# Neg – OCOs 2 – BFHR 7wk

### Notes

Thanks a ton to Chanden Climaco, Brandon Yang, and Marshall Green for their work on this file.

Wave 2 of OCO’s aff/neg builds upon the starter pack OCO’s aff/neg file --- the NSA and Cybercom Tradeoff DA’s are designed to ideally apply to as many cyber affs as possible. The NSA DA in this file doesn’t reproduce every card in the starter pack. The aff section includes AT: new disads, a new zero-days mod, and various aff patchwork updates.

Please email [khirn10@gmail.com](mailto:khirn10@gmail.com) with any questions or concerns

# CYBERCOM Tradeoff DA

## CYBERCOM Tradeoff DA

### 1NC CYBERCOM DA

#### CYBERCOM DA.

#### CYBERCOM is securing election integrity now, but resources are key.

Malbot 5/5, Malware News, 5/05/2022, “Nakasone to remain at helm of NSA, Cyber Command for at least one more year,” https://malware.news/t/nakasone-to-remain-at-helm-of-nsa-cyber-command-for-at-least-one-more-year/59887, Marsh

The command, in particular, saw its authorities and responsibilities greatly expanded by the Trump administration and Congress.

Most notably, Cyber Command — backed by intelligence from the NSA — has taken a central role in keeping U.S. elections free of foreign interference. In 2018, the military launched a campaign called Operation Synthetic Technology to protect the midterm elections that year.

The effort saw the command deploy “hunt forward” teams to Eastern Europe; send direct messages to Russian disinformation operators letting them know that they had been identified; and launch an offensive strike that temporarily knocked the Internet Research Agency — an entity notorious for trying to sow discord among Americans — offline in the days around the election.

The organizations also took action against Iranian hackers backed by the Islamic Revolutionary Guard Corps in the run-up to the 2020 election. The hackers posed as a far-right group to send threatening emails to American voters and posted a video to shake confidence in the U.S. voting process.

Speaking at Vanderbilt, Nakasone said the U.S. would face “many more” such threats in the future.

#### The plan trades-off and hinders future cyber developments.

Ben FitzGerald 14, adjunct senior fellow at CNAS; Lt Col. Parker Right some military bro, 4/1/2014, “Digital Theaters: Decentralizing Cyber Command and Control,” *Center for a New American Security*, pp 16-18, JSTOR, Marsh

Meeting military service cyber requirements is key to sustaining critical service investment in the development of cyber capability. The military services provide the trained cyber forces that USCYBERCOM employs. Although part of the joint cyber team, the services nonetheless expect that their service requirements and those of their service components at the combatant com­mands will be met in kind with their joint force contribution. If service cyber requirements are underserviced, the services will question their investment. For the services, cyber is a zero-sum game. Every additional unit of cyber costs them another unit of capacity elsewhere in the force. A theater cyber C2 structure that obscures service contributions or weakens the link between the service, its operational cyber units and its various service component requirements risks losing ser­vice interest and investment in developing cyber.

#### Election integrity is vital to democracy---maintaining robust cyber defense and resources is key.

Carrie Cordero 20, Robert M. Gates Senior Fellow and General Counsel at CNAS, 11/12/2020, “How Cybersecurity Saved U.S. Democracy,” https://www.cnas.org/publications/commentary/how-cybersecurity-saved-u-s-democracy, Marsh

According to a 12 November 2020 joint statement of U.S. election officials, the 2020 U.S. presidential election “was the most secure in American history.” That success was a result not of accident, but instead of deliberate, sustained, and comprehensive efforts at the local, state, and federal levels to ensure that it was secure from foreign interference. Those efforts to secure the election were borne out of the attempts by the Russian government to influence the outcome of the 2016 U.S. presidential election. In the end, however, the efforts to enhance the cybersecurity of the U.S. electoral infrastructure in 2020 ended up protecting the integrity of the election not only from malign foreign activities, but also from domestic anti-democratic and illiberal efforts to undermine confidence in the 2020 presidential election.

In 2020, the threats compounded as compared to 2016.

A range of activities designed to protect the American election infrastructure from foreign malign activity ended up providing a bulwark against threatening domestic efforts to undermine and overturn the lawful election result. The U.S. experience in 2020 suggests that cybersecurity itself can play a critical role in protecting not only election infrastructure as a technical matter, but also providing a technical basis to counter illiberal forces as a mechanism to protect the democratic process of conducting a fair election. Cybersecurity itself just may have saved U.S. democracy from careening of the rails, continued sustained efforts to continue to harden election infrastructure cybersecurity and create a cadre of trusted officials, will likely be needed again.

#### Democracy solves extinction

Daniel Twining 21, PhD and President of the IRI, 10/10/2021, “America must double down on democracy,” https://thehill.com/opinion/campaign/575693-america-must-double-down-on-democracy?rl=1, Marsh

Democracy is under assault. China and Russia are pursuing strategic campaigns to undermine liberal values and U.S. leadership. Authoritarians from Belarus to Burma brutalize their citizens to stay in power. The debacle of U.S. troop withdrawal from Afghanistan and our national soul-searching in the wake of the 20th anniversary of 9/11 led some to wonder if support for democracy should remain a component of American foreign policy.

The hard truth is that a world that is less free is one that is less secure, stable and prosperous.  The greatest dangers to the American way of life emanate from hostile autocracies. There are no quick fixes, but the best antidotes to the challenges of great-power conflict, terrorism and mass migration of desperate refugees lie in the building of inclusive democratic institutions — and working with allied democracies to sustain the free and open order that China, in particular, wishes to replace with a world that’s safe for autocracy.

The conventional wisdom that authoritarianism has popular momentum is wrong. No one anywhere is taking to the street to demand more corrupt governance, the adoption of one-man rule, a stronger surveillance state, or greater intervention by malign foreign powers.

Democratic freedoms are unquestionably under assault in many nations. Autocrats are aggressive precisely because of the growing demands for change in their more modern, connected societies — and the rising risk that middle classes in nations such as China and Russia will not be willing forever to forfeit political rights for prosperity.

American retrenchment and isolationism compound the danger. It would be nice to live in a world where failed states and dictatorships were a problem for someone else to worry about. But rather than producing stability, Western retreat only emboldens autocrats in ways that amplify dangers to American national security.

We know that violent extremism flourishes under state failure and dictatorship. Broken states become breeding grounds for extremist groups because they leave vacuums that terrorists are only too happy to fill. In nations without democratic accountability, citizens become drawn to the only forms of expression available to them, which are often violent and extreme.

The good news is that we have billions of allies around the world: citizens on every continent chafing for greater freedom and dignity. They do not want U.S. military-led nation-building.  They want peaceful support for their independent efforts to create democratic space in systems distorted by overweening government control, dangerous governance gaps and foreign malign influence.

The free world cannot be neutral in the face of autocracy’s resurgence. Rather, it should play to its strengths. The appeal of democratic opportunity is a strategic asset for the United States — despite our own shortcomings — because people around the world similarly aspire to live in societies that guarantee justice, rights and dignity.

America’s closest allies are democracies. Democracies don’t fight each other, export violent extremism, or produce the conflicts that drive mass migration. Democracies are better partners in fighting terrorism, human trafficking and poverty, as well as establishing reliable trading relationships.

Open societies incubate the technologies that will help solve the world’s most pressing problems, including climate change. Citizens can hold leaders accountable when they fall short, and democratic institutions are stronger than any man — as America itself witnessed after the assault on the U.S. Capitol on Jan. 6.

### 2NC---Uniqueness---Resources

#### CYBERCOM’s budget is tight, but sufficient to cover its current tasks.

Michael S. Rogers 18, former United States Navy admiral who served as the second commander of the United States Cyber Command giving a statement for a House Hearing, “HEARING ON NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2018 AND OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS BEFORE THE COMMITTEE ON ARMED SERVICES HOUSE OF REPRESENTATIVES ONE HUNDRED FIFTEENTH CONGRESS FIRST SESSION,” https://www.govinfo.gov/content/pkg/CHRG-115hhrg25869/html/CHRG-115hhrg25869.htm, cc

As we begin the process of looking at the 2018 budget, I am interested to know to what extent you were able to factor in strategy and threats and sort of strategic thinking about what needs to be done as you put together the budget for Cyber Command and to what extent you have still been hamstrung by the BCA and by those cap numbers.

Admiral Rogers. So like any entity, it is all about prioritization for us. So we spend a lot of time figuring out with finite resources, even with growth, with finite resources how are we going to prioritize.

So our input for the fiscal year 2018 budget in truth in lending, we just rolled it out as a government, as a Department this afternoon, during the midday today, so I have not yet seen the specifics yet. I know what the broad number for us is, but I haven't seen the sub-elements of that, so I will talk broadly. I apologize, but I will talk broadly.

For the 2018 input, we tried to identify those priorities. At a macro sense, in no particular order, I have been arguing manpower; investment in core capabilities; and then, number three, how can I accelerate number one and number two, how can I do both of those faster.

Because in some ways, even though as the WannaCrypt ransomware issue that we have been going through shows, there is capability in the Department. There are a lot of motivated men and women who are doing some good work. We were not impacted by WannaCrypt, and that wasn't from a lack of effort.

We had spent significant time starting in March asking ourselves how might this play out, how do we position ourselves in the case of--because Microsoft had put out the patch for the vulnerability. We, as Microsoft users, saw that and started asking ourselves how might an opponent attempt to exploit this vulnerability even as we were working to patch.

It is one of the reasons why we use a defense in-depth strategy. There is no one single solution. There is no one single way to fix this problem. It is layers built on top of each other. That really has been the key to our success.

So we are asking ourselves how can we do this faster. Every day, one of my biggest concerns is--and I have never really had this same viewpoint in almost 36 years of commissioned service--every day I literally think to myself, we are in a race to generate more capacity and more capability at the same time that I am watching a host of global actors do the exact same thing.

And so we are trying to sustain both staying up with them, but, quite frankly, my objective is to get ahead of the problem set. I don't like reacting to things. It is not an effective or efficient way to do business, and I don't think that is what the Nation wants from us.

So until I am able to bore into the specifics of the budget, that kind of gives you a broad sense of what I thought we needed to focus on.

Ms. Cheney. So would you say, Admiral, that the budget as it has been proposed provides the resources necessary to regain superiority in areas that we have lost it?

Admiral Rogers. It certainly moves us along that road, but no one should think for one moment that this mission set, not unlike some others, is going to require increased and sustained investment over time. This is not going to be a 1 or 2 years we have increased you by some reasonable number, which has been the case for the last 2 years, and that is all you are going to need.

If you look at the scope of the challenges associated with this mission set and from where we are starting, we have got a lot of hard work ahead of us.

#### They’re gaining more autonomy now but skate on thin ice.

Lauren Williams 22, Senior Editor at FCW, 3/30/2022, “Cyber Command’s acquisition growing pains,” https://fcw.com/acquisition/2022/03/cyber-commands-acquisition-growing-pains/363836/, Marsh

U.S. Cyber Command is still getting its footing when it comes to steering acquisitions, but more resources are needed especially as the command gains more autonomy over its buying and budget power.

A Government Accountability Office report released March 30 found that while the command responsible for DOD’s cyberspace operations has matured its Joint Cyber Warfighting Architecture, it doesn’t yet have the metrics needed to justify acquisitions of new capabilities.

The report states that while Cyber Command has taken necessary steps to assess the value of JCWA acquisitions, it still needs to develop outcome-based metrics, per DOD policy, to track whether a capability is delivering what a mission requires.

“The command has been slow to determine metrics, in part because of inexperience conducting Value Assessments and the challenge of accounting for other factors—like new cyber operations tactics—on mission outcomes,” the report states. “If Cyber Command does not develop outcome-based metrics to inform future Value Assessments, it risks not being able to understand whether and how new capabilities benefit the cyber warfighting mission.”

JCWA acquisitions are largely software based and include the data management-centric Unified Platform, Persistent Cyber Training Environment, Joint Common Access Platform, and Joint Cyber Command and Control for situational awareness. Value assessments are evaluations used to determine whether a capability is worth the investment.

The watchdog body recommended Cyber Command “develop outcome-based metrics” that would be used for future acquisition value assessments.

DOD concurred with the recommendation but in its response noted that Cyber Command had asked for additional resources to [enhance] the command’s ability to develop in this area.” A decision on that is pending with the Office of Management and Budget, according to the report. identified steps it is taking to develop metrics for future Value Assessments.

Workforce challenges

But there are also resource challenges, particularly with the workforce, according to the report.

Cyber Command officials described understaffing in its acquisitions offices as “creating an all-hands-on-deck atmosphere, with individuals attempting to address emergent issues regardless of their office’s role, rather than a more coordinated approach.”

Additionally, officials told the GAO that staff in its JCWA Integration Office would need to expand from seven staff to 55 personnel to meet responsibilities.

“It will take time to fill additional positions, in part, because Cyber Command officials said they must first justify and validate the command has a need before beginning to bolster the workforce in fiscal year 2025,” the report states. “Cyber Command has a workforce study underway that officials anticipate will be complete later in fiscal year 2022.”

Cyber Command has long been looking to increase its acquisition capacity, which has been bolstered by recent legislation, lawmakers’ support, and budget requests.

The Biden administration's 2023 budget requests for nearly $11.2 billion to be spent on cyber operations, would help create five new cyber teams, while also investing in improvements to cyber ranges used for training and exercises. Some of those funds would go to enhancing the command’s role in acquisition of cyberspace programs and capabilities, according to the request.

#### CYBERCOM has enough resources to operate.

Joshua Rovner 20, John Goodwin Tower Professor of International Politics and National Security at Southern Methodist University John Goodwin Tower Professor of International Politics and National Security at Southern Methodist University, 9/14/2020, “More Aggressive and Less Ambitious: Cyber Command’s Evolving Approach,” https://warontherocks.com/2020/09/more-aggressive-and-less-ambitious-cyber-commands-evolving-approach/, Marsh

This year, U.S. Cyber Command celebrated its tenth birthday. It has much to celebrate: It achieved the status of a unified combatant command, its budget is healthy, and its commander, Gen. Paul Nakasone, is popular on both sides of the aisle. Nakasone’s more aggressive posture in cyberspace — what the command calls persistent engagement — has won the support of policymakers and legislators who wanted to see action against those who had been targeting U.S. interests. Before, U.S. cyber forces had shown restraint even in the face of repeated cyber attacks. Now, they will reach out into cyberspace to discover and mitigate threats before they could reach U.S. networks and damage U.S. interests.

### 2NC---Uniqueness---Ukraine

#### Ukraine ops were small-scale AND shrouded in secrecy---can’t vote for a thumper you know nothing about!

Sean Lyngaas 6/2, CNN’s cybersecurity reporter, 6/02/2022, “US confirms military hackers have conducted cyber operations in support of Ukraine,” <https://www.cnn.com/2022/06/02/politics/us-hackers-ukraine-support/index.html>, cc

"We've conducted a series of operations across the full spectrum; offensive, defensive, [and] information operations," General Paul Nakasone said in an interview with Sky News. A spokesperson for the command did not dispute the accuracy of the article but declined to elaborate on what the command's operations in Ukraine have entailed.

It's a rare public acknowledgment from US military officials of hacking operations that are often shrouded in mystery.

Nakasone's comments, and the White House's response to them, suggest that cyberspace is a domain in which the Biden administration feels comfortable countering Russia without fear of escalation. President Joe Biden has pledged not to engage directly with Russia militarily during the Ukraine war so long as the US and its allies aren't attacked.

Pro-Russia online operatives falsely claimed Zelensky committed suicide in an effort to sway public opinion, cybersecurity firm says

Pro-Russia online operatives falsely claimed Zelensky committed suicide in an effort to sway public opinion, cybersecurity firm says

"We don't see it as such," White House press secretary Karine Jean-Pierre said Wednesday when asked at a news conference whether Cyber Command's actions contradicted Biden's pledge.

Officials from Biden on down have for months warned about the threat of retaliatory Russian cyberattacks against US infrastructure after the US and its allies imposed sweeping sanctions on the Kremlin over its war in Ukraine.

While analysts have proffered a range of theories, including improvements in US defenses, for why such a hack hasn't apparently happened yet, US officials tell CNN that Russian fear of escalation in cyberspace could be one factor.

For one, Moscow may not want to risk retaliatory US cyberattacks that could hinder Russian military operations, a senior US defense intelligence official told CNN.

The Russians have already had enough problems in Ukraine executing military operations, "I think that adding any kind of potential for US cyber into that mix ... [is] probably factoring into their decision calculus," said the official, who spoke on the condition of anonymity to speak candidly about a sensitive national security issue.

US and European allies blame Russia for cyberattack on satellite provider as Ukraine invasion began

The paucity of Russian hacking on US targets may reflect the "fear of escalation and what the US response might be, particularly if the US response affects Russian combat power in some form or fashion," the official added.

The statements, from an interview with a senior official tasked with keeping a close eye on Russian cyber activity, offer a window into US thinking on Russian hacking at a critical time in the war -- as the Kremlin targets eastern Ukraine after failing to take Kyiv.

The official's analysis also reflects the uncertainty and ambiguity of big-power competition in cyberspace, where governments try to keep each other guessing on their hacking capabilities and willingness to use them.

"For Russia, understanding the full scope of US cyber combat power is a gap for them which leaves them unsure about opening this front, at least at this time," the senior US official said. "Cyber warfare is a new domain ... It hasn't been around long enough for any one nation-state to dominate it."

'Attribution in peacetime is tricky enough'

Analysts say Cyber Command has matured considerably since its inception more than a decade ago and has increasingly become a tool of US power projection. The command sent personnel to Ukraine in December, in anticipation of the Russian invasion, to help Kyiv bolster its cyber defenses and to gather information about potential Russian hacking threats, officials have said.

There are a range of activities, including low-level intrusions into computer networks, that may qualify as "offensive" cyber operations but which the Russians may not necessarily interpret as escalatory, according to Bobby Chesney, an associate dean at the University of Texas School of Law who focuses on cyber and national security law.

Some of the command's previous hacking operations have included knocking a Russian troll farm offline during 2018 US midterm elections, according to a Washington Post report, and targeting ransomware operatives who threaten US organizations.

While big hacks of US organizations related to the Ukraine war have been in short supply, a plethora of attempted cyberattacks have been reported in Ukraine and Russia as digital vigilantes take sides in the war. The websites of Russian government ministries and media mouthpieces have been knocked offline or altered to broadcast anti-war slogans.

The senior US defense intelligence official expressed concern that the Russian government may mistakenly assess that that type of hacking is coming from the US government.

"Attribution in peacetime is tricky enough ... I would say there's a real danger of unintentionally attributing something to the United States that the United States or its allies simply did not do," the official said.

### 2NC---Link---General

#### CYBERCOM resources are zero-sum---new programs sacrifice old ones.

Erica Lonergan 21, Assistant Professor in the Army Cyber Institute and a Research Scholar in the Saltzman Institute of War and Peace Studies at Columbia University; and Lauren Zabierek, Executive Director of the Cyber Project at Harvard Kennedy School’s Belfer Center, 12/16/2021, “Cyber Command Is in the Ransomware Game—Now What?,” https://www.lawfareblog.com/cyber-command-ransomware-game%E2%80%94now-what, cc

Finally, over the summer we warned about the twin risks of mission creep and prioritization against a backdrop of finite resources and personnel to tackle the diverse and growing set of missions that have fallen within Cyber Command’s purview. How trade-offs will be made between new activities, like counter-ransomware operations, and existing missions remains underspecified. In fact, this issue was implicit in Nakasone’s remarks; at the same time that he discussed the military’s role in ransomware, he also highlighted its role in election defense and conveyed that Cyber Command was already preparing to defend the inevitable next round of election interference. This begs the question: What is being sacrificed or put on the backburner when the military is used to counter ransomware, and what is the process that governs decision-making around shifting prioritizations?

As we argued in our previous post, there is a compelling case for the military to get involved in counter-ransomware operations that reach the threshold of significant risk to national security—and we stand by that argument. However, making this case demands greater transparency and clarity around how military authorities and resources are utilized, and how they relate to other governmental authorities and capabilities. As military cyber operations are possibly ongoing, as we brace for the likelihood of further attacks, and as the cyber force is likely to grow, now is the time to address these concerns.

#### No link turns---even creative ways of garnering funds trigger the link.

Allan Friedman 11, Fellow and Research Director, Center for Technology Innovation The Brookings Institution, 3/16/2011, “Defense Challenges and Future Operations,” The 21st Century Defense Initiative’s Second Annual Military and Federal Fellow Research Symposium, https://www.brookings.edu/wp-content/uploads/2012/04/20110316\_defense\_challenges\_panel\_2.pdf, Marsh

Besides these characteristics, there are some constraints that impact DOD's command-and-control in cyberspace. First of all is personnel. It is a relatively small pool of cyber-experts within DOD. So trying to divide those up and place them all around the world dilutes the pool, and dilutes efficiencies.

Secondly, for the most part, personnel is a zero-sum game. If you want to create more cyber wars, you've got to take it from somewhere else. We're not going to expect to see an increase in N-strength within DOD, personnel N-strength, in order to make up a cyber force. While DOD may come up with some creative ways to bring on some civilians and Reserve Guard capability, there's still a cost there that will affect the choice of a command-and-control structure.

#### Resources are finite.

Joseph Marks 17, Senior Correspondent for Nextgov, 5/23/17, “CYBERCOM Budget Request Focused on Elevation to Full Command”, https://www.nextgov.com/cybersecurity/2017/05/cybercom-budget-request-focused-elevation-full-command/138109/, Marsh

Outdated computer and technology systems across DOD and the services make the military vulnerable to cyberattacks, Rogers said, partly because defense acquisition has historically prioritized purchasing new weapons systems, ships, planes and other hardware over shoring up cyber vulnerabilities in existing systems.

“In a world of finite resources, you’ve got to make those resource tradeoffs,” Rogers said, “and in general, the acquisition world hasn’t historically always been incentivized for cybersecurity outcomes as its primary metric.”

### 2NC---Link---AT: Not CYBERCOM

#### Title 10 cyber ops are led by CYBERCOM.

Keith Alexander 10, former commander of United States Cyber Command, 9/23/2010, “U.S. CYBER COMMAND: ORGANIZING FOR CYBERSPACE OPERATIONS,” https://www.govinfo.gov/content/pkg/CHRG-111hhrg62397/html/CHRG-111hhrg62397.htm, cc

General Alexander. Well, for the--for the Title 10, they operate under the CYBERCOM hand. Cyber Command operates under Title 10 authorities to this committee, the House Armed Services Committee.

#### Recent Security Cooperation with NATO allies proves.

DoD News 18, 10/2/2018, “U.S., Montenegro conduct groundbreaking cyber defense cooperation,” https://www.cybercom.mil/Media/News/News-Display/Article/1651540/us-montenegro-conduct-groundbreaking-cyber-defense-cooperation/, Marsh

U.S. Cyber Command, in cooperation with U.S. European Command, has worked closely with partners from Macedonia in conducting Cyber Defense Security Cooperation to increase interoperability and deter malign influence on the democratic processes of the U.S., our allies and our partners.

“This is part of an ongoing effort to support NATO allies and European partners by building their cyber defense capabilities while learning from one another,” said a U.S. Cyber Command spokesperson. “These efforts serve to deter foreign malign influence on the democratic processes of our allies, partners, and the U.S.”

### 2NC---Link---AT: Not CYBERCOM

#### CYBERCOM is normal means for cybersecurity cooperation with NATO.

CYBERCOM 20, U.S. Cyber Command, 12/03/2020, “Estonia, U.S. Conduct Joint Defensive Cyber Operation,” https://www.defense.gov/News/News-Stories/Article/Article/2434474/estonia-us-conduct-joint-defensive-cyber-operation/, cc

U.S. Cyber Command, in cooperation with U.S. European Command and NATO allies, continuously works to deter malicious cyber activity in the region.

The two countries have ongoing cooperation at various levels within Cybercom, U.S. European Command, the Maryland National Guard and the Sixteenth Air Force — U.S. Air Forces Cyber.

"U.S European Command’s robust Cyber Security Cooperation program is focused on building allied and partner cyberspace operational capabilities, which strengthens trust and cultivates strong ties with our cyber partners throughout Europe," Army Brig. Gen. Maria Biank, director of Eucom’s command, control communications, and computers, or C4, and cyberspace directorate, said.

"Through bilateral and regional security cooperation efforts and information sharing initiatives, we are able to further enhance our collective cybersecurity posture as well as enable Hunt Forward operations in our area of responsibility," she said.

#### CYBERCOM oversees all cyber operations, including with allies.

Todd Lopez 19, DOD News, 5/14/19, “Persistent Engagement, Partnerships, Top Cybercom’s Priorities,” https://www.defense.gov/Explore/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/, Marsh

Persistent engagement also involves persistent presence -- the sharing of information to enable partners -- and persistent innovation of technology and techniques with partners that include other government agencies, allied nations and industry, Luber said. Both are critical to Cybercom’s success as it moves into its second year.

Persistent Engagement With Persistent Force

“In the face of cyber threats, we’ve adjusted our strategic vision to one of persistent engagement with a persistent force,” Luber said. “No longer reactive, but actually working in cyberspace in an area where there is no sanctuary or operational pause. It is the center of strategic rivalry in this era of renewed power competition. We are in constant contact with our adversaries. Success is determined on how we enable and act.”

Getting outside of just U.S. networks and working with allies -- “defending forward” — is a second area of focus for Cybercom, Moore said. It’s something lawmakers have enabled the command to do.

Changes to national policy and language in the 2019 National Defense Authorization Act, for instance, have in a limited way enabled Cybercom to step outside the Defense Department information networks and given it additional authorities to operate more effectively.

### 2NC---Elections---CYBERCOM Key

#### There are new measures for security now that restore public trust in elections.

CW 22, CyberWire Magazine, 6/24/2022, “American Data Privacy and Protection Act. US President signs three cybersecurity bills. US senator tasks Cybercom with election security reporting. US Navy sets its sights on cybersecurity.,” https://thecyberwire.com/newsletters/policy-briefing/4/121, Marsh

US senator tasks Cybercom with election security reporting.

Maine Senator Angus King of the US state of Maine is pushing for a measure that would require US Cyber Command (Cybercom) to publish two unclassified reports connected with each biennial election. The first report would focus on assessing foreign threats before an election takes place, and the second would be a post-election assessment of voting security. King, who is also Co-chair of Cyberspace Solarium, told the Washington Post, “We want to be kept informed of what the threats are, how they're developing, what direction they're taking. We also want to be able to reassure people about the security of our elections.” Public confidence in election security has plummeted in recent years, and King asserts that having the assessment come from a trusted, independent source like Cybercom – as well as making the information as transparent and accessible as possible – could rebuild Americans’ faith in the election process. To improve the measure’s chance of passage, King included it in the National Defense Authorization Act (NDAA), an annual must-pass defense policy bill that both Republicans and Democrats already support.

### 2NC---Elections---Key to Democracy

#### Election security and its public trust is the lifeline of democracy---otherwise, extinction.

Jennifer Panning 21, Chair of Northwood Board of Trustees, 4/12/21, “Election Integrity Is an Important Product of the Rule of Law,” https://www.northwood.edu/afeu/when-free-to-choose/election-integrity-is-an-important-product-of-the-rule-of-law, [gendered language edited], Marsh

Rule of law is a fundamental component of The Northwood Idea. Society cannot exist without it. It is the wall between freedom and anarchy.

Elections are a part of American life where the rule of law is especially important. Many brave ~~men and women~~ [people] have fought for our freedom, including the privilege and duty to vote for our leaders, and we owe it to them to conduct our elections with high standards of integrity. Democracy is the greatest form of governance ever devised, a system by which free people choose their leaders and hold them accountable. In other words, a government of, by, and for the people. We might not always be happy with how our democracy functions, but it beats any and all alternatives.

Democracy only fulfills its potential when elections are free and fair. If the true will of the citizenry is not reflected in election results, people will lose faith in their government, and government will not be accountable to the people. If that happens, everyone loses.

So, everyone should be able to agree on two basic goals of election law: we want all legal voters to have easy access to voting, but we should make it more difficult for bad actors to cheat.

In fact, our democracy can be hamstrung by nothing more than the widespread belief that elections are not free and fair, even if convincing evidence of wrongdoing cannot be produced. In a system where cheating is possible, the possibility of cheating creates problems of its own.

That’s why it is so important that we take strong, decisive action to ensure the integrity of our election process. Anything short of that risks undermining the democracy that has been so integral to American greatness.

In October 2020, Judicial Watch President Tom Fitton released his latest book, “A Republic Under Assault,” raising serious allegations of widespread campaigns to change electoral laws in ways that make voter fraud more likely. Less than a month later, the 2020 General Election became one of the most contentious in history, with significant segments of society stubbornly unconvinced that the official results accurately reflected the true will of the people. Again, this is a bad outcome for everyone.

### 2NC---Democracy---Impact

#### It causes extinction---there are multiple scenarios

Dr. Eric W. Orts 18, Guardsmark Professor of Legal Studies & Business Ethics and Professor of Management at The Wharton School, University of Pennsylvania, MA in Political Science from the New School for Social Research, LLM from Columbia Law School, JD from the University of Michigan School of Law, BA in Government from Oberlin College, “Foreign Affairs: Six Future Scenarios (and a Seventh)”, 6/27/2018, https://www.linkedin.com/pulse/foreign-affairs-six-future-scenarios-seventh-eric-orts/

7. Fascist Nationalism. There is another possible future that the Foreign Affairs scenarios do not contemplate, and it’s a dark world in which Trump, Putin, Xi, Erdogan, and others construct regimes that are authoritarian and nationalist. Fascism is possible in the United States and elsewhere if big business can be seduced by promises of riches in return for the institutional keys to democracy. Perhaps Foreign Affairs editors are right to leave this dark world out, for it would be very dark: nationalist wars with risks of escalation into global nuclear conflict, further digital militarization (even Terminator-style scenarios of smart military robots), and unchecked climate disasters.

#### Shoring up democracy solves every impact

Dr. Joseph S. Nye 17, University Distinguished Service Professor at the Harvard Kennedy School of Government, January/February 2017, “Will the Liberal Order Survive?,” Foreign Affairs, https://www.foreignaffairs.com/system/files/pdf/anthologies/2017/b0033\_0.pdf

The order will inevitably look somewhat different as the twenty-first century progresses. China, India, and other economies will continue to grow, and the U.S. share of the world economy will drop. But no other country, including China, is poised to displace the United States from its dominant position. Even so, the order may still be threatened by a general diffusion of power away from governments toward nonstate actors. The information revolution is putting a number of transnational issues, such as financial stability, climate change, terrorism, pandemics, and cybersecurity, on the global agenda at the same time as it is weakening the ability of all governments to respond.¶ Complexity is growing, and world politics will soon not be the sole province of governments. Individuals and private organizations—from corporations and nongovernmental organizations to terrorists and social movements—are being empowered, and informal networks will undercut the monopoly on power of traditional bureaucracies. Governments will continue to possess power and resources, but the stage on which they play will become ever more crowded, and they will have less ability to direct the action.¶ Even if the United States remains the largest power, accordingly, it will not be able to achieve many of its international goals acting alone. For example, international financial stability is vital to the prosperity of Americans, but the United States needs the cooperation of others to ensure it. Global climate change and rising sea levels will affect the quality of life, but Americans cannot manage these problems by themselves. And in a world where borders are becoming more porous, letting in everything from drugs to infectious diseases to terrorism, nations must use soft power to develop networks and build institutions to address shared threats and challenges.¶ China is unlikely to surpass the United States in power anytime soon.¶ Washington can provide some important global public goods largely by itself. The U.S. Navy is crucial when it comes to policing the law of the seas and defending freedom of navigation, and the U.S. Federal Reserve undergirds international financial stability by serving as a lender of last resort. On the new transnational issues, however, success will require the cooperation of others—and thus empowering others can help the United States accomplish its own goals. In this sense, power becomes a positive-sum game: one needs to think of not just the United States’ power over others but also the power to solve problems that the United States can acquire by working with others. In such a world, the ability to connect with others becomes a major source of power, and here, too, the United States leads the pack. The United States comes first in the Lowy Institute’s ranking of nations by number of embassies, consulates, and missions. It has some 60 treaty allies, and The Economist estimates that nearly 100 of the 150 largest countries lean toward it, while only 21 lean against it.¶ Increasingly, however, the openness that enables the United States to build networks, maintain institutions, and sustain alliances is itself under siege. This is why the most important challenge to the provision of world order in the twenty-first century comes not from without but from within.

#### Democratic governance prevents multiple scenarios for extinction---apprehension creates openings for Russia and China to embed and authoritarian order, causing nuclear war

Dr. Edward A. Kolodziej 17, Emeritus Research Professor of Political Science at the University of Illinois, Urbana-Champaign, “Challenges to the Democratic Project for Governing Globalization”, EUC Paper Series, Volume 1, https://www.ideals.illinois.edu/bitstream/handle/2142/96620/Kolodziej%20Introduction%205.19.17.pdf?sequence=2&isAllowed=y

The Rise of a Global Society

Let me first sketch the global democratic project for global governance as a point of reference. We must first recognize that globalization has given rise to a global society for the first time in the evolution of the human species. We are now stuck with each other; seven and half billion people today — nine to ten by 2050: all super connected and interdependent. In greater or lesser measure, humans are mutually dependent on each other in the pursuit of their most salient values, interests, needs, and preferences — concerns about personal, community, and national security, sustainable economic growth, protection of the environment, the equitable distribution of the globe’s material wealth, human rights, and even the validation of their personal and social identities by others. Global warming is a metaphor of this morphological social change in the human condition. All humans are implicated in this looming Anthropogenic-induced disaster — the exhausts of billions of automobiles, the methane released in fracking for natural gas, outdated U.S. coal-fired power plants and newly constructed ones in China. Even the poor farmer burning charcoal to warm his dinner is complicit.

Since interdependence surrounds, ensnares, and binds us as a human society, the dilemma confronting the world’s diverse and divided populations is evident: the expanding scope as well as the deepening, accumulating, and thickening interdependencies of globalization urge global government. But the Kantian ideal of universal governance is beyond the reach of the world’s disparate peoples. They are profoundly divided by religion, culture, language, tribal, ethnic and national loyalties as well as by class, social status, race, gender, and sexual orientation. How have the democracies responded to this dilemma? How have they attempted to reconcile the growing interdependence of the world’s disputing peoples and need for global governance?

What do we mean by the governance of a human society?

A working, legitimate government of a human society requires simultaneous responses to three competing imperatives: Order, Welfare, and Legitimacy. While the forms of these OWL imperatives have differed radically over the course of human societal evolution, these constraints remain predicable of all human societies if they are to replicate themselves and flourish over time. The OWL imperatives are no less applicable to a global society.

1. Order refers to a society’s investment of awesome material power in an individual or body to arbitrate and resolve value, interest, and preference conflicts, which cannot be otherwise resolved by non-violent means — the Hobbesian problematic.

2. The Welfare imperative refers to the necessity of humans to eat, drink, clothe, and shelter themselves and to pursue the full-range of their seemingly limitless acquisitive appetites. Responses to the Welfare imperative, like that of Order, constitute a distinct form of governing power and authority with its own decisional processes and actors principally associated either with the Welfare or the Order imperative. Hence we have the Marxian-Adam Smith problematic.

3. Legitimacy is no less a form of governing power and authority, independent of the Order and Welfare imperatives. Either by choice, socialization, or coerced acquiescence, populations acknowledge a regime’s governing authority and their obligation to submit to its rule. Here arises the Rousseaunian problematic.

The government of a human society emerges then as an evolving, precarious balance and compromise of the ceaseless struggle of these competing OWL power domains for ascendancy of one of these imperatives over the others. It is against the backdrop of these OWL imperatives — Order, Welfare, and Legitimacy — that we are brought to the democratic project for global governance.

The Democratic Project

For Order, open societies constructed the global democratic state and, in alliance, the democratic global-state system. Collectively these initiatives led to the creation of the United Nations, the World Bank, the International Monetary Fund, the World Trade Organization, and the European Union to implement the democratic project’s system of global governance.

The democratic global state assumed all of the functions of the Hobbesian Westphalian security state — but a lot more. The global state became a Trading, Banking, Market, and Entrepreneurial state. To these functions were added those of the Science, Technology and the Economic Growth state. How else would we be able to enjoy the Internet, cell phones and iPhones, or miracle cures? These are the products of the iron triangle of the global democratic state, academic and non-profit research centers, and corporations. It is a myth that the Market System did all this alone. Fueled by increasing material wealth, the democratic global state was afforded the means to become the Safety Net state, providing education, health, social security, leisure and recreation for its population. And as the global state’s power expanded across this broad and enlarging spectrum of functions and roles, the global state was also constrained by the social compacts of the democracies to be bound by popular rule. The ironic result of the expansion of the global state’s power and social functions and its obligation to accede to popular will was a Security state and global state-system that vastly outperformed its principal authoritarian rivals in the Cold War. So much briefly is the democratic project’s response to the Order imperative.

Now let’s look at the democratic project’s response to the Welfare imperative. The democracies institutionalized Adam Smith’s vision of a global Market System. The Market System trucks and barters, Smith’s understanding of what it means to be human. But it does a lot more. The Market System facilitates and fosters the free movement of people, goods and services, capital, ideas, values, scientific discoveries, and best technological practices. Created is a vibrant global civil society oblivious to state boundaries. What we now experience is De Tocqueville’s Democracy in America on global steroids.

As for the imperative of Legitimacy, the social compacts of the democracies affirmed Rousseau’s conjecture that all humans are free and therefore equal. Applied to elections each citizen has one vote. Democratic regimes are also obliged to submit to the rule of law, to conduct free and fair elections, to honor majority rule while protecting minority rights, and to promote human rights at home and abroad.

The Authoritarian Threat to the Democratic Project

The democratic project for global governance is now at risk. Let’s start with the challenges posed by authoritarian regimes, with Russia and China in the lead. Both Russia and China would rest global governance on Big Power spheres of influence. Both would assume hegemonic status in their respective regions, asserting their versions of the Monroe Doctrine. Their regional hegemony would then leverage their claim to be global Big Powers. Moscow and Beijing would then have an equal say with the United States and the West in sharing and shaping global governance. The Russo-Chinese global system of Order would ascribe to Russia and China governing privileges not accorded to the states both aspire to dominate. Moscow and Beijing would enjoy unconditional recognition of their state sovereignty, territorial integrity, and non-interference in their domestic affairs, but they would reserve to themselves the right to intervene in the domestic and foreign affairs of the states and peoples under their tutelage in pursuit of their hegemonic interests. President Putin has announced that Russia’s imperialism encompasses the millions of Russians living in the former republics of the Soviet Union. Russia contends that Ukraine and Belarus also fall under Moscow’s purported claim to historical sovereignty over these states. Forceful re-absorption of Crimea and control over eastern Ukraine are viewed by President Putin as Russia’s historical inheritances. Self-determination is not extended to these states or to other states and peoples of the former Soviet Union. Moscow rejects their right to freely align, say, with the European Union or, god forbid, with NATO.

In contrast to the democratic project, universal in its reach, the Russo-Chinese conception of a stable global order rests on more tenuous and conflict-prone ethno-national foundations. Russia’s proclaimed enemies are the United States and the European Union. Any means that undermines the unity of these entities is viewed by Moscow as a gain. The endgame is a poly-anarchical interstate system, potentially as war-prone as the Eurocentric system before and after World War I, but now populated by states with nuclear weapons.

### 1NC---NC3

#### Hamstrung resources directly trade off with NC3 defenses.

Morgan Dwyer 20, fellow in the International Security Program and deputy director for policy analysis in the DefenseIndustrial Initiatives Group at the Center for Strategic and International Studies (CSIS), 10/15/2020, “Cross-domain Competition,” http://defense360.csis.org/wp-content/uploads/2020/10/Dwyer\_NuclearNexus\_Cross-domain-competition1.pdf, cc

Faced with budget constraints, however, Cyber Command’s focus on persistent engagement may require trade-offs, such as allocating less funding towards preparing for future kinetic conflicts.29 Already, several reports have noted that DOD has insufficiently prioritized efforts to identify and mitigate cyber threats to its weapon systems, including threats to NC3.30 In 2018, the Government Accountability Office (GAO) stated that DOD did not know the full extent of the cyber vulnerabilities in its weapon systems.31 In 2020, the Cyberspace Solarium Commission echoed the GAO’s concerns and recommended that Congress require DOD to annually assess the NC3 system for potential cyber vulnerabilities.32 More broadly, American University’s Joshua Rovner noted that Cyber Command’s focus on “persistent engagement” may create risks to the command’s support to traditional DOD missions; in particular, Rovner warned that “if great-power hostilities continue to rise, Cyber Command may have to pump the brakes on persistent engagement and devote more attention to the missions for which it was originally designed.”33 Those missions, of course, include preparing for future wars—presumably by defending DOD’s weapon systems, including NC3.

#### NC3 attacks cause extinction.

Erica Lonergan 22, assistant professor in the Army Cyber Institute at West Point and a research scholar at the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University; and Keren Yarhi-Milo, the Arnold A. Saltzman Professor of War and Peace Studies in the political science department and the School of International and Public Affairs and the director of the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University, 4/21/2022, “CYBER SIGNALING AND NUCLEAR DETERRENCE: IMPLICATIONS FOR THE UKRAINE CRISIS,” https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/, cc

How Cyberspace Is Creating Nuclear Risks

Policymakers and academics are attuned to the cyber risks to nuclear command and control. The practitioner community has largely focused on U.S. vulnerabilities and how to mitigate them. Scholars, in turn, worry about how cyber operations could have unintended escalatory consequences. But less attention has been paid to another likely scenario: the use of cyber operations for signaling purposes (operations with visible effects that aim to convey a message to another state) in a nuclear context. The ambiguity of cyber operations can sometimes be useful for signaling — but the same ambiguity can be dangerous during a nuclear crisis. The problem is that civilian leaders in particular, distinct from the military, are inclined to see cyber attacks as effective signaling tools.

Cyber operations could have nuclear implications, especially because modern nuclear command and control systems, like those in Russia and the United States, are becoming increasingly dependent on digital infrastructure. Nuclear command, control, and communications systems, which include early warning, information collection, and communications capabilities, alert decision-makers to impending nuclear strikes and also enable leaders to control decisions about nuclear use (or non-use). But their digital dependencies are creating opportunities for exploitation using cyber means. In a 2020 report, the Nuclear Threat Initiative found that “almost 9 out of 10 planned nuclear modernization programs involve at least some new digital components or upgrades.”

Vulnerabilities inherent in the digital infrastructure that undergird modern nuclear systems provide opportunities for actors to engage in cyber espionage — gaining access to a network or system to steal information — or even conduct cyber attacks. Hypothetically, a cyber power like Russia could conduct a cyber attack against a U.S. early warning satellite to degrade its functionality. This has become an urgent concern for practitioners. U.S. Strategic Command, for instance, is currently working to “operationally harden NC3 systems against cyber threats.” Congress has also gotten involved, requiring the Defense Department to evaluate the cybersecurity of major weapon systems. And the Government Accountability Office has published multiple reports decrying the state of cybersecurity and scope of vulnerabilities of weapon systems, including elements of the nuclear triad.

From an academic perspective, scholars have investigated how cyber operations targeting nuclear systems could exacerbate escalation risks. Focusing on nuclear forces, early research, such as work by Martin Libicki, was skeptical of the dangers posed by cyber operations. Nuclear forces were seen as being largely immune from digital attacks because they were “air gapped,” meaning that they were separated from information technology systems.

However, as nuclear systems have become increasingly intertwined with the digital environment — not to mention the dual-use nature of many elements of nuclear command, control, and communications systems (like early warning or position, navigation, and timing satellites) — the protection offered by being segregated from the internet is less robust. Jacquelyn Schneider, Benjamin Schechter, and Rachael Schaffer, for instance, ran a series of wargames demonstrating that decision-makers in hypothetical crises are likely to use their cyber exploits against an adversary’s nuclear systems. They found that this could have negative effects on states’ respective nuclear strategies, especially decisions to pre-delegate nuclear launch authority or automate nuclear responses. Erik Gartzke and Jon Lindsay argue that the clandestine nature of cyber operations means that one state could secretly gain access to an adversary’s nuclear command, control, and communications systems, giving the former an information advantage or even creating an incentive for the latter to use its nuclear weapons out of the fear that it may lose them. James Acton notes that the difficulties of distinguishing between cyber espionage and attack could lead a state to misperceive the intent behind a cyber operation, generating a similar “use it or lose it” calculus.

### 2NC---NC3---CYBERCOM Key

#### Offensive cyber posture is expensive, trading-off with defensive measures.

Jason Healey 22, Senior Research Scholar and adjunct faculty at Columbia University’s School for International and Public Affairs and president of the Cyber Conflict Studies Association, 6/24/2022, “The Cyber Budget Shows What the U.S. Values—And It Isn’t Defense,” https://www.lawfareblog.com/cyber-budget-shows-what-us-values%E2%80%94and-it-isnt-defense, Marsh

The most obvious implication for national security is that more could be done to reduce America’s significant cyber vulnerabilities. Defense through offense may be a promising experiment or operational concept, but it may not be fully developed as a strategy. The government, both the executive and legislative branches, must work to rebalance these efforts with significantly more funding for federal cybersecurity, critical infrastructure, information sharing and a wide range of other defensive priorities.

The Cyberspace Solarium Commission noted that within the Homeland Security budget, only 15 percent is “committed to initiatives supporting the private sector.” Overall, that is perhaps 1 percent of Defense Department funding. This percentage must increase many times over, targeted at embracing those innovations that give defenders the greatest advantages over attackers at the greatest scale and least cost; working toward major political goals, such as getting to zero botnets; creating new organizations to directly collaborate on response and not just share information; and countless other critical civilian cyber tasks. The U.S. strategy should place non-state actors, with their unique agility and capabilities, at the center of defense and help fund them accordingly.

Just as serious is the misconception in U.S. strategic thinking that sees U.S. moves as beneficial and stabilizing but our adversaries’ as dangerous militarizing escalations. Brazen, reckless attacks like WannaCry and NotPetya are destabilizing and nothing like more precise U.S. operations. We must recognize that adversaries are responding in part to U.S. actions—like Stuxnet and those revealed by Snowden—and perceived U.S. actions—such as Russian President Vladimir Putin’s belief that the Panama Papers were a U.S. covert action aimed at him.

While the budget comparisons I have presented may come as a surprise to some Lawfare readers, they will not surprise most U.S. adversaries, who have long feared U.S. cyber power. Recognizing the true U.S. priorities may help us recognize a more balanced perspective.

Moreover, as I wrote on Lawfare last year, there are tremendous risks when a “fearsome offense [is] paired with a weak defense.” If adversaries feel a war with the United States may be coming, our having “a more fearsome cyber offense makes it more likely they will [get in a sucker punch] on the U.S. before Cyber Command can bring its big guns to bear.”

While the Defense Department needs significant funding for its essential cyber missions, this money will not make the United States significantly more secure in cyberspace. If the U.S. government truly believes the top priority is defense—and that it is not militarizing cyberspace—then its budget for civilian cyber defense must be drastically increased to align more closely with these values.

### 2NC---NC3---Impact

#### The fed agrees.

Julia Berghofer 19, ELN Policy Fellow and Project Manager for the YGLN, 5/09/2019, “Apocalypse now? Cyber threats and nuclear weapons systems,” https://www.europeanleadershipnetwork.org/commentary/understanding-and-addressing-cyber-threats-to-nuclear-weapons-systems/, cc

Governments and legislators are struggling to keep pace with the rapid development of cyber capabilities. As military systems become more technically complex it would be easy to assume that they are more secure. The opposite is true. Increased automation and connectivity increases vulnerabilities to cyber attacks. Measures such as air-gapping a system (ie. de-connecting it from the internet) can fall short. A recent US Government Accountability Office (GAO) report assessed the cyber security of US weapons systems and found “mission critical cyber vulnerabilities in nearly all weapons systems […] under development.“ While the report does not make reference to any specific system type, one can reasonably assume that nuclear weapons systems are vulnerable to cyber attacks.

### 1NC---Taiwan

#### Expansive CYBERCOM resources cushion a Chinese invasion of Taiwan.

Joel Wuthnow 21, Senior Research Fellow in the Center for the Study of Chinese Military Affairs, Institute for National Strategic Studies, at the National Defense University, 12/29/2021, “Defending Taiwan in an Expanded Competitive Space,” https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2884395/defending-taiwan-in-an-expanded-competitive-space/, cc

Taiwan’s defense has always been precarious, and the dangers are only likely to grow as China’s power increases.1 Chinese economic inducement since the 1990s has done little to persuade Taiwan’s citizens to embrace China’s vision of a “one country, two system” model for cross-strait relations, prospects that are even lower with China’s recent steps to erode political freedoms in Hong Kong. To deter Taiwan independence and to pressure Taiwan’s leaders to accept Beijing’s proposals, China’s People’s Liberation Army (PLA) has amassed significant forces across the Taiwan Strait, including more than 600 short-range ballistic missiles opposite the island.2 Taiwan’s will to resist Chinese pressure depends, in part, on the speed and efficacy of U.S. intervention in a conflict. China’s military has thus built an arsenal of long-range missiles and supporting capabilities to try to keep the United States out of the fight.

China’s basic advantages in any Taiwan scenario include a high level of political will—reunification is a “core interest” for the Chinese Communist Party (CCP), which aspires to resolve the problem on its own terms by the centennial of the People’s Republic of China in 2049—and a local military balance that pits a regional heavyweight against a small island with few diplomatic allies and limited resources. Taiwan’s proximity to the mainland and the “tyranny of distance” facing an attempt to surge U.S. forces across the Western Pacific are liabilities for the defense.

Much can still be done to address the threat head-on, but a prudent U.S. approach should also consider ways of shifting the competition to areas where China is at a disadvantage. Multiple pressures on the PLA, driven by China’s unfavorable geostrategic environment, provide the basis for a competitive strategy. In peacetime, the United States should create headaches for the PLA in other areas bordering China by increasing military assistance and training to China’s other rivals. This approach would leverage the demand that many states have for better capabilities to resist Chinese coercion and play to preexisting Chinese concerns about threats suddenly appearing in secondary theaters. A PLA that is simultaneously having to counter many different challenges will be less able to focus on Taiwan.

Looking at Taiwan’s defense through a competitive strategy lens also suggests different options for confronting the PLA in wartime. China’s military structure is built on the notion that the PLA must be prepared to fight in many theaters at once. By necessity, it contains a centralized command and control and logistics system designed to manage and reallocate forces in a war. Targeting those critical links would complicate Chinese decisionmaking, reduce the PLA’s capacity to mass forces, and support U.S. and Taiwan operations in the main theater. To limit escalation risks, those operations should rely, wherever possible, on nonkinetic means. Ensuring Taiwan’s defense is no easy feat but will be easier with operations that defray China’s local advantages and keep the PLA off balance.

A New Lens for an Old Problem

Most discussions on improving Taiwan’s defenses focus on two issues. First is modernizing Taiwan’s military and equipping it with the means of resisting Chinese aggression. This is the subject of Taiwan’s “overall defense concept,” which focuses on asymmetric weapons such as sea mines and coastal defense cruise missiles needed to blunt an invasion.3 Taiwan’s limited ability to weather a Chinese offensive even with advanced equipment has led to a second focus: preserving a credible U.S. intervention capability so that the United States would be able to meet its obligations under the Taiwan Relations Act to “maintain the capacity” to resist China’s use of force (acknowledging that any military intervention would ultimately be a political decision).4 In recent years, all the services have rolled out revised operational concepts designed to allow U.S. forces to operate within China’s antiaccess/area-denial envelope, such as using stealthier ships more, reducing reliance on large bases, operating more from austere airstrips, and exploiting long-duration unmanned technology.

Both approaches are helpful in instilling doubt in the Chinese leadership about the PLA’s prospects in an amphibious invasion. Nevertheless, a problem for the defense is that China has built large advantages in most categories of conventional power across the Taiwan Strait—in submarines, for instance, the ratio is 34 Chinese submarines assigned to the relevant theaters versus 2 for Taiwan—forcing Taipei to rely on U.S. intervention to ensure its ability to resist a blockade and successive waves of amphibious and airborne assaults. Yet this is a gamble, if one credits reports that wargames consistently show U.S. forces losing to China, due in part to China’s impressive counter-intervention capabilities and in part to the vast distances that U.S. forces need to traverse. Some concepts of intervention also envision extensive strikes on the mainland, which would carry a high risk of retributive Chinese strikes on U.S. targets, such as military bases in Japan or Guam.5

Given those limitations, more thought is needed on how to move the competition to different playing fields where China has fewer advantages (reflecting the logic of the “competitive strategies” approach pioneered by Andrew Marshall in the early 1970s).6 Adopting this philosophy, the 2018 National Defense Strategy encourages U.S. policies that “expand the competitive space, seizing the initiative to challenge our competitors where we possess advantages and they lack strength.”7 U.S. doctrine has emphasized a related point: that adversary decisionmaking should be complicated by presenting it with “multiple dilemmas,” overwhelming its capacity to reach timely decisions on the use of force.8 Both tenets encourage U.S. strategists to think creatively about our adversary’s constraints while taking a more holistic view of our own comparative strengths.

The PLA’s Fundamental Dilemma

The basis of a competitive strategy is the tension in Chinese military strategy between preparing for a war with Taiwan and fulfilling the dizzying array of other requirements with finite resources.9 A war with Taiwan has been the PLA’s top planning scenario since the early 1990s. The rise of a new generation of Kuomintang leaders who had less interest in a political union with the mainland, combined with a Taiwan electorate largely opposed to unification, meant that the PLA needed to prepare to seize and occupy the island. This led to investments in short-range ballistic missiles, submarines, and amphibious capabilities, as well as training in what used to be called the Nanjing Military Region, recently rebranded as the Eastern Theater Command, focused on capturing offshore islands. The possibility of U.S. intervention, underscored by the involvement of two U.S. aircraft carriers in the 1995–1996 Taiwan Strait Crisis, sparked an emphasis on developing long-range antiship missiles and other capabilities to forestall U.S. intervention in a conflict.

The PLA could not, however, fully commit to preparations for a war with Taiwan and the United States. The crux of the problem is a highly unfavorable geostrategic environment. Within China itself, the western third of the country is occupied by ethnic Uighurs and Tibetans who have their own dreams of independence. Regionally, China shares land borders with 14 countries and maritime borders with an additional 7, including states that are either unstable, such as North Korea and Afghanistan, or that have territorial disputes with China, including Japan, India, the Philippines, and Vietnam.10 Defending China’s long borders and dissuading other countries from asserting their sovereignty claims put competing demands on China’s finite military resources. U.S. military presence and the specter of U.S. involvement in conflicts ranging from Korea to the South China Sea also mean that the PLA must prepare for high-end conflicts outside the Taiwan Strait.

An additional problem, from the PLA’s perspective, is the fear that China’s rivals—both within the region and domestic forces opposed to Chinese Communist Party rule—could take advantage of a war with Taiwan to challenge the regime or seize Chinese territory. Chinese strategists write of the possibility of a “chain reaction” of wars cascading across China’s frontiers. Such concerns are not new. Mao himself reputedly warned the PLA not to overlook problems outside the main theater. Indeed, Chinese historians note that none of the wars that China fought during the Cold War was in an area then designated as the “main strategic direction.”11 In the PLA’s jargon, the military should not overemphasize the main strategic direction (the southeast coast; and the Taiwan Strait, in particular); it also needs to prepare for combat in other theaters.12

Combined, these competing concerns mean that the PLA has needed to generate capabilities less relevant to island landings, widely disperse its resources across the country (including allocating advanced fighters and other modern capabilities to other regions), balance the three naval fleets, and develop plans and train for a variety of contingencies.13 The theater command system itself, as noted below, is optimized for smaller border clashes and not a single major conflict of the sort that would be prosecuted on Taiwan. Compounding the problem is the PLA’s personnel system in which officers spend most of their careers in a single theater and are thus less fungible across different contingencies than, for instance, their American peers who frequently rotate to new assignments.

The June 2020 escalation with Indian troops along the disputed Himalayan border illustrates the countervailing pressures on PLA resources and attention.14 The area is what the PLA refers to as a “secondary strategic direction,” where the threats facing China are less intense than in the main strategic direction, but still require significant forces to deter or defeat a rival. To counter India and perform other missions such as defending China’s Central Asian borders and deterring uprisings in ethnic majority regions, the PLA has allocated roughly a quarter of its ground forces to the Western Theater Command and the Tibet and Xinjiang military districts, complemented by eight fighter/ground attack brigades and four missile brigades.15 These forces train for missions such as counterterrorism and high-altitude warfare and against the capabilities of particular adversaries that have little bearing on the operations China would conduct in a war with Taiwan.

Concerns about flare-ups in other regions and a broad distribution of capabilities have not prevented the military balance across the strait from shifting gradually in China’s favor. PLA capabilities have regularly been used to intimidate Taiwan’s leaders—for instance, by a steady rhythm of H-6 bomber flights around the island—and are sufficient for a range of cross-strait operations, including missile bombardments and a blockade.16 Moreover, there are some circumstances in which Beijing might accept a high degree of risk to its other interests to launch a war against Taiwan. For instance, a Taiwanese declaration of independence could generate a high degree of domestic pressure on the CCP to act. However, Taiwanese leaders have been careful to avoid such provocations, meaning that the likeliest scenario for China would be a calculated war of choice.17 Yet competing considerations reduce China’s ability to mass its forces in wartime and make the task of Taiwan’s defense more manageable for Taipei and Washington.

A Chain of Porcupines

China’s force planning dilemma provides options for thinking differently about Taiwan’s defense prior to and during a conflict initiated by Beijing. Applying a competitive strategies approach, U.S. defense strategy in peacetime should aim to reduce China’s ability to focus on Taiwan by maximizing the range and complexity of challenges facing the PLA in other theaters. This requires, in part, that the United States maintain a strong presence at many points along China’s periphery, voice support for the defense of allies, and conduct high-end exercises with China’s other rivals. Such activities, which are central to the current Indo-Pacific strategy, play into Chinese concerns about encirclement and add to the pressure to divide up resources among many theaters.18

Expanding security cooperation with other states would enhance those effects. Using Michael Beckley’s twist of a phrase coined by William S. Murray, an explicit goal of U.S. strategy should be to ring China with “prickly porcupines” by supplying other states with the military tools necessary to resist coercion.19 Providing additional training and advanced weapons and equipment, like antiship missiles, to states such as Vietnam, the Philippines, Indonesia, and Malaysia, would serve their interests in maintaining sovereignty while also ramping up the challenges the PLA Navy, Marines, and Air Force would have to counter outside the Taiwan Strait. By pursuing their own ends, these countries could indirectly contribute to Taiwan’s defense without requiring them to be actively involved in cross-strait affairs.

From this perspective, expanded security cooperation with states far from China’s southeast coast is particularly useful. India is a prime example. Upgrading defense ties with New Delhi has been a goal of the last few U.S. administrations, pursued most recently through renewed efforts to expand defense industry cooperation; approval of $3 billion in arms sales, including high-end items like air defense radars, MK 54 torpedoes, and Harpoon missiles; an agreement on the sharing of military intelligence; and combat-focused exercises in the Indian Ocean featuring India and Japan. Further arms sales and other assistance would not only serve India’s interest in countering Chinese coercion, which has been piqued because of the 2020 border crisis, but also draw PLA resources away from the Taiwan Strait.

As Andrew Marshall explained regarding the Soviet Union, competitive strategies should also leverage bureaucratic fissures in the target country. Relevant here are China’s tendency to carve up the budgetary pie with as many “winners” as possible, contestation between different parts of the PLA for scarce resources, and the lack of a strong central mechanism to adjudicate bureaucratic disputes. Increasing threats from smaller rivals in the South China Sea would not only take up time and capacity for the Southern Theater Command but also provide an argument for that theater to demand resources, which might otherwise go to the Eastern Theater Command. Deepening defense cooperation with India, for instance, would serve as a powerful rationale for the Western Theater Command to argue for more resources.

Selling more advanced arms to China’s other neighbors in a bid to take pressure off Taiwan would probably not dissuade China from using force—any decision to use force assumes a high risk and cost tolerance and would be undertaken only in exigent circumstances. But it does encourage the PLA to spread out its limited resources, which ultimately works in favor of Taiwan’s defense.

U.S. strategy could also try to move the competition in new directions during a conflict. Such moves are typically discussed under the label of “horizontal escalation,” involving attacks on an adversary’s interests in a secondary theater.20 In a Taiwan scenario, it is tempting to imagine U.S. forces leveraging their maneuverability to pose problems that tie up PLA resources elsewhere. However, opening a second front would be difficult because of the near certainty that India or other countries in the region would stay out of the conflict and the likelihood that U.S. leaders, attuned to the costs of a wider regional conflagration, would also try to avoid a larger war. As the congressionally mandated National Defense Strategy Commission argued, “It is unlikely that the United States could force its adversary to back down by applying pressure—military or otherwise—in secondary areas.”21

In an indirect way, however, China’s geostrategic circumstances give the United States additional warfighting options that do not rely on kinetic strikes or futile diversions. The starting point is that the PLA has adopted an organizational structure attuned to many small conflicts, and not to a single large contingency. This preference for smaller contingencies is reflected in the PLA’s theater command system (which replaced the former military regions as part of the broad restructuring of the military that began in late 2015).22 The Eastern Theater Command lacks all the capabilities that would be necessary to execute a war: amphibious and airborne units are based in adjacent theaters and space and cyber assets are under the Strategic Support Force. Countering U.S. intervention would require long-range missiles that are likely under the direct control of the Central Military Commission. In addition to mobilizing reinforcements, frontline commanders may have to request ammunition and equipment based in other theaters if major losses are sustained at the war’s outset.

The limitations of China’s theater command structure mean the war would be centrally managed, most likely by the Joint Staff Department in Beijing. Logistics operations would rely on a distributed network of depots controlled by the Joint Logistic Support Force in Wuhan.23 Then, rather than focusing mainly on the Taiwan Strait, U.S. operations should try to sever the command and control and logistics networks critical to Beijing’s ability to manage the war (while preserving critical U.S. networks that would be targeted by the PLA). Such operations would leverage what one RAND study deems potential Chinese weaknesses in cyber defense,24 and may benefit from recent investments, such as the U.S. Army’s creation of information operations detachments within its multidomain task force concept, which include both cyber and electronic warfare capabilities.25 Even if the PLA is able to reconstitute those systems, the disruption could frustrate China’s decisionmaking process and buy valuable time for U.S. forces to intervene, without the need for kinetic strikes. An added virtue is that this approach exploits a PLA organizational culture that emphasizes centralization, in contrast to the U.S. “mission command” philosophy of empowering commanders to implement approved policy aims without precise direction and intensive management oversight.

Generating those effects would also benefit from information operations that try to exploit cleavages in Chinese civil-military relations. During a conflict, the PLA would likely argue that it is fully capable of managing the conflict while adequately defending China’s security in secondary theaters. However, civilian leaders, prone to years of PLA dissembling and obfuscation, would approach those assurances with at least some skepticism.26 Information operations that raise questions about the PLA’s competence—such as misinformation suggesting that key systems may not be completely reliable—would exacerbate those doubts and potentially lead to additional delays as problems are investigated. This would create new opportunities for U.S. forces to seize the initiative and sustain a higher decision tempo than PLA leadership can operate within.

Conclusion

Taiwan benefits from regional disturbances, such as the recent clash with India, in direct and indirect ways. The possibility of a conflict with other rivals forces China’s constrained resources to be broadly dispersed and its troops trained and equipped for diverse scenarios. Such contingencies have also produced a theater structure not well suited to a war. These are systemic weaknesses for the PLA that could be leveraged to shift the competition to areas beyond the Taiwan Strait, rendering the task of countering Chinese operations in the main theater more manageable. Playing to existing concerns among Chinese strategists, U.S. alliances could be deepened to overextend PLA assets, while critical links in the PLA’s command structure could be targeted in a conflict to reduce its capacity to mass force. Success depends on prudent stewardship of U.S. defense relations and smart investments, including greater resources for U.S. Cyber Command to pursue electronic warfare capabilities.27

#### Invasion swiftly goes nuclear.

Stacie L. Pettyjohn 22, senior fellow and director of the defense program at the Center for a New American Security; and Becca Wasser, a fellow in the defense program and co-lead of The Gaming Lab at the Center for a New American Security, 5/20/2022, “A Fight Over Taiwan Could Go Nuclear,” https://www.foreignaffairs.com/articles/china/2022-05-20/fight-over-taiwan-could-go-nuclear/, BB

Russia’s invasion of Ukraine has raised the specter of nuclear war, as Russian President Vladimir Putin has placed his nuclear forces at an elevated state of alert and has warned that any effort by outside parties to interfere in the war would result in “consequences you have never seen.” Such saber-rattling has understandably made headlines and drawn notice in Washington. But if China attempted to forcibly invade Taiwan and the United States came to Taipei’s aid, the threat of escalation could outstrip even the current nerve-wracking situation in Europe.

A recent war game, conducted by the Center for a New American Security in conjunction with the NBC program “Meet the Press,” demonstrated just how quickly such a conflict could escalate. The game posited a fictional crisis set in 2027, with the aim of examining how the United States and China might act under a certain set of conditions. The game demonstrated that China’s military modernization and expansion of its nuclear arsenal—not to mention the importance Beijing places on unification with Taiwan—mean that, in the real world, a fight between China and the United States could very well go nuclear.

Beijing views Taiwan as a breakaway republic. If the Chinese Communist Party decides to invade the island, its leaders may not be able to accept failure without seriously harming the regime’s legitimacy. Thus, the CCP might be willing to take significant risks to ensure that the conflict ends on terms that it finds acceptable. That would mean convincing the United States and its allies that the costs of defending Taiwan are so high that it is not worth contesting the invasion. While China has several ways to achieve that goal, from Beijing’s perspective, using nuclear weapons may be the most effective means to keep the United States out of the conflict.

China is several decades into transforming its People’s Liberation Army (PLA) into what the Chinese President Xi Jinping has called a “world-class military” that could defeat any third party that comes to Taiwan’s defense. China’s warfighting strategy, known as “anti-access/area denial,” rests on being able to project conventional military power out several thousand miles in order to prevent the American military, in particular, from effectively countering a Chinese attack on Taiwan. Meanwhile, a growing nuclear arsenal provides Beijing with coercive leverage as well as potentially new warfighting capabilities, which could increase the risks of war and escalation.

China has historically possessed only a few hundred ground-based nuclear weapons. But last year, nuclear scholars at the James Martin Center for Nonproliferation Studies and the Federation of American Scientists identified three missile silo fields under construction in the Xinjiang region. The Financial Times reported that China might have carried out tests of hypersonic gliders as a part of an orbital bombardment system that could evade missile defenses and deliver nuclear weapons to targets in the continental United States. The U.S. Department of Defense projects that by 2030, China will have around 1,000 deliverable warheads—more than triple the number it currently possesses. Based on these projections, Chinese leaders may believe that as early as five years from now the PLA will have made enough conventional and nuclear gains that it could fight and win a war to unify with Taiwan.

Our recent war game—in which members of Congress, former government officials, and subject matter experts assumed the roles of senior national security decision makers in China and the United States—illustrated that a U.S.-Chinese war could escalate quickly. For one thing, it showed that both countries would face operational incentives to strike military forces on the other’s territory. In the game, such strikes were intended to be calibrated to avoid escalation; both sides tried to walk a fine line by attacking only military targets. But such attacks crossed red lines for both countries, and produced a tit-for-tat cycle of attacks that broadened the scope and intensity of the conflict.

For instance, in the simulation, China launched a preemptive attack against key U.S. bases in the Indo-Pacific region. The attacks targeted Guam, in particular, because it is a forward operating base critical to U.S. military operations in Asia, and because since it is a territory, and not a U.S. state, the Chinese team viewed striking it as less escalatory than attacking other possible targets. In response, the United States targeted Chinese military ships in ports and surrounding facilities, but refrained from other attacks on the Chinese mainland. Nevertheless, both sides perceived these strikes as attacks on their home territory, crossing an important threshold. Instead of mirror-imaging their own concerns about attacks on their territory, each side justified the initial blows as military necessities that were limited in nature and would be seen by the other as such. Responses to the initial strikes only escalated things further as the U.S. team responded to China’s moves by hitting targets in mainland China, and the Chinese team responded to Washington’s strikes by attacking sites in Hawaii.

A NEW ERA

One particularly alarming finding from the war game is that China found it necessary to threaten to go nuclear from the start in order to ward off outside support for Taiwan. This threat was repeated throughout the game, particularly after mainland China had been attacked. At times, efforts to erode Washington’s will so that it would back down from the fight received greater attention by the China team than the invasion of Taiwan itself. But China had difficulty convincing the United States that its nuclear threats were credible. In real life, China’s significant and recent changes to its nuclear posture and readiness may impact other nations’ views, as its nuclear threats may not be viewed as credible given its stated doctrine of no first use, its smaller but burgeoning nuclear arsenal, and lack of experience making nuclear threats. This may push China to preemptively detonate a nuclear weapon to reinforce the credibility of its warning.

China might also resort to a demonstration of its nuclear might because of constraints on its long-range conventional strike capabilities. Five years from now, the PLA still will have a very limited ability to launch conventional attacks beyond locations in the “second island chain” in the Pacific; namely, Guam and Palau. Unable to strike the U.S. homeland with conventional weapons, China would struggle to impose costs on the American people. Up until a certain point in the game, the U.S. team felt its larger nuclear arsenal was sufficient to deter escalation and did not fully appreciate the seriousness of China’s threats. As a result, China felt it needed to escalate significantly to send a message that the U.S. homeland could be at risk if Washington did not back down. Despite China’s stated “no-first use” nuclear policy, the war game resulted in Beijing detonating a nuclear weapon off the coast of Hawaii as a demonstration. The attack caused relatively little destruction, as the electromagnetic pulse only damaged the electronics of ships in the immediate vicinity but did not directly impact the U.S. state. The war game ended before the U.S. team could respond, but it is likely that the first use of a nuclear weapon since World War II would have provoked a response.

The most likely paths to nuclear escalation in a fight between the United States and China are different from those that were most likely during the Cold War. The Soviet Union and the United States feared a massive, bolt-from-the-blue nuclear attack, which would precipitate a full-scale strategic exchange. In a confrontation over Taiwan, however, Beijing could employ nuclear weapons in a more limited way to signal resolve or to improve its chances of winning on the battlefield. It is unclear how a war would proceed after that kind of limited nuclear use and whether the United States could de-escalate the situation while still achieving its objectives.

AN OUNCE OF PREVENTION

The clear lesson from the war game is that the United States needs to strengthen its conventional capabilities in the Indo-Pacific to ensure that China never views an invasion of Taiwan as a prudent tactical move. To do so, the United States will need to commit to maintaining its conventional military superiority by expanding its stockpiles of long-range munitions and investing in undersea capabilities. Washington must also be able to conduct offensive operations inside the first and second island chains even while under attack. This will require access to new bases to distribute U.S. forces, enhance their survivability, and ensure that they can effectively defend Taiwan in the face of China’s attacks.

Moreover, the United States needs to develop an integrated network of partners willing to contribute to Taiwan’s defense. Allies are an asymmetric advantage: the United States has them, and China does not. The United States should deepen strategic and operational planning with key partners to send a strong signal of resolve to China. As part of these planning efforts, the United States and its allies will need to develop war-winning military strategies that do not cross Chinese red-lines. The game highlighted just how difficult this task may be; what it did not highlight is the complexity of developing military strategies that integrate the strategic objectives and military capacities of multiple nations.

Moving forward, military planners in the United States and in Washington’s allies and partners must grapple with the fact that, in a conflict over Taiwan, China would consider all conventional and nuclear options to be on the table. And the United States is running out of time to strengthen deterrence and keep China from believing an invasion of Taiwan could be successful. The biggest risk is that Washington and its friends choose not to seize the moment and act: a year or two from now, it might already be too late.

### 2NC---Taiwan---CYBERCOM Key

#### Only cyber cooperation can stop a swift Chinese strike.

Klon Kitchen 22, senior fellow at the American Enterprise Institute, 1/13/2022, “Securing Taiwan Requires Immediate Unprecedented Cyber Action,” https://www.lawfareblog.com/securing-taiwan-requires-immediate-unprecedented-cyber-action, Marsh

As the head of Taiwan’s Department of Cyber Security noted, Taiwan’s “critical infrastructure, such as gas, water and electricity are highly digitized,” meaning that the right cyberattack from China could prove catastrophic and leave the island in disarray. More than a few commentators have suggested that, in the event of an invasion, Beijing would very likely seek a fait accompli victory—a decisively rapid takeover of the island involving a debilitating cyberattack that would avoid a longer and more costly war with the U.S. Due to Taiwan’s level of networked sophistication and Beijing’s strategic imperatives, the unprecedented use of cyberwarfare in Taiwan is more likely than not.

But emerging cyberwarfare tactics differ markedly from conventional dynamics, not least in the degree to which they are covert and preemptive. Networks can be infiltrated silently and exploited months later in an explosive instant. And while the estimated 200-400 cyberattacks that Taiwan endures from China each month don’t constitute acts of war, even one successful attempt to worm into Taiwan’s networks could prove more destructive than any bomb if a military conflict were to kick off. Put simply, cyberwarfare would commence well before formal conflict.

Building on successful U.S.-Taiwan joint cyberwar exercises, the U.S. needs to work with Taipei to threat-hunt on Taiwanese networks as soon as possible. Cyberattacks do not necessarily constitute acts of war, so the U.S. aiding Taiwan’s defense in cyberspace most likely wouldn’t substantively risk upsetting today’s delicate political equilibrium in the Taiwan Strait, save perhaps further deterring Chinese aggression. It would, however, give the island-state a fighting chance against the legions of Chinese military hackers arrayed against it.

### 2NC---Taiwan---Impact

#### An invasion is on the horizon.

Kathrin Hille 6/7, Greater China Correspondent at FT; and Demetri Sevastopulo, US-China Correspondent at FT, 6/07/2022, “Taiwan: preparing for a potential Chinese invasion,” <https://www.ft.com/content/0850eb67-1700-47c0-9dbf-3395b4e905fd>, cc

“This is the decade of concern, particularly the period between now and 2027,” says Phil Davidson, a retired admiral who commanded US forces in the Indo-Pacific until last year. “I make that assessment because of the staggering improvements in Chinese military capabilities and capacities, the political timeline for Xi Jinping and the long-range economic challenges in China’s future.”

Taipei wants to retain military capabilities, such as its F-5 fighter jets, to counter Chinese incursions © Ritchie B Tongo/EPA-EFE

Although China’s threat to seize Taiwan by force has been in place ever since the Chinese Nationalist government and army fled to Taiwan in 1949 after losing the civil war on the mainland, Beijing had long focused on pulling the island into its fold with economic lure and political pressure.

But many Taiwanese policymakers now believe that as the Chinese Communist party loses hope these measures will ever work and with its armed forces modernising rapidly, Xi might opt for war soon.

Taiwan came into renewed focus as an increasingly dangerous flashpoint just days after Biden’s inauguration last year when Chinese warplanes simulated missile attacks on a US aircraft carrier sailing in the vicinity of the country. Over the following months, China then boosted the tempo and size of fighter jet and bomber sorties near Taiwan.

Davidson sounded the alarm in March last year, telling the Senate armed services committee that he believed the threat of a Chinese attack on Taiwan would “manifest . . . in the next six years”. Shortly thereafter, a senior US official told the Financial Times that Xi was flirting with the idea of seizing control.

Since then such warnings have become more widespread — the background to Biden’s comments about responding to a Chinese invasion. It has also accelerated a shift in the conversation between Taiwan and the US over how to defend the island.

Although Washington has been urging Taipei for years to take that risk more seriously, the Taiwanese government and military were slow to respond. But the war in Ukraine has served as a wake-up call. Senior Taiwanese officials say Russia’s assault on its neighbour has highlighted the threat they face.

Phil Davidson, former US Indo-Pacific Commander, believes the threat of a Chinese attack on Taiwan will manifest by 2027 © Hugh Gentry/Reuters

“The danger comes from Xi Jinping and the fact that he will begin a third term later this year,” says one official. “Under China’s previous process where they would have a new leader every 10 years, their ‘historic mission’ of unifying Taiwan could be passed on to the next leader. But when a national mission becomes one man’s mission, the danger rises.”

“Putin would not have made a decision like this to invade Ukraine if he wasn’t deciding everything by himself. So Xi Jinping could well make this kind of misjudgement as well,” the official adds.

A shift from ambiguity

While the Russian invasion of Ukraine has focused attention on the potential threat to Taiwan, there is one big difference between the two situations: a Chinese war on Taiwan could be a war with the US.

When Washington switched diplomatic recognition from Taipei to Beijing in 1979, it replaced its mutual defence treaty with Taiwan with the Taiwan Relations Act. The law requires the US to give the country the weapons needed to defend itself, and to maintain the US’s own capacity to resist force or coercion that would jeopardise Taiwan’s security.

In the past, the US kept it ambiguous how far that commitment went. In an attempt to both deter Beijing from considering military force and discourage Taipei from formalising its independence, Washington declined to spell out whether it would enter a war between the two.

Biden appears to have drastically reduced that ambiguity. Asked by a reporter during his recent trip to Japan if he was willing to use force to defend Taiwan, he said: “Yes. That is the commitment we made.” The White House hurried to stress — as it did after Biden’s previous similar statements which some analysts viewed as gaffes — that US policy towards Taiwan has not changed.

President Joe Biden, during a recent trip to Japan, told a reporter he was willing to use force to defend Taiwan © Eugene Hoshiko/Pool/EPA-EFE

But senior officials in Taiwan and countries allied with the US believe Biden is trying to deter Beijing by signalling more clearly it might have to fight the US, too. “We think Biden has made a political decision to demonstrate that this option cannot be excluded,” says a senior Taiwanese official.

“In the Ukraine case, he said beforehand that the US would not enter the war. But when China feels that their military capability has reached the level ready for taking Taiwan, just using financial or economic sanctions will not create an effective deterrence,” he says. “So you must absolutely not let China believe that you will not take military action.”

Although there is growing concern about a possible invasion, the timeframe of any military action — and China’s real intentions — are still the subject of intense debate.

The year Davidson sees as the potential time horizon for a Chinese attack, 2027, is the centenary of the People’s Liberation Army. In November 2020, the Chinese Communist party said it wanted to “ensure that the 100-year military building goal is achieved by 2027”, called for faster military modernisation and reiterated the goal of making the Chinese military fit for networked, “intelligentised” warfare.

Although those are stock phrases China has used before, the Pentagon calls 2027 a “new milestone”. “If realised, the PLA’s 2027 modernisation goals could provide Beijing with more credible military options in a Taiwan contingency,” it said in its annual report on the Chinese military last year.

Some analysts doubt Davidson’s date. But one year on from his testimony, government and military officials in both Taipei and Washington say the window from now to 2027 is a genuine threat.

Avril Haines, director of national intelligence, told Congress the threat to Taiwan was ‘acute’ between now and 2030 © Evelyn Hockstein/Reuters

Last October, Taiwan’s defence minister Chiu Kuo-cheng said the PLA would have the “complete capability” to attack Taiwan by 2025. “The current situation is really the most dangerous I have seen in my more than 40 years in the military,” he told lawmakers.

### \*1NC---Misinformation

#### CYBERCOM is tackling information warfare, but maintained resources are key.

Mark Pomerleau 22, reporter for DefenseScoop, covering information warfare and cyberspace, 3/11/22, “Cyber Command moving toward an integrated information warfare approach,” https://www.fedscoop.com/cyber-command-moving-toward-an-integrated-information-warfare-approach/, Marsh

U.S. Cyber Command is looking to more tightly link cyberspace “effects” operations with information operations, according to its deputy commander.

When asked where he sees the command headed in the next five to 10 years, Lt. Gen. Charles Moore said he hopes it will broaden the concept of a “truly synchronized and integrated information warfare approach.”

“Without a doubt, what we have learned is that cyber effects operations in … more of a combined arms approach with what we call traditionally information operations, is an extremely powerful tool,” he said Thursday at Cybercom’s legal conference.

Cybercom has reportedly begun engaging in some level of combined operations along these lines. It has been reported that the command has sent messages to Russian cyber operatives letting them know the U.S. military knows who they are and what they’re doing as a means of deterring their potential future malicious activity aimed against the U.S.

Many of the organization’s subordinate commands have taken on a larger role in info warfare for their respective services, reorganizing and consolidating similar capabilities to provide an integrated approach.

Former officials have pushed for a stronger alignment of cyber ops and information ops.

“When you can perform information operations to influence adversaries’ perceptions and maybe their behavior in conjunction with those effects, you can position yourself to see real-time reflections on how they’re assessing what you’re conducting. And then you can stay ahead of their decision cycle, inside of their OODA loop: their observe, orient, decide and action [cycle]. And you can do that at speed over time,” Moore said. “That’s where we want to be. That’s an extremely powerful tool inside the Department of Defense’s toolkit.”

Previously, Moore had explained that under DOD’s authorities and ability to gain access to different types of networks and social media, it can be positioned to see what the adversary is thinking.

“What that allows us to do is in a very precise manner to target individuals or groups of messages that we know will have an effect. And then when you combine that with actual cyber effects itself in a very combined arms approach … [it allows Cybercom] to drive the enemy’s decision calculus and cycle,” he said during an event hosted by C4ISRNET last year.

While cyber operators are experts in networks, not information ops, the services have begun aligning information operations specialists to work alongside cyber operators.

Despite having the necessary policies and authorities in place to execute these types of operations, Moore said DOD will need to harness emerging technologies such as artificial intelligence, big data analytics and even quantum computing to truly be successful in the future.

“You’re going to need these types of capabilities to execute across the breadth, the scope, the depth and the speed that’s going to be necessary to stay ahead of the adversaries and really drive their decisions cycles, drive their perceptions as opposed to being driven,” he said.

A better grasp of information warfare and what that looks like across the federal government and Department of Defense is warranted, Moore said. He explained that the Pentagon and the nation need to focus on a strategy aimed at affecting adversary perceptions.

Such a strategy or an approach should inform the government on what types of things to invest in, what to reveal and conceal, what and when to exercise capabilities and concepts, and when to conduct troop movements.

#### Impact---Fire

Herbert Lin 19, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, “The existential threat from cyber-enabled information warfare,” *Bulletin of the Atomic Scientists*, 75(4), pp. 187-196, T&F, DOI: 10.1080/00963402.2019.1629574, Marsh

On the existential threat from cyber-enabled information warfare

Corruption of the information ecosystem has become an existential threat to civilization as we know it because prosperity and advancement depend on a secure information infrastructure and environment that provides human beings with contextualized, reli­able, trustworthy information when and where it is needed. Information is as much a part of human ecol­ogy and the essence of being human as DNA (itself a form of information!) is a part of the evolutionary processes in biological systems.

Today, chaos reigns in much of the information ecosys­tem on which societies depend. In many forums for poli­tical and societal discourse, national leaders shout about fake news, by which they mean information they do not like. These same leaders lie shamelessly, calling their lies truth, or perhaps "truthful hyperbole." Acting across national boundaries, these leaders and their surrogates exacerbate existing divisions, creating rage and diminish­ing confidence in elections and democratic institutions. Using unsupported anecdotes and sketchy rhetoric, deni- alists undermine well-established science about climate change and other urgent issues. Established institutions of the government, journalism, and education - institutions that have traditionally provided stability - are under attack precisely because they have provided stability.

The founding of the Bulletin predates by several dec­ades the widespread availability of computers, the Internet, smart phones, search engines, and social media. Few could imagine in 1945 a technological envir­onment that affords today's high-speed and widespread connectivity, high degrees of anonymity, insensitivity to distance and national borders, easy and customized information searches, democratized access to publishing capabilities, inexpensive production and consumption of information content (including and increasingly impor­tantly emotionally evocative video and audio content), disintermediation of established information sources, and ubiquitous, always-on, always-available access to information sources through mobile devices.

Such advances in information technology have her­alded the arrival of the information age, a world in which taking near-immediate advantage of information opens up enormous opportunities in both the private and pub­lic sectors for improved delivery of existing products and services and, perhaps more important, the creation of entirely new products and services. Products and ser­vices can be customized to individual needs and prefer­ences on a large scale and at more affordable costs. Transactional friction can be tremendously reduced. Through the Internet of Things, actuators and sensors can be connected to process control computers to opti­mize the behavior and function of physical systems. Everywhere that information can be used to create and improve new and existing functionality (that is, essen­tially everywhere), one can find or imagine new informa­tion technologies to do so.

At the same time, advances in information technology have a dark side. The same increases in the volume and velocity of information have created a louder and more chaotic information environment that stimulates fast, angry, reflexive, intuitive, and visceral thinking, reaction, and action in people and thus displaces more complex, reflective, and rational thought. In a chaotic environment of information overload, people are more likely to use mental shortcuts as a way to reduce the cognitive bur­den that such an environment places on their thinking.

In recent years, we have seen how the Internet, social media, and mobile devices (and other technologies) can be used by foreign adversaries to interfere in elections and to disrupt the democratic process. We have seen:

Social media exploitation of cognitive biases to increase their impact and reach - short messages of 280 characters and emotionally evocative video/ audio clips are nearly ubiquitous and much more the norm than they ever were two decades ago.

Disintermediation of established information sources that reduces the role and influence of those pre­viously responsible for providing factual information and proliferates information sources. The US Supreme Court noted in Associated Press v. US (1945) that "the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public, that a free press is a condition of a free society." Today, modern information technol­ogy has enabled the creation of a larger number of information sources than the 1945 US Supreme Court could possibly have imagined.

Search engines that return highly visible results for queries based in large part on the popularity of those results and the inferred desires of the user for specific information rather than their actual importance to those queries. Such functionality also makes it easier than ever for people to find information online "by doing their own research," thus indulging in their confirmation biases by selectively finding and attend­ing only to information that confirms one's beliefs. Search engine optimization techniques enable gam­ing of search algorithms to promote the visibility of false, misleading, or worthless information.

Many-to-many connectivity that enables the for­mation of echo chambers and media bubbles that reinforce pre-existing beliefs.

Large-scale data mining that allows adversaries to sift huge amounts of personal data on individuals to identify and target those most susceptible to customized, inflammatory, false, malign, or mis­leading messages - and also to keep such mes­sages away from public view.

Near-immediate data transfer, which enables pro­paganda and other malign information to spread far and wide quickly, while efforts to correct false information are more expensive, often fall short, and frequently fail altogether.

Inauthentic voices that are largely indistinguishable from authentic ones. Macedonian entrepreneurs discovered ways to monetize an affinity of Trump voters for fake news (Subramanian 2017). Paid human employees of the Internet Research Agency created and spread false information on behalf of the Russian government prior to the 2016 U.S. election (MacFarquhar 2018). And automated "bots"-accounts purportedly associated with human users but in fact managed entirely or mostly by machines - add further chaos to the information environment.

Is this state of information affairs really new? Haven't adversaries of all stripes always employed propaganda and lies - otherwise known as information warfare (or at least a big part of it) - to advance their interests?

Yes. Information warfare indeed has a long pedigree that reaches into the past for at least the three millen­nia since the Trojan Horse enabled Greek warriors to breach the walls around the city of Troy. Much more recently, the rise of the Nazi regime in Germany relied on propaganda. As Hitler (1925, 155-56) wrote:

[I]ts purpose must be ... to attract the attention of the masses and not by any means to dispense individual instructions to those who already have an educated opi­nion on things or who wish to form such an opinion on grounds of objective study - because that is not the pur­pose of propaganda, it must appeal to the feelings of the public rather than to their reasoning powers. . . . The art of propaganda consists precisely in being able to awaken the imagination of the public through an appeal to their feel­ings, in finding the appropriate psychological form that will arrest the attention and appeal to the hearts of the national masses. ... The receptive powers of the masses are very restricted, and their understanding is feeble.

But more so today than at any earlier point in human history, human beings are vulnerable to information war­fare. At the same time that new information technologies have led to an increase in the volume and velocity of information available on Earth by many orders of magni­tude in the past few decades, the cognitive architecture of the human mind is more or less unchanged on the time scale of centuries or even millennia.

On human cognition

Research in the fields of cognitive and social psychol­ogy has formalized what Hitler knew intuitively. We now understand that human cognitive processing cap­ability is not unlimited; humans have finite cognitive resources that can be "used up" under mentally stress­ful circumstances. Findings from the same cognitive psychology that has transformed neoclassical econom­ics into behavioral economics (and resulted in three Nobel Prizes in economics) have made clear the "bounded rationality" of human thought and the simultaneous existence in every individual of the cap­ability to engage in two types of cognitive processing.

Specifically, heuristic dual-system cognitive theory posits that human beings have two systems for cogni­tive processing - an intuitive, reflexive, and emotionally driven mode of thought (often designated as System 1) and a slower, more deliberate, analytical mode of thought (often designated as System 2). Kahneman (2011) provides a primer on System 1 and System 2 thinking. (See Petty and Cacioppo 1986; Chaiken 1987 for other variants of dual-system cognitive theory; see Kruglanski and Thompson 1999 for a contrary view on dual-system cognitive theory.)

System 1 is designed to operate rapidly, but it can do so because it does not take account of all available information and is thus more prone to error (also called bias). System 2 operates more slowly but is more likely to take into account the available information and is less prone to error. People engaging in System 1 infor­mation processing respond more emotionally and less rationally or critically than in System 2 processing.

Most important, System 1 thinking is the default mode of thought for human beings - it uses smaller amounts of cognitive resources, relies on simple gut- based judgments, and is used more often when humans are under stress. For most situations encoun­tered in everyday life, System 1 thinking is adequate and produces mostly valid and useful outcomes, but it often fails when a situation requires complex inferences for understanding. For such situations, System 2 think­ing, which is effortful and consumptive of cognitive resources, is more often appropriate - and when indi­viduals fail to use System 2 when it is appropriate to do so, they are easily misled.

Most individuals are capable of both System 1 and System 2 thinking; thus, the important operative question is the circumstances under which they select one or the other type of thinking. Psychology has accumulated considerable evidence relevant to this question.

For example, Taber and Lodge (2006) show that an individual tends to be less critical of information that is favorable to his or her position than of information that is not favorable - that is, he or she is more likely to engage in System 1 thinking for favorable information. People have a confirmation bias in their information seeking and processing behavior - they preferentially seek out information that is consistent with their beliefs and they are highly critical of (or ignore) information that contradicts their beliefs. In a meta-analysis of 91 studies, Hart et al. (2009) considered two motivations for how an individual might select information to consume - the desire to gain an accurate understanding of reality and the desire to feel validated in his or her beliefs. These two motivations conflict when an accurate understanding of reality does not validate one's beliefs, and such a situation motivates the question of which of these motivations is more powerful. Hart et al. concluded that both motivations drive human information- seeking behavior, thus moderating each other to a certain extent, but that on balance, humans do exhibit a tendency towards the validation of their beliefs. People are also subject to belief perseverance (a.k.a. a continuing influence effect) - a cognitive bias through which individuals do not revise beliefs based on erro­neous information even when they know for sure that such information is erroneous (Lewandowsky et al. 2012).

Maintenance of an individual's social identity is an important influence on his or her invocation of System 1 or System 2 thinking. Evidence suggests that indivi­duals tend to adopt the views of the peer groups that are most salient to them, even if the "objective" or "factual" information available to them contradicts those views. (Asch 1951 performed the classic "confor­mity experiments" that demonstrated this phenomenon in the early 1950s.) Uncritical System 1 thinking is active in processing information that is consonant with the beliefs and attitudes of those peer groups. Critical and skeptical System 2 thinking is active in processing infor­mation that is dissonant to those groups' beliefs. These effects (that individuals tend to accept salient group norms) are even more pronounced in an anonymous environment, such as that which characterizes much online interaction (Postmes et al. 2001).

Lastly, there is evidence that emotion and motivation affect cognition. For example, people who are angry tend to rely more heavily on simple heuristic cues (sug­gestive of System 1 thinking) than those who are not angry (Bodenhausen, Sheppard, and Kramer 1994). Individuals are more likely to stereotype people (a form of System 1 thinking) when that stereotype is consistent with their desired impression of those people; conver­sely, when the stereotype is inconsistent with their desired impression, individuals tend to inhibit the use of this stereotype (Kunda and Sinclair 1999). Negative emotions (such as those induced by the receipt of infor­mation incongruent with a person's prior beliefs) can improve the ability of a person to reason logically, thus enabling him or her to negate or discount that informa­tion (Goel and Vartanian 2011).

In the new information environment, exploitation of human cognitive architecture and capabilities - which are largely unchanged from what existed millennia ago - provides the 21st century information warrior with cyber- enabled capabilities that Hitler, Stalin, Goebbels, and McCarthy could have only imagined. By exploiting cogni­tive limitations, the perpetrators of cyber-enabled infor­mation warfare have learned to exacerbate prejudices, biases, and ideological differences; to add heat but no light to political discourse; and to spread widely believed "alternative facts" in advancing their political positions.

Russian interference in the 2016 US presidential elec­tion has dominated news headlines ever since. But interference by authoritarian countries in the elections of democratic states - as undesirable and threatening as it may be - is hardly the only negative consequence of cyber-enabled information warfare. The problems of nuclear war and climate change are hard enough to solve even when well-intentioned, well-informed par­ties on all sides share a basic understanding and knowl­edge of the relevant facts. Yes, they may have different values and different priorities, may act under different constraints, and be able to bring to bear different levels of resources to these problems.

But without shared, fact-based understandings of the blast, thermal, and radiation effects of nuclear explosions, what hope is there for national leaders to reach agreements to reduce the threat of nuclear holo­caust or to make good decisions about nuclear weap­ons use in times of crisis? Without shared, fact-based understandings that rising atmospheric carbon dioxide concentrations caused by human beings result in cor­responding increases in global temperature and cli­matic disruption, what hope is there for national leaders to reach agreements to begin serious efforts at decarbonizing their economies?

Climate change denialism

Climate change denialism can be fairly characterized as cyber-enabled information warfare against the reality of large-scale anthropogenically-induced climate change. In the responses of people resistant to taking action to miti­gate climate change, we see a number of psychological factors at work (Zaval and Cornwell 2016). For example, one key element of System 1 thinking is the availability heuristic, with which individuals tend to associate the like­lihood of an event with the ease with which they can remember similar events in the past. But the long-term consequences of climate change are unprecedented in recorded human history and obviously people have no personal memories of unprecedented events.

Moreover, climate change is a long-term process whose inexorable progression is easily masked by short-term fluc­tuations in local weather conditions. For example, public concerns about climate changes correlate with local weather conditions (Krosnick et al. 2006). Climate change deniers are also quick to flag for public attention days that are particularly cold as "evidence" that global warming is not occurring and thus, they claim, discrediting theories of climate change. This illustrates a bias known as attribute substitution, as Kahneman and Frederick (2002) describe, through which individuals substitute salient information (such as the cold temperature today) for information that is more relevant but harder to understand (such as infor­mation about global climate change).

People are also subject to a loss-aversion bias, in which they place greater weight on losses than gains of equal value. In 1992, the United States committed itself to the United Nations Framework Convention on Climate Change, although President George HW Bush also stated that "the American way of life is not up for negotiation" - and in 2018, the United States withdrew from the Paris Agreement (which was based on the convention). The argument? That the United States would have to give up too much if it kept to the agreement.

To close this (merely illustrative) exploration of biases relevant to climate change denialism, the optimism bias suggests that people consider themselves exceptions when considering the likelihood of a negative event occurring. That is, bad things may happen to other peo­ple, but they won't happen to me, even though I and those other people are similar in important and relevant ways. In a climate context, the bad things may involve sea level rise or heat waves - and the misperception that "others may suffer from such problems but I won't" diminishes the power of personal concern as a driver for rational decision making.

Connecting the operation of these cognitive biases to the affordances of modern information technologies is not difficult. For example, Roxburgh et al. (2019) demonstrate how the characteristics of specific weather events (e.g. hurricanes or snowstorms) and "short-term socio-political context can play a critical role in deter­mining the lenses through which climate change is viewed." Note especially the importance of "short-term socio-political context" - precisely the context that social media shapes.

Elsasser and Dunlap (2013) noted the influential role of a variety of newspaper columnists in advancing denialist arguments and thus amplifying these argu­ments to a broad segment of the American public. Fewer in number then, essentially all columnists today (of all political leanings) have a social media presence that they use to publicize their work, and in many instances their online presence is driven in significant part by social media and reach many more readers online than in print. Furthermore, subtleties and nuan­ces in their extended written pieces are likely to be lost when they are represented in social media.

Another important element of climate change denial- ism is the easy accessibility of seemingly-authoritative information that casts doubt on the well-established science of climate change. As reported by The Guardian, a variety of largely secret funding sources distributed $118 million to 102 denialist organizations (Goldenberg 2013). Oreskes and Conway (2011) provide the definitive work on deliberate information campaigns to obscure the scientific truth on a range of issues from smoking to climate change. These denialist organizations have gen­erated a variety of products for public and policy con­sumption (but - unsurprisingly - not many peer-reviewed scientific articles) that are easily accessible to the public, mainstream media outlets, and policy makers. Their pro­ducts are broadly disseminated through social media and easily found through customized search, and they are sought by reporters who seeking to cover "both sides" of a controversy that is intellectually equivalent to a "controversy" about whether the earth is round or flat.

Nuclear conflict

On the risks of nuclear conflict, theories and approaches to nuclear deterrence and strategic stability developed prior to the collapse of the Soviet Union in the late 1980's and early 1990's rest on the presumption of rationality in national decision makers. In particular, they assume that adversaries are deterred from attacking by a threat of retaliation that would impose costs on the adversary that would outweigh any conceivable benefits that it would gain from an attack (Morgan 2003). Central to this assumption is a rational adversary that can and does make a calculation of expected costs and benefits, com­pares them, and then acts accordingly.

But the psychologically informed understanding of real- world decision making described above was not accepted widely in the scientific literature until approximately the same time as the collapse of the Soviet Union, and the seminal work in such understanding occurred only in the decade previous to that. What a psychologically-informed understanding of real-world decision making tells us is that the rationality assumption at the base of much traditional thinking on deterrence and strategic stability is untenable, given that humans have evolved to rely on intuitive, reflex­ive, heuristic System 1 thinking to make decisions, particu­larly when faced with time pressures, surprise and other obstacles to the deliberate calculation implied by System 2 thinking (Kahneman 2011). Psychology tells us that - more often than not - the fast, intuitive judgements of System 1 often take precedence over the slower, more analytical thinking of System 2.

The challenges posed by reflexive reliance on System 1 thinking are greatly accentuated by characteristics of today's information environment. Social media networks in particular are optimally designed to stimulate System 1 thinking - emotional, reflexive, immediate - and they rapidly transmit content among like-minded individuals, creating the ideal conditions for public polarization and divisiveness to occur (Pfeffer, Zorbach, and Carley 2014). Multiple narratives rapidly emerge around complex events; citizens splinter into their own informational universes and are unable to agree on an underlying reality. Political leaders themselves are subject to these conflicting narratives and may even be active and influ­ential participants in one or another of them.

It is thus easy to posit that in this information envir­onment, manipulated information - either artificially constructed or adopted by a strong grassroots base - could be used by interested parties to generate pres­sure on leaders to act. At the same time, leaders them­selves are likely to be facing information overload and less able to distinguish analyzed information from their own intelligence sources and other, unvetted informa­tion originating from their constituencies.

The coming information dystopia

Nuclear war and climate change are arguably the most important existential challenges today that are com­pounded by the corruption of the information ecosys­tem. But even if a single miraculous stroke the laws of physics were changed to make nuclear weapons impos­sible to build and operate and to immediately eliminate anthropogenic emissions at zero cost, cyber-enabled information warfare could still can lead to an informa­tion dystopia. Here are some possible elements:

• Adversaries manufacture numerous graphic videos of American soldiers (complete with sound effects) committing battlefield atrocities, and spread them widely through the Internet. Once upon a time, high- quality video forgeries were difficult and expensive to make. AI-based technologies will bring this so- called deepfake capability to the masses, and anyone with imagination, a modicum of technical skill, and a personal computer will be able to distribute rea­sonably realistic forgeries. Denials will be issued but of course will also not be believed by large fractions of viewers. Even if proof of inauthenticity can be provided, such evidence will not affect the responses of many viewers.

Political campaigns conduct similar efforts to dis­credit political opponents (e.g. "showing" an oppo­nent making controversial or disqualifying remarks before an election). But they also use the existence of deepfake technologies to deflect attention from authentic and real evidence of their own political and personal misdeeds. For example, a real video of a candidate punching an old lady who supports his opponent will be dismissed as "one of those deepfakes that anyone could have produced."

Financial markets are disrupted by falsified videos of CEOs making announcements regarding company prospects that are much more pessimistic than expected. Attempts to correct the record are drowned out in a subsequent flood of contradictory informa­tion, all of which appear at firstglance to be authentic.

Public safety is compromised by reports of local disasters (e.g. explosions of chemical plants that result in the release large amounts of toxic gases). These reports, along with "authentic" video of peo­ple choking amidst locally familiar locations (e.g. well-known fields or sport stadiums), cause sponta­neous mass evacuations. Contradictory directions for evacuation broadcast using social media result in chaos on the streets and highways.

Public health is placed at risk when the safety and efficacy of medical treatments known to be safe and effective are publicly questioned through active disinformation campaigns conducted on the Internet and in bookstores. Attempts to pro­vide valid information are met with responses such as "that's what the pharmaceutical companies and medical establishment want you to think, but just look at what's happened to our children."

Children in schools are threatened by online cam­paigns to spread rumor, innuendo, and positive or negative information about various students. Conducting such campaigns for pay becomes the business model of entrepreneurs who advertise that they can guarantee admission to selective colleges, boost the social standing of the children of their cli­ents, or take revenge on those who have harmed such children, all in anonymous and untraceable ways.

Journalists, political leaders, and judges are com­promised by artfully forged emails and alterations to other documents that are mixed with entirely authentic leaked emails and documents and are indistinguishable from them.

A world with these elements - and many more com­parable ones - will be the inevitable result if and when deployment and use of the tools of cyber-enabled infor­mation warfare become widespread. And even more troubling is the fact that not every bit of information needs to be corrupted for this dystopian outcome to occur - it will require only a fraction of it to be corrupted for people to lose faith entirely in "objective" and "trust­worthy" sources of information, the result of which will be that people will fractionate into their own information realities.

Fearing the end of the enlightenment

The Enlightenment established reason and reality as the foundational pillars of civilized discourse. In such discourse, logic matters, and a logical contradiction between state­ment A and statement B means that at least one of those statements is false. The truth of a statement about the world is tested by its correspondence to objective reality rather than by how many people believe it; that is, empiri­cal data are influential. Furthermore, statements known to be wrong or false do not affect conclusions or choices between alternative courses of action.

Cyber-enabled information warfare provides the tac­tics, tools, and procedures - in short, the means - to replace the pillars of logic, truth, and reality with fan­tasy, rage, and fear. In a world of ubiquitous cyber- enabled information warfare, communication and infor­mation inflame passions rather than informing reason, play to the worst in people's cognitive architectures rather than the best, and divide rather than unify. Deliberate corruption of the information ecosystem could be seen as an analog of poisoning water supplies that can be done remotely, inexpensively, and anon­ymously. All of this is just another way of saying that today it is possible to see glimmerings of an anti- Enlightenment that can possibly take root and that would indeed be the end of civilization as we know it.

Adversaries foreign and domestic that make use cyber-enabled information warfare turn our internal cognitive processes and our external institutional and legal processes against us. Under the cover of "fair play" rubrics and the First Amendment, they have turned us against ourselves. Desperately needed are ways of countering the insidious tactics of cyber-enabled infor­mation warfare for ourselves.

How might we proceed? We need action to develop better ways of identifying adversary cyber-enabled infor­mation warfare campaigns in progress; good counter- measures to help human beings resist the use of cyber- enabled information warfare operations targeted against them; and good measures to degrade, disrupt, or expose the adversary's use of cyber-enabled information warfare operations. All of this is easier said than done, however, as cyber-enabled capabilities for information warfare increase while human cognitive limitations remain the same. Our work is cut out for us. If we fail, the world is at increasing risk of large-scale and long-term societal frac­ture, the end of the Enlightenment, and the start of an informational Dark Age.

# NSA/Splitting DA

## 1NC

### NSA DA---1NC

#### The DOD’s Cyber Command will remain wedded to the NSA for now, but growing capacity for CYBERCOM can break it off.

Mark Pomerleau 22, reporter for DefenseScoop, covering information warfare and cyberspace, 3/08/2022, “Cyber Command and NSA still working to meet measures necessary to split,” <https://www.fedscoop.com/cyber-command-and-nsa-still-working-to-meet-measures-necessary-to-split/>, cc

Several years ago, in response to rumors a split was imminent, Congress felt such a decision was premature and Cyber Command was not ready to stand alone. As such, Congress outlined a series of metrics for the Pentagon to meet in the 2016 annual defense policy bill. Those metrics were then tweaked in the 2017 policy bill adding more restrictions necessary to split the dual hat. They included that each organization have robust command and control systems for planning, deconflicting and executing military cyber operations and national intelligence operations as well as ensuring tools and weapons used in cyber operations are sufficient for achieving required effects. It also sought to ensure that Cyber Command can acquire or develop these tools, weapons, and accesses.

In recent years, Cyber Command has gained significant, yet still maturing, acquisition authority to purchase its own capabilities. It also developed what it calls the Joint Cyber Warfighting Architecture, which guides the command’s acquisition priorities and includes major programs for infrastructure and tools separate from those of the NSA.

Nakasone said that decisions to separate the infrastructures were made before he took command, but he added they were good decisions and they continue to carry out separate infrastructures.

The dual-hat arrangement has been a hotly debated topic in the cyber and intelligence world, with proponents saying the military can benefit from the unique intelligence insights and access of NSA, leading to faster decision-making and operational outcomes. Opponents argue the roles are too powerful for one person and relying on intelligence infrastructure and tools, which are meant to stay undetected, for military activity poses risks to such espionage activity.

Despite the initial dual-hat relationship, it was always understood that it would not be permanent given the inherently different missions of each organization: foreign intelligence and warfighting.

However, officials have increasingly spoken favorably about the nature of the relationship, saying it provides a degree of speed and synergy needed to keep pace in the modern digital world.

#### Funneling more resources and responsibility to CYBERCOM gives it unprecedented autonomy, spurring separation from the NSA.

Jon R. Lindsay 20, assistant professor at the Munk School of Global Affairs and Public Policy and the Department of Political Science at the University of Toronto, 10/30/2020, “Cyber conflict vs. Cyber Command: hidden dangers in the American military solution to a large-scale intelligence problem,” *Intelligence and National Security* 36(2), https://doi.org/10.1080/02684527.2020.1840746, cc

Classic organization theory stresses that bureaucratic organizations seek resources, autonomy, and control, guided by their historical cultural heritage or essential identity.64 For military organizations this translates into a predilection for offensive doctrines, often described as ‘the cult of the offensive,’ because they require expensive capabilities, necessitate authority for independent operations, reduce uncertainty by setting the operational tempo, and are consistent with a warrior ethos.65 The institution of the U.S. Air Force is an instructive example in this regard. Even when the Air Corps was formally part of the U.S. Army, airmen developed an ambitious new doctrine – strategic bombing – that advertised the ability to deliver victory independently of the other services.66 The ideology of strategic bombing served the Air Force well in interservice competition during its formative years as an independent service, even if the theory often proved disappointing in practice.67 A doctrine of independent strategic effects helped to bolster the legitimacy of a newly independent command. The newly autonomous U.S. Space Force tends to advance similar arguments, cribbed from classic airpower theory, about the unique strategic importance of the space domain and the specialized technical skills needed to exploit it.68

From this perspective, CYBERCOM’s doctrine of persistent engagement plays a similar institutional role as strategic bombing did for the early Air Force. New ideas about cyber campaigns, and accompanying authorities to carry them out, are supposed to enable CYBERCOM to create meaningful strategic effects. CYBERCOM advertises its intention to act beneath the threshold of war to influence strategic adversaries. Persistent engagement, from this perspective, might be described as a nonlethal version of strategic bombing. Much as the Air Force seeks to attack critical nodes in an enemy target system, using technology to create strategic effects, cyber campaigns target critical information nodes in the adversary’s computer network to shape its behavior. The comparison to the Air Force experience may be more than metaphorical. As Sarah White notes in her study of U.S. military cyber subcultures, ‘By the end of 2007, the Air Force had emerged as the recognized service leader in cyberspace. While the other services were engaged in the patchwork pursuit of various cyberspacerelated initiatives, neither the Army nor the Navy had the level of decisive senior leader engagement or senior leader direction that existed in the Air Force in 2007.’69 The Air Force approach, which has been influential in CYBERCOM’s doctrinal ruminations, was ‘marked by the firm distinction of cyberspace as a warfighting domain, the increasingly aggressive pursuit of autonomy in cyberspace operations and organizations, and the creation of a dedicated cyberspace career field.’70

Questions of strategic validity notwithstanding, CYBERCOM’s new doctrine is instrumentally useful for enhancing bureaucratic identity, control, autonomy, and resources. A supposed technological imperative to ‘defend forward’ in the ‘cyber domain’ provides an intellectual justification for a military organization like CYBERCOM to do what is inclined to do anyway, namely conduct autonomous offensive operations to create strategic effects. Proactive campaigning to influence or disrupt the adversary’s networks is consistent with the offensive warrior ethos of military institutions. Offensive operations, rather than reactive defense, also enables CYBERCOM to assert control in a highly uncertain environment. Expanded authorities for peacetime operations provide some autonomy from other services, as well as the intelligence community. To ‘man, train, and equip’ the cyber mission forces that will implement the new doctrine, finally, CYBERCOM needs plans, budget allocations, and personnel. It is also helpful to use the same language that other military commands use to explain how and why cyber warriors should be included in joint task forces.

A crowded house CYBERCOM needs to do two things to persuade decisionmakers throughout the Department of Defense and the Executive and Legislative branches to provide the authorities and resources it needs to pursue its preferred course of action. First, CYBERCOM needs to make itself comparable to other services by arguing that it performs familiar categories of military operations – command, intelligence, fire, maneuver, protection, sustainment – in a warfighting domain just like other military services. Second, it must also distinguish itself from its former homes in U.S. Strategic Command (STRATCOM) and the National Security Agency (NSA), as well as superficially similar organizations like U.S. Special Operations Command (SOCOM).

CYBERCOM was formally created in 2010 as a sub-unified command under STRATCOM and became a fully-fledged unified military command in 2018. It incorporated elements that had previously functioned under STRATCOM such as, on the offensive side, Joint Functional Component Command for Network Warfare, and on defense, Joint Task Force Global Network Operations.71 CYBERCOM’s defensive mission also overlaps with the network administrators at the Defense Information Systems Agency and the cryptographers at the NSA Central Security Service. As of early 2019, CYBERCOM had a full-time staff of ‘1,520 military and civilians, plus contractors’ together with ‘4,406 Service members and civilians in our Cyber Mission Force.’72

The service components each brought distinct organizational cultures and institutional histories to CYBERCOM.73 The Air Force articulated an early vision of cyber power as strategic airpower but then struggled to find its cyber warriors a permanent home, resulting in a split between the air intelligence and cyber communities. Army cyber personnel were initially split across different branch baronies before being consolidated in Army Cyber Command, which had a notably more tactical focus, with some friction between the military intelligence and signals (network administration) communities. The Navy approach to cyber was dominated by cryptologists, who enjoyed a long and close working relationship with NSA, under the umbrella of a vague new construct of maritime information dominance. With so much institutional diversity in its ranks, CYBERCOM has strong incentives to articulate common doctrinal concepts to coordinate and control other organizations’ resources.

#### That split erodes unity of command, decimating speed and communication in cyberdefense.

Chris Demchak 21, Grace M. Hopper Chair of Cyber Security and Senior Cyber Scholar, Cyber and Innovation Policy Institute, U.S. Naval War College, 3/05/2021, “FIVE REASONS NOT TO SPLIT CYBER COMMAND FROM THE NSA ANY TIME SOON – IF EVER,” <https://warontherocks.com/2021/03/five-reasons-not-to-split-cyber-command-from-the-nsa-any-time-soon-if-ever/>, cc

Nonetheless, a divorce of this kind is the wrong long-term solution for both agencies and for the nation. Cutting up what’s known as the “dual hat” — an arrangement under which the same leader runs both Cyber Command and the NSA — fragments American “defend forward” capabilities when the nation needs them to be integrated the most. These capabilities allow Cyber Command in particular to operate outside of formal military networks to disrupt malicious attacks at their sources, and are deeply dependent on the closely combined skills of both organizations. The proposal risks reigniting turf battles between the intelligence and operations arms of the secretary of defense and mistakes the intertwined relationship between defense and offense in cybered conflict. Instead of simplistic organizational surgery, therefore, what’s needed is a longer-term plan incorporating Cyber Command and, especially, the capabilities of the National Security Agency into a resilient and adaptive whole-of-society cyber defense system.

Reasons to Avoid Recreating Silos

Reason 1: Scale of Adversaries

First, the scale of adversary cyber threats is unprecedented, prompting cyber commands not only in the United States but elsewhere to expand budgets and personnel. The latest attack, the so-called SolarWinds campaign, is only one of a legion of campaigns attacking the nation as well as its allies. The massive volume of systemic assaults against the United States and allies requires a matching scale of coordinated units with integrated knowledge and capability for action. Cybered conflict today involves countering adversaries that are operating at a scale and with a reach that is already overwhelming to the combined size of the dual-hatted unit, other federal civilian cyber entities, and the huge commercial cyber security community of the United States. Scale is needed to defeat scale when the battlefield is the interconnected cyberspace substrate underlying all modern national socio-technical-economic systems. Separating the two organizations means withdrawing the huge intelligence agency’s knowledge-generating and cyber security assets back to more traditional strategic national intelligence and defensive information-assurance missions, and away from the more offense-oriented but smaller Cyber Command. There is already a national shortage of people with advanced computer skills. These folks are now shared relatively readily between the joined organizations. A split would increase the competition for such talented employees just when collectively employing the limited set of “wizards” efficiently is essential. Splitting the dual-hat arrangement further weakens an already too small and fragmented U.S. national effort in cyber defense.

Reason 2: Speed in Trade-Off Decisions

Second, the split is likely to hand the speed advantage to adversaries. Unity of command has long been taken for granted as key to a faster decision in a crisis, even given the size of the organization. Having a single leader is even more important in cybered conflict, where offense and defense are inextricably linked, and the guidance of a shared boss helps ensure more speedy trade-off decisions. Weapons in cyber operations need to be tailored to cybered targets in ways more traditional weapons do not. That tailoring requires careful, highly responsive timing and constantly refreshed intelligence. Cyber defense requires a more in-depth understanding of corresponding offensive tools and operations than is required in conventional military forces. Executing cyber offense requires a similar knowledge of cyber defense. Exquisitely detailed intelligence therefore becomes exceptionally important to knowing whether the cyber tools have any discernible offense and defense effects, let alone those desired.

Having the two organizations share the same person as commander in the dual hat is far from what later critics might explain as a convenient, short-term nurturing arrangement for the infant Cyber Command. Rather, it is intended to achieve a longstanding military desire of having close and effective — and therefore accurate and rapid — integration of intelligence and operations. With a dual-hat arrangement, the single individual at the head of Cyber Command and the NSA can more effectively and quickly tailor demand signals to both planners and developers about the intelligence needs of operations against specific targets. Suboptimal speed in trade-off decision-making is certainly more likely if there are two peer organizational leaders viewing themselves as having two different missions.

Reason 3: Synergy in Innovative Shared Operations

Third, separating intelligence from operations as it was before the dual-hat arrangement cedes a critical synergy advantage to adversaries. In all conflict, having knowledge in advance is key to success, resilience, and innovation around future threats, and it is often found by accidental exchanges among colleagues or peers routinely working with each other. Unexpected information discoveries would be less readily shared if the two organizations split. Cyber Command’s operational interests would no longer be prominent in the intelligence analysts’ chain of command or field of view. The traditional distinctions between operations and intelligence concerns are likely to return, with less frequent shared daily practices marking the current operational teams.

To be clear, it is much easier to decouple two organizations than to integrate them — to destroy synergy than to create it. The evolution of a more integrated understanding of cyber operational needs has been a long, hard-fought success so far, and it is not guaranteed to survive a separation. There are always voices in favor of decoupling, irrespective of the overarching benefits. For example, an NSA colleague remarked in a private conversation several years ago that they thought the intelligence agency itself was becoming too “military” in its organization and short-term in its thinking under the dual-hat arrangement. Similarly, in 2016 the executive director of U.S. Cyber Command was quoted as saying, “As the United States Cyber Command, we need totally separate tools and infrastructure to conduct our operations.” If the organizations split, these opinions may gain more adherents and dominate collective efforts. The turf-reinforced bureaucratic divisions would return and the commonality of understanding developed over the past 10 years would wither. So would the spontaneous support in ideas, sacrifice, additional time, and innovative action. If the organizations are separated, the consequences are likely to be less agile, intuited, and innovative cyber operations in both organizations.

#### Rapid response and info-transmission avoid cyberattacks on NC3 systems---those go nuclear.

Michael Klare 19, professor emeritus of peace and world security studies at Hampshire College and senior visiting fellow at the Arms Control Association, November 2019, “Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation,” <https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation>, cc

These links exist because the NC3 systems of the United States and other nuclear-armed states are heavily dependent on computers and other digital processors for virtually every aspect of their operation and because those systems are highly vulnerable to cyberattack. Every nuclear force is composed, most basically, of weapons, early-warning radars, launch facilities, and the top officials, usually presidents or prime ministers, empowered to initiate a nuclear exchange. Connecting them all, however, is an extended network of communications and data-processing systems, all reliant on cyberspace. Warning systems, ground- and space-based, must constantly watch for and analyze possible enemy missile launches. Data on actual threats must rapidly be communicated to decision-makers, who must then weigh possible responses and communicate chosen outcomes to launch facilities, which in turn must provide attack vectors to delivery systems. All of this involves operations in cyberspace, and it is in this domain that great power rivals seek vulnerabilities to exploit in a constant struggle for advantage.

The use of cyberspace to gain an advantage over adversaries takes many forms and is not always aimed at nuclear systems. China has been accused of engaging in widespread cyberespionage to steal technical secrets from U.S. firms for economic and military advantages. Russia has been accused, most extensively in the Robert Mueller report, of exploiting cyberspace to interfere in the 2016 U.S. presidential election. Nonstate actors, including terrorist groups such as al Qaeda and the Islamic State group, have used the internet for recruiting combatants and spreading fear. Criminal groups, including some thought to be allied with state actors, such as North Korea, have used cyberspace to extort money from banks, municipalities, and individuals.4 Attacks such as these occupy most of the time and attention of civilian and military cybersecurity organizations that attempt to thwart such attacks. Yet for those who worry about strategic stability and the risks of nuclear escalation, it is the threat of cyberattacks on NC3 systems that provokes the greatest concern.

Gen. Paul M. Nakasone, commander of U.S. Cyber Command, testifies during a Senate Armed Services Committee hearing on February 14. He warned that China and Russia are conducting sustained cybercampaigns against the United States. (Photo: Mark Wilson/Getty Images)Gen. Paul M. Nakasone, commander of U.S. Cyber Command, testifies during a Senate Armed Services Committee hearing on February 14. He warned that China and Russia are conducting sustained cybercampaigns against the United States. (Photo: Mark Wilson/Getty Images)This concern stems from the fact that, despite the immense effort devoted to protecting NC3 systems from cyberattack, no enterprise that relies so extensively on computers and cyberspace can be made 100 percent invulnerable to attack. This is so because such systems employ many devices and operating systems of various origins and vintages, most incorporating numerous software updates and “patches” over time, offering multiple vectors for attack. Electronic components can also be modified by hostile actors during production, transit, or insertion; and the whole system itself is dependent to a considerable degree on the electrical grid, which itself is vulnerable to cyberattack and is far less protected. Experienced “cyberwarriors” of every major power have been working for years to probe for weaknesses in these systems and in many cases have devised cyberweapons, typically, malicious software (malware) and computer viruses, to exploit those weaknesses for military advantage.5

Although activity in cyberspace is much more difficult to detect and track than conventional military operations, enough information has become public to indicate that the major nuclear powers, notably China, Russia, and the United States, along with such secondary powers as Iran and North Korea, have established extensive cyberwarfare capabilities and engage in offensive cyberoperations on a regular basis, often aimed at critical military infrastructure. “Cyberspace is a contested environment where we are in constant contact with adversaries,” General Paul M. Nakasone, commander of the U.S. Cyber Command (Cybercom), told the Senate Armed Services Committee in February 2019. “We see near-peer competitors [China and Russia] conducting sustained campaigns below the level of armed conflict to erode American strength and gain strategic advantage.”

## Impact

### Impact---NC3---Coop Key---2NC

#### Overlaps in authority wreck NC3 defenses---but unity of command solves.

Morgan Dwyer 20, fellow in the International Security Program and deputy director for policy analysis in the DefenseIndustrial Initiatives Group at the Center for Strategic and International Studies (CSIS), 10/15/2020, “Cross-domain Competition,” <http://defense360.csis.org/wp-content/uploads/2020/10/Dwyer_NuclearNexus_Cross-domain-competition1.pdf>, cc

When separate authority stovepipes intersect but values conflict, cooperation is challenging, even in the context of shared missions.43 In these circumstances, outside intervention is required to determine which organization is actually in charge. For example, in the traditional nuclear community—which not only includes the military services and Strategic Command but also the Department of Energy (DOE)—policymakers established the Nuclear Weapons Council.44 The authorities and responsibilities for council participants are specified by law, policy, and memorandums of agreement between DOD and DOE.45 Without a similar governance structure or single authority capable of compelling interorganizational change, it seems unlikely that DOD’s separate space or cyber institutions will poactively declassify any capabilities, even those which might help deter attacks on NC3.46

Separate authority stovepipes may also create barriers to employing offensive weapons. For example, if an adversary attacks the NC3 architecture in the cyber domain, and DOD does not wish to retaliate using a nuclear weapon,47 which combatant command is in charge of the response, Strategic or Cyber Command? DOD’s cyber doctrine specifies that Cyber Command’s role vis-à-vis the other combatant commands varies as a function of whether operations are local or global.48 Furthermore, it states that the support/supporting relationships between commands are established on a by-mission basis.49 These public statements, of course, leave the unanswered the question of which combatant command—Cyber or Strategic Command—is in charge of non-nuclear responses to cyberattacks on NC3.

Furthermore, what happens if attacks cross domains? How then should DOD integrate three separate authority stovepipes—in the Strategic, Space, and Cyber Commands—to effectively and efficiently respond? If DOD is to credibly threaten any response to space or cyber-based attacks on NC3, these basic unity of command questions deserve answers.50 To date, however, Vice Chairman John Hyten admits that DOD has not sufficiently addressed these questions, noting: “We just decided that we’d call each other combatant commands, and not put an adjective on the front.”51 By failing to specify a critically important adjective—whether a command is supporting or supported—DOD leaves unanswered the question of who is in charge when attacks cross domains.

### Impact---NC3---AT: Safe---2NC

#### The software’s vulnerable.

Suzanne Smalley 6/15, reporter covering intelligence and disinformation at CyberScoop and former Mandiant exec tapped to run CTIIC, ODNI's cyber threat intelligence center, 6/15/2022, “House Armed Services chair calls national security software, systems 'too vulnerable',” <https://www.cyberscoop.com/adam-smith-national-security-software-house-armed-services/>, cc

Rep. Adam Smith, the chairman of the House Armed Services Committee, said Tuesday that the United States needs to invest far more in protecting national security communications and software.

“Our number one biggest vulnerability in the cyber world is we have systems that are too vulnerable to attack right now because they’re old and we just, we haven’t updated those systems,” the Washington Democrat said. “Rather than buying another how many ever F-35s [combat planes] … I’d rather pour that money into developing the JADC2 [Joint All-Domain Command and Control] vision of a secure communication system that we can protect.”

JADC2 refers to the Department of Defense’s aspiration to connect sensors from all of the military services into a single network.

“DOD officials have argued that future conflicts may require decisions to be made within hours, minutes or potentially seconds compared with the current multi-day process to analyze the operating environment and issue commands,” the Congressional Research Service said of JADC2 in January. “They have also stated that the department’s existing command and control architecture is insufficient to meet the demands of the National Defense Strategy.”

### Impact---NC3---AT: Defense---2NC

#### Risk of NC3 attacks are high---discard outdated evidence about ‘airgapping’

Erica Lonergan 22, assistant professor in the Army Cyber Institute at West Point and a research scholar at the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University; and Keren Yarhi-Milo, the Arnold A. Saltzman Professor of War and Peace Studies in the political science department and the School of International and Public Affairs and the director of the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University, 4/21/2022, “CYBER SIGNALING AND NUCLEAR DETERRENCE: IMPLICATIONS FOR THE UKRAINE CRISIS,” <https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/>, cc

How Cyberspace Is Creating Nuclear Risks

Policymakers and academics are attuned to the cyber risks to nuclear command and control. The practitioner community has largely focused on U.S. vulnerabilities and how to mitigate them. Scholars, in turn, worry about how cyber operations could have unintended escalatory consequences. But less attention has been paid to another likely scenario: the use of cyber operations for signaling purposes (operations with visible effects that aim to convey a message to another state) in a nuclear context. The ambiguity of cyber operations can sometimes be useful for signaling — but the same ambiguity can be dangerous during a nuclear crisis. The problem is that civilian leaders in particular, distinct from the military, are inclined to see cyber attacks as effective signaling tools.

Cyber operations could have nuclear implications, especially because modern nuclear command and control systems, like those in Russia and the United States, are becoming increasingly dependent on digital infrastructure. Nuclear command, control, and communications systems, which include early warning, information collection, and communications capabilities, alert decision-makers to impending nuclear strikes and also enable leaders to control decisions about nuclear use (or non-use). But their digital dependencies are creating opportunities for exploitation using cyber means. In a 2020 report, the Nuclear Threat Initiative found that “almost 9 out of 10 planned nuclear modernization programs involve at least some new digital components or upgrades.”

Vulnerabilities inherent in the digital infrastructure that undergird modern nuclear systems provide opportunities for actors to engage in cyber espionage — gaining access to a network or system to steal information — or even conduct cyber attacks. Hypothetically, a cyber power like Russia could conduct a cyber attack against a U.S. early warning satellite to degrade its functionality. This has become an urgent concern for practitioners. U.S. Strategic Command, for instance, is currently working to “operationally harden NC3 systems against cyber threats.” Congress has also gotten involved, requiring the Defense Department to evaluate the cybersecurity of major weapon systems. And the Government Accountability Office has published multiple reports decrying the state of cybersecurity and scope of vulnerabilities of weapon systems, including elements of the nuclear triad.

From an academic perspective, scholars have investigated how cyber operations targeting nuclear systems could exacerbate escalation risks. Focusing on nuclear forces, early research, such as work by Martin Libicki, was skeptical of the dangers posed by cyber operations. Nuclear forces were seen as being largely immune from digital attacks because they were “air gapped,” meaning that they were separated from information technology systems.

However, as nuclear systems have become increasingly intertwined with the digital environment — not to mention the dual-use nature of many elements of nuclear command, control, and communications systems (like early warning or position, navigation, and timing satellites) — the protection offered by being segregated from the internet is less robust. Jacquelyn Schneider, Benjamin Schechter, and Rachael Schaffer, for instance, ran a series of wargames demonstrating that decision-makers in hypothetical crises are likely to use their cyber exploits against an adversary’s nuclear systems. They found that this could have negative effects on states’ respective nuclear strategies, especially decisions to pre-delegate nuclear launch authority or automate nuclear responses. Erik Gartzke and Jon Lindsay argue that the clandestine nature of cyber operations means that one state could secretly gain access to an adversary’s nuclear command, control, and communications systems, giving the former an information advantage or even creating an incentive for the latter to use its nuclear weapons out of the fear that it may lose them. James Acton notes that the difficulties of distinguishing between cyber espionage and attack could lead a state to misperceive the intent behind a cyber operation, generating a similar “use it or lose it” calculus.

#### The fed agrees.

Julia Berghofer 19, ELN Policy Fellow and Project Manager for the YGLN, 5/09/2019, “Apocalypse now? Cyber threats and nuclear weapons systems,” <https://www.europeanleadershipnetwork.org/commentary/understanding-and-addressing-cyber-threats-to-nuclear-weapons-systems/>, cc

Governments and legislators are struggling to keep pace with the rapid development of cyber capabilities. As military systems become more technically complex it would be easy to assume that they are more secure. The opposite is true. Increased automation and connectivity increases vulnerabilities to cyber attacks. Measures such as air-gapping a system (ie. de-connecting it from the internet) can fall short. A recent US Government Accountability Office (GAO) report assessed the cyber security of US weapons systems and found “mission critical cyber vulnerabilities in nearly all weapons systems […] under development.“ While the report does not make reference to any specific system type, one can reasonably assume that nuclear weapons systems are vulnerable to cyber attacks.

### Impact---Militarization---1NC

#### CYBERCOM primacy wrecks CMR and unleashes World War III.

Benjamin Jensen 18, holds a dual academic appointment at Marine Corps University and American University, School of International Service and is a senior fellow at the Atlantic Council; and J.D. Work, the Bren Chair for Cyber Conflict and Security at Marine Corps University and an adjunct associate professor at the School of International and Public Affairs, Columbia University, 9/04/2018, “CYBER CIVIL-MILITARY RELATIONS: BALANCING INTERESTS ON THE DIGITAL FRONTIER,” <https://warontherocks.com/2018/09/cyber-civil-military-relations-balancing-interests-on-the-digital-frontier/>, cc

Parallel to these efforts, the National Security Council and U.S. Cyber Command are rescinding and replacing Presidential Policy Directive 20, an Obama-era policy framework governing offensive cyber operations. According to Politico, “in rescinding PPD-20, [President] Trump put cyberattacks on the same level as kinetic operations, which do not require high-level approval or interagency discussions.” In theory, this change empowers Cyber Command to conduct short-notice attacks without White House approval or interagency coordination. Seen in the context of civil-military relations, this shift assumes positive objective control: a professional military cyber force capable of autonomously protecting society absent constant civilian oversight.

Under the Obama administration, offensive cyber operations required extensive interagency vetting and executive approval, similar to what Samuel Huntington called subjective control. In an article for the Washington Post, reporter Ellen Nakashima quoted the State Department’s former cyber coordinator on the need to balance the desire for offensive cyber operations with “ ‘other national equities’ … to ensure that a cyber operation does not compromise intelligence collection, law enforcement investigations and diplomatic relations.” Multiple officials complained this interagency staffing process slowed or stalled cyber operations as officials struggled to get buy-in from different stakeholders. Subjective control reduced the efficacy of cyber operations.

Balancing Equities: Cyber Operations Meet Bureaucratic Politics

At its core, the debate about Presidential Policy Directive 20 concerns the distinctions in U.S. legal code between traditional military activity (governed by Title 10) and covert action (governed by Title 50) as well as the diplomatic risks and legal challenges triggered by cyber operations. There are real questions concerning where to draw the line between the world of soldiers (i.e., Title 10) and the world of spies (i.e., Title 50). How civilian leaders draw this line and exert control over the foreign policy process amplifies bureaucratic interests and competition for resources at the commanding heights of government.

There are few clear distinctions between soldiers and spies in cyber space given the rapid rate at which adversary capabilities and tradecraft — often deliberately deployed to thwart response — evolve. There is a reason why Russian military intelligence leased servers in Arizona while targeting the 2016 U.S. presidential election. Placing data on servers in the United States made it difficult for American intelligence and military agencies to respond.

Beyond bureaucratic intrigue, key interagency stakeholders maintain competing theories of victory for cyber strategy. To date, cyber space has been a world of spies where espionage, covert action, and sabotage — not conventional military operations — play the dominant role. From sabotaging Iranian centrifuges to high-profile espionage operations, U.S. strategy since 2000 reflects classical political warfare optimized for new technology. This theory of victory lends itself to subjective control. Covert action, as Americans have unfortunately learned all too often, requires extensive civilian oversight.

As more military resources and personnel align with cyber missions, there are growing calls for a forward-leaning posture focused less on intelligence and more on seizing the digital high ground. In this theory of victory, cyber strategy is not just a world of spies, but more akin to traditional military strategy. Since Americans’ social lives, consumer habits, and precision munitions all rely on global connectivity, defending U.S. core interests requires allowing soldiers to safeguard digital infrastructure absent civilian oversight or extensive interagency coordination.

Just as Alfred Thayer Mahan looked at the intersection of economics and military power to advocate securing sea lines of communication, the next generation is likely to see soldiers securing network society. In place of battleships and dreadnoughts, the new theory of victory sees a vital role for cyber military options countering hostile intrusion campaigns targeting U.S. and allied critical infrastructure and key intellectual property interests. Soldiers, not spies, become the main effort.

Cyber Command has floated the idea that the contemporary cyber environment is marked by persistent engagement — a near-constant state of pressure against key aspects of American national power by adaptive adversaries who tailor sustained, long-term campaigns precisely to avoid triggering a response by the U.S. government. This idea parallels the concept of “contact” in the 2018 National Defense Strategy. Contact is the gray zone, a layer of defense in which the United States, including the Department of Defense, competes with adversaries beneath the level of armed conflict. As a cyber extension of this concept, persistent engagement is vital for understanding how, and why, Obama-era policy mechanisms for responding to hostile acts in cyber space are changing. Soldiers, not just spies, secure U.S. economic and military interests along global networks.

The Obama-era Presidential Policy Directive 20 sought to establish subjective civilian control and create a political framework balancing political warfare and persistent engagement. The process acknowledged that soldiers and spies, as well as diplomats and law enforcement personnel, all have a seat at the table. For example, a high-profile hack back against a country tampering with elections or stealing intellectual property from leading U.S. businesses carries reputational risk (i.e., what if the hack fails or unintentionally hits U.S. citizens) and diplomatic consequences. Government agencies best placed to discuss these issues had a seat at the table under the Obama-era framework. Yet, this interagency de-confliction process suffered from delays, bureaucratic inertia, ill-defined decision pathways, and the lack of a clear “referee” to resolve competing positions at the working level.

As a result of such weaknesses, the prior version of the directive can be seen as at times failing to serve its intended purpose — with major stakeholders frequently if not exclusively seeking to pursue mission objectives under other standing processes governed by separate authorities. Consistent with Huntington’s characterization of subjective control, this bureaucratic quagmire likely affected cyber responses. Civilian oversight and interagency coordination mechanisms produced delays and, in all likelihood, diminished options for responding to time-sensitive crisis events.

Furthermore, the process amplified rather than diminished bureaucratic competition. Bureaucratic struggles at the heart of the policy process surrounding national security decision-making can lead to wayward soldiers assuming more risk than civilians are often willing to accept in a crisis. Alternatively, when intelligence considerations are given primacy a procedural bias often emerges against actions that would result in a loss of collection visibility. Spies want to keep reporting, not jeopardize their placement and access. While such access is essential for providing warnings about future threats, potential intelligence loss considerations must be weighed against the operational impact of adversary action on victim organizations. Soldiers want to safeguard key terrain and are reluctant to cede ground to enable spies. These arguments play out against a backdrop of diplomatic concerns, where advocacy for the perspectives of third-party states often results in avoiding counteroffensive operations in favor of law enforcement or administrative remediation measures.

New Threats: The Changing Character of Cyber Operations

A changing threat environment further complicates finding the right policy framework for ensuring civilian oversight of cyber operations and balancing competing stakeholders. The majority of cyber operations since 2000 are best classified as 21st century political warfare. Rival states used disruption, espionage, and degradation to undermine their adversaries and signal the risk of escalation. In this digital gray zone, cyber operations provided a low-cost, low-threat means of engaging in competition short of violent conflict. These operations were often related to larger influence campaigns, such as Russian efforts to target the 2016 U.S. presidential election and undermine democratic institutions in Western Europe.

While the utility of cyber operations for great powers and emerging players to date has largely been driven by the logic of political warfare, the ongoing evolution of capabilities strongly suggests different intentions. For example, ongoing warnings of Russian penetration of U.S. critical infrastructure provide early indications of hostile operational preparation of the environment. Russia is using cyber intrusions to signal the risk of escalation in a crisis and gain a position of advantage in the event of a militarized dispute. Future meetings in the situation room during a tense standoff will involve more than identifying Russia’s nuclear force. Analysts will need a better understanding of Russian cyber posture and the risk of unknown exploits emerging in key systems like power grids and cellular networks — capabilities Russia demonstrated in the live-fire “battle lab” of Ukraine.

In this scenario, who responds: soldiers or spies? Even more importantly, what is the civil-military context in which they respond: objective or subjective control? At stake is not just an optimal policy process, but the stability of a connected world. Leaving the planning to any single group produces bureaucratic pathologies that risk inadvertent escalation.

The Risks of Soldiers Left Unchecked

Insights from the literature on civil-military relations and planning suggest not leaving cyber strategy to soldiers alone. Military planning in isolation historically tends to produce narrow plans prone to worst-case biasing and escalation risks. Risa Brooks demonstrates the importance of information sharing and strategic coordination in her work on civil-military relations and strategic planning. There are real distributional conflicts in domestic institutions that affect strategic assessments and planning. When military actors are isolated, they tend to safeguard information to gain a bargaining advantage and capture resources. In his work on military planning on the eve of World War I, Jack Snyder finds that insular military organizations are prone to a cult of the offensive, exaggerating gains to ensure their bureaucratic autonomy. Furthermore, small groups of soldiers engaged in classified planning are prone to cognitive bias, including false optimism, overconfidence, and an implemental mindset that closes them off to new information.

The second fatal flaw of leaving cyber space to the soldiers is that it diminishes the probability of successful, coercive diplomacy. Cyber security scholars increasingly describe the domain in terms of coercion. States, and other interest groups, use cyber operations to coerce rivals. This diplomacy of violence, to use Thomas Schelling’s famous phrase, is designed to change behavior short of war. Seen as coercive diplomacy, this implies combining multiple instruments of power — such as military threats, economic sanctions, and diplomatic outreach — to change the cost-benefit calculation of the rival.

In fact, research suggests that the majority of political concessions produced by or linked to cyber operations involve other instruments of power. The campaign against Iran involved not just cyber espionage and degradation operations, but a concurrent threat of military pressure and economic sanctions alongside the promise of future trade deals and reintegration into the global community if Iran signed a nuclear deal. Real strategy, like combined arms, involves combining different ways and means to achieve objective ends. Furthermore, this coordination requires civilian oversight and subjective control. Consistent with agency theory, both soldiers and spies need to know civilians are monitoring them and willing to punish officials who cross the line.

Striking the Right Balance

Developing American cyber strategy starts with getting the policy framework right and ensuring civilian oversight. This framework must empower interagency planning that generates response options leveraging multiple instruments of power. These plans should address the possibility of time-sensitive crises involving defensive cyber fires intended to target hostile intrusion and/or computer network attack infrastructure while balancing competing equities between soldiers and spies alongside diplomats and law enforcement officials. In coordinating a response, the plans — which should be monitored by civilians, including Congress — must reconcile interagency conflict before they reach the Oval Office or situation room. Much like major war plans in the Department of Defense, these contingency plans should be periodically reassessed, to include war games and crisis simulations, and approved by appointed civilian officials. This review process has the added benefit of identifying critical vulnerabilities and requirements for new capabilities and partnerships that maintain America’s advantages in cyber space.

Consider the following example. Cyber Command and the intelligence community identify intrusion attempts targeting critical infrastructure in the United States. Initial assessments attribute the incident to Russia but cannot determine whether the incident is espionage or an attempt to insert payloads for use in future crises. Worse still, the incident takes place during a large Russian military exercise.

Objective control would imply the military is authorized to respond against the worst-case scenario and not only counterattack the point of origin of the attacks but potentially unleash a barrage of cyber degradation operations against Russian command and control facilities. In the best case, the counterattack only heightens diplomatic tension and burns multiple covert, cyber espionage campaigns. In the worst, case it unleashes a cyber Able Archer, the 1983 training exercise that some argue almost triggered World War III.

#### Breakdown of civil-military cooperation prevents effective response to a host of existential challenges

Jim Golby 21, senior fellow at the Clements Center for National Security at the University of Texas at Austin; and Peter D. Feaver, professor of political science and public policy and director of the American Grand Strategy Program at Duke University, 1/1/21, “BIDEN INHERITS A CHALLENGING CIVIL-MILITARY LEGACY,” <https://warontherocks.com/2021/01/biden-inherits-a-challenging-civil-military-legacy/> /jpb

Civil-military relationships are not an end in themselves. These relationships exist only to provide effective national security policies in a given geopolitical environment in the context of democratic accountability. Unfortunately, the environment is not benign. As they sort through the civil-military and institutional baggage — the items they bring with them and the items they inherit — Biden’s team must also navigate intensified great-power conflict, persistent instability in the broader Middle East, strained ties with key allies, and little progress on all of the other stubborn problems that have bedeviled leaders in the post-Cold War era, including: the proliferation of weapons of mass destruction, transnational networks of terrorism, failed states, and ethnic rivalries. And, of course, Biden must still lead the country out of the worst pandemic in a century while recovering from all of the associated economic upheaval. There will be no strategic holiday during which the Biden team can painstakingly sort through its civil-military affairs.

The new commander-in-chief starts with the enormous advantage of being “not Trump.” He will need all of that advantage — and will need to have learned from Obama-era missteps — in order to navigate through the tricky civil-military waters we have described above. Members of the Biden team come in as seasoned professionals, but we hope that leads them to caution and humility rather than unwariness and hubris as they conduct national security policy. If Lloyd Austin wins over the critics and proves himself to be both fully sensitive to these civil-military realities and savvy in how he seeks to overcome them, he may yet emerge as the successful and strong secretary of defense the Department of Defense so desperately needs. The early slate of civilian nominees named for key roles is a welcome sign. The initial weeks after the inauguration will be of particular importance in setting the tone, especially after the tumultuous and stressful transition. Even so, the norm of civilian management of the Defense Department will be more difficult to reestablish, like so many other civil-military norms that have weakened in recent years, if Congress does grant another recently-retired general legal permission to serve as secretary of defense. Biden, and Austin, will need all the top civilian defense talent they can get.

Notwithstanding all of the other urgent priorities vying for his attention, neglect of the civil-military file would likely impose intolerable costs on Biden down the road — a price that would be vividly evident, sooner or later, when an urgent national security crisis takes center stage. The only prudent course is for the Biden team to attend to both policy and process at the same time — to move out quickly on the pandemic and the economy, while also setting the national security establishment on the path to healthier civil-military relations. Problems in the civil-military foundations of an administration must be fixed before a crisis lays bare the rot that may lie just out of view.

### Impact---Militarization---2NC

#### Military culture and cybersecurity are incompatible---meshing them risks war AND public-private incongruity.

Jon R. Lindsay 20, assistant professor at the Munk School of Global Affairs and Public Policy and the Department of Political Science at the University of Toronto, 10/30/2020, “Cyber conflict vs. Cyber Command: hidden dangers in the American military solution to a large-scale intelligence problem,” *Intelligence and National Security* 36(2), https://doi.org/10.1080/02684527.2020.1840746, cc

At the same time, the institutional characteristics that make military organizations so effective at scaling up operations also raise serious concerns when the operations in question are intelligence and covert action. These can be considered alongside the same three characteristics that define intelligence itself.

First, intelligence is deception. The essence of intelligence tradecraft is the abuse of trust to infiltrate the same institutions and infrastructures that enable cooperation in the target society. Whether secret vulnerabilities and accesses are leveraged to collect or inject information is a secondary distinction. Defenders can employ deception as well as attackers, which complicates and limits the strategic effectiveness of intelligence by any means. This is all second nature to intelligence professionals, but the subversion of trust stands in stark tension with martial ideals of open and heroic combat, even as stratagem has a long history in war. Feints and ambushes are one thing, but subversion and treachery are quite another. It is understandable why a military organization might resist thinking of itself as an intelligence organization, even setting aside the subordinate or supporting connotation that intelligence usually has in a military setting. CYBERCOM is an honorable military organization, but intelligence is at its core a duplicitous business. The mismatch between military culture and intelligence practice is also likely to complicate CYBERCOM’s efforts to recruit, retain, and manage the unconventional hackers it needs to subvert the most sophisticated trust networks humanity has ever constructed. This all raises an important ethical question: should the same militaries that openly man the ramparts also be digging through firewalls?

Second, intelligence is political. Secret statecraft is politically attractive because it promises to reduce the costs and risks of pursuing contested policy goals. Militaries are also political, of course, but in a very different way. Intelligence is organized deception to gain an information advantage. Militaries are organized force to gain a coercive advantage. Military forces can be employed to win battlefield contests, brandished to threaten punishment, or deployed to reassure allies. Intelligence, by contrast, is more preoccupied with lowering policy costs and risks on the sly, rather than increasing power and credibility in the open. The political logic of intelligence stands in stark tension with the noisy confrontation of battle or the deliberate signaling of deterrence. Intelligence can be used to make war more efficient in terms reducing force requirements while boosting capabilities, of course, but this sometimes comes at the expense of effectiveness in terms of power and credibility.87 Increasing military reliance on intelligence capabilities in space and cyberspace is only making these ‘cross domain’ tradeoffs more difficult.88 The tension between deceptive contestation and strategic stability lies at the root of contemporary concerns that CYBERCOM’s doctrine of ‘persistent engagement’ will lead to inadvertent escalation.89

The relative prioritization of power, credibility, or efficiency in any given situation is a profoundly political problem. Different leaders, parties, and organizations, furthermore, can be expected to have different opinions about the way it should be solved. The American military has internalized strong professional norms of apolitical service to the nation, of course, and CYBERCOM can be expected to carry on this Huntingtonian tradition. Yet military professionalism can also be leveraged for advantage in domestic politics, and it can distort political assessment or oversight of military operations.90 CYBERCOM will struggle to appear politically neutral in the very political controversies that its subversive activities enable. In general, the inherent political sensitivity of intelligence operations may not be a good fit for military preferences for operational autonomy. Professional intelligence agencies approach the problem of politicization differently, with varying levels of success, by nurturing close relationships with their political masters while hidden from the harsh light of public politics.91 As CYBERCOM scales up intelligence operations, whatever it decides to call them, this will likely exacerbate the complexity and controversy of political tussles over speech, privacy, and public safety, with CYBERCOM stuck in the middle.

Third, intelligence is increasingly civilian. One important implication for cybersecurity is that ‘cyberspace’ as such does not exist. Digital networks are the lifeblood of governance, finance, trade, industry, administration, and political activism in the twenty-first century, and cyber operations work by, with, and through these networks. Civilian firms build and operate most of the enabling infrastructure. Civilian cybersecurity firms play an important role in both offensive collection and influence and defensive counterintelligence, but their economic interests may not always align with public cybersecurity.92 Civil society actors, meanwhile, bear the brunt of much cyber conflict as the targets of political surveillance, disinformation, and information control. Cyber operations are deeply embedded within and constrained by all this civilian activity, but this poses serious challenges for military culture. Military organizations tend to neglect or only grudgingly perform missions like counterinsurgency and peacekeeping that require them to work by, with, and through civilian populations; militaries would rather prepare for major combat operations that allow for greater autonomy and are more consistent with warrior identities.93 Given that military interventions to stabilize and rebuild nations have so often proved controversial, how much more problematic are intelligence operations to subvert and protect the digital infrastructure of civil society itself? Efforts to combat foreign disinformation campaigns are especially fraught as they become, in effect, military interventions into democratic polities riven by political disagreement.

### Impact---Turf Wars---2NC

#### Demchak says splitting causes turf wars.

#### Those deck law enforcement of financial cybercrime.

Susan W. Brenner 13, NCR Distinguished Professor of Law and Technology at the University of Dayton School of Law, “Cyber-threats and the Limits of Bureaucratic Control”, Minnesota Law Journal of Science & Technology, Winter 2013, 14 Minn. J.L. Sci. & Tech. 137, Lexis

If these statutes parsed investigative authority out among the five agencies listed above in a fashion analogous to how [\*193] combat jurisdiction is parsed out among the five military branches, this would go a long way toward reducing the turf wars that currently plague federal law enforcement. Unfortunately, the statutes rarely do this, which means agencies often have overlapping investigative jurisdiction, which "can open the doors" to turf battles. In a 2011 investigation of jurisdictional overlap among federal agencies, many agents reported that they had encountered uncertainty and disagreements about the appropriate allocation of investigative authority and said these disagreements often negatively affected investigations. Criminals' increasing use of cyberspace is only exacerbating the difficulties federal agents already face.

While turf wars and overlapping or uncertain investigative jurisdiction continue to impede U.S. law enforcement's ability to respond to crimes, they are not the only factors that are eroding its ability to respond to cyber-threats. The problem law enforcement must confront is the civilian correlate of the problem General Alexander faces: we can no longer assume that attacks which appear to constitute "mere" cybercrime are just that, i.e., are carried out by civilians who are "in" the United States and whose motives are purely personal. An attack on a financial institution might be a cybercrime committed by a greedy United States citizen "in" the United States, but it might, instead, be (i) a cybercrime committed by a non-United States citizen operating from abroad or (ii) a cyber-sortie carried out by a hostile nation-state's own cyber command.

#### U.S. financial crimes drive global organized crime

W. Joseph Salvador 15, Managing Articles Editor of the Rutgers Computer and Technology Law Journal, J.D. Candidate at Rutgers School of Law-Newark, B.A. from The George Washington University, “Dismantling the Internet Mafia: RICO's Applicability to Cyber Crime”, Rutgers Computer & Technology Law Journal, 41 Rutgers Computer & Tech. L.J. 268, Lexis

III. The Emergence of Cyber Crime

In his 2013 State of the Union address, President Barack Obama stated, on the topic of cyber security, that "we cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy." It is now estimated that cyber crime solicits $ 110 billion globally every year. The Federal Bureau of Investigation recognizes three categories of cyber threats: organized crime groups, state sponsors, and terrorist [\*280] groups. It is organized crime groups and terrorist organizations that are susceptible to RICO violations.

International organized criminal syndicates use the Internet in furtherance of more traditional real world activities like drug distribution and sex trafficking. However, they have also taken advantage of the digital world to find new outlets for criminal activity including mass fraud schemes, identity theft, online banking crimes, and money laundering. Also, groups composed of specialized criminals have evolved to commit all of their crimes online. These groups differ from traditional organized criminals because they gain illicit profits purely via computer and maintain no clearly defined structural hierarchy. Nevertheless, their loose association in continual criminal schemes fit the definition of an "enterprise" as defined in RICO.

These specialized organized cyber crime groups employ new tools to commit their acts. The emergence of botnets, a network of infected computers, is essential to the profitability of the group. The botnet allows for an attack on thousands of private users or corporate networks instead of criminally infiltrating the systems on an individual basis. Similarly, "mules" are essential to the vitality [\*281] of the criminal enterprise. A "mule" is recruited for the sole purpose of receiving the illicit funds, often via bank account, and turning these funds into cash. Generally, mules receive small portions in monetary value and are scattered across the globe so as not to endanger the entire scheme if one is apprehended by law enforcement.

#### Extinction

Dr. Michael Miklaucic 13, Adjunct Professor of U.S. Foreign Policy at American University, and of Conflict and Development at George Mason University, Director of Research, Information and Publications at the Center for Complex Operations (CCO) at National Defense University, Jacqueline Brewer, 07/05/2013, “Convergence: Illicit Networks and National Security in the Age of Globalization,” Government Printing Office, Google Books

Public-Private Partnerships to Combat Illicit Trade and Illegal Economy  
The illegal economy poses an existential threat when it begins to create criminalized markets and captured states, which launches a downward, entropic spiral toward greater insecurity and instability. In countries that have been corrupted by criminal networks, market- and state-building become less attainable, economic growth is stunted, efforts toward development and poverty eradication are stifled, and foreign direct investment is deterred.

The United States is supporting the OECD, the World Economic Forum (WEF), and other international partners to provide knowledge-based platforms for international public and private stakeholders to raise awareness of the threat posed by illicit trade and illegal economy to economic growth, development, and global security, and to share experience on practical approaches to the control of illicit activities as well as of the negative externalities of the illicit economy. Engaging the public and private sectors through innovative public-private partner-ships will be particularly important for securing the integrity of the global supply chains and for ensuring long-term sustainable licit commerce and productive markets.

The steep rise in mobility of goods, people, capital, and information that has accompanied globalization is largely comprised of lawful and beneficial exchanges, but an increasing share is illicit. Criminal entrepreneurs and illicit networks sometimes use or exploit legitimate businesses and legitimate global supply chains to carry out financial frauds, industrial espio-nage, money laundering, and other illicit activities. Hundreds of billions of dollars of revenue from these activities flow through the global economy every year, distorting local economies, diminishing legitimate business revenues, deteriorating social conditions, and fueling conflicts.

### Impact---Cyberterror---2NC

#### Cross-agency cooperation checks back cyberterror.

David Vergun 21, writer-editor for the DOD at the Pentagon, 6/29/2021, “NSA, Cybercom Leader Says Efforts Have Expanded,” <https://www.defense.gov/News/News-Stories/Article/Article/2675824/nsa-cybercom-leader-says-efforts-have-expanded/>, cc

Another challenge with weapons systems is ensuring that cybersecurity considerations are implemented in the earliest phases of the acquisition cycle, he said.

Protecting DOD's data is also a major challenge, he said.

Understanding how state and non-state adversaries are able to successfully carry out cyberattacks is important, he said. "They learn over time in terms of what they can do. They're not static in the terms of how they approach cyberspace."

In about the past 150 days, adversaries have successfully conducted supply chain attacks, particularly ransomware attacks, he said. In the last several years, election cybersecurity has taken on an increasingly important role.

Terrorist groups are also mounting cyberattacks, he said. In response, the department has emphasized close teamwork between the NSA, Cybercom, and other commands — U.S. Special Operations Command, in particular.

"We learned how to work closely with U.S. Special Operations Command, both to support their efforts against kinetic targets and to leverage their capabilities against virtual ones," he said.

Nakasone also emphasized the importance of working with industry, academia, interagency partners like the FBI and the Department of Homeland Security, as well as with allies and partners.

Having a skilled and motivated workforce is also critically important, he said. They need to have the right training and career paths and professional development opportunities, and the DOD must be open to their new ideas.

#### Cyberterror imperils nuclear stability.

Keren Snider et al. 21, postdoctoral scholar in the School of Political Science at the University of Haifa, Israel; Ryan Shandler, postdoctoral research fellow at the Blavatnik School of Government, University of Oxford, and a research fellow at Nuffield College; Shay Zandani; and Daphna Canetti, 10/07/2021, “Cyberattacks, cyber threats, and attitudes toward cybersecurity policies,” *Journal of Cybersecurity,* 7(1), <https://doi.org/10.1093/cybsec/tyab019>, edited for ableist language, cc

Despite the sizeable literature dealing with the effects of exposure to violence, few studies directly investigate the effects of exposure to destructive cyberattacks. This is despite the growing recognition that these threats have become a very tangible part of modern life. In a complex scenario described in the Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare, the authors contemplated how new forms of cyberattacks could be used to “acquire the credentials necessary to access the industrial control system of a nuclear power plant… with the intent of threatening to conduct cyber operations against the system in a manner that will cause significant damage or death…” [30]. Even more recently, reports have acknowledged how cyberterror attacks could ~~immobilize~~ [destroy] a country's or region's electrical infrastructure [31], ~~disable~~ [decimate] military defense systems [32], and even imperil nuclear stability [33]. While there is a difference between capability and intent, and we acknowledge that physically destructive cyber threats have remained scarce until now, understanding how civilians respond to such digital cyberattacks will become particularly important as the threat matures.

### Impact---NSA Good---Prolif---2NC

#### Clogs pipelines for signals intelligence.

Jane Edwards 21, staff writer at Executive Mosaic and covers stories about federal cybersecurity, citing Mark Milley, chairman of the Joint Chiefs of Staff, 3/09/2021, “Gen. Mark Milley: NSA-Cybercom Split Could Impact Flow of Signals Intelligence,” <https://executivegov.com/2021/03/gen-mark-milley-nsa-cybercom-split-could-impact-flow-of-signals-intelligence/>, cc

Gen. Mark Milley, chairman of the Joint Chiefs of Staff and a four-time Wash100 Award, said the organizational criteria for separating the National Security Agency from Cyber Command have not yet been met and that the split will impact the military’s access to signals intelligence, Defense One reported Monday.

“For us in the military, the signals intelligence we get from the NSA is … unbelievably good. It’s among the most valuable pieces of intelligence we get on a daily basis,” Milley told reporters.

“The last thing we want to do is anything that would cause harm to … the production and dissemination of that information. So we want to make sure we do it right, slow, step by step. You can’t miss a beat with this thing,” he added.

#### SIGINT’s key to counterproliferation.

Phil Gurski 21, President and CEO of Borealis Threat and Risk Consulting Ltd. Phil is a 32-year veteran of CSE and CSIS and the author of six books on terrorism, 3/01/2021, “Do we need intelligence to stop nuclear weapons proliferation?,” <https://borealisthreatandrisk.com/do-we-need-intelligence-to-stop-nuclear-weapons-proliferation/>, cc

One of the reporting series I recall was that which had to do with states which were pursuing nuclear weapons programs. There were quite a few of them in the 1980s and 1990s: Libya, South Africa, Taiwan, North Korea, India and Pakistan. As we all know, only the last three have attained that capability (we’ll leave aside Israel for now: also, the so-called Permanent 5 UNSC members – the US, USSR/Russia/, the UK, France and the PRC – already had ‘the bomb’). Then there is Iran….more on that in a bit.

Back then, there was no Internet. There was no easy way to keep tabs openly on who was doing what. Thankfully, we had SIGINT to help us gain insight. Through the targeting, collection, processing and analysis of communications (verbal, written, imagery, telemetry, etc.) we could see which countries were making progress and suss out who were the key officials (scientists, civil servants) with the keys to this breakthrough. We learned a lot and were able to keep our political masters informed in ways which would have been impossible without intelligence.

Wow, what a difference a couple of decades make!

A proliferation of information

Now we have so much more information at our fingertips: the World Wide Web, social media platforms, even commercial imagery! As this recent article in The Economist noted: “Non-governmental organisations regularly unearth and publicise secret facilities using “open” sources—most notably images taken by satellites like those which researchers at MIIS (NB Middlebury Institute of International Studies) used to spot North Korea’s looming missile test and Saudi Arabia’s rocket plant.”

In other words, it is harder today to hide a nuclear weapons program. This does not obviate the need for intelligence: after all, there is nothing like a highly-placed human source that can be tasked and directed to find out specific information to determine exactly what a state’s intentions are. And only states can actually take steps to interfere with a nation’s quest for nuclear weapons, even if those steps are of dubious legality (hello assassination of Iranian nuclear scientist Mohsen Fakhrizadeh, probably by Mossad, Israel’s foreign spy service: oh wait, Israel surreptitiously developed their own nuke capability didn’t they?).

#### Proliferation causes extinction.

Dr. Andrew Futter 21. Professor of International Politics at the University of Leicester; Samuel I. Watson, Associate Professor at the University of Warwick; Peter J. Chilton, Research Fellow at the University of Birmingham. "Nuclear Proliferation and Nuclear Ages.” In The Politics of Nuclear Weapons: New, updated and completely revised. Palgrave Macmillan, Cham. pp. 71-78. 2021. Springer. //EM edited for errors.

In the Second Nuclear Age, the greatest risk no longer appears to be from a large-scale conflict between major powers (although this possibility always remains) but instead from regional instability in the Middle East, South or Northeast Asia, or even a non-state actor armed with a nuclear weapon (see Chap. 9).18 This threat has been exacerbated by the spread of Weapons of Mass Destruction technology, and particularly the combination of nuclear and ballistic missile capabilities to new actors across the globe. Ultimately, the central theme of the Second Nuclear Age is that the spread of the bomb, along with the means to build and deliver nuclear weapons, to new actors has changed the central dynamics of the global nuclear order, and consequently we may no longer be able to rely on the nuclear thinking and toolkit that helped us to survive the First Nuclear Age. In the words of Fred Ikle, writing in 1996:

Half a century after it began, the nuclear drama has reached the conclusion of its first act—a rather happy ending in spite of the gloomy prospects for civilization that darkened the stage at the outset. Tis respite, though, is not a lasting redemption from the dangers of nuclear warfare.19

The Nuclear Proliferation Debate: Optimists and Pessimists

The thinking that led to a conceptualization of nuclear history into two distinct nuclear ages is also reflective of the broader debate about the role of nuclear weapons in international politics. In essence, the relative stability, or at least the lack of major interstate war, of the First Nuclear Age gave rise to the notion that nuclear weapons had helped to “keep the peace” during the Cold War, and that horizontal nuclear proliferation might therefore be stabilizing. This is based on the theory of the nuclear revolution (discussed in the next chapter) and specifically the notion that the advent of nuclear weapons fundamentally changed warfare, because no rational actor would want to risk attacking an adversary if they could retaliate with nuclear weapons. Thus, a certain level of stability might be achieved between nuclear-armed states that might not otherwise exist. However, this view of nuclear history, and of the stabilizing potential of nuclear weapons, is challenged by those who believe that vertical nuclear proliferation and a reliance on rationality and luck are not a good basis for international politics and security. They also question the post-hoc view that nuclear weapons were the main reason that the Cold War didn’t turn hot and warn against using this potentially flawed analogy today.

The concern that nuclear weapons will spread to new actors that characterize the Second Nuclear Age has provided the backdrop for the nuclear proliferation debate. The question at the heart of this debate is whether nuclear proliferation to new actors will stabilize or destabilize international politics and whether nuclear proliferation makes inter-state, and possibly nuclear, war more or less likely. This subject is at the center of a discussion between two political scientists, Kenneth Waltz and Scott Sagan. The debate can be succinctly explained as follows:

Kenneth Waltz argues that fear of the spread of nuclear weapons is exaggerated: “More may be better” since new nuclear states will use their weapons to deter others from attacking them. Scott Sagan argues that the spread of nuclear weapons will make the world less stable: “more will be worse” since some new nuclear states will engage in preventive wars, fail to build survivable forces, or have serious nuclear weapons accidents.20

We can think of this debate as being split between proliferation optimists and proliferation pessimists and centering on the wisdom and reliability of Mutual Assured Destruction as a mechanism for stability and security (see Chap. 5). Kenneth Waltz is seen as the champion of the nuclear proliferation optimists, and Scott Sagan for the pessimists. The central tenets of these two positions are explained below:

The proliferation optimists hold that horizontal nuclear proliferation should not necessarily be viewed as automatically destabilizing. As Kenneth Waltz explained in 1981:

Those who dread a world with more nuclear states do little more than assert that more is worse and claim without substantiation that new nuclear states will be less responsible and less capable of self-control than the old ones have been. … Such fears have proved unfounded as nuclear weapons have slowly spread. I have found many reasons for believing that with more nuclear states the world will have a promising future.21

This is partly because:

New nuclear states will confront the possibilities and feel the constraints that present nuclear states have experienced. New nuclear states will be more concerned for their safety and more mindful of dangers than some of the old ones have been.22

Ultimately, this viewpoint believes that “Nuclear weapons reasonably used make wars hard to start.”23 As such, the spread of nuclear weapons—in certain circumstances—should actually be welcomed, and retaliatory nuclear deterrence and MAD does and should remain the bedrock of global nuclear relations.

The proliferation pessimists contend that horizontal nuclear proliferation can only ever lead to an increase in nuclear dangers and the possibility of nuclear use. Pessimists point to a number of factors that make horizontal proliferation potentially dangerous: the growth of the threat posed by nuclear terrorism and illicit nuclear networks (see Chap. 8); the possibility of nuclear accidents; the difficulties of ensuring civilian control and safe and secure command and control of nuclear weapons (see Chap. 5); the specter of preventive war against aspirant nuclear states (see Chap. 8); the problem of building survivable second strike forces; and the fact that stability through proliferation rests on actors always behaving rationally at all times.24

Foremost amongst these however is a critique of the misplaced belief that nuclear weapons helped keep the peace during the First Nuclear Age. In the words of Sagan, writing in 2006:

Deterrence optimism is based on mistaken nostalgia and a faulty analogy. Although deterrence did work with the [United States and] the Soviet Union and China, there were many close calls; maintaining nuclear peace during the Cold War was far more difficult and uncertain than US officials and the American public seem to remember today.25

Proliferation pessimists focus on the problems of organizational culture and the fact that new nuclear actors are perhaps more likely to experience nuclear accidents. As Scott Sagan explains, “professional military organizations— because of common biases, inflexible routines, and parochial interests—display organizational behaviors that are likely to lead to deterrence failures and deliberate or accidental nuclear war”.26 Newly armed nuclear states might also be less likely to be able to prevent unauthorized use because they lack the positive mechanisms of strong civilian control.27 Consequently, pessimists argue that retaliatory nuclear deterrence (and MAD) may not represent the panacea that it is held to be by proliferation optimists. We can compare and contrast these views in Table 4.5 below:

Nuclear Latency and Virtual Nuclear Arsenals

While only a small number of states have taken the decision to build nuclear weapons, (and the vast majority have decided not to) the peculiarities of nuclear technology means that there exist a number of states theoretically capable of building nuclear weapons at short notice should they chose to, but which are not currently considered to be nuclear armed states. These states

[[TABLE 4.5 OMITTED]]

possess their own civilian nuclear programs, often including the ability to produce highly enriched uranium or plutonium 239 and have a relatively advanced military infrastructure that could be used to develop a nuclear weapon (for more on this see Chap. 11). While these states may not be able to build a working bomb overnight (or in total secrecy), they could probably do so in a relatively short space of time should they choose to—although estimates of this vary from case to case and amongst experts. These states are known as virtual nuclear weapons states or threshold nuclear weapons states because they adopt a position referred to as nuclear latency. As Anver Cohen and Joseph Pilat explain:

Virtual weapons are indeed a reality of physics and cannot be ignored, because knowledge, experience, materials and other requirements to make nuclear weapons are widespread. A continuum of virtual capabilities exists, ranging from general technology diffusion and the existence of nuclear energy programs to conscious decisions to develop or maintain militarily significant nuclear weapons capabilities.28

Nuclear latency remains one of the biggest proliferation challenges facing the international community today.

The complication with nuclear latency stems from the fact that the technology needed for a civilian nuclear power program is very similar to that needed to produce fissile material for a bomb, and because some military hardware designed for non-nuclear weapons systems can be modified to deliver nuclear weapons (aircraft or missiles for example). The problem is compounded by the central bargain of the 1968 Nuclear Non-Proliferation Treaty whereby all states that have signed the Treaty as Non-Nuclear Weapons States have a right to produce their own civilian nuclear energy (for more on the NPT see Chap. 8). As a result, states can move fairly close to acquiring a nuclear “breakout” capability without actually undermining the NPT or breaking international law (this is at the heart of the current controversy over Iran’s civilian nuclear program and whether or not that is being used as a cover to develop nuclear weapons). With hundreds of civilian nuclear facilities and powerplants operating in dozens of countries worldwide,29 the challenge of nuclear latency is ever present. According to the then Director of the Atomic Energy Agency, Mohammed ElBaradei in 2010:

Some estimates indicate that 40 countries or more now have the know-how to produce nuclear weapons, which means that if they have the required fissile material—high enriched uranium or plutonium—we are relying primarily on the continued good intentions of these countries.30

While ElBaradei’s statement should not necessarily be interpreted as meaning that all of these states will or could easily build nuclear weapons, it does underline the importance of this challenge. Indeed, and despite the Fukushima nuclear disaster in Japan and the decision taken by Germany in 2011 to phase out civilian nuclear power,31 the global trend could be toward more rather than less nuclear power generation in the future (for the implications of this see Chap. 11).

In theory, any country with an active civilian nuclear industry and a modern weapons program could build a nuclear bomb, although this would not be a straightforward task for any nation that decided to do so. The best-placed states to do this have full control of the nuclear fuel cycle, i.e. they can enrich the fuel for (uranium) and/or separate the by-products of nuclear fission (plutonium). States that operate a civilian nuclear power capability but have to buy nuclear fuel from abroad are far less of a proliferation risk, although because plutonium is a by-product of uranium fission (see Chap. 2) these civilian power plants must be closely monitored by the relevant international authorities, such as the International Atomic Energy Agency (IAEA). However, technological capabilities are only one dynamic of proliferation and must of course be matched with the political will required to build a bomb. Developing a nuclear warhead small enough to be placed on a missile and that can survive the pressures of fight and possibly atmospheric re-entry for example is a very difficult task, although by no means insurmountable for a modern state. In general, a nation wishing to move from latency to full nuclear weapons capability would meet significant challenges, not least keeping the program secret from the international community and the International Atomic Energy Agency (the world’s nuclear watchdog).

Below are a number of examples of states that we might consider as having various degrees of nuclear latency:

• Japan. Japan is usually held up as the model of a latent nuclear weapons state because it has an advanced civilian nuclear industry, the ability to produce highly enriched uranium or plutonium (in addition to the large stockpiles it already has) and a modern military. Given the geopolitical tensions in Northeast Asia, the threat that Japan may decide to “go nuclear” is ever-present, although most observers suggest that there is little enthusiasm for such a move, and Japan remains a key member of the Non-Proliferation Treaty. However, Japan could probably build a deliverable nuclear weapon if it chose to within a relatively short space of time (maybe less than a year).32 As Mark Fitzpatrick noted in 2019, “The biggest obstacles to a Japanese nuclear weapons program aren’t technical or logistic; they are political, legal, and cultural.”33

• South Korea. South Korea operates a number of civilian nuclear power plants and has expressed an interest in acquiring the technology necessary to control the nuclear fuel cycle (it can’t currently enrich uranium or reprocess plutonium).34 It also theoretically has the infrastructure and manufacturing base to support a nuclear weapons programme.35 Like Japan and Taiwan, South Korea sits in a potentially volatile region and future changes could drive the case for a bomb. South Korea also previously hosted US tactical nuclear weapons on its territory during the Cold War (until 1991) and is believed to have entertained the idea of a home-grown nuclear weapons effort in the past.36 The likelihood of a future nuclear-disarmed North Korea and the credibility of the US-extended guarantee are probably the key variables in any future move toward acquiring the bomb.37

• Taiwan. Taiwan is not a member of the Non-Proliferation Treaty given its unique status in international society and has previously had an indigenous nuclear weapons programs in the 1970s. While it is not currently believed to have enrichment or reprocessing capabilities, Taiwan does have specific regional concerns that could lead to arguments for a nuclear weapons capability, but the costs of doing so are possibly too high for the time being (US opposition, international condemnation, or even a Chinese pre-emptive strike). Taiwan would probably also need to build a suitable missile and warhead.38 As Arthur Ding suggested in 2012, “Despite the logic that strategic logic might dictate the acquisition of a modest nuclear arsenal. Taiwan is unlikely to develop nuclear weapons.”39 But this could of course change in the future.

• Brazil. Brazil possesses all the major elements needed to produce fissile material for a bomb (from an indigenous supply of uranium ore to enrichment and the ability to fabricate nuclear fuel) but currently lacks the means to deliver nuclear weapons should it choose to build them, although it has previously had a nuclear bomb program (see Chap. 10). Brazil is also an active member of the Non-Proliferation Treaty and is seen as an unlikely future nuclear weapons state at the time of writing.40

• Iran. Iran is a member of the Non-Proliferation Treaty, but it has long been suspected that its nuclear program could be designed for military purposes. Iran appears to be seeking to achieve full control of the nuclear fuel cycle, which would mean an ability to produce highly enriched uranium and plutonium, and has a large military, including a relatively advanced ballistic missile program. Iran is perhaps the biggest concern for future proliferation due to its current geopolitical situation,41 and especially after the US withdrew from the Joint Comprehensive Plan of Action in 2018 (for more on Iran and the Iran Nuclear Deal see Chap. 7).

• Saudi Arabia. Sitting at the heart of a region with ever-changing security requirements—not least the possibility of a nuclear-armed Iran on its doorstep, coupled with a perceived decline in US influence, and with an advanced infrastructure and burgeoning economy, Saudi Arabia represents a serious nuclear proliferation concern.42 Saudi Arabia has only a rudimentary civilian nuclear infrastructure, but it is rumored to have close nuclear ties with Pakistan and other Gulf Emirates states that do.43 It also has the resources to support a nuclear weapons program.

### Impact---Elections---2NC

#### Collaboration between CYBERCOM and the NSA secures elections.

David Vergun 21, writer-editor for the DOD at the Pentagon, 3/25/2021, “Cybercom's Partnership With NSA Helped Secure U.S. Elections, General Says,” <https://www.defense.gov/News/News-Stories/Article/Article/2550364/cybercoms-partnership-with-nsa-helped-secure-us-elections-general-says/>, cc

[Title: Cybercom's Partnership With NSA Helped Secure U.S. Elections, General Says]

Being both the commander of U.S. Cyber Command and director of the National Security Agency improves the ability to provide the nation with speed, agility and flexible responses to adversaries who are increasingly modernizing, getting quicker and getting more sophisticated, the agencys' director said.

Army Gen. Paul M. Nakasone testified today at a Senate Armed Services Committee hearing on the defense authorization request for fiscal year 2022 and the future years defense program.

"We operate in a domain that changes rapidly, and this change is measured in weeks rather than months. Being able to rapidly react to that, as we've been able to prove in the security of elections in 2018 and 2020, is empowered by that relationship," he said, referring to his dual-hatted role.

To defend against foreign interference in electsions the Election Security Group was created, he said, noting that it consists of a combined team from Cybercom and NSA.

Nakasone also mentioned the importance of partnerships with the Federal Bureau of Investigation, the National Guard Bureau and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, which involves sharing information with those who need it as quickly as possible.

Cybercom conducted more than 2,000 operations to get ahead of foreign threats before they interfered or influenced the 2020 elections, Nakasone said.

The general said he wanted to make three important points: "First, Cybercom must be and is able, ready and willing to act. Second, Cybercom's partnership with NSA remains the foundation of our success. And third, we enable our domestic industry, allies and partners by providing critical threat information and insights, which improve their ability to act under their unique authorities."

## Uniqueness

### UQ---No Split---2NC

#### A split is unlikely, but not locked in.

Martin Matishak 3/18, senior cybersecurity reporter for The Record, 3/18/2022, “DoD official: Keeping Cyber Command, NSA leadership together will be ‘looked at’,” <https://therecord.media/dod-official-keeping-cyber-command-nsa-leadership-together-will-be-looked-at/>, cc

A senior Pentagon official on Thursday said the Biden administration will review the joint leadership structure that has long governed U.S. Cyber Command and the National Security Agency.

“I believe that the ‘dual-hat’ will be looked at again, just by this administration, just to ensure that we understand what the value added is, but also what the impacts are. And so that discussion is still ongoing within the department today,” Ronald Moultrie, Under Secretary of Defense for Intelligence and Security testified during a House Armed Services Committee subpanel hearing.

“We understand that there is sentiment — on both sides — to really not do any harm,” he added. “But I believe that it will be looked at. It’ll be an objective look.”

The two agencies, which are co-located at Fort Meade, Md., have shared leadership under a so-called dual-hat arrangement ever since the Defense Department stood up Cyber Command in 2009.

While there have been attempts to split up the two in the past — most notably near the end of the Obama administration and an 11th-hour push in the final weeks of the Trump administration — desire to do so has largely waned since Army Gen. Paul Nakasone assumed command of the military’s top digital warfighting unit and the federal government’s largest intelligence agency nearly four years ago.

### UQ---NSA Primacy---2NC

#### NSA has renewed control over national security systems

Teri Robinson 22, digital content specialist and award-winning journalist specializing in cybersecurity, 1/21/2022, “Biden Signs Authority for NSS to NSA: Think CISA for Military, Intel Systems,” <https://securityboulevard.com/2022/01/biden-signs-authority-for-nss-to-nsa-think-cisa-for-military-intel-systems/>, cc

But better late(ish) than never. “The NSA has a great deal of expertise in the domain of cybersecurity, and further empowerment of this agency to advise, support and direct the broader mission is likely to mitigate risks to our nation’s information system infrastructure,” said Tim Wade, technical director, CTO team, Vectra. “This order reflects the consensus that technology reflects a critical war front in today’s digital age and one of national importance.”

Biden’s directive, bearing the officious name National Security Memorandum 8, “Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems,” represents the implementation of last spring’s EO 14028 that set out cybersecurity requirements for national security systems (NSS) sprawled across the federal government and those that contain classified information or are crucial to military and intelligence activities. The memorandum named General Paul M. Nakasone, Commander, U.S. Cyber Command, Director, NSA/Chief, Central Security Service as national manager for NSS.

“We stand ready to fulfill our role, and our responsibility, in securing our nation against foreign malicious actors, and any efforts to exploit our national security systems,” Nakasone said in a release.

Nakasone’s authority will include the ability to issue binding directives to those agencies and departments operating NSS. Those directives include requiring they take action against cybersecurity threats and vulnerabilities and report mitigation actions and assessments to Nakasone. And Biden’s guidance requires those agencies to also alert the national manager to any suspected NSS incidents and compromises.

### UQ---AT: CYBERCOM High---2NC

#### Biden is stripping CYBERCOM’s free-ranging authority.

Suzanne Smalley 3/31, reporter covering intelligence and disinformation at CyberScoop and former Mandiant exec tapped to run CTIIC, ODNI's cyber threat intelligence center, 3/31/2022, “Biden administration is studying whether to scale back Trump-era cyber authorities at DOD,” <https://www.cyberscoop.com/biden-trump-nspm-13-presidential-memo-cyber-command-white-house/>, cc

The Biden administration is reviewing whether and how to change a Trump-era policy that gave unprecedented authority to the Department of Defense and U.S. Cyber Command to authorize cyber-operations without White House approval, two sources briefed on the discussions said.

The administration has launched an “interagency review process” paving the way for revisions to the Trump-era National Security Presidential Memorandum-13 (NSPM-13), one of the sources said. The White House National Security Council is spearheading the effort, according to the sources.

NSPM-13, which became policy in 2018, allowed the delegation of “well-defined authorities to the secretary of defense to conduct time-sensitive military operations in cyberspace,” according to a 2020 speech given by Paul Ney, then the general counsel for the DOD.

A spokeswoman for the National Security Council declined to comment.

NSPM-13 has long been controversial, and many Washington insiders called its 2018 implementation an unusual response by the Trump administration to historically slow decision-making in the cyber realm, particularly during the Obama administration. NSPM-13 built on the principle of persistent engagement, which Ney described as “continuously engaging and contesting adversaries and causing them uncertainty wherever they maneuver.” NSPM-13, which is classified, also was reportedly amended by another classified memo, NSPM-21, and figured into President Donald Trump’s draft executive order directing the defense secretary to seize voting machines, according to POLITICO.

“Persistent engagement recognizes that cyberspace’s structural feature of interconnectedness and its core condition of constant contact creates a strategic necessity to operate continuously in cyberspace,” Ney said in his remarks, which were made at the Cyber Command Legal Conference in March 2020. “As [Cyber Command chief] Gen. [Paul] Nakasone has said, ‘if we find ourselves defending inside our own networks, we have lost the initiative and the advantage.'”

One of the sources briefed on the administration’s plans to review NSPM-13 said that White House officials want to “regularize cyber operations.” The source described the Trump administration’s delegation of broad cyber authorities to the Defense Department as highly unusual.

“No other kind of weapon system [or] attack system do we do that so it’s unprecedented,” the source said of the Trump decision to allow DOD to launch cyber-operations without White House approval. “If you’re not in combat, the commander is supposed to check in with White House and the president. That’s how we’ve done it before. That’s how we usually do it … The White House should normally have control. That’s how it works. That’s how it works in most other countries.”

“We have very clear rules in the physical world that we don’t have in cyberspace yet. That lack of clarity is part of the problem … and why there’s an argument for being careful.”

FORMER OBAMA CYBERSECURITY COORDINATOR MICHAEL DANIEL

The lack of precedent underpinning many cyberwar scenarios makes the delegation of authority to the Defense Department even riskier, said Michael Daniel, a former Obama administration cybersecurity official who now runs the Cyber Threat Alliance, a cybersecurity nonprofit. Daniel pointed out that when it comes to traditional operations such as flying over another country’s airspace there is clear agreement on how high a plane can fly to respect other nations’ sovereignty. No such clarity exists for cyber operations, Daniel said.

“We have very clear rules in the physical world that we don’t have in cyberspace yet,” Daniel said. “That lack of clarity is part of the problem … and why there’s an argument for being careful about and having oversight over offensive cyber operations.”

Daniel, who served as cybersecurity coordinator on the National Security Council staff from 2012-2017, conceded that the Obama administration sometimes moved slowly making cyber decisions but said that 2012 was a different era than today. He rejected complaints by some that the Obama administration moved excessively slowly, however, and said it is important to remember the broader context before assessing these types of complaints.

“The fact that [an ally] may have been able to move faster than us is not necessarily a sign that that was the right speed to be going and their risk-benefit calculus is different than ours,” Daniel said.

From one administration to the next

The Trump administration decided to overturn Obama-era cyber authorities in order to allow the Department of Defense to move more quickly. John Bolton, Trump’s national security adviser, wrote about the administration’s path to negotiating NSPM-13 in his book “The Room Where It Happened.”

“The interagency process was frozen solid. The Department of Homeland Security and others wanted to keep a stranglehold on the Defense Department, as did the intelligence community,” Bolton wrote of the Trump administration’s infighting as it created NSPM-13. “The Pentagon didn’t want oversight from anyone, including the White House, and took an ‘all or nothing’ approach in negotiations that only infuriated everyone else involved.”

Bolton wrote that some in the intelligence community did not fully support NSPM-13, with many at the CIA envious of the Defense Department’s new authority.

“This reflected a long-standing, almost existential, CIA-Pentagon tension,” Bolton wrote.

Bolton did not return a call seeking comment for this story.

Christopher Painter, the former top cyber official in the Obama State Department, acknowledged that sometimes decisions took time to arrive at, but he said often DOD shared some of the blame.

“There were times when things were simply slower than they would like,” Painter said of the DOD in that era. “I think sometimes that was their own fault.”

Painter said the White House should take back control of cyber authorities so that no one agency is operating in a vacuum. He said it is important for the government to coordinate across agencies so that all tools — economic, diplomatic and military — can be used. He argued that by having the White House determine how and when to act on cyber operations, and by allowing the White House to deploy multiple tactics at once, strategic advantages will follow.

“If the flaming ball of cyber death is coming toward you you have to respond immediately,” Painter said. “But we also have some ability to plan and figure out how we’re going to respond and what tools we’re going to use … Having all of those tools together and doing them strategically as part of a plan, I think really does require the White House to be calling the shots.”

Others pointed to the balance of powers that is threatened when anyone who’s at an agency gets a level of authority which others lack. Tom Bossert, who was a homeland security adviser to Trump, said the debate is fueled in large part by how different government entities relate to each other as they vie for authority.

“There’s a trade off between acting on intelligence to further our national interests or foil a plot and tipping your hand, losing often fragile intelligence channels or burning human sources. In cyber, different agencies have different opinions on when and why we should break things or spy on them,” Bossert, now president of the threat prevention firm Trinity Cyber, said. “U.S. Cyber Command has the authority to weigh the various considerations and equities and other agencies sometimes disagree.”

#### Rescission is imminent.

Herb Lin 5/17, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, 5/17/2022, “President Biden’s Policy Changes for Offensive Cyber Operations,” <https://www.lawfareblog.com/president-bidens-policy-changes-offensive-cyber-operations>, cc

On May 13, a Washington Post story indicated that changes to U.S. policy regarding offensive cyber operations are imminent. These changes would refine the Trump administration policy as promulgated under National Security Presidential Memorandum 13 (NSPM-13) in 2018. To understand the story underlying this change, it is helpful to review the history of presidential guidance and policy regarding offensive cyber operations.

### UQ---AT: Ukraine---2NC

#### Cyber ops in Ukraine were conducted with civilian oversight---not full CYBERCOM autonomy.

Ines Kagubare 6/1, staff writer at The Hill, 6/01/2022, “Cyber Command chief confirms US took part in offensive cyber operations,” <https://thehill.com/policy/cybersecurity/3508639-cyber-command-chief-confirms-us-took-part-in-offensive-cyber-operations/>, cc

U.S. Cyber Command Director Gen. Paul Nakasone confirmed for the first time that the U.S. had conducted offensive cyber operations in support of Ukraine.

“We’ve conducted a series of operations across the full spectrum: offensive, defensive, [and] information operations,” Nakasone said in an interview Wednesday with Sky News, a British television news channel.

Although the general did not provide specifics, he said the operations were lawful and conducted with civilian oversight of the military.

#### Ukraine ops were small-scale AND shrouded in secrecy---can’t vote for a thumper you know nothing about!

Sean Lyngaas 6/2, CNN’s cybersecurity reporter, 6/02/2022, “US confirms military hackers have conducted cyber operations in support of Ukraine,” <https://www.cnn.com/2022/06/02/politics/us-hackers-ukraine-support/index.html>, cc

"We've conducted a series of operations across the full spectrum; offensive, defensive, [and] information operations," General Paul Nakasone said in an interview with Sky News. A spokesperson for the command did not dispute the accuracy of the article but declined to elaborate on what the command's operations in Ukraine have entailed.

It's a rare public acknowledgment from US military officials of hacking operations that are often shrouded in mystery.

Nakasone's comments, and the White House's response to them, suggest that cyberspace is a domain in which the Biden administration feels comfortable countering Russia without fear of escalation. President Joe Biden has pledged not to engage directly with Russia militarily during the Ukraine war so long as the US and its allies aren't attacked.

Pro-Russia online operatives falsely claimed Zelensky committed suicide in an effort to sway public opinion, cybersecurity firm says

Pro-Russia online operatives falsely claimed Zelensky committed suicide in an effort to sway public opinion, cybersecurity firm says

"We don't see it as such," White House press secretary Karine Jean-Pierre said Wednesday when asked at a news conference whether Cyber Command's actions contradicted Biden's pledge.

Officials from Biden on down have for months warned about the threat of retaliatory Russian cyberattacks against US infrastructure after the US and its allies imposed sweeping sanctions on the Kremlin over its war in Ukraine.

While analysts have proffered a range of theories, including improvements in US defenses, for why such a hack hasn't apparently happened yet, US officials tell CNN that Russian fear of escalation in cyberspace could be one factor.

For one, Moscow may not want to risk retaliatory US cyberattacks that could hinder Russian military operations, a senior US defense intelligence official told CNN.

The Russians have already had enough problems in Ukraine executing military operations, "I think that adding any kind of potential for US cyber into that mix ... [is] probably factoring into their decision calculus," said the official, who spoke on the condition of anonymity to speak candidly about a sensitive national security issue.

US and European allies blame Russia for cyberattack on satellite provider as Ukraine invasion began

The paucity of Russian hacking on US targets may reflect the "fear of escalation and what the US response might be, particularly if the US response affects Russian combat power in some form or fashion," the official added.

The statements, from an interview with a senior official tasked with keeping a close eye on Russian cyber activity, offer a window into US thinking on Russian hacking at a critical time in the war -- as the Kremlin targets eastern Ukraine after failing to take Kyiv.

The official's analysis also reflects the uncertainty and ambiguity of big-power competition in cyberspace, where governments try to keep each other guessing on their hacking capabilities and willingness to use them.

"For Russia, understanding the full scope of US cyber combat power is a gap for them which leaves them unsure about opening this front, at least at this time," the senior US official said. "Cyber warfare is a new domain ... It hasn't been around long enough for any one nation-state to dominate it."

'Attribution in peacetime is tricky enough'

Analysts say Cyber Command has matured considerably since its inception more than a decade ago and has increasingly become a tool of US power projection. The command sent personnel to Ukraine in December, in anticipation of the Russian invasion, to help Kyiv bolster its cyber defenses and to gather information about potential Russian hacking threats, officials have said.

There are a range of activities, including low-level intrusions into computer networks, that may qualify as "offensive" cyber operations but which the Russians may not necessarily interpret as escalatory, according to Bobby Chesney, an associate dean at the University of Texas School of Law who focuses on cyber and national security law.

Some of the command's previous hacking operations have included knocking a Russian troll farm offline during 2018 US midterm elections, according to a Washington Post report, and targeting ransomware operatives who threaten US organizations.

While big hacks of US organizations related to the Ukraine war have been in short supply, a plethora of attempted cyberattacks have been reported in Ukraine and Russia as digital vigilantes take sides in the war. The websites of Russian government ministries and media mouthpieces have been knocked offline or altered to broadcast anti-war slogans.

The senior US defense intelligence official expressed concern that the Russian government may mistakenly assess that that type of hacking is coming from the US government.

"Attribution in peacetime is tricky enough ... I would say there's a real danger of unintentionally attributing something to the United States that the United States or its allies simply did not do," the official said.

## Link

### Link---Overlap---2NC

#### OVERLAP

#### New cyber initiatives infringe on NSA authority, causing jurisdictional confusion and undermining their primacy.

Daniel Wilson 22, senior reporter covering government contract and defense-related legislative, regulatory and litigation issues for Law360, 1/24/2022, “New Biden Cybersecurity Memo May Sow Agency Confusion,” <https://www.law360.com/articles/1457119/new-biden-cybersecurity-memo-may-sow-agency-confusion>, cc

Law360 (January 24, 2022, 7:01 PM EST) -- A new White House memo aimed at improving cybersecurity coordination and standards across national security agencies may end up having the unintended effect of causing confusion when cybersecurity missions overlap with those of other federal agencies.

The Jan. 19 memorandum requires the U.S. Department of Defense and the 17 agencies and offices within the Intelligence Community to meet or exceed the same cybersecurity standards that "civilian" agencies — all the other executive branch agencies — are required to meet under a May 2021 executive order. The National Security Agency will take the lead in coordinating those efforts as a "national manager," according to the memo.

The document provides a framework for what should be done within the national security community to improve cybersecurity, but is not clear on when and how information and responsibility should be shared across civilian and intelligence agencies. This lack of clarity could potentially lead to jurisdictional clashes and confusion and to privacy risks related to information-sharing, according to Alex Major, co-chair of the government contracts practice at McCarter & English LLP.

"The fact that you now have NSA and [the Cybersecurity and Infrastructure Security Agency] in a position where they're conferring on cybersecurity and incident response could pose a potential risk that hopefully the national manager and CISA are both cognizant of," he said. "It's not really raised in the executive order, but those kinds of privacy issues can become problematic if not done appropriately."

One potential area of confusion may arise in circumstances where there is a "fine line" between whether an incident should be handled by the law enforcement arm of a civilian agency or by an intelligence agency, according to Major, who is a retired Air Force intelligence officer.

For example, if there is a cyberattack that might involve a foreign power against a federal system that is not considered to be a national security system, uncertainty over who is responsible could delay the federal government's response or result in an agency with insufficient expertise leading the response. Such a scenario has the potential to worsen damages to those systems.

The government will need to issue guidance to clarify how clashes between areas of civilian and national security responsibilities will be addressed, experts said. Such guidance would provide important clarity for contractors who will help implement new cybersecurity programs, Hogan Lovells counsel Stacy Hadeka said. But so far nothing has been released since the May executive order.

"We're still waiting on uniform guidance on the civilian side, and have yet to get any updates if there'll be any kind of more uniform government requirements," she said.

At least some possible clashes could be avoided, however, by a provision in the memo that allows national security agencies to invoke an exception to address "circumstances necessitated by unique mission needs," said Reed Smith LLP partner Liza Craig, a former Navy attorney.

"Baked into this process [is an] exception where they can do things … to address greater national security issues as they arise," she said. "I think that, in and of itself, will minimize those turf wars."

The memo also lays out a clear hierarchy within the national security community that places the NSA at the top. The ranking order could help minimize clashes between national security agencies and eliminate instances of agencies keeping important cybersecurity information to themselves, according to Major of McCarter & English.

The NSA could also ensure continuity across different agencies with its authority to issue binding operational directives to other national security agencies to address known or suspected cyberthreats.

"The national manager is supposed to be there as a referee or an umpire to make sure that entities are doing what they're supposed to be doing," Major said.

Any regulations that may be forthcoming are expected to be crafted in a way that allows them to change over time in response to new kinds of threats and evolving cybersecurity technology, and will hopefully lead to a standardized approach across federal agencies, according to Reed Smith's Craig.

"To me, the takeaway is that this is no longer going to be left just to the agencies to craft their own responses, but they're going to be able to pool all the resources and all the knowledge and awareness and experiences of these agencies to do something governmentwide," she said.

Other indications that the regulations will be a "living document" include the memo's references to cutting-edge technologies like quantum cryptography, as well as the fact that the intelligence community is often at the forefront of developing and using new technologies, according to Hadeka of Hogan Lovells.

"NSA, I think, will be in a good position to hopefully take the lead and spearhead [efforts to ensure requirements keep up with technology] so that by the time something's implemented it's not obsolete, which I think is a big struggle with the federal government overall," Hadeka said.

#### There’s a clear separation between NSA and CYBERCOM jurisdiction---the plan intrudes on NSA territory.

Andrew Schoka 19, active duty Army cyber operations officer assigned to U.S. Cyber Command at Fort Meade, Maryland, and Distinguished Military Graduate of Virginia Tech with a bachelor’s degree in systems engineering, 4/03/2019, “CYBER COMMAND, THE NSA, AND OPERATING IN CYBERSPACE: TIME TO END THE DUAL HAT,” <https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/>, cc

For every operation Cyber Command executes, joint leaders and operations planners must meticulously calculate and evaluate the risk associated with that particular operation. This is an exceedingly complicated task that requires detailed knowledge of the operations planning and approval process, in addition to technical familiarity with the underlying technologies associated with the operation. In developing this process, Cyber Command has relied heavily on the experience of NSA, using similar processes to ensure that risk is minimized. In so doing, Cyber Command has inadvertently patterned its own appetite for risk after NSA’s. But while NSA’s operations are conducted with scrupulous operational security, intelligence collection is not the primary mission of Cyber Command. In the words of Gen. Paul Nakasone, Cyber Command’s primary mission is to impose costs on adversaries who have acted in the cyberspace domain without fear of retaliation. Imposing cost implies inflicting noticeable damage to a target in a manner that would typically be considered too noisy, risky, or noticeable in signals intelligence operations.

When conducting offensive cyberspace operations, there are essentially two ways to acquire access to a target system: using credentials to masquerade as a legitimate user, and using a vulnerability to exploit a system. In a masquerade, an attacker uses valid credentials, such as a username and password, to log in to the target system as an authorized user. Masquerade attacks are usually difficult to detect because they rely on the system behaving the way it’s supposed to. Conversely, an exploit relies on the existence of a technical vulnerability that allows an attacker to gain unauthorized access to a system. Exploitation relies on a system functioning incorrectly, and is significantly more likely to produce alerts that can expose an attack.

To assess the risk associated with these types of operations, Cyber Command solicits approval from an array of staffs and reviewers. In part because Cyber Command has relied heavily on NSA training, support, and experience to establish these processes, exploitation operations — which by nature carry a greater risk of detection — are subject to increased standards of scrutiny. Likewise, operations that produce a noticeable effect, such as a denial-of-service attack, are typically viewed with aversion. This is detrimental to Cyber Command’s execution of its mission, as producing the desired outcomes against an adversary requires assuming more risk. In reality, the operations approval structure of Cyber Command is set up to prioritize the security of operations above all else, and is extremely risk-averse. Cyber Command’s mission is fundamentally different than NSA’s, and rather than copying approval processes used in intelligence operations, it ought to employ a structure more typical of a military command. However, as long as it relies on NSA tradecraft and expertise Cyber Command will continue to use a paradoxical operations process that is fundamentally opposed to the exact type of mission it is charged with conducting.

### Link---Overlap---AT: Same Function---2NC

#### They’re different. CYBERCOM is offense.

Matthew Tyson 22, Software Architect, CSO, 5/16/2022, “The US federal cybersecurity bureaucracy: A guide,” <https://www.csoonline.com/article/3659249/the-us-federal-cybersecurity-bureaucracy-a-guide.html>, cc

What is the difference between the two organizations? Given that the organizations are so steeped in secrecy, the difference is hard to determine exactly. The NSA and Cyber Command operate (largely) with different legal authority, the former under Title 50 intelligence and the latter under Title 10 military authority. This difference seems to be reflected in a more offensive-leaning posture to CYBERCOM.

Although the mission statements for the NSA and CYBERCOM both read as similar—bland, yet encompassing descriptions of almost any kind of virtual activity—there is a subtle difference.

For example, CYBERCOM has this to say: “United States Army Cyber Command directs and conducts integrated electronic warfare, information and cyberspace operations [...] through cyberspace and the information environment, and to deny the same to our adversaries.”

Notable in the description is the word “warfare.” Again the clandestine nature of the organization makes it hard to say, but perhaps CYBERCOM has its hand in alleged offensive activities like attacks on Iran and Russia.

#### NSA and CYBERCOM seek fundamentally distinct missions.

Fabio Vanorio 18, Executive Officer of the Italian Government at the Ministry of Foreign Affairs and International Cooperation at the Presidency of the Council of the Ministers, May 2018, “Breaking Up The Dual-Hat Leadership Of National Security Agency And United States Cyber Command The Central Debate In The United States Cyber Community,” <https://www.strategicstudies.it/wp-content/uploads/2018/05/BREAKING-UP-THE-DUAL-HAT-LEADERSHIP-OF-NATIONAL-SECURITY-AGENCY-AND-UNITED-STATES-CYBER-COMMAND.pdf>, cc

The debate about mixing-up military and civilian systems in the cyber security has pro and cons. According to Gen. Nakasone remarks,21 the dualhat arrangement has enabled an operationally close, mutually beneficial partnership, for instance, in mapping networks prior to operations.22 Similarly, the experience has also brought some issues23, such as for example a growing dependence of Military CYBERCOM Information Assurance (IA)24 on the civilian NSA IA25. About the cyber issue, NSA and USCYBERCOM have fundamentally different missions. From an NSA perspective, cyber is about gaining access to networks; from a USCYBERCOM point of view, it’s about every piece of software on the battlefield the adversary is using and preventing that software from working the way it was intended to work.26 In cyberspace, while the military wants to attack networks, intelligence objectives prioritizes gathering information from them.27 This keeps both agencies in potential disagreement about how to use intel and tools that they share.

### Link---Overlap---AT: Same Budgets---2NC

#### CYBERCOM and the NSA’s budgets are separate.

Andru Wall 11, Senior Associate with Alston & Bird LLP; former senior legal advisor for U.S. Special Operations Command Centra, 12/2/2011, “Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities & Covert Action,” <https://www.soc.mil/528th/PDFs/Title10Title50.pdf>, cc

[FOOTNOTE 14]

14 The DoD controls about 80% of the intelligence budget, which presumably only includes DoD agencies that are also part of the intelligence community; most of the 80% is spent on spy satellites and overseas listening posts. Mark Mazzetti, Nominee Promises Action as U.S. Intelligence Chief, N.Y. TIMES Jul. 21, 2010, at A16, available at <http://www.nytimes.com/2010/07/21/us/politics/21intel.html>.

[END FOOTNOTE 14]

### Link---Autonomy---2NC

#### AUTONOMY

#### CYBERCOM’s demonstration of independence allows it to break off from the NSA.

Fabio Vanorio 18, Executive Officer of the Italian Government at the Ministry of Foreign Affairs and International Cooperation at the Presidency of the Council of the Ministers, May 2018, “Breaking Up The Dual-Hat Leadership Of National Security Agency And United States Cyber Command The Central Debate In The United States Cyber Community,” <https://www.strategicstudies.it/wp-content/uploads/2018/05/BREAKING-UP-THE-DUAL-HAT-LEADERSHIP-OF-NATIONAL-SECURITY-AGENCY-AND-UNITED-STATES-CYBER-COMMAND.pdf>, cc

Taking a corporate view as an example, the strategy of breaking up NSA and USCYBERCOM is like a spin off. Until the benefits of a combined organizational structure justify the negative cost of duplicative management structures and synergies costs, the structure allows USCYBERCOM to take advantage of synergy opportunities. As soon as synergies and economies of scale diminish or disappear, NSA can split off part of its operations into USCYBERCOM.

### Link---Tech---2NC

#### TECH

#### The plan disrupts the NSA’s complete control over weapons tech security.

Morgan Dwyer 20, fellow in the International Security Program and deputy director for policy analysis in the Defense-Industrial Initiatives Group at the Center for Strategic and International Studies in Washington, D.C., 1/22/2020, “An Alternative to the Defense Department’s New, Technology-Focused Organizations,” <https://www.csis.org/analysis/alternative-defense-departments-new-technology-focused-organizations>, cc

National Security Agency (NSA) engineers similarly benefit from their agency’s end-to-end approach to technology management. By controlling all technology that contributes to its signals intelligence mission, NSA can develop a “coherent architecture” that optimally integrates collection, processing, exploitation, and analysis technologies. Because NSA manages all technologies that contribute to its mission, it empowers its engineers to design holistic architectures to optimally execute that mission.

By creating new organizations that focus on high-priority technology, today’s policymakers constructed institutional barriers to the type of end-to-end, mission-focused architecture development that exists in NRO and NSA. Even today’s new, technology-focused combatant commands may disrupt architecture development by complicating command-and-control relationships amongst the various components in an end-to-end architecture. It remains to be seen, therefore, whether these new organizations—all of which separate technologies from the missions they support—will overcome institutional barriers and allow missions to drive the demand for and design of new technology.

### Link---AT: UQ Overwhelms---2NC

#### Splitting apart the dual hat is possible---the plan drops the guillotine.

Erica Borghard 21, Adjunct Research Scholar in the Saltzman Institute of War and Peace Studies and an Adjunct Associate Professor in the Department of Political Science, “Time to end the dual hat?,” <https://www.cfr.org/blog/time-end-dual-hat>, cc

That said, the Biden administration will have significant discretion to shape the timing and sequencing of what is likely an inevitable split of the dual hat. While the law does stipulate six conditions that would need to be met to precipitate the dual hat’s separation, Congress did not provide much guidance in terms of metrics corresponding to those conditions. In other words, the type of evidence that would confirm or deny Cyber Command’s operational maturity remains underspecified, giving considerable latitude to the executive branch to shape the timing and conditions under which certification would occur.

### Link---AT: Plan is NSA---2NC

#### Plan can’t be the NSA. Security cooperation must be authorized under Title 10 or 22.

DSCU 21, Defense Security Cooperation University, May 2021, “SECURITY COOPERATION MANAGEMENT,” Edition 41 of the Greenbook, <https://www.dscu.edu/documents/publications/greenbook/v41_0/24_Greenbook_41_0_Complete.pdf>, cc

Security Cooperation (SC). Any Department of Defense program, activity, or interaction with foreign security establishments designed to 1) build security relationships that promote U.S. interests; 2) develop allied or other partner national military and security capabilities for self-defense or participation in U.S.-sanctioned multinational operations; or 3) provide U.S. forces with peacetime/contingency access to allied and partner nations. Security cooperation may be authorized under Title 10 or Title 22 of the United States Code, or under temporary (non-codified) U.S. laws.

## Internal

### Internal---Personnel---2NC

#### Ending the dual-hat arrangement cleaves personnel in half, undermining security.

James Di Pane 19, Policy Analyst, Defense Policy, Center for National Defense, 5/02/2019, “Should Cyber Command and the NSA Have Separate Leadership? How to Decide,” <https://www.heritage.org/defense/report/should-cyber-command-and-the-nsa-have-separate-leadership-how-decide>, cc

NSA and Cyber Command Pull from the Same Talent Pool. The NSA and Cyber Command operate jointly in many instances. Not only do they both hire the same type of employee, but a number of employees work for both organizations simultaneously, changing fluidly depending on the situation. Ending the dual-hat arrangement could result in personnel being forced to choose to work for either Cyber Command or the NSA, leading to personnel issues within both. Cyber Command still relies on NSA personnel for its command staff, even though it now operates independently of Strategic Command.

This would be challenging under most circumstances, but is especially a problem given the challenges that the NSA and Cyber Command have with attracting and retaining top tech talent. Additionally, cyber talent takes years to cultivate, meaning that the recruits filling the ranks would be less capable than their more experienced counterparts. Lieutenant General Stephen Fogarty, Commander of Army Cyber Command, testified before the Senate Armed Services Subcommittees on Cybersecurity and Personnel that the average operator can spend fully half of his or her six-year enlistment in training.29

Recent reporting shows that the U.S. government is struggling to attract and retain top cyber talent due to stiff competition from the private sector. The government has difficulty competing with the high salaries and swift onboarding processes large companies can offer. Cyber Command has outlined a series of initiatives to help improve talent recruitment and retention, including keeping close relationships with universities, increased pay scales, and retention bonuses. But the government may not be able to fill the necessary manpower demand it would create by splitting the organizations.30

The NSA and Cyber Command also share personnel because of the relative scarcity of cyber talent in the public sector. Despite Cyber Command’s Cyber Mission Force teams filling all of its 6,200 billets, recent Senate testimony revealed lawmakers’ concern about a “shortage of cyber-capable personnel.”31 This makes the efficiency of scarce resources essential for the command, and sharing personnel is key to that efficiency.

### Internal---AT: Still Cooperate---2NC

#### Splitting shoves the NSA back into its shell, severing cooperation.

Patrick Tucker 21, technology editor for Defense One, 3/08/2021, “Splitting NSA, CyberCom Now Could Reduce Military Access to Intelligence, Milley Says,” <https://www.defenseone.com/technology/2021/03/splitting-nsa-cybercom-now-could-reduce-military-access-intelligence-milley-says/172535/>, cc

As Michael Sulmeyer, currently the senior director for cyber with the National Security Council, wrote in 2017: “When Cyber Command needs NSA support, the fact that it’s the same person in charge of both organizations can break what might otherwise be a log-jam. Splitting the dual-hat could result in the NSA isolating itself and refocusing on its own core missions (the collection of signals intelligence and providing information assurance) while minimizing its support to Cyber Command.” (Sulmeyer was serving as the Cyber Project director for Harvard’s Belfer Center at the time of the writing.)

# Case

## OCO’s Bad

### UQ CP---1NC

#### The United States federal government should: ---fund cyber attribution and preemptive cyberdefense programs, including incentivizing development of similar allied defense capability for other NATO nations ---adopt a primarily defensive cybersecurity posture, clarifying to NATO allies that such posture is the West’s primary defense mechanism against cyber threats ---encourage NATO integration of the above defense policy, offering intelligence gained through defensive expansion in return

#### A defensive posture solves---prevents escalation and helps shape alliance norms

Jervis and Healey 20. Robert Jervis (Ph.D., California at Berkeley, 1968) is the Adlai E. Stevenson Professor of International Politics and has been a member of the Columbia political science department since 1980. Jason Healey is a senior research scholar and adjunct professor at the School of International and Public Affairs, Columbia University. He is also a senior fellow with the Cyber Statecraft Initiative at the Atlantic Council, where he was the program's founding director; “The Escalation Inversion and Other Oddities of Situational Cyber Stability”; Fall 2020; TNSR Vol. 3, Iss. 4; <http://dx.doi.org/10.26153/tsw/10962> //BY

Defense Is Likely the Best Defense

Attackers have the advantage. It takes a varsity defense to defeat a team of junior varsity attackers. If the attackers bring their own varsity team, the defenders need to have an all-star defense to have a chance. And if the attackers are themselves an all-star team, then few organizations in the world have much chance. There is certainly a role for the new U.S. push for persistent engagement and defending forward. When Russian cyber operatives are disrupting the opening ceremony of the Olympic Games and North Koreans conduct cyber bank heists around the world, it seems disingenuous to badmouth U.S. countermeasures as being escalatory.[122](https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/" \l "_ftn122) It is destabilizing, however, to elevate the operational concept of persistent engagement to a strategy, given the likelihood of destabilizing positive feedback.

A better option is for policymakers to prioritize defense and reverse attacker advantage though “leverage.” The New York Cyber Task Force analyzed five decades of “technology, operational, and policy innovations which most advantage the defender” and concluded a more defense-advantage cyberspace is possible with technical solutions that can scale across the entire internet (rather than just one enterprise at a time) and fresh investment in operational and process innovations.[123](https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/" \l "_ftn123)

If cyberspace were more advantageous to the defender, many of the most destabilizing dynamics would lose force with higher barriers to entry, leading to fewer capable adversaries and fewer serious attacks. Since fewer attacks might be catastrophic, the pressure for counter-offensive operations would be diminished with more room for agreement and norm building.

### Trust Turn---1NC

#### Cross-alliance intelligence-sharing collapses NATO cohesion and cyber operations

APRA, 20 (Association for Political Risk Analysis, “The Looming NATO Offensive Cyber Policy’s Challenges of Harmonizing Deterrence and Decision-making”, APRA, Sep 27, 2020, https://www.aprascpo.org/post/the-looming-nato-offensive-cyber-policy-s-challenges-of-harmonizing-deterrence-and-decision-making)

Testing Alliance Consensus and Decision-making The Alliance’s decision-making principle of consensus further complicates the negotiations and agreement of a NATO offensive cyber policy. The above-mentioned nuclear example almost exclusively concerns kinetic and state-level physical destruction of massive proportions. The dire consequences of the extremity of possible nuclear proliferation are enough to establish credibility, deterrence, and is a comparatively simpler way in getting its 30 member states on board, especially in the context of Cold War bipolarity. Cyberspace as a domain of war contains a myriad of vested technical issues including the difficulty of attributing attacks to specific adversaries. Even though this is one the most prominent difficulties according to a variety of research in cybersecurity, more recent analyses published by NATO's Cooperative Cyber Defence Centre of Excellence have suggested that the attribution gap is gradually decreasing in size due to heavy research and development investment into web tracing and identification designs largely spearheaded by the US (Burton 11). A dynamic understanding of deterrence in cyberspace as formerly suggested by taking into consideration social and historical context will also alleviate the traditionally ‘impossible’ problem of attribution. While such technical capabilities play a crucial role in swaying the allies’ considerations and decisions, the political and strategic issues of simply conceptualizing an offensive cyber policy are examined in closer detail here. Trust and Transparency The transparency and capability-sharing quality of NATO may give way for disagreement amongst allies. Although the Alliance’s communication on a strategic and policy level is transparent, it still possesses enough opaque room to maneuver on an operational and tactical level. Furthermore, the problem of American supremacy in cyber capabilities and NATO’s reliance on its critical perspective may displease EU member states like France in their pursuit of strategic autonomy aside from its prevailing aversion to today's American leadership. A new demand for cross-alliance intelligence-sharing on offensive cyber capabilities can also exacerbate internal trust issues with the US. The global surveillance disclosures from 2013 onwards revealed allied surveillance and spying activities which damaged confidence in NATO (Smeets; 2018). Discussion of further integrated intelligence-sharing strategy under an offensive cyber policy can create tension between Five Eyes states (Canada, the US, and the UK) and other NATO allies. Doctrine Diversity Another overarching aspect with the potential to determine allies’ reception and leniency towards an offensive cyber strategy is the diversity of threat perception among NATO allies. The diversity across allied standards in defining the parameters of cyberattacks and the lack of overarching offensive cyber policy could result in strategic ambiguity and discourage retaliation (Arts 2). These differences stem from varied threat perceptions and cyber norms. Nationally, both threat perception and cyber norms are influenced by the state’s experience with malicious cyberattacks and its media and public opinion; and externally, the state’s engagement in bilateral and multilateral engagements are the most effective ways in which threat perception and cyber norms are shaped (Lewis 575). This hints at the political interest of near-Russia states like Estonia and Finland to possess well-rounded cyber norms and threat perception. Conversely, policy engagements on offensive capabilities would also shape NATO allies’ understanding as a whole. Without multilateral definitions, allies like Luxembourg and Iceland who have not experienced similar events do not benefit from harmonized knowledge and may not find justification to prioritize the strengthening of cyber capabilities when allocating funds from the common NATO budget. Not to mention the financial commitment issue affects trust in the Alliance overall as well.

#### The plan destroys trust --- NATO hates the idea of OCO’s, and even the discussion creates backlash --- The plans forced disclosure also causes backlash to US surveillance

Fidler ’13 [David, Richard Pregent, and Alex Vandurme; Fall; James Louis Calamaras Professor of Law, Indiana University Maurer School of Law and Senior Fellow, Indiana University Center on Applied Cybersecurity Research; Legal Advisor, NATO Allied Command Counterintelligence; Head, Technical Center Engineering, NATO Computer Incident Response Capability; St. John’s Journal of International & Comparative Law, “NATO, Cyber Defense, and International Law,” 4:1, https://www.repository.law.indiana.edu/facpub/1672]

Concerning the three categories and the potential policy shifting described above, NATO finds itself in a difficult situation that, under current NATO practices, will be hard to escape. In terms of the cyber threat, defense, and technology approaches, NATO reflects behavior that puts the Alliance at a disadvantage. NATO tends to be conservative in terms of legal issues, meaning that the Alliance does not promise to be a fruitful forum for adapting or revising legacy rules to reflect the particular challenges **cyber** poses. Similarly, with NATO operating on the basis of consensus, the Alliance’s decision-making processes might have difficulty handling governance questions created by the cyber defense **approach**, such as how “active” should NATO cyber defense be. Operationally, NATO cyber defense appears more static and reactive than active in orientation—a situation that could lead NATO cyber defense to become a cyber “Maginot line” rather than an effective defensive strategy. It is not clear whether NATO members could reach consensus on what more active cyber defense activities would be permissible under international legal principles on sovereignty and non-intervention. As noted earlier, NATO functions with the capabilities its members make available to it, meaning that NATO’s technological capabilities in cyber might not reach cutting-edge status, leaving NATO cyber defense behind the global technological curve in cyberspace. This problem is exacerbated if policy makers in leading powers, such as the United States and China, are placing more reliance on developing, deploying, and using full-spectrum cyber technological capabilities because of the perceived pitfalls of other approaches and the mounting geopolitical competition now affecting cyberspace. NATO members are also extraordinarily sensitive to the Alliance having any offensive cyber capabilities or even discussing the need to think about the value of cyber capabilities and operations in missions NATO might undertake (as NATO has done with other technological developments affecting its military missions).44 The North Atlantic Council has not discussed, let alone authorized, the development of offensive capabilities, doctrine, or rules of engagement in the cyber realm.45 Whether NATO members could agree on what **offensive cyber operations** international law would permit is also not clear, especially in light of difficulties cyber presents to the international law on armed conflict **revealed by the Tallinn Manual** and other analyses.46 Events outside the specific context of NATO cyber defense might also adversely affect NATO cooperation. For example, in June 2013, negative European reactions to the disclosure of a secret U.S. surveillance program targeting cyber activities of foreign nationals, code-named PRISM, reflected new transAtlantic tensions on **government surveillance in cyberspace**, its implications for privacy and other civil liberties, and the potential for European-American cooperation on cybersecurity. The Washington Post reported that “[t]he **discontent from Europe pointed** to the breadth of fallout from the affair and to the potential for fresh strains between the United States and allies wary of American intrusiveness.”47 Whatever the long-term impact of this political fallout, the short-term consequences will likely not create more willingness among NATO members to become more ambitious with NATO cyber defense.

#### Allies say no to OCO’s and countries with OCO’s don’t want to integrate because of free-riding

Veenendaal et al 16 (Matthijs Veenendaal has been working for the Netherlands Ministry of Defence since 2006 in various policy positions. He is currently stationed as a researcher at the Strategy Branch of the NATO Cooperative Cyber Defence Centre of Excellence in Estonia. Kadri Kaska is a researcher at the NATO Cooperative Cyber Defence Centre of Excellence. MAJ Pascal Brangetto is a supply officer in the French Army. “Is NATO Ready to Cross the Rubicon on Cyber Defence?” June 2016 https://ccdcoe.org/uploads/2018/10/NATO-CCD-COE-policy-paper.pdf)

Given modern armed forces’ dependency on digital technology, it is legitimate to expect that NATO would adapt to this new reality. Since 2002, NATO has invested significantly in improving the defence of its networks. However, NATO has shown little inclination to move away from its current purely defensive posture in cyber defence. At the political level, Allies remain reticent when it comes to discussing the options of using military (offensive) capabilities within a NATO setting. For most of them, cyber operations are generally still uncharted territory in which confusion abounds. Moreover, Allies that have invested heavily in cyber capabilities worry that others might benefit without making a similar investment themselves. Allies therefore remain reluctant to engage in any meaningful discussion on the position and role of cyber capabilities in military operations within the Alliance.

### Defense Solves Deterrence---2NC

#### Only a strictly defensive posture solves---traditional deterrence fails in the cyber realm

Schneider 18. Jacquelyn Schneider is a Hoover Fellow at the Hoover Institution. Her research focuses on the intersection of technology, national security, and political psychology with a special interest in cybersecurity, unmanned technologies, and Northeast Asia; “Cyber and Cross Domain Deterrence: Deterring Within and From Cyberspace”; 2018; <https://www.academia.edu/30652154/Cyber_and_Cross_Domain_Deterrence_Deterring_Within_and_From_Cyberspace> //BY

III. Cross-Domain Deterrence of Cyberspace Operations. Cross-domain deterrence of cyberspace operations involves the use of punishment and denial across domains of warfighting and foreign policy in order to deter adversaries from utilizing cyberspace operations to create virtual or physical effects. In general, the major underlying debate for all arguments about cyberspace and deterrence is whether or not cyberspace is unique to conventional and nuclear models of deterrence. Advocates of cyberspace’s unique characteristics (Libicki 2009, Philbin 2013, Jensen 2012, Elliott 2011, Sterner 2011) argue that the technical qualities of cyberspace affect attribution, signaling, capabilities, and actors in a way that fundamentally negates how we traditionally view successful deterrence. These authors argue that it is uniquely difficult to attribute in a timely fashion, to signal capabilities overtly, to anticipate cyberspace effects, to use cyberspace weapons repeatedly, and to limit the amount of actors you need to deter. Taken in conjunction with the unique interdependence of military and civilian cyber infrastructures, the perceived asymmetries in vulnerabilities between the U.S. and its enemies, and the lack of existing norms, these critics argue that the U.S. cannot rely on retaliatory deterrence strategies or mutually assured vulnerability for effective deterrence of cyberspace operations. Advocates of cyberspace’s unique qualities recommend policies that are strategically ambiguous, focused on defense and resiliency, and that invest in attribution technologies over retaliatory measures.

#### The CP makes cyber-defense viable

Alperovitch et al. 18. Dmitri Alperovitch is a computer security industry executive. He is co-founder and former chief technology officer of CrowdStrike; “Building a Defensible Cyberspace”; 2018; New York Cyber Task Force; <https://www.sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF> //BY

A more defensible Internet is within reach. New game-changing technologies, such as the secure architectures permitted by cloud technologies, can radically alter cyberspace with advantage and scale in favor of defenders. But so too can operational and policy innovations, which are often overlooked or discounted. When presented with new proposals, decision makers should ask a few simple questions: Does this new policy, process, or technology clearly bring leverage? If the mechanism for creating leverage is not clear, then the innovation is probably at best an incremental improvement. Incremental improvements, while useful, should be treated as temporary band-aids and cannot (as information sharing legislation demonstrates) be the last word. For any given problem, where will leverage deliver the most impact? Leverage can be applied to many existing, low-payoff solutions. For example, leverage has been applied to reinvigorating cyber awareness education, the often mundane set of tasks that discourages users from clicking on links. A quarterly awareness video that provides less than one dollar of additional security for each dollar spent certainly doesn’t suffice. Many firms now conduct their own phishing campaigns as an educational exercise, targeting those who click on suspicious links for follow-up online training. This report has argued for a new approach to cyber defense, one that can break the stalemate of the past five decades, so that defenders finally have the high ground, to fight with the advantage. This approach does not have to be a highly complex, government-run “Moon Shot.” It certainly should not be a “Cyber Manhattan Project;” the Internet is a boon to individuals and societies, not a weapon. If anything, the world needs a cyber equivalent of Silent Spring to reveal to us how precious the Internet is and how our actions are destroying it, and energize stakeholders to make some hard tradeoffs. The NY Cyber Task Force has tried to bring new, pragmatic approaches to cybersecurity. Some of our solutions can be implemented with relative ease now that we’ve identified the lessons of success. Others will be far more difficult, as they create clear winners and losers. All task force members agree that smaller interventions are necessary now to avoid even harder decisions as the situation worsens. Defense is possible, but only through leverage, and the sooner the better.

#### Investment solves attacker advantage

Alperovitch et al. 18. Dmitri Alperovitch is a computer security industry executive. He is co-founder and former chief technology officer of CrowdStrike; “Building a Defensible Cyberspace”; 2018; New York Cyber Task Force; <https://www.sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF> //BY

In a little over 20 years, the percent of the global population with access to the Internet (and the larger cyberspace of connected devices and information, terms this report will use interchangeably) has gone from less than one to about 40, over 3.595 billion people.2 In the United States alone, the Internet sector makes up an estimated six percent of GDP; the “mobile internet and app services” subsector alone has a “contribution to the US GDP [of] approximately 3.11%, putting it at approximately the same size as the Automotive industry.”3 Yet, as the reach and benefits of the Internet have increased, so too have the economic costs. A 2015 study indicated that cybersecurity costs were likely to rise above $1.2 trillion by 2030 costing a total of roughly $20 trillion over those 15 years.4 The costs are high because attackers in cyberspace have for decades held fundamental advantages over defenders. The Internet was designed to be flexible and open, not secure. For years, nearly every device and piece of code added to cyberspace has reiterated this pattern: “minimum viable products” are rushed to market with security slapped on afterward as a band-aid, rather than built in. All this complexity has multiplied the costs and challenges of mounting a successful defense. Still, defense is possible. This report builds on an increasingly rich set of cybersecurity research on creating a “defense advantage” that raises costs to attackers and enables cost-effective risk management. Some of these ideas, such as to allow the least privileges or to failsafe in a secure manner, date back to the 1970s.5 Other work, especially in the business community, has centered on the return on investment of defensive innovations. Inspired by military tactics, others have sought to raise costs to attackers by making their task harder or actively disrupting their operations. The NY Cyber Task Force, through the experience of our members and interviews with other experts, has tried to combine these three perspectives. Our task force started by asking, “what technological, operational, and policy innovations have had the greatest impact in thwarting attackers?” We found that the highest-impact innovations shared two key traits: • Defense advantage: Any innovation by defenders must impose far greater costs on attackers. A “dollar of defense” (or hour or other measure of input) should yield not merely a “dollar of attack,” but should force attackers to spend considerably more to defeat it. • Hyperscale: The innovation must easily, even automatically, work across enterprises or cyberspace as a whole. The task force members and the colleagues we interviewed consistently agreed on the past innovations with the highest scale and leverage over attackers: strong encryption, software that updates automatically with little or no user intervention, and software that is secure because it was designed that way (rather than having security bolted on afterwards), among others. Importantly, the most transformative innovations have come not only from technology. Some of the greatest advances in defense advantage and hyperscale arose from improvements in organization, such as the creation of the first Computer Emergency Response Teams in the 1980s, and governance, such as the development of C-suite cybersecurity experts (e.g., Chief Information Security Officers) in the 1990s. Other successes have come from process innovations, like the “cyber kill chain” and “intelligence-driven operations.” And, better mapping and analysis of the way attackers intrude into systems has led to better strategies to keep them out. Policy actions, such as issuing legal indictments and threatening governmental sanctions, seem to have fostered bilateral norms and reduced the volume of espionage operations, particularly from China. In 2013, the White House set a new policy instructing   Building a Defensible Cyberspace: Report of the NY Cyber Task Force | 5 the US government to tell companies if it detects data breaches in their systems.6 Largely because of this policy (barely 200 words long), notification from law enforcement is now one of the most common ways companies learn of intruders. This public-private cooperation means faster responses, limiting the disruption attackers can cause.7 In each of these cases, the solution (while not necessarily cheap in hours or dollars invested) reaped benefits that significantly outweighed costs. This kind of leverage can make cyberspace more defensible for a company, a sector, a nation, and the world as a whole. Having carefully assessed a variety of innovations, we have concluded that defenders should adopt innovations that have the highest return. This, of course, requires that we assess each innovation for its benefits and costs, an analysis that seems obvious, but is not commonly employed today. The task force also identified several innovations with potentially large impact, such as reaching a consensus between policymakers and technology leaders to build a defensible cyberspace, promoting more secure cloudbased technologies, and improving authentication by finally dispensing with passwords. Certain innovations we assessed were controversial among the members of the task force, such as imposing regulations on network service providers and holding software and hardware makers liable for products with known but unpatched vulnerabilities. These and other approaches might deliver significant leverage, but would certainly be met with fierce resistance and potentially impose significant hurdles to innovation. Some solutions can be implemented easily; others will be more difficult because they create clear winners and losers. All members of the task force agree that the best solutions rely on leverage and are necessary now to avoid far more intrusive ones later. Text Box 1, below, summarizes the steps needed. Below we summarize certain of our key findings regarding steps needed. Taken together, these steps will help build a more defensible cyberspace

### OCOs Bad---2NC

#### NATO cyber-deterrence backfires---triggers conflict with adversaries through miscalc and wrecks alliance unity

Jacobson 21. Jeppe T. Jacobsen is the Cyber Coordinator at the Ministry of Foreign Affairs of Denmark where he coordinates Denmark’s cyber diplomacy. Jacobsen holds a master’s degree in International Politics from School of Oriental and African Studies, University of London, a master’s degree in Political Science from the University of Aarhus, Denmark, and is a Ph.D. candidate at the Danish Institute for International Studies and the Center for War Studies at the University of Southern Denmark; “Cyber offense in NATO: challenges and opportunities Get access Arrow”; May 10, 2021; International Affairs, Volume 97, Issue 3, May 2021, Pages 703–720; <https://academic.oup.com/ia/article-abstract/97/3/703/6205395> //BY

Deterring what? Much of the scholarly debate on NATO is preoccupied with the current strategic adaptation of the alliance and the renewed focus on deterring Russia.48 Only a few contributors to this debate have addressed the addition of offensive cyber capabilities in NATO force structure and response doctrine as an element in work to strengthen the alliance’s deterrence posture.49 Neither in these contributions nor among the former and current NATO employees who have publicly articulated this ambition is it clear what kind of activity the integration of cyber effects in NATO seeks to deter.50 Is it supposed to add to the classical deterrence (through the threat of punishment) of conventional Russian threats to the territorial integrity of eastern Europe? Or to the deterrence of hybrid activities—specifically cyber activities—against allied countries below the threshold of armed conflict? This section addresses each of these possibilities in turn. From Cold War deterrence and back NATO’s founding purpose was to maintain a sufficient military strength to deter aggression and attempts at coercion, to prepare for the eventuality of deterrence failing, and to ensure stability among European powers.51 During the Cold War, the debates over NATO deterrence posture largely centred on the role of nuclear weapons, and specifically whether the United States would retaliate with these weapons in the event of a Soviet conventional attack against allied states.52 In short, NATO deterrence was about credibly extending the US nuclear (as well as conventional force) deterrence to allies to discourage a Soviet military offensive into eastern Europe. While NATO and its member states adapted to the new security environment after the end of the Cold War by scaling down the military investments and presence in eastern Europe and by focusing more on crisis management,53 much of the Cold War deterrence language returned when the Russian–Ukrainian conflict broke out in 2014.54 What needs to be deterred today, much of the literature agrees, is not only a full-scale military invasion but to a larger extent the use and support of pro-Russian militant separatists who are willing to apply insurgency tactics in NATO’s post-Soviet member states.55 As a result, the allies’ military investments have been increasing again,56 a number of initiatives such as the Enhanced Forward Presence in the Baltic States and Poland have been introduced,57 and the discussions—and disagreements—on the nuclear deterrence (of non-nuclear threats) have re-emerged.58 Such responses are often presented as a renewed attempt by NATO to reassert its deterrence and assurance posture by signalling strength, preparedness and willingness to punish ‘bad’ behaviour.59 At first sight, the introduction of CYOC seems to add to these deterrence efforts. NATO added an offensive cyber option to reinforce its ability to impose costs sufficient to dissuade adversaries from acting aggressively. On closer examination, however, it is not self-evident that requesting member states’ delivery of offensive cyber effects in NATO operations constitutes a necessary or even a substantial addition to credibly signalling the ability and willingness to punish an adversary. NATO’s conventional capabilities are clearly already far superior to Russia’s—with or without fully integrated cyber effects. Thus, a deterrence failure, resulting for example in a scenario in one of the Baltic states similar to that which occurred in eastern Ukraine, will not be the result of NATO’s lack of available cyber tools in its military toolbox; rather, if the Russian leadership were to consider it in its interest to pursue such a scenario, it would mean that Russia’s decision-makers did not believe in the credibility of NATO’s article 5 or in NATO’s ability to mobilize its forces. The capacity to integrate cyber effects would do nothing to change that. Furthermore, if the establishment of CYOC is an attempt to signal defensive strength and unity in cyberspace, it remains difficult to imagine that such signaling would dissuade adversaries from trying to penetrate NATO and allied systems. CYOC does not change the fact that NATO is not tasked to govern and secure national IT systems. In an operational setting, states might connect to each other through so-called federated mission networking; 60 but there is no tradition of ceding control of the deployed national networks to NATO during military operations. Hence, CYOC can only realistically seek to become a hub for cyber-threat information-sharing and to support states’ coordination and synchronization of various national responses to these threats. In other words, CYOC is unlikely to become an active defender in cyberspace that causes doubt in the adversary’s evaluation of its own cyber capabilities. This also means that even if CYOC’s coordination and information-sharing efforts manage to contribute to the denial of intrusions into allied systems, an adversary’s military is unlikely to be deterred from trying to hack these systems. In fact, actively articulating that CYOC is supposed to deter (through denial) a perceived adversary such as Russia from hacking NATO and allied operational systems creates an incentive to do just that and thereby show that the alliance is incapable of doing what it says it seeks to do. However, the renewed concern about Russia’s intentions in NATO member states since 2014 is not confined to the need to deter hostile military invasions or paramilitary activity. It also encompasses a range of subversive, non-military activities that have become available and are often considered part of a broader Russian strategy of ‘hybrid warfare’.61 Can CYOC and the integration of cyber effects deter the non-military hybrid activities that have become possible with the new information and communication technologies? Deterring cyber activity below the threshold of collective defence ‘Hybrid’ has become a popular concept when describing the current threat environment. While discussions over the definition, novelty and usefulness of the concept continue, there seems to be agreement that, when used to qualify ‘threat’ or ‘warfare’, ‘hybrid’ refers to the blurring of the distinction between military and civilian, often in relation to the mixture of instruments used to obtain political objectives.62 NATO’s attempt to deter military and paramilitary instruments from being deployed has already been touched upon above. As a primarily military alliance, however, NATO is facing difficulty in addressing the instruments that are used deliberately to stay below the threshold of collective defence. NATO has not been able to deter the perpetration of random ransomware incidents, election interference and targeted propaganda campaigns through hacks and leaks, or industrial cyber espionage and intrusion into critical infrastructures. The alliance’s conventional capabilities are not credible (proportional) responses to such malicious cyber activity. Thus, it has responded only by ‘naming and shaming’, and by expressing encouragement to member states to enhance the resilience of their networks.63 These responses, however, have yet to prove effective in halting the malicious cyber activity conducted below the threshold of collective defence.64 And the introduction of SCEPVA is not likely to change that; the integration of cyber effects is tied to NATO military operations only. While NATO member states are already compelled to maintain a level of cooperation in collective defence (article 3), and to consult together whenever any of them feels that its territorial integrity, political independence or security is threatened (article 4), NATO—with or without integrated cyber effects—is not an alliance designed to deal with non-military threats from a peer competitor. The question then arises: does the lack of capacity to deter non-military hybrid cyber activities suggest that it is time for NATO to renegotiate the scope and substance of its collective defence clause?65 When it comes to cyberspace, the next section expresses scepticism about expanding NATO’s role. It addresses the escalation risk associated with having NATO, an organization that has refocused its attention on a more traditional military threat, become a more active player below the threshold of collective defence. It argues that a more active stance outside military confrontation risks undermining the intelligence norm that currently dominates in cyberspace—a norm whereby state activity in foreign networks is not considered escalatory. Escalation and the dominant intelligence norm The large overlap between intelligence collection and attack in cyberspace makes it difficult to send clear signals to adversaries, in terms of either capabilities or intentions. When a foreign entity is moving around in a network, is it then about to start a military operation? Is the activity part of a reconnaissance mission? Is it political or economic espionage? Is it active defence? The difficulty of answering these questions has created much nervousness among cyber-conflict experts. Ben Buchanan, for example, has shown how defensive hacking or intelligence-gathering in cyberspace is easily misinterpreted as aggressive behaviour.66 Why, then, have we not experienced serious misinterpretation and escalation in cyberspace? One way to explain this is through the existence and dominance of a largely unspoken but widely accepted norm. For decades, the predominant actors in cyberspace have been intelligence agencies; and the norms that characterize interactions between intelligence agencies are not primarily concerned with military concepts such as conflict escalation and deterrence.67 In the world of intelligence agencies, success is not about keeping a distance between oneself and the adversary by signalling one’s intentions and capabilities. It is about being able to outmanoeuvre adversaries in a space of constant contact.68 There are always risks, and the work usually takes place in legal grey zones where a clear distinction between war and peace is not the guiding principle. This is an arena where the opportunity to annoy, cheat and delay opponents is taken when it arises. In short, espionage and counter-espionage do not fit well with the thorough military operational planning that characterizes NATO operations. Intelligence operations, on the other hand, fit perfectly with a dynamic cyberspace where anonymity is easy to achieve and uncertainty a constant condition.69 The states that embrace cyberspace as a domain where the intelligence norm dominates are able to use a broader array of tools to pursue or respond to various foreign political objectives than only those that relate to military operations. In its 2018 ‘vision’, the US Cyber Command built implicitly on the dominant intelligence norm. Here, the objective is to become more agile and act as close to the adversary as possible (‘defend forward’).70 The United States considers ‘constant contact’ and ‘persistent engagement’ as the necessary guiding principles to achieve superiority in cyberspace and to take full advantage of the broader potential for pursuing its political objectives through cyberspace. During the 2018 US midterm elections, for example, the US Cyber Command worked closely with the NSA to disrupt servers operated by the Russian Internet Research Agency aiming to spread fake news and stir up tension in the United States.71 More recently, the US Cyber Command responded with various cyber effects against Iran after the Iranian Revolutionary Guards apparently placed mines on ships in the Strait of Hormuz.72 These practices illustrate that, for the United States, cyber effects provide political options when one does not want to escalate existing tensions into military confrontation. Defensive coordination between allies through CYOC supports such defensive use of cyber effects, increasing the possibility that US Cyber Command will be allowed to ‘defend forward’ and work persistently through allied networks.73 A more cyber-active NATO, however, risks being counterproductive to the ambition to ‘defend forward’ through allied networks. Unintended conflict escalation from ongoing cyber activity is mainly a risk if military analysts—in a strategic environment with heightened attention to military confrontation—ignore the dominant intelligence norm. If that happens, it becomes more likely that ‘persistent engagement’ and active cyber defence will be misinterpreted as military preparation, armament or the initial phase of an attack. If NATO, an organization that has publicly returned to its original raison d’être of deterrence and collective defence, becomes the entity that coordinates cyber effects below the threshold of armed conflict, then the likelihood increases that Russia misinterprets these effects as escalatory and acts accordingly. In other words, a more active NATO in the current strategic environment increases the risk that the existing intelligence norm will be undermined and replaced by a more militarized norm. This does not mean that states that face hostile hybrid activities below the threshold of armed conflict will be left alone. Intelligence cooperation between allied countries does exist, and threat information is occasionally shared. In addition to the current political collaboration facilitated by NATO to improve network security and resilience, the EU is engaging in similar civilian activities, as well as developing and implementing a cyber-diplomatic toolbox to create a common basis for responding to a variety of malicious activities against member states. Further strengthening the political partnership between the EU and NATO is thus the most appropriate way forward to avoid further militarization of cyberspace. Sustaining the intelligence norm as the dominant norm is not without potential problems. Openly embracing the fact that cyberspace is a domain in which intelligence agencies are constrained only by domestic laws, and where takedowns of servers in foreign countries are not necessarily perceived as serious breaches of sovereignty, is likely to lead to an increase in the exploitation of IT vulnerabilities in commercial software used in both enemy and allied networks. For smaller states, this could increase the risk of retaliation by larger adversaries, and it could increase the risk of divisions between allies—divisions that are not aligned with the United States’ political ambition to use cyber coordination in NATO as part of its attempt to ‘defend forward’.74 More exploitation could also ultimately make cyberspace less free, less open and less secure, rendering civilian populations susceptible to cybercrime, surveillance and disruptions of everyday services.75 This is why some states, NGOs and private corporations such as Microsoft continue to promote norms that emphasize restraint on the part of states’ intelligence agencies and militaries in cyberspace, and why other states promote more sovereign control of cyberspace.76 Conclusion This article has pointed to several challenges to the integration of military cyber effects in NATO operations, and has argued that even if the integration is successful, it will not add to the alliance’s deterrence posture. Importantly, the fact that CYOC does not send a strong signal to adversaries such as Russia does not mean that it is a waste of time. Far from it. As both conventional militaries and paramilitary groups are increasingly dependent on civilian networked technologies, the ability of NATO to disrupt, deny, degrade or destroy enemy networks through sovereign cyber effects—even if these amount only to temporary annoyances—will become more relevant in the years to come. This, of course, does not mean that conventional kinetic or electromagnetic capabilities will become redundant. Rather, cyber effects offer a substitute in case the intended target cannot be reached with conventional capabilities, and a supplement that works alongside conventional operations as persistent annoyances of enemy networked devices. The latter, however, demands an agile CYOC that provides member states with broad initial mandates and facilitates quick decision-making and rapid approval when member states stand ready to deliver even minor cyber annoyances. Furthermore, the article has argued that NATO and its CYOC should not seek to coordinate additional offensive cyber efforts to deter hybrid activities below the threshold of armed conflict. If an organization that is perceived by its main adversary primarily as a military organization engages in active cyber-defence measures and persistent cyber engagements outside of military confrontation, then the risk of escalation increases. This is because every potential NATO-initiated cyber activity in foreign networks is likely to be perceived through a military lens and thus to be (mis-)interpreted as an attack in the making. In fact, active cyber-defence measures in foreign networks and use of cyber means below the threshold of armed conflict to pursue political interests internationally are part of our current reality. Intelligence agencies know this to be a fact, and they live by it every day.

#### Formalized US OCO policy triggers rapid-fire prolif of adversary OCOs---that triggers conflict and wrecks cyber norms, turns both advantages

Lin and Smeets 18. Dr. Herb Lin is senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University. Max Smeets is a senior researcher at the Center for Security Studies (CSS) at ETH Zurich, director of the European Cyber Conflict Research Initiative, and author of “No Shortcuts: Why States Struggle to Develop a Military Cyber-Force”, published with Oxford University Press and Hurst in May 2022; “An Outcome-Based Analysis of U.S. Cyber Strategy of Persistence & Defend Forward”; November 28, 2018; Lawfare; <https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward> //BY

One path towards escalation involves adversaries becoming more aggressive and conducting attacks that are highly disruptive to society—in other words, adversary activity leads to a less stable cyberspace. This could be the result of either an adversary’s increased willingness to conduct attacks using existing capacities or increased capacities of the adversary. Indeed, with respect to the latter, the U.S. vision—and associated changed course of action—may encourage other actors to grow their budgets to conduct offensive cyber operations. The proliferation literature on weapons of mass destruction has extensively covered the role of special interests in stimulating demand for weapon development. This makes it a strong possibility that the new U.S. vision can be used by those groups within a given country favoring a growing cyber command to justify and lobby for increased military spending.

A second possibility is that increased U.S. offensive cyber activity that operates below the threshold of armed attack activity reduces the value of cyber norms of behavior that support a more stable cyberspace. Even today, some observers believe that the high level of offensive activity in cyberspace today demonstrates quite forcefully that nations find value in conducting such activity, and that such activity points to the difficulty of establishing a more peaceful cyber norms regime. These observers argue that there is no reason to expect that increasing the U.S. contribution to such activity worldwide will make it easier to establish such a regime. Finally, a third possibility is that increased U.S. offensive cyber activity will complicate diplomatic relations with allies and other nations whose cyber infrastructures are used in support of such activity.

Increased aggressiveness by adversaries could also result from growing incentives to conduct offensive cyber operations of a highly disruptive nature. In this case, heightened aggressiveness might be a symptom of the U.S. strategy actually being effective in making the U.S. more powerful. Consider, for example, the current war against the Islamic State: losing territory and grip in the Middle East, the terrorist organization is said to be keen to recruit followers in Europe and other places in the world to conduct attacks outside of Iraq and Syria. These attempted mass killings are a way to show that the group still needs to be feared and potentially to help recruiting—but they do not change the balance of power in the region. Actors in cyberspace might become more noisy and aggressive purely to increase friction, gain attention and so on —and perhaps also to influence international public opinion in ways that drive the United States toward changing its strategy.

Finally, worst-case outcomes—that is, a United States that is less powerful in cyberspace along with a less stable cyberspace—could stem from a multitude of sources. One possibility is that the United States could overplay its hand in terms of cyber capabilities. The USCYBERCOM is operating in a space in which it has to seize the initiative against a large and ever-growing number of actors. The dangers of fighting on multiple fronts—even for the most capable actors—are well known from conventional warfare. As the number of potential cyber “fronts” is much higher compared to conventional warfare, the risks of overextension have become much higher as well. The Defense Department vision’s explicit focus on Russia and China, following the USCYBERCOM vision’s silence on the issue of priorities, makes us less concerned about this scenario —though it is still a possibility.

#### OCO’s cause escalation with Russia over Ukraine

Healey, 22 (Jason Healey, Healey is a senior research scholar at Columbia University’s School for International and Public Affairs, 3-9-2022, accessed on 6-19-2022, War on the Rocks, "Preventing Cyber Escalation in Ukraine and After - War on the Rocks", [https://warontherocks.com/2022/03/preventing-cyber-escalation-in-ukraine-and-after/)](https://warontherocks.com/2022/03/preventing-cyber-escalation-in-ukraine-and-after/)//Babcii)

Second, Western offensive cyber operations might **spark war.** U.S. cyber espionage and operations against Putin, his cronies, or Russia’s military forces will appear far more ominous to Putin if he believes they are aimed at regime change. Could Putin turn the other cheek if the United States were to electronically raid the cryptocurrency wallets of Russia’s sanctions-avoiding kleptocrats? He might feel the need to escalate his own cyber operations as part of his own version of defending forward. **Escalation could happen on the battlefield as well**. [According to the New York Times](https://www.nytimes.com/2022/03/06/us/politics/us-ukraine-weapons.html), teams from U.S. Cyber Command are “in place to interfere with Russia’s digital attacks and communications.” Other teams are almost certainly collecting digital intelligence on the location and intent of Russian combat forces. The United States is sharing such intelligence with the Ukrainians but [apparently not yet providing any real-time targeting](https://www.nbcnews.com/news/investigations/biden-administration-walks-fine-line-intelligence-sharing-ukraine-rcna18542). That may change soon, as the United States seeks to alleviate intensifying attacks on civilians. And with his KGB-bred paranoia, Putin might already see the presence of U.S. defensive and intelligence teams operating on or against Russian military networks as evidence of direct U.S. involvement in the war. Confirming his apparent belief that Ukraine is just a NATO puppet, this might force a response, either inside or outside of cyberspace. Further, if Western governments have infiltrated Russia’s operational military networks, they may feel pressure to disrupt those networks to prevent civilian massacres. Because cyber capabilities are billed as non-lethal, reversible, and non-escalatory, tub-thumping newspapers may push decision-makers to take shots they might not otherwise: “We can’t create a no-fly zone but [can use cyber capabilities to prevent civilian harm](https://mobile.twitter.com/Jason_Healey/status/1498416936891387912).” Some [well-meaning national leaders](https://twitter.com/JacquiHeinrich/status/1500961829509636099) may succumb to this pressure, **potentially causing a larger conflict.** Future Risks Even if Russia and the West avoid direct conflict this time, they might not be so lucky the next. As relations worsen, future disruption of critical Western infrastructure by Russian intelligence, such as the [NotPetya](https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html) and [Olympic Destroyer](https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html) attacks, are less likely to be viewed as mere crimes. Repeated crises bordering on war may further erode the tacit agreements and relative restraint of quieter times. After repeated iterations of intensifying cyber operations, both Russia and the West may feel their backs to the wall with few options left other than military force when the next crisis — physical or cyber — emerges. Under extreme conditions, some of the same characteristics that lead cyber capabilities to be a pressure release might have the opposite effect, a mechanism that Bob Jervis and I have described as the [Escalation Inversion](https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/). If Putin believes a direct conflict with NATO is likely and expects its adversaries to [take measures to reduce vulnerabilities](https://www.cnas.org/publications/reports/a-new-era-in-u-s-russian-strategic-stability), he could conclude that the best possibility for success is to launch a massive preemptive cyber attack. Since the U.S. military may seem otherwise unbeatable, this [may lead](https://www.brookings.edu/book/surprise-attack/) Russia to “compensate with audacity in order to redress the balance.” The more the United States **brags about its overwhelming offensive cyber advantage**, but frets over weak defenses, the more any adversary might feel the need to [target the United States as early and as hard as possible](https://www.lawfareblog.com/getting-drop-cyberspace).

**An offensive cyber posture fails and causes escalation.**

**Valeriano & Jensen 19** – Senior Fellow at the Cato Institute, Bren Chair of Military Innovation at the Marine Corps University, serves as Senior Advisor for the Cyber Solarium Commission; Associate professor at the Marine Corps University and a scholar‐​in‐​residence at American University’s School of International Service

Brandon Valeriano, Benjamin Jensen, “The Myth of the Cyber Offense: The Case for Restraint,” The CATO Institute, Policy Analysis No. 862, January 2019, https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint

The Myth of the Offense

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.

Cyber Command’s 2018 persistent-action strategy aims to “expose adversaries’ weaknesses, learn their intentions and capabilities, and counter attacks close to their origins.”44 Put in simple terms, the best defense is a good offense: get on adversary networks and stop cyber operations targeting the United States before they occur. Under this strategy, offensive cyber operations will also be **preemptive** in that they are designed to “contest dangerous adversary activity before it impairs [U.S.] national power.”45 To use another sports metaphor, come out swinging. Go on the offense first and establish escalation dominance (that is, demonstrating such superior capabilities over the target state that it can’t afford to escalate in response).46

According to Cyber Command, preemptive strikes will “impose . . . strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks.”47 Whether through punishment, risk, or denial strategies, offensive actions theoretically alter the target’s behavior by increasing the expected costs of targeting U.S. interests.48 Offensive action, according to this thinking, deters future aggression by signaling resolve and establishing escalation dominance. Yet, there are well-established reasons to doubt that offensive options produce the intended results in cyberspace.

Defense and Deception

The rationale behind persistent action—that the best defense is a good offense—is **deeply flawed**. In fact, most military and strategic theory holds that the defense is the **superior posture**.49 For example, Sun Tzu describes controlling an adversary to make their actions more predictable, and hence easy to undermine, by baiting them to attack strong points.50 The stronger form of war is a deception-driven defense: confusing an attacker so that they waste resources attacking strong points that appear weak. This parallels cybersecurity scholars Erik Gartzke and Jon Lindsay’s claim that cyberspace is **not offense dominant**, but **deception dominant**.51 Rather than persistent action and preemptive strikes on adversary networks, the United States needs **persistent deception** and **defensive counterstrikes** optimized to **undermine adversary planning** and **capabilities**.

Fear and the Security Dilemma

New policy options proposed by Cyber Command and the Trump administration **risk exacerbating fear** in other countries and creating a **self-reinforcing spiral** of **tit-for-tat escalations** that ri**sk war** even though each actor feels he is acting defensively—or, as it is called in the scholarly literature, a security dilemma.52 As shown above, most cyber operations to date have not resulted in escalation. The cyber domain has been a world of spies collecting valuable information and engaging in limited disruptions that substitute for, as well as complement, more conventional options. Shifting to a policy of **preemptive offensive cyber warfare** risks **provoking fear** and **overreaction** in other states and possibly **producing conflict spirals**. Even limited-objective cyber offensive action defined as “defending forward” can be misinterpreted and lead to inadvertent escalation.53 As the historian Cathal Nolan puts it, “intrusions into a state’s strategically important networks pose serious risks and are therefore inherently threatening.”54

More worryingly, with a more offensive posture, it will be **increasingly difficult** for states to differentiate between cyber espionage and more damaging degradation operations.55 What the United States calls defending forward, China and Russia will call preemptive strikes. Worse still, this posture will likely lead great powers to assume all network intrusions, including espionage, are preparing the environment for follow-on offensive strikes. According to cybersecurity scholar Ben Buchanan, “in the [aggressor] state’s own view, such moves are clearly defensive, merely ensuring that its military will have the strength and flexibility to meet whatever comes its way. Yet potential adversaries are unlikely to share this perspective.”56 The new strategy risks producing a “**forever cyber war**” prone to **inadvertent escalation** because it implies all cyber operations should be interpreted as escalatory by adversaries.57

The Myth of Decisive Cyber Victory

There is a tendency in the military profession, at least in the United States and Europe, to uphold the concept of decisive battle as central to the Western way of war.58 Often, disruptive technologies—from strategic bombers in the mid-20th century to cyber operations in the 21st century—are seen as providing decisive offensive advantages in crises. In the interwar period between the world wars, airpower enthusiasts argued that bombers would reliably reach their targets, forcing political leaders to end hostilities or face the prospect of destroyed cities and economic collapse.59

Yet the search for decisive battle is often an **elusive**, if not **dangerous**, temptation for military planners and policymakers. In a comparative historical treatment of major 19th- and 20th-century battles, Nolan argues that “often, war results in something clouded, neither triumph nor defeat. It is an arena of **grey outcomes**, partial and ambiguous resolution of disputes and causes that led to the choice of force as an instrument of policy in the first place.”60 Decisive victories in any one battle are rare. Adversaries can refuse to fight.61 They can even signal resolve through demonstrating their ability to endure pain.

**Offensive operations are escalatory and fail.**

**Valeriano & Jensen 19** – Senior Fellow at the Cato Institute, Bren Chair of Military Innovation at the Marine Corps University, serves as Senior Advisor for the Cyber Solarium Commission; Associate professor at the Marine Corps University and a scholar‐​in‐​residence at American University’s School of International Service

Brandon Valeriano, Benjamin Jensen, “The Myth of the Cyber Offense: The Case for Restraint,” The CATO Institute, Policy Analysis No. 862, January 2019, https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint

New policy options proposed by Cyber Command and the Trump administration **risk exacerbating fear** in other countries and creating a **self-reinforcing spiral** of **tit-for-tat escalations** that **risk war** even though each actor feels he is acting defensively—or, as it is called in the scholarly literature, a security dilemma.52 As shown above, most cyber operations to date have not resulted in escalation. The cyber domain has been a world of spies collecting valuable information and engaging in limited disruptions that substitute for, as well as complement, more conventional options. Shifting to a policy of **preemptive offensive cyber warfare** risks **provoking fear** and **overreaction** in other states and possibly **producing conflict spirals**. Even limited-objective cyber offensive action defined as “defending forward” can be misinterpreted and lead to inadvertent escalation.53 As the historian Cathal Nolan puts it, “intrusions into a state’s strategically important networks pose serious risks and are therefore inherently threatening.”54

More worryingly, with a more offensive posture, it will be **increasingly difficult** for states to differentiate between cyber espionage and more damaging degradation operations.55 What the United States calls defending forward, China and Russia will call preemptive strikes. Worse still, this posture will likely lead great powers to assume all network intrusions, including espionage, are preparing the environment for follow-on offensive strikes. According to cybersecurity scholar Ben Buchanan, “in the [aggressor] state’s own view, such moves are clearly defensive, merely ensuring that its military will have the strength and flexibility to meet whatever comes its way. Yet potential adversaries are unlikely to share this perspective.”56 The new strategy risks producing a “**forever cyber war**” prone to **inadvertent escalation** because it implies all cyber operations should be interpreted as escalatory by adversaries.57

The Myth of Decisive Cyber Victory

There is a tendency in the military profession, at least in the United States and Europe, to uphold the concept of decisive battle as central to the Western way of war.58 Often, disruptive technologies—from strategic bombers in the mid-20th century to cyber operations in the 21st century—are seen as providing decisive offensive advantages in crises. In the interwar period between the world wars, airpower enthusiasts argued that bombers would reliably reach their targets, forcing political leaders to end hostilities or face the prospect of destroyed cities and economic collapse.59

Yet the search for decisive battle is often an **elusive**, if not **dangerous**, temptation for military planners and policymakers. In a comparative historical treatment of major 19th- and 20th-century battles, Nolan argues that “often, war results in something clouded, neither triumph nor defeat. It is an arena of **grey outcomes**, partial and ambiguous resolution of disputes and causes that led to the choice of force as an instrument of policy in the first place.”60 Decisive victories in any one battle are rare. Adversaries can refuse to fight.61 They can even signal resolve through demonstrating their ability to endure pain.

Planning and Assessment Pathologies

The new policy framework for offensive cyber operations **risks compounding common pathologies** associated with strategic assessments and planning. 62 **Removing interagency checks** increases the risks that an operation will **backfire** on the attacker or **compromise ongoing operations**.

**Misperception** is **pervasive** in insulated decisionmaking processes for several reasons.63 First, small groups unchecked by bureaucracy tend to **produce narrow plans** prone to escalation during crises.64 Second, leaders often give guidance to planners during crises that reflects their political bias or personality traits rather than a rational assessment of threats and options.65 Third, offensive bias in planning may have little to do with the actual threat and more to do with a **cult of the offensive** and the desire of officers to ensure their autonomy and resources.66 Removing interagency checks therefore risks compounding fundamental attribution errors and other implicit biases. Cyber operations are too important to be left to the generals at Cyber Command alone.

### Zero-Days Bad---1NC

#### Sharing zero-days with allies causes use-it-or-lose-it pressure---accelerates conflict escalation

Smeets ’22 [Max; May 31; Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich, co-founder and Director of the European Cyber Conflict Research Initiative (ECCRI.eu), an organization promoting the interdisciplinary study of cyber conflict and statecraft in Europe and beyond, also an Affiliate at Stanford University Center for International Security and Cooperation; CFR, “The Risks of Managing a Purchased Cyber Arsenal,” <https://www.cfr.org/blog/risks-managing-purchased-cyber-arsenal>]

We know that some government agencies are regular buyers on the market for zero-days, previously unknown vulnerabilities which vendors have not had time to prepare a patch for. Zero-days, and their use by threat actors, are a common topic, but how zero-day purchases complicate arsenal management decisions is rarely discussed. Not least, buying zero-day exploits, rather than developing them internally, increases the chances of early discovery due to potential non-exclusive sales (even if the exploit was supposed to be sold to only one buyer) which subsequently incentivizes the imprudent use of the exploits.

Types of exploits and their life span

Exploits come in three main flavors: zero-day exploits (those that use a vulnerability previously unknown to the vendor), unpatched N-day exploits (those that use a vulnerability in software or hardware that is known to the vendor but does not have a patch in place to fix the flaw), and patched N-day exploits (those that use a vulnerability in software or hardware that is known to the vendor and has a patch in place to fix the flaw).

Zero-days are the most powerful form of exploit, because companies and governments have no warning that a vulnerability may exist or any plans to patch the vulnerability. Whilst this makes zero-days particularly useful for penetrating computers and networks, note that mature cyber commands and intelligence organizations still primarily use known exploits for their operations.

The average life span of a zero-day exploit–i.e., before the exploit gets discovered–is long: seven years, according to a study from RAND Corporation. However, there is major variation; on average, about 25 percent of all exploits do not survive for more than one and a half years, but another 25 percent will survive more than nine and a half years.

The risk of co-discovery

The likelihood that two (or more) independent parties will discover a vulnerability is known as the vulnerability collision rate. A RAND study found that, for a given stockpile of zero-day vulnerabilities, after a year, almost 6 percent have been publicly discovered and disclosed by another entity.

Normally, this risk of co-discovery drives semi-calculated decisions about exploit use. A threat actor may, for example, decide to only go after the most valuable victims or keep exploits for some unusual circumstances to avoid discovery. In fact, we know from the Snowden leaks that the National Security Agency (NSA) developed “FOXACID”, a tool to help optimize exploit use. FOXACID is an “exploit orchestrator,” a tool that automatically matches targeted computer systems with different types of exploits. As Bruce Schneier, a computer expert, notes, FOXACID “is designed to be modular, with flexibility that allows [NSA’s Office of Tailored Access Operations (TAO), now Computer Network Operations,] to swap and replace exploits if they are discovered, and only run certain exploits against certain types of targets. The most valuable exploits are saved for the most important targets. Low-value exploits are run against technically sophisticated targets where the chance of detection is high.”

The risk of co-sales

However, when an intelligence agency or cyber command buys exploits, rather than develops them internally, it further complicates the decision-making process around their usage. A buyer, like the NSA, can either purchase an ‘exclusive’ or ‘non-exclusive’ exploit. Exclusive purchases mean that the exploit is only sold to one client and is thus pricier. Vice versa, non-exclusive exploits can be sold to multiple clients and are cheaper.

In the case of non-exclusive sales, the client has thus to take into consideration the chances that the exploit is sold to one or more other clients, and whether others who buy the exploit will use it discreetly.

A tragedy of the commons

A popular concept in economics is the “tragedy of the commons,” a situation in which individuals who have access to an open-access or unregulated resource, such as ocean fish stock, act independently according to their own self-interest and, contrary to the benefit of all users, cause depletion of the resource through their uncoordinated actions.

A non-exclusive exploit is not an open-access resource unhampered by shared social structures. But sales of exploits to independent actors–i.e., not knowing who else owns the exploit–does create similar incentives to use the resource imprudently. It incentivizes “use it or lose it” behavior, the belief that an exploit should be used quickly before it becomes ineffective.

This additional risk is also nonzero in the case of exclusive sales; there is no certainty that the broker does not sell it on to other actors, or that the developer does not shop it around to multiple brokers. These latter risks, however, are minimized in the case of trusted channels that carry repeated transactions between developer and broker, or broker and end user buyer.

Buying exploits can be convenient. It may lead to targeting options that are not otherwise available. Yet, it also further complicates the decision-making of government agencies that use these purchased capabilities and introduces additional risk into the already fraught world of cybersecurity.

## Case Defense

### AT: Escalation

#### Escalation is wrong---most comprehensive studies prove

Borghard and Lonergan 19. Erica D. Borghard is an Adjunct Research Scholar in the Saltzman Institute of War and Peace Studies and an Adjunct Associate Professor in the Department of Political Science. She is also a senior fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace. Shawn W. Lonergan is a Senior Advisor to the U.S. Cyberspace Solarium Commission. Shawn holds a Ph.D. in Political Science from Columbia University. Shawn is also a graduate of the United States Military Academy at West Point, where, from 2014-2017, he served as an Assistant Professor in the Academy’s Department of Social Sciences and Chief Research Scientist in the Army Cyber Institute.; “Cyber Operations as Imperfect Tools of Escalation”; Fall 2019; Strategic Studies Quarterly , Vol. 13, No. 3 (FALL 2019), pp. 122-145; <https://www.jstor.org/stable/pdf/26760131.pdf?refreqid=excelsior%3Aa99f8dadc6cb38b533342229ac7a6605&ab_segments=&origin=&acceptTC=1> //BY

There is a widespread view among practitioners and scholars that cyberspace is defined by an inherent potential for dangerous escalation dynamics between rivals.1 On the practitioner side, for example, senior US intelligence and military leaders expressed concerns about first-strike incentives leading to escalation in a 2017 joint statement to Congress, testifying that “adversaries equipped with [offensive cyber capabilities] could be prone to preemptive attack and rapid escalation in a future crisis, because both sides would have an incentive to strike first.”2 On the academic side, there is a palpable fear that cyberspace is an environment in which offense has advantages over defense and that this—coupled with factors such as problems of attribution, poor command and control, and the absence of meaningful thresholds or red lines—generates real risks of inadvertent escalation.3 Concerns about escalation grew even more passionate in the wake of the US Department of Defense’s release of its 2018 Cyber Strategy document, which articulates an operational concept of “defending forward” in which the DOD “disrupt[s] or halt[s] malicious cyber activity at its source.”4 However, there are important empirical reasons to suspect that the risks of cyber escalation may be exaggerated. Specifically, if cyberspace is in fact an environment that (perhaps even more so than others) generates severe escalation risks, why has cyber escalation not yet occurred? Most interactions between cyber rivals have been characterized by limited volleys that have not escalated beyond nuisance levels and have been largely contained below the use-of-force threshold.5 For example, in a survey of cyber incidents and responses between 2000 and 2014, Brandon Valeriano et al. find that “rivals tend to respond only to lower-level [cyber] incidents and the response tends to check the intrusion as opposed to seek escalation dominance. The majority of cyber escalation episodes are at a low severity threshold and are non-escalatory. These incidents are usually ‘tit-for-tat’ type responses within one step of the original incident.”6 Even in the two rare examples in which states employed kinetic force in response to adversary cyber operations—the US counter-ISIL drone campaign in 2015 and Israel’s airstrike against Hamas cyber operatives in 2019—the use of force was circumscribed and did not escalate the overall conflict (not to mention that force was used against nonstate adversaries with limited potential to meaningfully escalate in response to US or Israeli force).7 We posit that cyber escalation has not occurred because cyber operations are poor tools of escalation. In particular, we argue that this stems from key characteristics of offensive cyber capabilities that limit escalation through four mechanisms. First, retaliatory offensive cyber operations may not exist at the desired time of employment. Second, even under conditions where they may exist, their effects are uncertain and often relatively limited. Third, several attributes of offensive cyber operations generate important tradeoffs for decision-makers that may make them hesitant to employ capabilities in some circumstances. Finally, the alternative of cross-domain escalation—responding to a cyber incident with noncyber, kinetic instruments—is unlikely to be chosen except under rare circumstances, given the limited cost-generation potential of offensive cyber operations. In this article, we define cyber escalation and then explore the implications of the technical features and requirements for offensive cyber operations. We also consider potential alternative or critical responses to each of these logics. Finally, we evaluate the implications for US policy making.

#### No escalation and cyber deterrence is fake

Rovner 19. Joshua Rovner is the John Goodwin Tower Professor of International Politics and National Security at Southern Methodist University, where he also serves as Director of Studies at the Tower Center for Political Studies; “CYBER WAR AS AN INTELLIGENCE CONTEST”; September 16, 2019; War on the Rocks; <https://warontherocks.com/2019/09/cyber-war-as-an-intelligence-contest/> //BY

The cyberspace competition is an intelligence contest in a technologically novel domain. It is a struggle to protect information, while corrupting and stealing information from rivals. Because it is not a test of overt military power, traditional strategic theories about force and war may not be our best guide.

Deterrence is mostly irrelevant in an intelligence contest. No combination of threats and promises will stop a rival intelligence service from collecting information. Nor is it easy to imagine what kind of signals would be strong enough to stop adversaries from influence activities such as those of Russia during the [2016 election](https://warontherocks.com/2018/02/obama-stopped-election-hack/) in the United States. Covert action is inherently hard to deter if the responsible party remains hidden. And in other cases, states might tacitly tolerate one another’s covert campaigns as a [safer substitute](https://press.princeton.edu/titles/13238.html) for war. Similarly, the coercive value of offensive cyber operations is likely to be modest at best. There is not much evidence that non-kinetic threats are enough to change anyone’s behavior. [Recent](https://warontherocks.com/2017/08/are-cyber-weapons-too-dangerous-to-use/) [research](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3104014) suggests that the victims are surprisingly tolerant of cyber operations. Strategy is fundamentally about coercion, but cyberspace operations carry little coercive value.

There are some exceptions. It is possible to deter significant cyberspace operations against critical infrastructure, for instance, because such operations require a great deal of time, money, and organization. They would invite a ferocious response, making deterrent threats inherently credible. The language and logic of strategy is useful here.

But in most cases the logic of intelligence is more appropriate. It helps to explain why the balance of capabilities is hard to assess. Long-term intelligence contests are not easy to measure, not least because the contestants work in secret. The relative position of rival intelligence services does not lend itself to quantitative measures. Who is “winning” an intelligence contest at any given moment is rarely clear.

To understand why, imagine having unfettered access to all the intelligence collected by two great power rivals. In this idealized setting, it might be possible to judge which side had collected the most. It might also be possible to determine which side had penetrated more difficult targets. But even here it would still difficult to judge winners and losers, because possessing information is not the same as understanding it. Intelligence services struggle to interpret data, and the more they collect, the more they face the challenge of separating meaningful information from background noise. It is also difficult to put technical knowledge of adversary capabilities to use. It is one thing to steal intellectual property, for instance, and quite another to reverse engineer it. Finally, comparing the volume of intelligence says nothing about the quality of intelligence-policy relations. Intelligence services may perform admirably and still be ignored.

Looking through the intelligence lens puts the cyberspace competition in perspective, but it requires a willingness to live with ambiguity. Signs that one side seems to be winning may be misleading. Breathless headlines about the latest cyber penetration may exaggerate the extent to which one intelligence service is racing ahead, or whether it is able to translate successful cyberspace espionage into meaningful policy advantage. Viewing the competition as an intelligence contest puts alarming headlines about “[cyber](https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/) [war](https://www.rollcall.com/news/u-s-is-woefully-unprepared-for-cyber-warfare)” into context.

### AT: NC3

#### Adversaries lack motive and capability to hack NC3 AND the US can easily counter attacks

Borghard and Lonergan 19. Erica D. Borghard is an Adjunct Research Scholar in the Saltzman Institute of War and Peace Studies and an Adjunct Associate Professor in the Department of Political Science. She is also a senior fellow in the Technology and International Affairs Program at the Carnegie Endowment for International Peace. Shawn W. Lonergan is a Senior Advisor to the U.S. Cyberspace Solarium Commission. Shawn holds a Ph.D. in Political Science from Columbia University. Shawn is also a graduate of the United States Military Academy at West Point, where, from 2014-2017, he served as an Assistant Professor in the Academy’s Department of Social Sciences and Chief Research Scientist in the Army Cyber Institute.; “Cyber Operations as Imperfect Tools of Escalation”; Fall 2019; Strategic Studies Quarterly , Vol. 13, No. 3 (FALL 2019), pp. 122-145; <https://www.jstor.org/stable/pdf/26760131.pdf?refreqid=excelsior%3Aa99f8dadc6cb38b533342229ac7a6605&ab_segments=&origin=&acceptTC=1> //BY

Key features of cyber operations—the role of access, nonuniversal lethality of offensive cyber capabilities, and the temporal nature of access and capability development and maintenance—may dramatically circumscribe the escalatory options available to states through cyber means during a time of crisis. First, escalatory cyber response options may simply not be available to a state because it lacks access to an appropriate set of targets against which to deliver an escalatory response. This is because offensive cyber operations deliver effects against targets through exploiting a vulnerability to gain access (through an attack vector) to a target’s network or system and deliver a payload that is activated by communicating back with a host or triggered by a command order written into the code.13 Absent the right access to deploy a capability, the latter might as well not exist.14 While critical to the success of offensive operations, the initial penetration of a target network or system can be resource intensive and net unpredictable results, which is why the employment of cyber capabilities that rely on access to a targeted network require prior planning and resource allocation Indeed, according to Chris Inglis, the planning staff at US Cyber Command during the 2009–10 period assessed that “the first 90 percent of cyber reconnaissance (i.e., ISR), cyber defense, and cyberattack consisted of the common work of finding and fixing a target of interest in cyberspace.”15 Therefore, rather than occurring at lightning speed, cyber operations have crucial aspects that take time and significant resource investments, even if at the tactical level a line of code can indeed be executed at “network speed.”16 Considering means of access and types of targets reveal the various aspects of gaining access that limit potential cyber escalatory responses at a given time. Table 2, Mainstream means of gaining access, depicts various common access methods and evaluates them along a spectrum of cost, risk, and reliability.17 The broadest distinction between means of access is remote (e.g., using the Internet) versus close (e.g., gaining access through a human agent or supply chain interdiction). Most of the low-cost and low-risk means of gaining access to a target (such as through various social engineering mechanisms) are not readily applicable against more hardened (and therefore more strategically valuable) targets, such as the air-gapped networks common in critical infrastructure systems and some military and defense systems. Conversely, the most reliable type of access, physical access through a human intermediary on the ground, is also the riskiest and costliest. The nature of the targeted network or system also shapes access requirements and consequent level of difficulty. For instance, gaining access to operational technology (OT) is typically more difficult than to information technology (IT), although this may be changing as IT and OT systems converge.18 OT networks tend to be closed (they do not touch the global Internet) and run unique protocols used to control highly specific processes and systems.19 Typically, these characteristics also mean that these networks require specific knowledge because the programs they run are customized to those systems and the networking protocols they employ may not be widely proliferated. Additionally, the simple fact of “gaining access” to a target network does not guarantee that an attacker has gained access at the requisite network layer from which to launch an offensive operation.20 Thus, most access operations are followed by operations that enable persistence through access escalation prior to the employment of any cyber weapon. Finally, gaining access to a target via a hardware implant— the actual physical components of a computer (e.g., motherboard, USB and other flash memory devices, routers, etc.)—is appreciably costlier and more difficult than gaining access to software (all of the digital programs on a computer, from the operating system to applications such as Microsoft Word).

\*TABLE OMITTED\*

21 Software vulnerabilities are relatively easier to detect and to patch, and manufacturers routinely disseminate information about known vulnerabilities and remediation protocols.22 Second, in addition to being dependent on access, offensive cyber capabilities lack universal effectiveness. While nuclear or conventional munitions are target agnostic—in most cases, the same munition can be used to target an aircraft hangar, a massed enemy formation, a munitions factory, or a hospital—some cyber weapons must be tailored to a specific target set or type.23 As Martin Libicki notes, “A piece of malware that brings one system down may have absolutely no effect on another. The difference between the two may be as simple as which patch version of a piece of software each system runs.”24 The 2017 WannaCry ransomware attack that wreaked billions of dollars in damage and was attributed to North Korea’s Lazarus Group, for instance, targeted hundreds of thousands of computers around the world across a range of industries that were running an older version of Windows.25 The widespread damage belies the highly specific and targeted nature of the malware—almost all of the affected systems were running a version of Windows 7; the same strain of malware had no effect on computers running more up-to-date operating systems. Moreover, asset owners of targets of strategic significance—such as critical infrastructure—typically employ highly customized software and specific hardware with tailored configurations that are unique to those systems and usually only intimately understood by the original developers and manufacturers. It has been reported, for example, that the malware employed in the Stuxnet cyberattacks against the Iranian nuclear program was tailored to target the specific model of Siemens programmable logic controllers (PLC) used at the Natanz enrichment facility.26 Indeed, while Stuxnet was discovered in computers around the world, it delivered destructive effects only against the centrifuges in Natanz.27 The non-substitutability of entire classes of offensive capabilities by definition increases the cost of developing an arsenal of offensive cyber capabilities.28 Therefore, the time and resource requirements to gain access and develop specific offensive capabilities may render important escalatory response options infeasible or impractical at the desired time. Operational planning and execution must consider that a given capability may not be usable or even exist at a chosen time of employment.29 As the above discussion illustrates, many of the target sets that would represent strategic (and therefore escalatory) targets, such as a state’s critical infrastructure or nuclear command and control, demand extensive planning, pre-positioning, and capability development in advance of employing offensive capabilities. Therefore, the timing of a crisis plays a crucial role in decisions about cyber escalation responses. Specifically, the time required to develop access to hold strategic targets at risk means that, even if a state seeks to escalate against an adversary using cyber means, it may find itself limited by the accesses and capabilities it possesses at the moment a crisis occurs. Cyber response options may be limited to less decisive or more vulnerable target sets, rather than those that are more strategically significant. Third, these limitations become even more salient when we consider how strategic interactions are likely to play out over time during repeated crisis interactions. Because the virtual domain is changeable in a way that the physical world is not, actions taken by defenders in the context of a crisis can radically and unpredictably alter an attacker’s ability to deliver and sustain effects against a target over time.30 Access and capabilities are neither guaranteed nor indefinite—they have a shelf life.31 Footholds into a target’s network that were time intensive to develop can unexpectedly disappear as vulnerabilities in a network are patched. Exploits may have a short shelf life as revealing information about them enables targets to identify indicators of compromise (IOCs) and use these to prevent further damage from specific malware strains or quarantine malicious traffic using known malware signatures. An example of the latter is the US Cyber Command initiative, beginning in 2018, to share information about adversary malware by uploading samples to VirusTotal.32 Therefore, a target can “transition from vulnerability (to a particular attack) to invulnerability in, literally, minutes.”33 Third-party disclosure about software vulnerabilities by governments or private actors can also unintentionally precipitate the loss of access as exposure about vulnerability information enables network defenders to take measures to remedy them.34 For instance, the disclosures that began in 2016 by the group Shadow Brokers of purportedly pilfered US National Security Agency exploits and zero days ostensibly put US government accesses at risk.35 Put simply, a vulnerability upon which an access relies may in theory be only one update or disclosure away from being patched. Thus, in the context of an ongoing crisis interaction between an attacker and defender, the former’s operational tempo is likely to be interrupted by the latter’s behavior, forcing the attacker to devote additional time to find or acquire new vulnerabilities and exploits in the midst of an offensive operation or campaign. As Inglis notes, to succeed in an offensive cyber campaign that unfolds over time, attackers must be able to sustain “the efficacy of tools under varying conditions caused by the defender’s response and the natural variability and dynamism of cyberspace.”36 The ability to build or acquire new accesses and capabilities “in real time” during a crisis is highly limited.37 Indeed, General Paul Nakasone remarked in a January 2019 interview on the radical difference in shelf life between conventional and cyber capabilities: Compare the air and cyberspace domains. Weapons like JDAMs [ Joint Direct Attack Munitions] are an important armament for air operations. How long are those JDAMs good for? Perhaps 5, 10, or 15 years, sometimes longer given the adversary. When we buy a capability or tool for cyberspace . . . we rarely get a prolonged use we can measure in years. Our capabilities rarely last 6 months, let alone 6 years. This is a big difference in two important domains of future conflict.38 Therefore, as a 2013 Defense Science Board report notes, “offensive cyber will always be a fragile capability” when pitted against network defenders who are “continuously improving network defensive tools and techniques.”39

### AT: Prolif

#### No prolif impact

John Mueller 16, Woody Hayes Senior Research Scientist, Mershon Center for International Security Studies; Adjunct Professor, Department of Political Science, Ohio State University, 6/5/16, “Embracing Threatlessness: US Military Spending, Newt Gingrich, and the Costa Rica Option,” <http://politicalscience.osu.edu/faculty/jmueller/CNArestraintCato16.pdf>

For decades there has been almost wall-to-wall alarm about the dangers supposedly inherent in nuclear proliferation.

However, the proliferation of nuclear weapons has been far slower than has been commonly predicted over the decades primarily because the weapons do not generally convey much advantage to their possessor.

And, more importantly, the effect of the proliferation that has taken place has been substantially benign: those who have acquired the weapons have “used” them simply to stoke their egos or to deter real or imagined threats.67 The holds even for the proliferation of the weapons to large, important countries run by unchallenged monsters who at the time they acquired the bombs were certifiably deranged: Josef Stalin who in 1949 was planning to change the climate of the Soviet Union by planting a lot of trees, and Mao Zedong who in 1964 had just carried out a bizarre social experiment that had resulted in artificial famine in which tens of millions of Chinese perished.68

Despite this experience, an aversion to nuclear proliferation continues to impel alarmed concern, and it was a chief motivator of the Iraq War which essentially was a militarized antiproliferation effort. The war proved to be a necessary cause of the deaths of more people than were inflicted at Hiroshima and Nagasaki combined.69

The subsequent and consequent Iraq syndrome strongly suggests there will be little incentive to apply military force to prevent, or to deal with, further putative proliferation. Thus, despite nearly continuous concern—even at times hysteria—about nuclear developments in North Korea and Iran, proposals to use military force (particularly boots on the ground) to deal with these developments have been persistently undercut. The invasion of Iraq presumably did prevent that country from going nuclear—assuming it ever would have been able to put together the effort.70 However, it scarcely seems likely that there will be much sympathy for repeating that disastrous experience. Thus, maintaining huge forces-in-being to deal with the proliferation problem scarcely seems sensible, even though almost everybody still considers proliferation to be major security concern. What seems to be required in these cases, as generally with the devils du jour of the Cold War era, is judicious, watchful, and wary patience.

#### No spread AND no impact

Jonas Schneider 20. Senior researcher at the Center for Security Studies, held post-​doctoral fellowships at the German Institute for International and Security Affairs (SWP) in Berlin and at the CSS and worked as a research associate at the Institute for Security Policy at the University of Kiel, holds a PhD in Political Science from the University of Kiel. 2020. “Chapter 26 Nuclear Proliferation and International Security.” Understanding Global Politics: Actors and Themes in International Affairs, edited by Klaus Larres and Ruth Wittlinger, Routledge, pp. 409–425.

Other analysts have sounded a much less alarmist tone, however. Some scholars even suggested that an Iranian bomb held great potential for stabilising an unbalanced and volatile Middle East (Waltz, 2012). Closer to the mainstream of Western strategic discourse, various experts have argued that despite the risks of proliferation, nuclear weapons, and the deterrent they provide should get (more) credit for contributing, in combination with other factors, to what has been labelled ‘the Long Peace’ among the great powers since 1945 (Gaddis, 1999, p. 268–271; Gavin, 2012a, p. 164; Acton 2010, pp. 16–17). Still others have contended that because nuclear proliferation is such a rare phenomenon, and since robust nonproliferation measures tend to be disruptive, the net destabilising effect of new nuclear countries is quite small and, therefore, manageable (Mueller 2010, pp. 95–99; Hymans 2013, pp. 293–296). The question of whether nuclear proliferation has stabilising or destabilising effects is not just fascinating for scholars of the nuclear age, but also highly consequential for practical policy issues. For in order to debate the merits of particular policy choices – such as preventive military strikes against nuclear facilities, grand bargains with potential proliferators or complete nuclear disarmament – we need to understand first how the spread of nuclear weapons impacts regional and global security. The chapter proceeds in three steps. The first section provides the foundation for the other parts by summarising what we know about empirical patterns of proliferation and the utility of nuclear weapons for statecraft. The second section then engages the literature on the consequences of proliferation, focusing in particular on how proliferation has influenced international stability. The final section explores whether some states have been more affected than others, and what measures these states have taken to prevent proliferation, or at least mitigate its negative consequences. Patterns of nuclear proliferation and the utility of nuclear weapons Nuclear proliferation is commonly defined as the spread of nuclear weapons to states that did not previously have them. Within a broader conceptual framework that is rarely used by scholars, yet popular in the arms control community, this diffusion of nuclear weapons to additional states is labelled horizontal proliferation. It is conceptually accompanied by the notion of vertical proliferation, which refers to qualitative improvements and increases in the number of nuclear weapons in the stockpiles of existing nuclear weapon states. In accordance with the typical usage of the term in the scholarly debate, this chapter focuses only on how the horizontal proliferation of nuclear weapons affects international stability. One important empirical pattern that has shaped how nuclear proliferation is understood concerns the way in which nuclear weapons have spread. The word ‘spread’ appears to suggest that the established nuclear powers have provided other interested nations with (at least a few) operational nuclear warheads. Yet such transfers have never been undertaken. Certainly, states that sought nuclear weapons have often received significant assistance from other nations (Schofield, 2014; Fuhrmann, 2012), sometimes in the form of highly sensitive technologies (Kroenig, 2010). Nonetheless, since all these transfers remained well below the weapons threshold, nations seeking nuclear weapons always had to build them indigenously. Hence, in reality, the spread of nuclear weapons has meant that merely the ambition to possess a nuclear arsenal has spread to additional states, each of which then had to pursue that goal primarily through indigenous efforts. Importantly, since a state’s national efforts to turn its desire for nuclear weapons into reality naturally span several (and sometimes many) years, nuclear proliferation must be conceived of as a process, as opposed to just a single step (Meyer, 1986). This point is reinforced by the fact that 29 out of 39 states that have embarked upon that path (Müller and Schmidt, 2010, p. 157; Mikoyan, 2012; Santoro, 2017) have not acquired a nuclear arsenal. Hence, a lot of nuclear proliferation activity has been undertaken by nations that did not ultimately become nuclear weapon states. Three patterns explain this situation. First, owing not just to the technological, but also the institutional and managerial challenges of the task, some nations simply failed in their efforts to build the bomb (Hymans, 2012; Braut-Hegghammer, 2016). Second, a few countries have chosen a nuclear ‘hedging’ strategy, intentionally confining their efforts to developing the technological capability to build an arsenal quickly while refraining from exercising that option (Narang, 2016–17, p. 134). Third, several states have undertaken a ‘nuclear reversal’, abandoning their nuclear weapons activities before developing nuclear explosive devices (Müller and Schmidt, 2010).