only 3% of what territory they used to have bc of ground troops

[Calimachhi 4-4-18 NYT](https://www.nytimes.com/interactive/2018/04/04/world/middleeast/isis-documents-mosul-iraq.html)

**One day in late 2016,** a flier decorated with the Iraqi flag floated down onto the Hamoud family’s home. The agricultural department official and his extended family were hunkered down inside the living room, sitting elbow-to-elbow on an L-shaped couch, he recalls. By then, the militants had banned both cellphones and satellite dishes. They were cut off from the world. The flier was one of millions dropped over Mosul warning the population to take cover. **The military assault was about to begin.** “Could this really be happening?” Mr. Hamoud wondered. Then he used a lighter to incinerate the flier.**The fighters** whose plans of building a state had been met with ridicule **proved surprisingly good** at it. It took nine months to wrest Mosul from the militants’ grip, a slog that one senior American general said was the most difficult battle he had witnessed in 35 years. **Since then, the militants have lost all but 3 percent of the territory in Iraq and Syria they once held.** But they clung so tightly to their caliphate that block after city block was leveled during the battle to take back cities and towns. Thousands of people have lost their homes. New mass graves are being discovered every month. One of them contains the remains of four of Mr. Hamoud’s cousins.

[2-1-19 UNSC Report](https://www.un.org/sc/ctc/wp-content/uploads/2019/02/N1901937_EN.pdf)

2**. ISIL is reported by some Member States to still have access to financial reserves of between $50 million and $300 million.** Although its territorial losses have removed some sources of revenue, it has correspondingly fewer liabilities and is expected to be able to sustain its operations. 13**. ISIL is assessed to have bulk-stored cash in its core area and smuggled some into neighbouring countries for safekeeping.** It is also reported to have invested some of its reserves in legitimate businesses. ISIL no longer has reliable access to oilproducing areas in the eastern Syrian Arab Republic for direct extraction; it earns more revenue by extorting oil cargos extracted by others. It has been reported that ISIL financial assets have largely been concealed, with a strategic view to funding larger-scale attacks once the opportunity arises again.

Khalid [Taie 4-4-19](https://diyaruna.com/en_GB/articles/cnmi_di/features/2019/04/04/feature-01)

Legit source: Diyaruna is a website sponsored by USCENTCOM to highlight movement toward greater regional stability through bilateral and multilateral cooperative arrangements. Diyaruna also focuses on developments that hinder both terrorist activity and support for terrorism in the region. This site features news from across and about the Middle East and features analysis, interviews and commentary by paid Diyaruna correspondents. It is designed to provide the audience with a portal to a broad range of information about future stability in the region.

Following the military defeat of the "Islamic State of Iraq and Syria" (ISIS) in Iraq, **Iraqi forces have been stepping up their efforts to identify and destroy the group's funding sources**, security sources said. **Cutting off these revenue streams is a "top priority**", Counter-Terrorism Service (CTS) spokesman Sabah al-Numan told Diyaruna, noting that a shortage of funds will help to prevent ISIS terror cells from regrouping. Since late 2017, when ISIS was defeated in Iraq, **Iraqi forces have captured dozens of financiers who were working behind the scenes to move and collect money and hand it over to the group**. "Money transfers via exchange bureaus and brokerages used to be the main source of funding for ISIS," said Fadel Abu Ragheef, a security expert specialising in terrorist groups. **As part of a crackdown on terror financing, some major financial networks have been implicated in funneling funds to ISIS**, he told Diyaruna. These include al-Rawi financial network, which owned holding companies and foreign investments "estimated in the millions of dollars across a range of sectors such as car dealerships, real estate and fish farming", he said. **Ten members of the network, led by Fawaz al-Rawi, were arrested during an Iraqi Special Operations Forces and Kurdish Counter-Terrorism Forces operation in Baghdad and Erbil backed by the international coalition in October**.

[Dep of Treasury April 15, 2019](https://home.treasury.gov/news/press-releases/sm657)

Washington **– Today, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) designated seven individuals and one entity pursuant to Executive Order (E.O.) 13224, which targets terrorists and those providing support to terrorists or acts of terrorism.** Specifically, OFAC designated key financial facilitators and conduits for the Islamic State of Iraq and Syria (ISIS) operating in Europe, Africa, and the Middle East. Six individuals, located in Iraq, Turkey, and Belgium, and the entity, an Iraq, Turkey, and Syria-based money services business (MSB), are part of the Rawi Network, a key ISIS financial facilitation group based out of Iraq, which was the target of a joint Treasury-Department of Defense (DOD) action in October 2018. In that action, OFAC designated Iraq-based MSB Afaq Dubai, and the Combined Joint Task Force-Operation Inherent Resolve (CJTF-OIR) released details regarding its support to a joint Iraqi Special Operations Forces and Kurdish Counter Terrorism Forces action against members of the Rawi Network who leveraged Afaq Dubai to facilitate the movement of funds for ISIS. The seventh individual designated today is a Kenya-based female financial facilitator who has played an important role in an ISIS facilitation network in East Africa. “This action is directed at the Iraqi-based Rawi Network, which has used hawalas and money service businesses to circumvent the formal banking sector and move terror funds for ISIS across Europe, Africa and the Middle East.  **Treasury is dedicated to ensuring the enduring defeat of ISIS by cutting off all remaining sources of their terror funding around the globe,”** said Sigal Mandelker, Under Secretary for Terrorism and Financial Intelligence. “Our sanctions underscore how the ISIS threat has morphed, with financial cells on multiple continents, and with female operatives such as Halima Adan Ali, a Kenya-based financial facilitator.”

[Berger Brookings 3-2015](https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf)

**There is clear intelligence value to be extracted from the ISIS accounts we examined.** Although the volume of material created challenges in approaching this material systematically, the data analysis provided a number of clear insights. **Most prominently, a significant number of accounts provided reliable GPS coordinates in ISIS territories. A subsequent data collec-tion in late December 2014 detected even more relevant GPS coordinate data in Iraq and Syria, even as ISIS was warning its members against the practice.**

**(better turn 2)**

**In the wake of Twitter’s suspension campaign, users re-sponded by aggressively promoting new accounts that had replaced suspended accounts.** Typically, tweets promoting ISIS accounts included a list of accounts with descriptive text. Our analysis isolated these as “non-reply mentions”—the inclusion of a Twitter handle in a tweet that is not a reply to another tweet.In the February collection, users sent an average of 17.4 non-reply mentions to other users in the net-work, but received only 12 in return. In the Demo-graphics Dataset from fall 2014, users sent an aver-age of 12 non-reply mentions and received 10.4. To produce a cleaner comparison, we also looked at these figures for accounts with fewer than 20,000 followers in both sets, expected to result in a higher proportion of ISIS-supporting accounts per the earlier analysis. The noise in the February dataset was especially concentrated among high-follower accounts. This figure was particularly telling. In the February collection, these users sent an average of 40.3 non-reply mentions to other users in the network, but received only 8.6. In the Fall 2014 collection, users sent 11.9 non-reply mentions and received 9.8.

This data yields two major implications:

 1. **The amount of activity devoted to rebuilding the Twitter network** (as opposed to disseminat-ing propaganda, recruiting and other activities)**more than tripled.**

2. A five-to-one disparity opened up between the average non-reply mentions sent and the aver-age received, indicating that the greatly increased activity was directed at fewer accounts. **In other words, users were working much, much harder to promote the top accounts in the network**. The increased amount of promotional activity did not correlate to an increase in the number of in-network accounts being promoted. An interesting result running counter to the overall trend of depressed activity in the network pertained to follower counts. **For the sets delimited to fewer than 20,000 followers each, the average number of followers nearly doubled from fall 2014 to February 2015**—from 725 to 1408—with significantly fewer accounts recorded as having less than 200 followers, when compared to the Demographics Dataset.**A pos-sible explanation is discussed in section 4.3**, which ex-amines some of the potential tradeoffs incurred when degrading the network’s overall performance.

**(this is section 4.3)**

While the current debate over the value of account suspensions leaves much to be desired, our research identified one unintended consequence that merits serious consideration as an argument against main-taining a program of suspensions. One effect of sus-pending more visible ISIS accounts is that the net-work becomes more internally focused over time. While our data was insufficient to fully address this question, the process of trying to create the February 2015 comparison set described in section 2.5.4 vividly illustrated this change in dynamic. We made several attempts to develop a network of similar size to the original collection with new seeds, only to be met with frustration. There was substantial overlap in the accounts followed by the new seed accounts, pointing toward a much more inwardly focused network, even as the average number of followers increased. Much of what follows is observational, although future research may be able to quantify the ef-fects. **We suspect that as the network comes under mounting pressure, ISIS supporters will increasing-ly follow and interact with other supporters,** and will be less and less inclined to follow and interact with people outside the supporter network**.** The re-peated suspension of the most visible accounts has the effect of peeling away many users who are less engaged with ISIS and its ideology. In short, ISIS social networks on Twitter are becoming even more insular than they were to begin with. There are potential hazards here. First, ISIS supporters who have more out-of-net-work relationships may be exposed to moderating or deradicalizing influences. While ISIS’s status as the most extreme Islamic radical group raises very legitimate doubts about whether the majority of adherents are even vulnerable to moderating in-fluences, we have seen examples of people turning away from its toxic ideology.25 When we segregate members of ISIS social networks, we are, to some extent, also closing off potential exit ramps. Secondly, while the suspensions raise the barrier to joining the social network—in the sense that they reduce the number of invitations ISIS can success-fully broadcast—they do not by any means make joining impossible. The interior of this network is changing as a result of the suspensions, making it a much louder echo chamber. The increased stridency and monotonic content may discourage some new members of the network from remaining. For others, **there is a risk that the more focused and coherent group dynamic could speed and intensify the radicalization process.** Prior to the advent of social media, al-Qa’ida training camps practiced cult-like techniques of indoctrina-tion which included cutting new recruits off from the outside world. While the barriers to outside engage-ment in a virtual environment are obviously far more porous, the segregation of ISIS’s social network may create a smaller but similar effect. I**n some ways, this effect may be more pernicious as it creates the illusion of access to unfiltered information, when in fact ISIS news sources are extraordinarily filtered and biased. This allows ISIS to powerfully manipulate the selec-tion of information its adherents can access.**

#### **ISIS has turned to recruiting from refugee and prison camps where there is no internet - OCOs can’t do anything**

Huber 11/6/19 <https://thehill.com/opinion/international/469319-the-fate-of-vulnerable-refugees-as-isis-evolves>

**With this certainty, ISIS’ propaganda and recruiting techniques will likewise find currency with vulnerable refugee populations caught up in Syria’s war-torn landscape**. The United Nations Office of Drugs and Crime (UNODC) recently held a workshop in Beirut that highlighted **newly emerging security risks posed by refugee camps and millions of Syrians displaced by that conflict.**

Discussions highlighted terrorism concerns emanating from the ISIS prison camps and ISIS family camps at al-Hol (which were informed by a previous article we had written about the situation there). Tens of thousands of people face a fight-or-flight response to a life-threatening situation. A reported 200,000 additional Syrians have been displaced since Turkey invaded Syria less than a month ago.

**Lebanon is also struggling with refugees and the potential prospect of an ISIS influence within these vulnerable populations.** Refugees make up a quarter (1.5 million) of Lebanon’s population (approximately six million). The ungoverned spaces, such as Afghanistan and Pakistan, that once facilitated the recruitment and training of terror organizations like al Qaeda and ISIS are largely less available. **Refugee camps like those in Lebanon present an appealing haven for terrorist organizations to exploit.**

[CSIS 19](https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents) (YZ)

**March 2019: The Australian Signals Directorate revealed that it had conducted cyber attacks against ISIS targets in the Middle East to disrupt their communications in coordination with coalition forces.**

[Bloomberg Fortune 4-12-18](https://fortune.com/2018/04/12/uk-isis-cyberattack/)

**Britain carried out its first major cyber-attack in 2017, disrupting ISIS’s communications and propaganda infrastructure for much of the year, one of Britain’s intelligence chiefs has revealed.**

Jeremy Fleming, the director of GCHQ, which is better known for its communications interception work, said his agency had worked with the Ministry of Defence to make “a significant contribution to coalition efforts” against the al-Qaeda splinter group. **He said that as well as making it “almost impossible” for the group to spread its message, the attack had protected forces on the battlefield.**

[Brookings 11-13-15 of Foriegn Policy](https://foreignpolicy.com/2015/11/13/anonymous-hackers-islamic-state-isis-chan-online-war/) (YZ)

For more than a year, a**ragtag collection of casual volunteers, seasoned coders, and professional trolls has waged an online war against the Islamic State and its virtual supporters. Many in this anti-Islamic State army identify with the infamous hacking collective Anonymous.** They are based around the world and hail from every walk of life. They have virtually nothing in common except a passion for computers and a feeling that, with its torrent of viral-engineered propaganda and [concerted online recruiting](http://www.nytimes.com/2015/06/28/world/americas/isis-online-recruiting-american.html?_r=0), the Islamic State has trespassed in their domain. **The hacktivists have vowed to fight back.**

The effort has ebbed and flowed, but the past nine months have seen a significant increase in both the frequency and visibility of online attacks against the Islamic State. **To date, hacktivists claim to have dismantled some 149 Islamic State-linked websites and flagged roughly 101,000 Twitter accounts and 5,900 propaganda videos**. At the same time, this casual association of volunteers has morphed into a new sort of organization, postured to combat the Islamic State in both the Twitter “[town square](http://www.bloomberg.com/bw/articles/2012-11-28/dick-costolo-twitter-is-a-reinvention-of-the-town-square-but-with-tv)” and the bowels of the [deep web](http://www.cnn.com/2015/05/12/politics/pentagon-isis-dark-web-google-internet/).

[Nakashima (WaPo) 2017](https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html) (DS)

**U.S. intelligence officers**, in contrast, **concluded** about a month into the campaign **that the impact on the Islamic State was short-lived at best as the group either restored the content or moved it to new servers**, current and former officials said.

Rita Katz, director of SITE Intelligence Group, said the group’s primary means to release propaganda is on the encrypted messaging app, Telegram, through a channel called Nashir, which has suffered no significant disruptions in the past six months. **“ISIS media isn’t something you can just shut off or directly disrupt**,” she said. “**The group and its network of supporters are too adaptive and persistent, and they’ll adjust to any attempts to do so.”**

US alone is pretty ineffective in cyber-oping ISIS due to bureaucracy issues. Pull out wouldn’t change much.

Ash [Carter Oct 17 (former US Sec of Defense) of Belfer Center](https://www.belfercenter.org/LastingDefeat) (YZ)

No U.S. adversary had ever made the Internet such an important part of its operations. ISIS communicated via secure Internet messaging; it recruited new members via social media; it spread its hateful ideology online; and it used the Internet to inspire or direct attacks on the U.S. and Europe. I acknowledged in congressional testimony in May 2016 that I had directed U.S. Cyber Command to initiate offensive cyber operations against ISIS—a first for the U.S. military**. Our goal, I said, was to disrupt ISIS finances, recruiting and propaganda**. “In the modern world,” I said to the Senate Armed Services Committee, “that’s necessary to defeat an enemy, and we’ve got to use every tool that we have.”12 Nearly all the details of those operations remain classified. **I was largely disappointed in Cyber Command’s effectiveness against ISIS. It never really produced any effective cyber weapons or techniques. When CYBERCOM did produce something useful, the intelligence community tended to delay or try to prevent its use, claiming cyber operations would hinder intelligence collection.** This would be understandable if we had been getting a steady stream of actionable intel, but we weren’t. **The State Department, for its part, was unable to cut through the thicket of diplomatic issues involved in working through the host of foreign services that constitute the Internet. In short, none of our agencies showed very well in the cyber fight.** One exception was an international effort to combat ISIS’s hateful online presence with counter-messaging, an effort that did achieve significant reach and had a real impact.

[Byers 17 of Foriegn Affairs](https://www.foreignaffairs.com/articles/middle-east/2017-05-05/winning-cyberwar-against-isis) (YZ)

Yet **U.S. efforts to monitor ISIS’ use of social media—and counter its online propaganda—have thus far been** [**tentative, hesitant, and amateurish**](https://www.foreignaffairs.com/articles/middle-east/2017-04-07/how-fight-isis-online)**. Responsibility for countermessaging has shifted among various organizations**, including the State Department’s Center for Strategic Counterterrorism Communications and the military’s Central Command (CENTCOM) WebOps team.

## A2: NK Prolif

1. [Barnes NYT 6-19] The effects of cyberattacks can be reversed given time/work - NK always restores ability to launch missiles after US OCOs
2. [Melendez 17]
	1. Limited intelligence bc closed off from the rest of the world
	2. North Korea has dozens of missile launch sites (some of them hidden), which means its unlikely for the US to be able to disable every single one of them to prevent launches.
	3. They can literally just work around a lot of the hacks
3. [Greenberg 19]
	1. Vast majority of infra disconnected - nothing to hack
	2. Missile Systems are likely not connected to the internet/intranet - can’t be hacked
	3. qualifies that because of this, hacking North Korea’s nuclear capabilities would be nearly impossible
4. [Sanger 3-17 NYT] US doesn’t have the ability to effectively counter NK nuke/missile program
5. Kim won’t attack
6. [Belfer Center 2017] Kim is rational actor [Bell CBC 16] any aggressive action will lead to its own destruction since [Bando Cato 09] US Naval/Air forces can instantly take it down
7. [Mckinney 38 North 2017] Kim nuke dev is used to compel concession, not attack

[Barnes 6-22-19 NYT](https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html)

The effect of Thursday’s cyberattack is almost certain to be temporary. **Computer networks taken offline can, with work, be restored to regular operations.** Such attacks are most effective when done in coordination with other actions, and at best they will set back — but not eliminate — an adversary’s military abilities. The Iranian intelligence operatives will be able to restore their computer systems, just as the Internet Research Agency restored its network after the midterm election operation.

**American cyberattacks on North Korea’s missile program may have contributed to a series of launch failures. But even if those attacks were successful, Pyongyang eventually restored the ability to test-launch the country’s long-range missiles.**

[Sanger 3-4-17 NYT](https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html?module=inline)

**An examination of the Pentagon’s disruption effort,** based on interviews with officials of the Obama and Trump administrations as well as a review of extensive but obscure public records,**found that the United States still does not have the ability to effectively counter the North Korean nuclear and missile programs**. **Those threats are far more resilient than many experts thought,** The New York Times’s reporting found, and pose such a danger that Mr. Obama, as he left office, warned President Trump they were likely to be the most urgent problem he would confront.

## A2: Arms Race

1. [Olejnik CFR 4-19] more and more people getting cyber capabilities - incentive always exists even w/out US

[Olejnik](https://www.cfr.org/blog/global-consequences-escalating-us-russia-cyber-conflict) of the Council on Foreign Relations 4-2-2019 (RL)

**The number of potential cyber conflict participants continues to increase, with dozens of countries globally building military cyber capabilities.** In conventional military operations, armed forces in close proximity are often at an increased risk of escalatory events, like Russian involvement in Eastern Ukraine or the recent events on the Indian and Pakistani border. **The concept of borders and distance does not really exist in cyberspace; dozens of armed forces are constantly within the virtual arm’s length, creating a constant possibility of interaction and escalation.** Additionally, despite the meticulous preparation and execution of cyber operations,**the situation can quickly spin out of control in a manner difficult to predict. The further militarization of the internet might lead to an increased escalation risk.**

## A2: Deterrence

1. NU/[Jensen CATO 1-19] Vast majority of retal to OCO happens in non-cyber areas like individual sanctions - if deterence exists it will always exist
	1. [Lewis CSIS Jan 18] Fear of retal in the form of armed conflict deters cyberattacks - incentive not to attack always exists
	2. [Wharton 7-18] Defence alone can deter - if the cost to create a successful cyberattack is too high, countries won’t bother
2. T/[Klare ACA 12-18] Cyber attacks destroy out early-warning and communication technology, pressuring countries to act immediately
	1. [Lin SSQ 12] Lack of information means leaders resort to worst-case view - unnecessary escalation/response
3. T/[Valeriano 1-15-19 CATO] Even if deterrence worked in the past, new policy changes by Trump risk OCO’s crossing the threshold. Offence creates fear, suspicion, and misperception - risks offensive retal
4. DL/[Schneider WPo 10-19] Cyber fails at deterrence:
	1. Hard to detect cyber attack - usually just masked as systems failures
	2. Hard to attribute source
	3. Not long term threat - can be patched after first attack
	4. Because of a)-c), U.S. public won’t support and lawmakers won’t pass retal measures, meaning deterrence threat is nonexistent
5. DL[Volz 7-19 WSJ] Russia/Iran have launched 800 cyberattacks in the past year, gearing up to disrupt 2020 elections - deterrence clearly not working

[Volz July 17, 2019 WSJ](https://www.wsj.com/articles/russia-iran-north-korea-launch-hundreds-of-cyberattacks-on-u-s-political-groups-microsoft-says-11563397201)

**Suspected nation-state hackers from Russia, Iran and elsewhere have launched nearly 800 cyberattacks against political organizations over the past year**that have been detected by Microsoft Corp. , with the vast majority of the attempts targeting groups based in the U.S.

Think tanks and nongovernmental groups that work with candidates or political parties—or on issues important to their campaigns—have suffered most of the attacks. The assaults could be a precursor to direct attacks on campaigns and election systems, a trend in recent election cycles in the U.S. and Europe, Microsoft said Wednesday.

**The findings are the latest indication that foreign governments are laying the groundwork ahead of the 2020 presidential election to potentially disrupt American politics,** as senior U.S. intelligence officials have repeatedly warned.

[Valeriano 1-15-19 CATO](https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint)

**We demonstrate that, while cyber operations to date have not been escalatory or particularly effective in achieving decisive outcomes, recent policy changes and strategy pronouncements by the Trump administration increase the risk of escalation while doing nothing to make cyber operations more effective.** These changes revolve around a dangerous myth: offense is an effective and easy way to stop rival states from hacking America. New policies for authorizing preemptive offensive cyber strategies risk crossing a threshold and changing the rules of the game.

It is thus not surprising that given the limited objectives of most cyber operations, to date rival states have tended to respond proportionally or not at all. Returning to the data, between 2000 and 2016, only 89 operations (32.72 percent) saw a retaliatory cyber response within one year. Of those, 54 (60.7 percent) were at a low-level response severity (e.g., website defacements, limited denial of service attacks, etc.). Table 1 in the appendix compares the severity scores for cyber operations between rival states between 2000 and 2016.37 When rival states do retaliate, the responses tend to be proportional: that is, they tend to match the severity of the initial attack.38

Contrary to observed patterns of limited disruption and espionage, Cyber Command sees cyberspace as a domain fraught with increasing risk, where great powers such as China and Russia will undermine American power. The only solution, from this perspective, is to go on the offense.**Yet, the benefits of an offensive posture, especially in cyberspace, are mostly illusory to date. Instead, the cyber domain tends to be optimized for defense and deception, not decisive offensive blows. Not only is offense likely the weaker form of competition in cyberspace, it also risks inadvertent escalation. The fear, suspicion, and misperception that characterize interstate rivalries exacerbate the risk of offensive action in cyberspace.**

[Sanger](https://www.nytimes.com/2019/09/23/world/middleeast/iran-cyberattack-us.html) from the NYT 9-23-2019 (LY)

The Pentagon and other military officials have told the White House that **neither another cyberattack nor the new deployment announced Friday will likely prove robust enough to re-establish deterrence and prevent another attack by Iran on United States allies.**

Part of the problem is that most cyberactivity is clandestine, so it is easy for a government to play down the consequences of an attack or deny it even took place.

But some people who favor stepping up cyberoperations suggest that officials are simply thinking too small. **If a cyberstrike is damaging enough** — taking a refinery offline or shutting down an electric grid, for example — it would be hard to hide. That might have a much more deterrent effect than the smaller bore operations the United States has undertaken so far, they argue.

But **such a devastating cyberoperation would also increase the risk of escalation** — just as a bombing run on the oil refineries would. Iran, or any other adversary, could claim that people were killed or injured, and that might be difficult to disprove.

**A key element of deterrence is ensuring that an adversary understands the other side’s basic capabilities.** Unlike nuclear weapons, though, which are widely understood, **the American cyberarsenal is shrouded in secrecy**, for fear adversaries will develop counter measures if even basic capabilities are known.

Jul 19, 2018, 7-19-2018, "Can Anything Stop Cyber Attacks?," Knowledge@Wharton, <https://knowledge.wharton.upenn.edu/article/creating-tougher-defenses-cyber-attacks/>

The recent indictment of 12 Russian intelligence officers by the Justice Department for interfering in the 2016 U.S. presidential election underscores the severity and immense reach of cyber attacks, like no other in history. To influence the election’s outcome, authorities said these agents hacked into the computer networks of the Democratic Party to get information, and strategically released it on the internet. In the private sector, companies have to step up their game against cyber attacks that are becoming all too common. Against that backdrop, fighting cyber threats has never been more important. It is the “greatest terror on the economy, bar none,” but policy makers’ response to it has been moving at a snail’s pace, according to high-ranking cyber-security and risk management experts who spoke at a panel discussion on cyber risks at the Penn Wharton Budget Model’s first Spring Policy Forum, which was held last month in Washington. **Experts called for greater awareness of cyber threats at all levels, an inclusive approach to protect all parties affected, and steps to “harden our defenses to make the cost too high for the payoff to carry out these cyber attacks.”** Russia is at the top of the list of sophisticated cyber adversaries faced by the U.S., a group that also includes Iran, China and North Korea, according to Matthew Olsen, co-founder and president of IronNet Cybersecurity and former director of The National Counterterrorism Center. “Russia has made information conflict a critical and central pillar of its national security strategy,” he said. “Cyber is a means of carrying out their geopolitical strategy.” And Olsen believes such political meddling will continue. There is “every reason” for Russia to interfere in the 2018 and 2020 elections as well, he warned, and “with even more fervor and more effort.”

[Schneider WP Oct 1 19](https://www.washingtonpost.com/politics/2019/10/01/are-cyber-operations-us-retaliatory-option-september-oilfield-strikes-would-this-deter-iran/)

<https://outline.com/hGKjrd>

**As** [**other scholars have noted**](https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-13_Issue-3/Borghard.pdf)**, the best deterrence signals are ones that are costly, visible and credible. Here’s why cyber-operations often fail this test: They may be hard to detect, hard to attribute to their source and hard to turn into a credible threat, because they may rely on vulnerabilities that are easy to plug if the target knows about them. This all makes cyber-operations less escalatory, but also harder to use to send clear signals.**

**Moreover, as Sanger and Barnes note, the United States is in a particularly vulnerable position when it uses cyberattacks, because the U.S. way of life is more** [**dependent on digitally dependent technologies**](https://www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned-fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies) **than Iranian society. So if Iran retaliates to a cyberattack with another cyberattack, the United States may come off worse. Furthermore, the United States depends more on the global communications infrastructure than Iran does, generating further vulnerabilities that might deter America from using cyberattacks.**

[Recent work](https://academic.oup.com/cybersecurity/article/5/1/tyz007/5575971?guestAccessKey=3ee385bd-8909-4200-a638-ce59ba1d927a) by myself and Sarah Kreps finds that **the American public is less likely to support retaliation against cyberattacks than against an airstrike, even when they create similar effects. U.S. government security decision-makers seem to feel the same way.** Research by [Brandon Valeriano and Benjamin Jensen](https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint), as well as [evaluation of strategic war games](https://pacs.einaudi.cornell.edu/sites/pacs/files/Schneider.Cyber%20and%20Crisis%20Escalation%20Insights%20from%20Wargaming%20Schneider%20for%20Cornell.10-12-17.pdf), **finds that players are less likely to respond to a crisis by escalating when they are given cyber-tools — and less likely to respond with violent escalation when the adversary conducts a cyberattack.**

[Klare 12-18](https://www.armscontrol.org/act/2018-12/features/challenges-emerging-technologies) (AK)

Even more worrisome, some of the weapons now in development, such as unmanned anti-submarine wolfpacks and the TBG system, could theoretically endanger the current equilibrium in nuclear relations among the major powers, which rests on the threat of assured retaliation by invulnerable second-strike forces, by opening or seeming to open various first-strike options. **Warfare in cyberspace could** also **threaten nuclear stability by exposing critical early-warning and communications systems to paralyzing attacks and prompting anxious leaders to authorize the early launch of nuclear weapons.** These are only some of the challenges to global security and arms control that are likely to be posed by the weaponization of new technologies. Observers of these developments, including many who have studied them closely, warn that the development and weaponization of AI and other emerging technologies is occurring faster than efforts to understand their impacts or devise appropriate safeguards.

[Lin Fall Strategic Studies Quarterly 12](https://www.jstor.org/stable/pdf/26267261.pdf?refreqid=excelsior%3A5b47d7d7f663abad97021cba14d060ba) (MM)

In many kinds of cyber attack, the magnitude of the impact of the first attack will be uncertain at first and may remain so for a considerable period of time. **Decision makers may then be caught between two challenges—a policy need to respond quickly and the technical fact that it may be necessary to wait until more information about impact and damage can be obtained.** These tensions are especially challenging in the context of active defense and active threat neutralization. **Decision makers often feel intense pressure to “do something” immediately after the onset of a crisis**, **and** sometimes such pressure is warranted by the facts and circumstances of the situation. On the other hand, **the lack of immediate information may prompt decision makers to take a worst-case view of the attack** and, thus, to assume that the worst that might happen was indeed what actually happened. **Such a situation has obvious potential for inappropriate and unintended escalation or kinetic response.**

[Jenson 1-15-19 of CATO](https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint)

It is thus not surprising that **given the limited objectives of most cyber operations, to date rival states have tended to respond proportionally or not at all**. Returning to the data, **between 2000 and 2016, only 89 operations (32.72 percent) saw a retaliatory cyber response within one year. Of those, 54 (60.7 percent) were at a low-level response severity** (e.g., website defacements, limited denial of service attacks, etc.). Table 1 in the appendix compares the severity scores for cyber operations between rival states between 2000 and 2016.37 **When rival states do retaliate, the responses tend to be proportional**: that is, they tend to match the severity of the initial attack.38

Low-level responses beget low-level counter­responses as states constantly engage in a limited manner consistent with the ebbs and flows of what famed Cold War nuclear theorist Herman Kahn called “subcrisis maneuvering.”39 Rarely does a response include an increase in severity. **Instead, we witness counterresponses of a similar or lower level than the original intrusion or a response outside the cyber domain (for example, economic sanctions or legal indictment of specific individuals). The engagement is persistent but managed, and often occurs beneath an escalatory threshold.**40 As seen in Table 2 in the appendix, this behavior appears to apply equally to each possible cyber strategy: disruption, espionage, and degradation. **Espionage saw little retaliatory escalation, while disruption and degradation both exhibited more low-level responses.**

## A2: China/IP

1. [Bunch AAM 9-18] China responsible for 90% of cyber econ espionage against US - Aff clearly aint solving
2. [Demchak 4-26-19 BAS] China is chasing global dominance in cyber
	1. [SACKS 6-18 Atlantic] Xi’s vision to define global cyber norms - involves giving China access to all the data/tech - meaning that IP theft is literally part of China’s future econ vision - nothing changes that

[Bunch SEPTEMBER 6, 2018 AAM](https://americanmanufacturing.org/blog/entry/chinas-cyber-espionage-continues-and-theres-a-big-cost)

It’s not a secret that **China is engaging in massive cyber espionage against the United** States, and a new report from the Foundation for Defense of Democracies highlights some of the consequences.

**The findings are astounding. China is responsible for 50 to 80 percent of cross-border intellectual property theft worldwide, and more than 90 percent of all cyber-enabled economic espionage in the United States.**

The foundation also notes that China has “demonstrated a willingness to use cyber attacks as a tool of economic coercion to pressure governments and private companies to change their policies.”

[Demchak 4-26-19 Bulletin of the Atomic Scientists](https://www.tandfonline.com/doi/abs/10.1080/00963402.2019.1604857?journalCode=rbul20)

China: Determined to dominate cyberspace and AI

**China is chasing dominance in emerging artificial intelligence (AI) technologies in both the private and military sectors, as a central part of its effort to be the leading global cyber power.** The rise of AI – a subset of cyber as are machine learning, quantum computing, and other new technologies – does not herald a new arms race equivalent to that of the Cold War. Rather, the concern should be on the profound disruption to the existing westernized global order. This piece reviews how the 1990s westernized national creation called cyberspace created so many ubiquitous, embedded vulnerabilities whose easy exploitation directly accelerated the rise of an otherwise impoverished authoritarian and aggressive China. Today no single democracy has the scale and sufficient resources to alone match the foreknowledge and strategic coherence of the newly confident and assertive China. To change current global trends, the small group of consolidated democratic civil societies needs a collective approach to counter China’s growing dominance across all fields of cyberspace. The piece ends describing the Cyber Operational Resilience Alliance (CORA) to provide the public and private scale and collective strategic coherence required to ensure the future wellbeing and security of democracy in an overwhelmingly authoritarian, post-western, cybered world.

[SAMM SACKS JUNE 18, 2018 Atlantic](https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/)

Beijing Wants to Rewrite the Rules of the Internet. In late April, just days after the Commerce Department announced the denial order against ZTE, **Xi Jinping, the president of China, gave a major speech laying out his vision to turn his country into a “cyber superpower.**” His speech, along with other statements and policies he has made since assuming power, outlines his government’s ambition not just for independence from foreign technology, but **its mission to write the rules for global cyber governance—rules that look very different from those of market economies of the West. This alternative would include technical standards requiring foreign companies to build versions of their products compliant with Chinese standards, and pressure to comply with government surveillance policies. It would require data to be stored on servers in-country** and restrict transfer of data outside China without government permission. It would also permit government agencies and critical infrastructure systems to source only from local suppliers.

<https://www.newsweek.com/china-using-cyber-espionage-gain-military-and-technology-advantages-over-us-1108162>

**China is using its vast cyberespionage capabilities to steal intellectual property from U.S. businesses, gain the upper hand in economic negotiations, and put pressure on foreign governments, according to the report. These activities have allowed China to advance rapidly, overtake the U.S. in certain key industries** and even gain some military advantages. "For China, there are levels of economic and industrial espionage. There's also the technique of gaining access to non-public knowledge and using that to their benefit in trade negotiations. We've seen this in Alaska," Priscilla Moriuchi, director of strategic threat development at Massachusetts-based tech company Recorded Future and former threat manager for East Asia and Pacific at the National Security Agency (NSA), told Newsweek. **"After a company makes overtures to China, about a joint venture or investment, you would see hackers targeting the server or executive to see what they thought of the meeting."**

## A2: Checkback Iran Aggression

1. Alt deterrence check backs iran aggression
	1. [Yee 5-12-19] U.S. ended waivers that allowed countries to buy Iran oil
	2. Sent warships/bombers to persian gulf
	3. Declare Iran mili as terror orgs
	4. Sanctions on all the shit
	5. [Nakashima 6-19] U.S. mili can sink every vessel in Strait of Hormuz in 24 hours - that's why Iran never aggresses in the past, even when U.S. didnt use cyber capabilities
	6. [Reuters 11-7-19] Prob a 1 time thing - US leading naval coalition in the Gulf and opening command centers in Bahrain to counter Iran oil tankers aggression
2. Cyber deterrence fails
	1. DL/[Barnes 6-22-19 NYT] Cyberattacks are short term/temp, easily restored
3. TURN/[Sanger NYT 9-23-19] Pentagon has said that their cyberattacks won’t provide enough of a deterrent to prevent Iran attacks - as they increase in power, it just risks escalation from Iran
4. TURN [Cockerill 9-7-19 Gasworld] Routine Cyberattacks remove norm of cyber restraint - increase instability/violence in Middle East
5. TURN[Sen 3-15 Atlantic Council] Iran’s budget for cyber has increased 1200% in 3 years bc of US cyber attacks on Iran like Stuxnet - us oco enable cyber spending and conflict
6. **US never mili strike**
	1. [Meierding FP 9-18-19] Strikes on iran raise oil prices, undermine Trump's election chances
	2. [Pollack 5-19] Trump goal is to end American involvement in wars in the Middle East - thats why he pulled troops from Syria
	3. [Ioanes Business Insider 6-19] Trump uncomfortable with mili escalation (literally ran on anti-intervention policies), the dialogue is just empty rhetoric - twitter diplo
7. **Saudi never mili strike**
	1. [Meierding FP 9-18-19] Escalating conflict destroys oil revenue, needed for econ diversification and general revenue (probably the most important thing for SA)
8. **A2 Alt/Minutes away**
	1. [Marks WPo 7-25-19] Trump also used sanctions as a replacement - cyber isn't a uq alt
	2. T/ [Barnes NYT 8-19] Cyber retal has created a back and forth endless round of cyberattacks - that would’ve been avoided with a calculated non-lethal mili strike that doesn't risk casualties

[**Pollack**](https://www.foxnews.com/opinion/kenneth-pollack-iran-war-united-states-trump-truth) **5/16/19 Fox**

resident scholar of the American Enterprise Institute where he works on Middle Eastern political-military affairs. Before joining AEI, Dr. Pollack was affiliated with the Brookings Institution, where he was a senior fellow at the Center for Middle East Policy.

**Is the United States going to war with**[**Iran**](https://www.foxnews.com/category/world/conflicts/iran)**? Probably not.** Should the United States go to war with[Iran](https://www.foxnews.com/category/world/conflicts/iran)? Probably not. Now that that’s out of the way, we can unpack the current tensions with Iran, where they are likely to lead, and the potential pitfalls the[United States](https://www.foxnews.com/us)should avoid on the road ahead. **It is unlikely that we will find ourselves in a war with Iran in the near term because both sides are eager to avoid one.** **Although some of President Trump’s advisors may welcome a clash with Tehran, he has consistently made clear that he wants to end American wars in the Middle East, not start new ones. That has been behind his impetus to pull U.S. troops out of Syria** and his unwillingness to become further involved in the Yemeni civil war.

[Sanger](https://www.nytimes.com/2019/09/23/world/middleeast/iran-cyberattack-us.html) from the NYT Sept. 23, 2019 (LY)

The Pentagon and other military officials have told the White House that **neither another cyberattack nor the new deployment announced Friday will likely prove robust enough to re-establish deterrence and prevent another attack by Iran on United States allies.**

Part of the problem is that most cyberactivity is clandestine, so it is easy for a government to play down the consequences of an attack or deny it even took place.

But some people who favor stepping up cyberoperations suggest that officials are simply thinking too small. **If a cyberstrike is damaging enough** — taking a refinery offline or shutting down an electric grid, for example — it would be hard to hide. That might have a much more deterrent effect than the smaller bore operations the United States has undertaken so far, they argue.

But **such a devastating cyberoperation would also increase the risk of escalation** — just as a bombing run on the oil refineries would. Iran, or any other adversary, could claim that people were killed or injured, and that might be difficult to disprove.

**A key element of deterrence is ensuring that an adversary understands the other side’s basic capabilities.** Unlike nuclear weapons, though, which are widely understood, **the American cyberarsenal is shrouded in secrecy**, for fear adversaries will develop counter measures if even basic capabilities are known.

[Sen of the Atlantic Council 4-10-15](https://www.atlanticcouncil.org/blogs/new-atlanticist/iran-s-growing-cyber-capabilities-in-a-post-stuxnet-era/)

Iran has vastly ramped up its cyber capabilities transforming itself from a “Tier 3” country to one that poses a significant global threat in the years following a massive cyber attack on its nuclear facilities, panelists said at the Atlantic Council April 8.

“Iran is definitely not a Tier 3 country any more,” said Andretta Towner, Senior Intelligence Analyst at CrowdStrike, a provider of security technology. **Over the past three years, Iran’s budget for cyber security has increased 1,200 percent,** said Towner.

“They’re building this up as they would any other capability, but it seems that when we look forward we want to know are they building it up specifically to use it or are they just building this up in case they need it,” she added.

**Iran’s focus on cyber security appears to have been driven, at least in part, by a massive cyber attack on its nuclear facilities five years ago.** In 2010, [the United States and Israel used the Stuxnet computer virus](https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html) to disable centrifuges Iran was using to enrich uranium at its facility in Natan

<https://outline.com/TDVcyG>

[Barnes](https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html)  NYT 8-28-19

**On the other hand, the Trump administration could have reduced the likelihood of retaliatory cyberattacks by instead opting for a smaller conventional attack that didn’t risk casualties,** Michael Morell, a former acting CIA director, told me in an email.

**“It would have sent the strongest message possible without creating escalation risk and it would not have created the potential for endless rounds of cyberattacks,**” said Morell, who hosts the Intelligence Matters podcast.

[Barnes 6-22-19 NYT](https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html)

The **effect of** Thursday’s **cyberattack is almost certain to be temporary. Computer networks taken offline can, with work, be restored to regular operations.**

Such attacks are most effective when done in coordination with other actions, and at best they will set back — but not eliminate — an adversary’s military abilities. **The Iranian intelligence operatives will be able to restore their computer systems, just as the Internet Research Agency restored its network after the midterm election operation.**

[Marks WPo 7-25-19](https://outline.com/FzELyH)

The situation is especially precarious because President Trump said he was within minutes of launching a conventional attack against Iran after it downed a U.S. surveillance drone, but pulled back after learning that as many as 150 people might be killed. **Trump opted instead for** **a digital strike aimed at disabling systems controlling Iranian missile and rocket launchers and a new round of sanctions.**

[Cockerill 9-7-19 Gasworld](https://www.gasworld.com/mena-series-cybersecurity-and-the-geopolitical-balance/2018034.article)

“However, all of the players involved have an incentive to use cyber attacks judiciously,” she adds. “Part of the reason for this **is that if the use of cyber attacks becomes more routine, we risk normalising this activity and losing the element of restraint that has generally prevailed between nations in times of high tension to date. Such a change would ratchet up the already large threat that instability and violence in the Middle East pose to Western businesses and infrastructure.”**

 [Ellen Ioanes BUsiness Insider Jun 21, 2019](https://www.businessinsider.com/trump-iran-strike-civilian-death-toll-10-minutes-nsc-2019-6?r=US&IR=T)

Ryan Goodman, the former special counsel to the Department of Defense under Obama, tweeted that Trump's story "doesn't add up." "Is Trump suggesting the Pentagon brought him a plan without having those figures?" he tweeted, referring to casualty estimates. "I don't believe that anyone told him that 150 people were going to die — it's too precise a number," Daalder said, telling INSIDER he thought that casualty estimates would have come up in the process.

**Daalder said Trump has been uncomfortable with recent military escalation, repeatedly signaling that he doesn't want to go to war with Iran.**

**"I just think he stepped back. That is his pattern. He speaks loudly and carries a small stick," Daalder said. "The fact that he actually constructed that entire tweet thread suggests that he was trying to create a new narrative."**

[EMILY MEIERDING | SEPTEMBER 18, 2019](https://foreignpolicy.com/2019/09/18/the-real-reason-trump-wont-attack-iran-saudi/)

**An escalating conflict in the Persian Gulf would jeopardize many states’ energy interests. Saudi Arabia would be hit on multiple fronts from an intensified Gulf conflict**. Its oil installations would incur additional physical damage, and **the state would lose more resource revenue** from suspended oil sales. More importantly, **state oil company Saudi Aramco’s reputation as a reliable oil supplier would take another severe hit.**

Saudi officials have already been scrambling to restore confidence in the national oil company after this weekend’s attacks. Saudi Aramco’s CEO, Amin Nasser, announced on Tuesday that Abqaiq’s output will be restored by the end of the month and that the company’s long-anticipated initial public offering (IPO) will proceed as planned. However, skepticism is rampant, and any additional disruptions will wreak havoc on the company’s valuation, as well as on Saudi leader Mohammed bin Salman’s plans to use IPO proceeds to finance his country’s economic diversification. **Fear of further instability limits Riyadh’s room for maneuver. As Robin Mills of Qamar Energy observed, “It will be all but impossible to proceed with the IPO if there are ongoing attacks.”**

Iran is widely assumed to be responsible for last weekend’s bombardment in Saudi Arabia, in which drone and missile attacks struck two critical Saudi oil facilities, cutting the country’s oil production by 5.7 million barrels per day and reducing global oil supplies by 5 percent. If the Trump administration decides to retaliate militarily for these attacks, the ensuing confrontation would likely to be labeled another U.S. oil war in the Middle East.

**This would be a serious mischaracterization, however. In this case, oil interests are far more likely to prevent war than provoke it.**

A war in the Persian Gulf would profoundly destabilize the global oil system. I**f the Trump administration strikes Iran, unilaterally or in conjunction with Saudi Arabia, and targets the state’s oil facilities, these attacks will take more resources offline**. Although Iran’s oil output has declined significantly since the United States reimposed sanctions in 2018, the country still produces more than 2 million barrels of oil per day and exports about half a million barrels per day of petroleum products and liquefied petroleum gas to a variety of resource consumers. Airstrikes would remove these supplies for the market, while other oil producers are struggling to compensate for the loss of Saudi resources.

**However, the Trump administration also has strong incentives to avoid conflict escalation.** Although the United States is now the world’s leading oil producer, as President Donald Trump recently observed, the country is not immune to instability. **The oil market is global, so even if the United States becomes a net oil exporter, it will still be affected by rising oil prices**. U.S. refineries will pay more for crude, regardless of where it originates. And when they pass this price hike on to their customers, Americans pay more at the pump. Rising gasoline prices are never popular. **However, they are especially dangerous in an election year. The hit to American pocketbooks could immediately undermine support for Trump’s reelection**. Persistently elevated oil prices could push the country into recession, further harming his prospects.

<https://www.fifthdomain.com/thought-leadership/2019/10/23/what-will-be-the-effect-of-the-latest-us-cyberattack-on-iran/>

**Even some of the most prominent examples of offensive U.S. cyber operations are not clear successes.** For example, Jon Lindsay and Ivanka Barzashka have called into question the success of the Stuxnet operation, arguing that it was not merely ineffective in achieving its goals but may even have been counterproductive. Jason Healey concurred, **arguing that unmatched U.S. offensive cyber capabilities have not deterred adversaries like Iran “but, instead, has done the opposite. Iran became a far more serious cyber threat after Stuxnet.”**

month

<https://www.nytimes.com/reuters/2019/11/07/world/middleeast/07reuters-usa-gulf-iran.html>

Nov 7, 2019

**DUBAI — The U.S.-led naval coalition in the Gulf, established in response to a series of attacks on oil tankers, opened a command center in Bahrain on Thursday, the U.S. Fifth Fleet said in a statement.**

<https://www.japantimes.co.jp/opinion/2019/06/14/commentary/world-commentary/irans-gulf-aggression-can-stopped-without-war/>

**In response, the U.S. military is exploring options to deter Iran, which is thought to be behind the tanker attacks. This has included increasing the level of operational readiness of U.S. troops throughout the region; deploying long-range B-52 bombers and F-15 fighters to the U.S. base in Al Udeid, Qatar; sending a carrier strike group, led by the nuclear-powered Abraham Lincoln, into the waters of the Persian Gulf; exploring options to deploy up to 120,000 new troops to the region; and issuing strong statements from the White House promising significant military retaliation if Iran provokes an incident.**

**All of this comes as the United States further pressures the Iranian economy through harsh sanctions, which are having a significant effect.**

By Vivian Yee May 12, 2019

Accessed 10/26/2019. Published 9/16/2019.<https://www.nytimes.com/2019/05/12/world/middleeast/us-iran-sanctions-rouhani.html>.

“We are in a difficult situation today, but at the same time, I am not disappointed,” Mr. Rouhani said, according to the semiofficial ISNA news agency. “I believe that we can overcome these conditions, provided we are together and join hands.” Linking the current financial emergency to one of modern Iran’s defining traumas is a sign of the seriousness of the situation. Since President Trump withdrew from the 2015 nuclear accord, which limited Iran’s capacity to produce nuclear fuel for 15 years, his administration has been steadily escalating sanctions on Iran in hopes of getting a better deal. In recent weeks, it has increased the pressure, ending waivers that had allowed other countries to buy Iran’s oil, sending warships and bombers to the Persian Gulf, declaring Iran’s Islamic Revolutionary Guard Corps a terrorist organization and imposing sanctions on the country’s steel, aluminum, iron and copper industries. Those sectors account for about a tenth of its exports, according to the administration. But analysts on opposing sides of the debate over the Trump administration’s pressure tactics drew differing conclusions from the historical parallel. After nearly eight years of war with Iraq, the Ayatollah Khomeini, who was then Iran’s supreme leader, accepted a United Nations-brokered cease-fire in 1988, despite having vowed to wage war until victory. He likened the agreement to drinking from a “poisoned chalice.” To Behnam Ben Taleblu, a senior fellow at the Foundation for Defense of Democracies, a hawkish Washington think tank that advocates pressuring Iran into submission, that history suggests that Iran will fold if under enough strain. “To say that there are pressures on Iran now that they didn’t have to undergo during the war is a major testament to how effective the sanctions are,” he said. “Iran will double down, triple down, quadruple down, but then ultimately do a 180 if they perceive that there’s no way out.”

**This is my tag (Ellen Nakashima – Washington Post)**

Accessed 10/26/2019. Published 6/22/2019.<https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html>.

The United States in April designated the Revolutionary Guard as a foreign terrorist organization in response to its destabilizing behavior across the Middle East. Iranian cyber forces have tried to hack U.S. naval ships and navigation capabilities in the Persian Gulf region for the past few years. The Strait of Hormuz is a strategically important sea lane through which about one-fifth of the world’s oil passes daily. On Saturday, the Department of Homeland Security issued a warning to U.S. industry that Iran has stepped up its cyber-targeting of critical industries — to include oil, gas and other energy sectors — and government agencies, and has the potential to disrupt or destroy systems. AD “There’s no question that there’s been an increase in Iranian cyber activity,” said Christopher Krebs, director of DHS’s Cybersecurity and Infrastructure Security Agency. “Iranian actors and their proxies are not just your garden variety run-of-the-mill data thieves. These are the guys that come in and they burn the house down. “This operation imposes costs on the growing Iranian cyberthreat, but also serves to defend the United States Navy and shipping operations in the Strait of Hormuz,” said Thomas Bossert, a former senior White House cybersecurity official in the Trump administration. “Our U.S. military has long known that we could sink every IRGC vessel in the strait within 24 hours if necessary. **And this is the modern version of what the U.S. Navy has to do to defend itself at sea and keep international shipping lanes free from Iranian disruption.”** Thursday’s strikes against the Revolutionary Guard represented the first offensive show of force since Cyber Command was elevated to a full combatant command in May. It leveraged new authorities, granted by the president, that have streamlined the approval process for such measures. It is also a reflection of a new Cyber Command strategy — called “defending forward” — that its leader, Gen. Paul Nakasone, has defined as operating “against our enemies on their virtual territory.”

Accessed 10/27/2019. Published 7/18/2019.<https://www.bloomberg.com/news/articles/2019-07-17/iran-says-it-could-close-strait-of-hormuz-but-doesn-t-want-to>.

Iran is capable of shutting the Strait of Hormuz -- a crucial choke-point for oil flows -- but doesn’t want to do it, the country’s foreign minister said. “We certainly have the ability to do it, but we certainly don’t want to do it because the Strait of Hormuz and the Persian Gulf are our lifeline,” Mohammad Javad Zarif said Wednesday in an interview with Bloomberg Television in New York. “It has to be secured. We play a big role in securing it, but it has to be secure for everybody.” For more from the interview, click here About one-third of the world’s seaborne crude and fuels passed through the Strait of Hormuz last year, highlighting its key role in global oil markets. In May and June, six tankers were attacked in the region. While Iran has been blamed for attacks on merchant shipping, it has denied responsibility. “It’s dangerous because it is very crowded,” Zarif said, adding that the last time the area was this crowded, the U.S. shot down an Iranian plane with 290 passengers in 1988. “We feel the danger and that is why we want to avoid a dangerous escalation, but we cannot give up defending our country.”

## A2: State Cyberattacks

1. [Banks WPo 4-18] Cyber attacks are one-use, use it and lose it, since it can be reverse engineered/patched after first attack - only use it in emergency scenarios
2. [Lewis CSIS Jan 18] Fear of retal in the form of armed conflict deters cyberattacks - incentive not to attack always exists
3. [Maness Oxford Press 12-15] Massive cyber attacks unlikely:
	1. Chance of civilian collateral harm - could escalate into conventional war
	2. Most countries don’t have the means for large scale attacks
	3. Cyberattacks can be replicated by the victim once attacked - risk for attacker high
	4. Blowback/retribution cost are too high - retal comes in all forms
4. [Gartzke Lawfare 1-13] Cyberattacks are generally temp/short term, once systems back online, victim can retal - serves no purpose to attack
5. [Jensen 1-15-19] Only 4% of OCO have resulted in political concessions - doesn’t even work

[Valeriano and Jensen 1 - 15 - 19](https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint) (RK)

To date, cyber operations do not appear to produce concessions by themselves. **Offense, whether disruption, espionage, or degradation, does not produce lasting results suffi- cient to change the behavior of a target state**. **Only** 11 operations **(4 percent) appear to have produced even a temporary political concession**, with the majority associated with sustained, multiyear counterespionage operations by U.S. operatives usually targeting China or Russia.

#### **No risk of cyberwar: norm is cooperation/dialogue:**

Valeriano and Maness, Senior Lecturer of Politics at the University of Glasgow, and Visiting Fellow of Security and Resilience Studies at Northeastern University in Boston, respectively, 2015

[Brandon and Ryan C., CYBER WAR VERSUS CYBER REALITIES: CYBER CONFLICT IN THE INTERNATIONAL SYSTEM, Oxford University Press, Kindle edition, 12.16.2015 RGorman]

**Just because something can happen does not mean it will.** We argue that for now and for the foreseeable future, restraint dominates in cyberspace despite the worst-case predictions of prognosticators. States generally react in the international environment in a manner conducive to their interests. Sometimes, however, the security dilemma enters the elite and public discourse and can push states toward overreaction. The fear from perceived threats, such as those in the cyber domain, may influence the foreign policy decisions made by states (Jervis 1979). **While there are counter-examples of the worst practices and failures, the norm is to cooperate and participate in constructive dialogue in the system. Considerations such as collateral damage and escalation usually guard against an unleashing of damaging cyber weapons.** We find that the security dilemma has no place in these international interactions. The cyber world is nebulous; an infiltration against a military facility in this realm could bleed into the public sector. **Malicious cyber incidents on infrastructure have been and will continue to be rare to nonexistent because states are restrained due to the high probability of civilian harm, the nature of the weapons (single use), and the weak payoffs if utilized (Gartzke 2013).** These types of offensive cyber actions are just as unlikely as interstate nuclear or chemical weapons attacks. There is a system of normative restraint in cyber operations based on the conditions of collateral damage, **plus the factors of blowback and replication**. Foreign policy tactics in the cyber world can be replicated and reproduced. **Any cyber weapon used can be turned right back on its initiator. On top of this, it is likely that severe cyber operations will be bring retribution and consequences that many states are not willing to accept**. We have seen many interstate conflicts since the advent of the Internet age, but the largest and only cyber operation thus far during a conventional military conflict, the 2008 Russo-Georgian skirmish, consisted of almost trivial DDoS and vandalism. Since then, Russia has even avoided using cyber weapons during the Crimean and Ukrainian crises larger of 2014. Other operations are mainly propaganda operations or occur in the realm of espionage. **That the United States did not use cyber tactics against Iraq, Afghanistan, or Libya**, at least as directed at the executive level, **signifies that cyber tactics are typically restrained despite significant constituencies in the military that want to use the weapons**. Stuxnet is the outlier, as our data demonstrate, not the norm or the harbinger of the future to come. Cyber operations are limited in that their value is negligible, the consequences of a massive cyber incident are drastic, and the requirements to carry one out are vast. The idea of a lone cyber hacker being able to bring states to their knees is a fantastic one. Cyber operations like Stuxnet require an exceptional amount of funds, technical knowledge, luck, and on-the-ground assets for successful implementation. **Massive and truly dangerous cyber operations are beyond the means of most countries. These statements are not opinions, but contentions made based on the facts at hand and the data we have collected.**

[**https://www.lawfareblog.com/foreign-policy-essay-erik-gartzke-fear-and-war-cyberspace**](https://www.lawfareblog.com/foreign-policy-essay-erik-gartzke-fear-and-war-cyberspace)

**Gartzke 1-1-13**

**The bigger issue, however, is that the effects of internet attacks are temporary.**  Unlike a rocket strike on an oil refinery or demolition of critical elements of the transportation grid, **cyber attacks generally achieve “soft kills,” temporary incapacitation that can be reversed relatively quickly at moderate cost**. Unless it has a lasting effect on the balance of power, internet aggression serves either as an irritant, or as an adjunct to other, more traditional, forms of coercion or force.

Imagine that some unspecified cyber attack disables communication or transportation nodes in a target country. What then? **While inconvenient, the target will eventually get the lights back on and vehicles running. The target will then attempt to retaliate. Permanent harm inflicted over the internet can weaken an opponent and serve as a motive for aggression.** Yet, harm inflicted over the internet, or at Pearl Harbor for that matter, only benefits the attacker if it can extract concessions from the target, or if the attack can be made to permanently weaken an opponent.

Banks, WPO, 4-26-18

<https://outline.com/YTWSbd>

Second, **fears of large-scale cyber operations are likely overblown due to cyber’s unique “use it and lose it” character. Individual cyberattacks could potentially wreak considerable damage, but any such exploits could — once deployed — be quickly reverse-engineered and the vulnerability in target networks patched.**

Here’s the catch: Once you convert network access and cyber espionage into an attack payload, you signal your capabilities and lose the ability to conduct similar attacks. There is a unique shadow of the future in cyber statecraft. States have to assess whether they want to jeopardize an exploit in the short term — and lose long-term coercive options against rivals.

**Measured escalation possible**

**Simon, Oct 12 2017**

[**https://www.csis.org/analysis/raising-consequences-hacking-american-companies**](https://www.csis.org/analysis/raising-consequences-hacking-american-companies)

**Taken together, these variables—nature, duration, and scope—should inform which elements of a sliding scale of potential responses the United States ultimately chooses to employ in defense of U.S. government and U.S. private-sector entities**. The possible response options should not only include digital or kinetic measures, but all the tools at America’s disposal, from economic sanctions to “naming and shaming” perpetrators. **This flexible approach will allow the United States to tailor its response to reflect the severity of any given cyber attack** and to hit the offending country where it is the most vulnerable, **while reducing the possibility for escalation and avoiding categorical issue linkages across domains, such as trade and cyber.**24 **In particular, when responding to cyber hacks on the less intense end of the spectrum, the U.S. response should incorporate reversible and temporary measures directed against our adversaries corresponding in magnitude to the initial attack against the U.S. private sector**. These measures might include, for instance, vigorous bot-takedown efforts that degrade the ability of our foreign adversaries to engage in malicious digital activity.

[Jenson 1-15-19 of CATO](https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint)

It is thus not surprising that **given the limited objectives of most cyber operations, to date rival states have tended to respond proportionally or not at all**. Returning to the data, **between 2000 and 2016, only 89 operations (32.72 percent) saw a retaliatory cyber response within one year. Of those, 54 (60.7 percent) were at a low-level response severity** (e.g., website defacements, limited denial of service attacks, etc.). Table 1 in the appendix compares the severity scores for cyber operations between rival states between 2000 and 2016.37 **When rival states do retaliate, the responses tend to be proportional**: that is, they tend to match the severity of the initial attack.38

Low-level responses beget low-level counter­responses as states constantly engage in a limited manner consistent with the ebbs and flows of what famed Cold War nuclear theorist Herman Kahn called “subcrisis maneuvering.”39 Rarely does a response include an increase in severity. **Instead, we witness counterresponses of a similar or lower level than the original intrusion or a response outside the cyber domain (for example, economic sanctions or legal indictment of specific individuals). The engagement is persistent but managed, and often occurs beneath an escalatory threshold.**40 As seen in Table 2 in the appendix, this behavior appears to apply equally to each possible cyber strategy: disruption, espionage, and degradation. **Espionage saw little retaliatory escalation, while disruption and degradation both exhibited more low-level responses.**

# Impacts

## A2: Cyberwar

1. [Maness Oxford Press 12-15] Massive cyber attacks unlikely:
	1. Fear of blowback/retribution high - not worth it (both cyber and non)
	2. Cyberattacks can be replicated by the victim once attacked - risk for attacker high
	3. Most countries don’t have the means for large scale attacks

## A2: Grids

1. [Wagenseil 3-11-19] Grid Failure unlikely and not a threat:
	1. Power plants use different hardware/software - no single hack to take them all down
		1. Hacks take months/years for specific power plants - no scaled harm
	2. Defence already exists to prevent cyberattacks
	3. Outages resolved in hours/days, not weeks/months
	4. Historical power grid attacks have not even been scalable past a single power plant - Ukraine

Wagenseil 3-11-19

[https://www.tomsguide.com/us/blackout-hack-threat-rsa2019,news-29594.html](https://www.tomsguide.com/us/blackout-hack-threat-rsa2019%2Cnews-29594.html)

"There are lots of misunderstandings about threats to the electric grid," said Selena Larson, an intelligence analyst at Maryland cybersecurity firm Dragos and a former CNN reporter. "**The reality is that a destructive incident at one site would require highly tailored [malware] tools and operations, and would not effectively scale." That's because U.S. power plants use different makes and models of hardware and software, are often at least partly isolated from the internet and from each other, and have already undergone a fair degree of hardening against cyberattacks.** There's very little chance that a single hacker or group of hackers could knock out the power across a large swath of North America at once. But as Dragos founder and CEO Robert M. Lee stated in a 2017 blog posting describing the CrashOverride malware, **"the public must understand that the outages**

**could be in hours or days, not weeks or months."** Lee said that Dragos had "high confidence" that the CrashOverride hackers were the same who had in fact targeted U.S. and European infrastructure companies in 2014. And CrashOverride contained modules to "delete files and processes off of the running systems" to sabotage computer systems. **Larson said, however, that the CrashOverride creators had spent months or years planning the attack, and that the malware was specifically designed for that power plant. The attacks couldn't easily scale across the world, or even across Ukraine. The public should be reassured, she added, that the North American power grid (there are in fact three grids) has always been engineered to limit both the duration and the geographic reach of blackouts, and that there's no single power switch that can turn it all off.**

## A2: Financial

1. [Boghard Air University 19] Financial attacks not a threat
	1. Even the most costly cyberattacks haven’t been harmful enough to be a threat
	2. Recovery happens quickly
	3. Way better than conventional attacks
2. U.S. econ is connected across globe - global recession + dom recession in attacking country not worth it
3. [Chabrow 3-16] Iran DDOS 46 banks repeatedly from 2011-2013, denied access to banks for hundreds of thousands - no system collapse (you prob didnt even hear about it)

[Chabrow 3-24-16 BankInfoSecurity](https://www.bankinfosecurity.com/7-iranians-indicted-for-ddos-attacks-against-us-banks-a-8989)

**The Justice Department has unsealed indictments against seven Iranians - allegedly working on behalf of the Iranian government,** including the Iranian Revolutionary Guard Corps, a branch of Iran's armed forces - who are suspected of conducting distributed denial-of-service attacks against dozens of American banks as well as attempting to seize control of Bowman Dam outside New York City.

**The DDoS attacks started in December 2011 and continued sporadically until September 2012, when they escalated in frequency on a nearly weekly basis, t**ypically between Tuesdays and Thursdays, through May 2013, according to the indictment. The indictment alleges the **hackers** over 176 days **targeted 46 major financial institutions** and corporations - including Bank of America, Capital One, JPMorgan Chase and PNC Banks as well as the New York Stock Exchange and Nasdaq - **leaving hundreds of thousands of customers unable to access their bank accounts**, resulting in tens of millions of dollars being spent by victimized organizations to mitigate and neutralize the attacks. The government said the Iranians also targeted AT&T.

Companies are resilient to economic shocks from cyberattacks AND no lash out

**Borghard 19**—Assistant Professor in the Army Cyber Institute at the United States Military Academy at West Point [Erica D. **Borghard** and Shawn W. Lonergan (Assistant Professor of International Relations in the Department of Social Science at USMA), Fall 2019, “Cyber Operations as Imperfect Tools of Escalation”, Strategic Studies Quarterly, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-13\_Issue-3/Borghard.pdf]

It is also possible to measure the cost of offensive cyberattacks in treasure rather than blood. By this standard, the financial or economic costs of cyberattacks are significant.For example, the most devastating and expensive cyberattack to date—the 2017 NotPetya malware that inflicted widespread economic damage against multinational corporations—reportedly cost Maersk and FedEx $300 million each, and the total cost of the Not-Petya attacks is estimatedto be $10 billion.53 Despite this, **even the most financially costly cyberattacks have thus far failed to invoke“act of war” or “act of force” thresholds.**54 **Targets have also demonstrated a consistent ability to recover even from destructive cyberattacks with relative speed**.In two such cases attributed to North Korea—the 2013South Korean banks’ attack and the 2014 Sony attack—“despite the destruction of files, all are still in business, and none spent more than an inconsequential amount of time recovering.”55 This does not imply that the economic costs of cyber operations are unimportant or lack strategic consequence. However, **particularly when they occur in the absence of physical violence, contextualizing the cost of offensive cyber operations raises doubts about their effects in comparison to other types of offensive military operations.**