# Neg – Cyber – Michigan Starter Packet

## Russian Cyberattacks Adv

### Russia Cyberwar Adv---1NC

#### No large-scale Russian cyberattacks

Baezner ’17 [Marie and Patrice Robin; Feb; Cyber Defense Project (CDP) Center for Security Studies (CSS), ETH Zürich, “Cyber-Conflict Between the United States of America and Russia” https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/184547/Cyber-Reports-2017-02.pdf?sequence=1]

On the other hand, both states might not desire further escalation, preferring to restrain the conflict to cyberspace. Each would follow the “tit-for-tat” logic and accuse each other while never reaching a tipping point where the conflict spills over to a conventional war. Such a tipping point would be linked to the intensity of the attack or the nature of the targets. Both nations would keep the cyberattacks small enough not to trigger a bigger reaction. The same would be observed on the choice of targets, with both avoiding certain critical or sensitive targets, for instance critical infrastructures. In order to contain the conflict in cyberspace, both states would have to demonstrate their restraint by selecting options with low risk of miscalculation (Lin, 2012, pp. 64–66). In the future, it might also be possible to see a deescalation in the form of the emergence of an international treaty or at least further bilateral treaties between the USA and Russia on cyberattacks. For example, during the last few years, businesses in the USA were often hacked and spied on by the Chinese military. These intrusions were mostly cyber-economic-espionage and were said to have supported the theft of billions of dollars’ worth of intellectual property (Bamford, 2016). In September 2015, the USA and China signed an agreement engaging both countries not to support or conduct cyber-theft of intellectual property. Moreover, the parties have made the commitment not to use cyberattacks against each other’s critical infrastructures in peace-time and to support the establishment of international behavioral norms in cyberspace (Rosenfeld, 2015). Both states also highlighted the fact that they could not control each individual in their country and therefore could not be held responsible for individual acts. Since then it seems that the number of attacks on commercial targets has diminished (Timm, 2016). Former President Obama suggested the creation of a position of cybersecurity ambassador to deal with bilateral or multilateral treaties concerning cyber-norms (Lee, 2016). For this kind of de-escalation to take effect, the termination of the conflict at hand must be the stated aim of both parties. A clear common understanding of the terms of agreement is required and must be based on trust-building efforts, as well as the assurance of mutual adherence. The difficulty of tracking the implementation of such agreements in cyberspace has been an obstacle preventing more states consenting to such solutions (Lin, 2012, pp. 62–64). Nevertheless, a dialogue on cyberspace already exists between the USA and Russia since July 2013. This cooperation includes Confidence Building Measures (CBM) such as the creation of working groups on the issue of ICT security, exchange of information between the two national Computer Emergency Response Teams (CERT), and the creation of a direct communication line to directly manage ICT incidents (Segal, 2016; The White House, Office of the Press Secretary, 2013). In October 2016, former President Obama used the latter to inform Russian President Putin that the USA was accusing Russia of interference in the election process (Ignatius, 2016). Furthermore, Russia and the USA take part in the UN GGE supporting the future establishment of international norms on actions in cyberspace. They stated that international law can be applied in cyberspace and therefore, the rules of proportionality and limited collateral damage should also be respected in cyberattacks (Ignatius, 2016; United Nations General Assembly, 2015). These examples demonstrate that even though the two states are involved in a “tit-for-tat” logic in their relations on a tactical level, there was still a dialogue on the strategic level, at least until 2015. The recent cyberattacks in USA and the election of Donald Trump as US President, bring new uncertainties.

#### No nuclear retal

Tucker ’18 [Patrick; Feb 2; Technology Editor for Defense One, MA from Johns Hopkins University, BA from Sarah Lawrence College, Former Deputy Editor for The Futurist; “No, the US Won’t Respond to A Cyber Attack with Nukes,” https://www.defenseone.com/technology/2018/02/no-us-wont-respond-cyber-attack-nukes/145700]

No, the US Won’t Respond to A Cyber Attack with Nukes Defense leaders won’t completely rule out the possibility. But it’s a very, very, very remote possibility. The idea that the U.S. is building new low-yield nuclear weapons to respond to a cyber attack is “not true,” military leaders told reporters in the runup to the Friday release of the new Nuclear Posture Review. “The people who say we lowered the threshold for the use of nuclear weapons are saying, ‘but we want these low-yield nuclear weapons so that we can answer a cyber attack because we’re so bad at cyber security.’ That’s just fundamentally not true,” Gen. Paul Selva, vice chairman of the Joints Chiefs of Staff, said Tuesday at a meeting with reporters. It’s an idea that military leaders have been pushing back against since the New York Times ran a Jan. 16 story headlined, “Pentagon Suggests Countering Devastating Cyberattacks With Nuclear Arms.” When would the U.S. launch a nuclear attack in response to a non-nuclear event? The Defense Department says the threshold hasn’t changed since the Obama administration’s own nuclear posture review in 2010, but a draft of the new review that leaked online caused a bit of drama in its attempts to dispel “ambiguity.” The new review gives examples of “non-nuclear strategic attacks,” Robert Soofer, deputy assistant secretary for nuclear and missile defense policy, told reporters on Thursday. “It could be catastrophic attacks against civilian populations, against infrastructure. It could be an attack using a non-nuclear weapon against our nuclear command-and-control [or] early-warning satellites. But we don’t talk about cyber.” In his own conversation with reporters, Selva broadened “early warning” systems to include ones that provide “indications of warning that are important to our detection of an attack.” He also emphasized, “We never said ‘cyber.’” There’s a reason for that. While cyber attacks on physical infrastructure can be very dangerous, they are unlikely to kill enough people to provoke a U.S. nuclear response. An National Academies of Science and Engineering analysis of the vulnerability of U.S. infrastructure makes that point. A major cyber attack could cut off electrical power, resulting in “people dying from heat or cold exposure, etc.,” said Granger Morgan, co-director of the Carnegie Mellon Electricity Industry Center and one of the chairs of the report. “A large outage of long duration could cover many states and last for weeks or longer. Whether and how many casualties there could be would depend on things like what the weather was during the outage.” It’s a huge problem but not an event resulting in tens of thousands of immediate deaths. Contrast that with a nuclear attack on a city like Moscow, even one using a device of 6 kilotons, much smaller than the ones the United States used against Japanese targets in World War II. The immediate result: there would be 40,000 deaths, according to the online nuclear simulation tool NukeMap. Russia has demonstrated a willingness to take down power services with cyber attacks, as they did in Ukraine on Christmas Eve 2015. But these attacks were brief and occured in the context of actual fighting. In other words, the worst cyber physical attack that top experts believe credible likely does not meet the threshold that the Defense Department has set out for deploying a nuclear weapon.

#### Cyber attacks won’t take down the grid

Craig ’16 [Victoria; Feb 2; Analyst at Fox Business, Citing the Senior Manager of Industrial Control Systems at Mandiant, “The U.S. Power Grid is 'Vulnerable,' But Don't Panic Just Yet”, http://www.foxbusiness.com/features/2016/02/02/u-s-power-grid-is-vulnerable-but-dont-panic-just-yet.html]

The idea of the nation's power grids becoming the next battleground for cyber warriors could make hacking into consumers’ credit card accounts and personal information seem like child’s play. While U.S. power companies are likely targeted by foreign governments and others in increasingly sophisticated breaches, actually shutting off the lights and causing chaos is far more complicated than many pundits make it seem. Dan Scali, senior manager of industrial control systems at Mandiant, a cybersecurity consulting arm of FireEye ([FEYE](http://www.foxbusiness.com/quote.html?stockTicker=FEYE)), explained that while cyber criminals may gain access to power and utility data systems, it doesn’t necessarily mean the result will be a power outage and a total takedown of power grid control systems. In other words, the power grid is controlled by more than just a panel of digital buttons. “Losing the control system is bad from the perspective that it takes you out of your normal mode of operations of being able to control everything from one command center, but it doesn’t mean you’ve lost control or all the lights go out [in the city],” Scali explained. While many of the systems have been modernized to include digitized control panels, if a hacker were to infiltrate the system, a utility worker could still have the ability to manually control the machines by flipping a switch, pushing a button, or tripping a breaker. As the world saw with the recent attack in Ukraine, which caused a blackout for 80,000 customers of the nation’s western utility, the biggest problem may be ensuring the power grid’s control systems are not vulnerable to cyber break ins. The January attack in Ukraine was likely caused by a corrupted Microsoft Word attachment that allowed remote control over the computer, according to the U.S. Department of Homeland Security. Scali said there was no evidence from the incident in Ukraine that the hacker’s malware was able to physically shut down the power. “It wiped out machines, deleted all the files. Kill disk malware made it impossible to remotely control things. It caused chaos on the business network, and the area where control system operations sat. But the attacker, we believe, would have had to actually used the control system to cause load shedding, which caused the power to go out, or trip breakers to cause the actual problem. Malware itself didn’t turn the power out,” Scali said. He said what most likely happened in that incident was the hacker stole user credentials and logged into the system remotely. The bottom line: Yes, a similar event could happen in the U.S. And corporate America is concerned. A recent survey released in January on the state of information security, conducted by consulting firm Pricewaterhouse Coopers, showed cybersecurity as one of the biggest concerns among the top brass at U.S. power and utilities firms. Part of the problem, Brad Bauch, security and cyber sector leader at PwC said, is the interconnectedness of the industry’s tools. “Utilities want to be able to get information out of [their] systems to more efficiently operate them, and also share that information with customers so they have more real-time information into their usage,” he explained. While allowing access to their own consumption data allows the companies to give their customers more of what they want, it also opens up a host of access points for hackers, making the systems more vulnerable than they otherwise would be. But to say that the power grid is susceptible to cyber hackers is a bit of an oversimplification.

#### Cyberwar stabilizing---forestalls escalation

Lonergan ’22 [Erica; April 15; assistant professor in the Army Cyber Institute and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University; Foreign Affairs, “The Cyber-Escalation Fallacy,” <https://www.foreignaffairs.com/articles/russian-federation/2022-04-15/cyber-escalation-fallacy>]

A third lesson of cyber-operations over the past decade is that U.S. officials should adopt a more flexible mindset in their response to them. Rather than focusing on retaliatory action, the United States should devote more resources to enhancing resilience—the ability to absorb and rapidly recover from disruptive occurrences. Embracing this type of approach means accepting that cyberattacks are likely to take place and, more important, that the overwhelming majority of them will not have cataclysmic effects. Over the past several years, the United States has improved its resilience to such attacks, expanding the agencies responsible for working with and maintaining critical infrastructure, such as the Cybersecurity and Infrastructure Security Agency. The U.S. government has also created the Office of the National Cyber Director to harmonize its cybersecurity efforts and collaborate with the private sector. But these entities are still relatively new, and efforts to implement meaningful regulation of the private sector to promote resilience still have a long way to go.

A CYBER ESCAPE VALVE?

Just because cyber-operations have not yet caused escalation does not mean that they will never do so. If conflicts such as the war in Ukraine lead to greater instability in the international system and increased great-power competition, the risks of cyber-escalation may grow. The opposite is also possible, however: in a more unstable world, cyber-operations may provide an important outlet for recurring tensions, given their lack of physical violence and relatively limited effects. As international politics become more dangerous, cyberspace can offer a way for states to respond to perceived aggressions without causing physical destruction or loss of life, thus providing a kind of stability in itself.

Ultimately, escalation is in the eye of the beholder—it depends as much on the target’s perception of an event as on the perpetrator’s intent or the reality of the strategic context. Therefore, a further priority of U.S. policymakers should be to improve their understanding of how adversaries interpret Washington’s activities in cyberspace and leverage that knowledge to conduct cyber-operations that minimize the risk of escalation. During a crisis, for instance, the United States may want to avoid conducting cyber-operations in a manner that an adversary might perceive as a precursor to conflict or to a military strike, especially if that is not the intent. If there is a pressing strategic or military imperative to conduct these types of operations, they should occur in tandem with efforts to communicate their purpose to avoid misunderstandings.

For too long, policymakers have drawn the wrong lessons from cyber-operations. The absence of escalation across decades of strategic interaction in cyberspace—a record that has only been reinforced in the conflict in Ukraine—should cause policymakers to reevaluate long-standing assumptions about the cyber-domain. In doing so, they may be able to see how cyber-actions are but one of a number of strategic tools that, properly understood, can limit the risk of conflict as much as increase it. Of course, the potential for cyberattacks to temporarily paralyze large information networks or even whole sectors of an economy should not be discounted. But in a world in which armed conflict continues to destroy entire cities and wreak terrible human costs, both civilian and military, cyber-operations should be regarded less as another form of hard power than as a way for states to pursue strategic goals by other means.

#### Cyberattacks fail and have minimal chance of escalation---Ukraine proves

Mueller ’22 [John; March 22; Political Scientist at Ohio State University and a Senior Fellow at the Cato Institute; Foreign Affairs; “The Cyber-Delusion,” https://www.foreignaffairs.com/articles/russia-fsu/2022-03-22/cyber-delusion]

When Russian forces launched their invasion of Ukraine last month, governments and experts worldwide warned about the danger of catastrophic cyberattacks. Indeed, in the days leading up to Moscow’s invasion, hackers defaced Ukrainian websites, unleashed malware on government systems, and targeted the country’s banking system—albeit with limited effect. Although no cyber-Armageddon has materialized, officials increasingly fear that Russia might eventually step up its efforts and even target the United States.

Russia’s invasion is no doubt catastrophic. But in reacting to it and preparing for what comes next, leaders in Washington and elsewhere should eschew the alarmism that has long warped cybersecurity policy. Mike Mullen, then chairman of the Joint Chiefs of Staff, claimed in 2011 that “the single biggest existential threat out there, I think, is cyber.” The following year, his successor, Martin Dempsey, noted that “a cyberattack could stop our society in its tracks.” Former Defense Secretary Leon Panetta sternly warned in 2012 of an impending “digital Pearl Harbor.” Nicole Perlroth, a cybersecurity reporter at The New York Times, has routinely asked insiders when “a cyber-enabled cataclysmic boom will take us down” and has always been told “18 to 24 months.” She began her survey well over 100 months ago.

This contemporary approach to cyberthreats resembles the aftermath of 9/11, when almost all experts believed an even larger terrorist attack would soon take place. Then, as now, the threat is overblown. Although occasionally dramatic, cyberattacks have turned out to be a comparatively minor and manageable threat. Far too much discussion around the issue focuses on worst-case scenarios, fails to contextualize the problem, and neglects to weigh the costs of cyberattacks against the enormous value of the Internet and artificial intelligence. Most commentary, moreover, does not fully appreciate the ability of the business sector—by far the most tempting of targets for malevolent hackers—to develop effective countermeasures.

Over the past decade, the global obsession with digital threats has taken various forms, with a particular focus on the potential military implications of emerging cyber-capabilities. To be sure, the military needs to worry about keeping its communications and command and control operations secure from hostile attackers. Any disruptions, however, are more likely to be instrumental or tactical than strategic.

Despite statements to the contrary, the U.S. military itself seems to have recognized this reality. When Panetta proclaimed in 2013 that cyber was “without question, the battlefield for the future,” political scientist Micah Zenko observed at the time that the Pentagon was spending less than one percent of its budget on cybersecurity, and an assessment from 2019 suggests it may be more like one-tenth of one percent. If those funds prove adequate for the challenge, it would be something of a bargain.

Cyber also supposedly enhances a state’s ability to carry out such ancient endeavors as espionage, propaganda dissemination, and sabotage. Analysts have even coined a new term, “hybrid warfare,” that usually includes these three enterprises—although, since the term does not include direct armed conflict, it might more plausibly be called “denatured warfare.” Cyber’s contribution to these three areas, however, is relatively limited.

Should invading hackers engage in digital espionage against the United States, for instance, they are likely to find that most of what they come across is already well known, and that much of the rest is not worth knowing in the first place. Wikileaks’ 2010 publication of thousands of classified U.S. government documents demonstrated the degree to which governments worldwide have fallen victim to over-classification. When Bill Keller, the editor in charge of poring over the documents at The New York Times, was asked whether the reporting team found anything they didn’t already know, he responded “no” without hesitation.

Much the same holds for concerns over the theft of intellectual property. Not only is this practice centuries old, but systematic stealing has often proved unwise because it distracts governments from homegrown innovation. Cyber-propaganda efforts, in turn, are more likely to increase the overall amount of available information and disinformation—an age-old problem in warfare—than to provide a decisive advantage.

The achievements of cyber-sabotage have also been quite modest. The United States and Israel famously used a computer virus known as Stuxnet to hamper Iran’s progress toward developing a nuclear weapon. Although observers hailed the operation as a dangerous new development in modern conflict, the damage proved temporary. Iran quickly rebuilt its centrifuges, and the attack actually proved counterproductive, as it encouraged Tehran to accelerate its nuclear program. There have also been efforts by the United States to physically interfere with missile development in North Korea. Yet, much like the Iranians, Pyongyang eventually solved whatever the problem was, and the attacks had little long-term effect on their program.

Cyber-alarmists have also warned about hackers disabling major infrastructure such as power grids—potentially crippling entire countries. Grids do go down occasionally, but the culprits are typically squirrels and lightning. Regardless of the source, such disruptions are usually brief and bearable, and engineers are increasingly designing systems that are resilient to such threats. Estonia, for instance, the victim of a major and oft-discussed cyberattack in 2007, is now the home of NATO’s Cooperative Cyber Defence Centre of Excellence.

#### Squo solves NATO cyber clarity

Khatuna Burkadze 18, PhD, a Fulbright scholar at the MIT Center of International Studies, a visiting researcher at Columbia University, Bard College and the Fletcher School of Law and Diplomacy, graduate of the Fletcher School of Law & Diplomacy, “A Shift in NATO's Article 5 in the Cyber Era?” The Fletcher Forum of World Affairs, Volume 42, Issue 2, Summer 2018, 215-226

NATO'S CYBER DEFENSE AND INTERNATIONAL LAW The U.N. Charter and the North Atlantic Treaty (the founding treaty of NATO) were adopted in 1945 and 1949 when the creation of cyberspace was a matter of the future rather than a consideration of the times. Currently, it is clear that information and communication technologies have transformed the nature of war and changed historical understanding of armed attacks. Traditional applications of the use of force prohibition fail to adequately safeguard shared community values threatened by Computer NetworkAttacks (CNA)." The use of force is strictly limited in international law according to the U.N. Charter. Consequently, the central questions are the following: Could a cyberattack be equated to an armed attack according to international law? If a cyberattack equates to an armed attack, how should the principle of collective defense of NATO be interpreted to give member states legal guidance on the concept of a cyberattack? Do we need amendments in Article 5 of the North Atlantic Treaty to clearly define what constitutes a cyberattack? Answers to these questions can provide insights for defining rules of cyber operations in case of cyberattacks. The definitions of the use of force and armed attack are not provided in the U.N. Charter. In this regard, in its argument on a case concerning Nicaragua, the International Court of Justice rejected a narrow interpretation of "use of force" that limits the term to the employment of either kinetic force or non-kinetic operations generating comparable effects. The Court held that a state's arming and training of guerrilla forces engaged in hostilities against another state qualified as a use of force, a position that has since become widely accepted.'" The logic of the holding leads to the conclusion that non-destructive cyber operations may amount to a use of force. For example, providing malware to a rebel group and training its members to employ that malware in a destructive manner would seemingly qualify.20 However, every unfriendly act does not cross the use of force threshold. The International Court of Justice held that financing guerrillas, albeit an unlawful "intervention," did not fall into the same category. Therefore, cyber operations intended to economically coerce another state to engage in, or desist from, a particular course of action would not amount to a use of force; nor would financing a rebel group's cyber operations. Beyond these directly parallel examples, uncertainty remains as to where the threshold lies.2 1 The NATO Cooperative Cyber Defense Center of Excellence launched a major research project in late 2009 to examine the public international law governing cyber warfare2 2 and cyber operations, resulting in the Tallinn Manual 1.0 and Tallinn Manual 2.0. These two documents provide international experts' analysis on how existing international law applies to cyber warfare and cyber operations. Through Tallinn Manual 1.0, the International Group of Experts developed a nonexclusive list of factors that would likely influence the characterization of cyber operations by a state as a use of force: severity, immediacy, directness, invasiveness, measurability, military character, state involvement, and presumptive legality. Additional factors found meaningful by the Experts included, inter alia, the prevailing political environment, the nexus of an operation to prospective military force, the attacker's identity, the attacker's track record with respect to cyber operations, and the nature of the target. These and other factors operate in concert as states make case-by-case determinations. Of them, severity alone can qualify a cyber operation as a use of force.23 In this regard, the Group unanimously agreed that any cyber operation causing greater than de minimis damage or injury suffices. For instance, they concurred that the damage to Iranian nuclear facilities in 2010 resulting from the Stuxnet virus crossed the threshold.24 As for the concept of cyberattacks and cyberwarfare, there are no widely accepted definitions. The U.S. Department of Defense defines "computer network attacks" as "actions taken by using computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."2 5 Yale Law Professor Oona Hathaway and her colleagues have devised a broader definition of a "cyberattack." In a 2012 article, they wrote: "A cyberattack consists of any action taken to undermine the functions of a computer network for a political or national security purpose." The article goes on to say that "any action" includes "hacking, bombing, cutting, inflecting, and so forth," as long as the action has the objective of undermining or disrupting a computer network. The word "purpose" seems to apply to the intent of the attacking party.26 According to the Tallinn Manual's Rule 30. "A cyberattack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."27 In this regard, Professor Antonia Chayes, in an article titled, "Rethinking Warfare: The Ambiguity of Cyber Attacks," highlights that a cyber operation can constitute an attack even before the damaging consequences of such an operation become evident, citing the example of implanting malware that will be activated at a later time, but for which the intended consequences meet the requisite threshold of harm as an event that could be defined as an attack "irrespective of whether the malware is activated" this is a direct parallel to implanting. In a similar vein, a cyberattack that has been launched but defeated still amounts to an attack. The Manual does warn that great care should be exercised when identifying the perpetrator of the attack.28 Professor Chayes emphasizes that these definitional iterations help to refine the issues, although they cannot be expected to answer all questions. They do serve to narrow differences in approach somewhat and to begin to assure that officials are addressing common issues. However, the lack of internationally accepted distinctions among "cybercrime," "cyberattack," and "cyber war" make concerted international action more difficult to achieve. The definitions alone do not delineate civilian and military roles, nor do they designate a legal framework under which to operate, since the issue of whether an attack warrants a military response-even in the military domain-remains ambiguous. Economic attacks may be handled through a variety of international means, judicial and diplomatic. But crippling economic attacks without serious casualties might not be sufficient to warrant acts in selfdefense under Article 51 of the U.N. Charter nor, as in the case of Estonia, a collective response under Article 5 of the North Atlantic Treaty. As for NATO's official position on interconnection between the existing international legal regulations and cyberspace, the Wales Summit Declaration (issued by the Allies in Wales on 4-5 September 2014) emphasizes: "Our policy recognizes that international law, including international humanitarian law and the U.N. Charter, applies in cyberspace. Cyberattacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defense is part of NATO's core task of collective defense. A decision as to when a cyberattack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."30 This means that, on the one hand, member states of the Alliance agreed that international law applies to cyberspace but, on the other hand, in the case of a cyberattack, a decision about invoking Article 5 will be made by the members of NATO based on the particular criteria. Therefore, the principle of collective defense is not an automatic mechanism. The exact criteria by which cyber incidents may trigger an Article 5 invocation of collective defense have not been determined. However, the North Atlantic Council is very likely to consider the following elements in its deliberations. " Scope: Is the incident widespread across a geographic area or industrial sectors? The wider the attack is, the more likely NATO action will be; " Duration: Is the incident a single event or does it last over time as part of a longer campaign? NATO is more likely to act for extended incidents; " Intensity/Scale: Has the incident caused death or substantial property destruction? If not, NATO is unlikely to declare collective defense; " External Actor: Is the incident directed from a foreign or domestic adversary? NATO is unlikely to act against a purely domestic foe.31

#### Human capital shortages gut NATO cyber defense

Porter ’19 [Christopher and Klara Tothova Jordan; Feb 14; nonresident senior fellow at the Atlantic Council; assistant director of the Atlantic Council’s Cyber Statecraft Initiative; Lawfare, “Don’t Let Cyber Attribution Debates Tear Apart the NATO Alliance,” https://www.lawfareblog.com/dont-let-cyber-attribution-debates-tear-apart-nato-alliance]

Now imagine the response of that ally when it’s being asked to take causus belli on faith: The United States is presenting attribution for a cyberattack elsewhere in the world, but perhaps is depending on the ally lacking critical details due to classification, and is presenting that information alongside a request for help that might well put the ally in the crosshairs of its own cyberattack or lethal action. How can allies with different capabilities to collect, analyze and understand intelligence be part of a consensus on using sovereign cyber effects to support a NATO operation? How can a commander achieve a common operational picture to authorize the use of sovereign effects in a NATO operation if all the allies are not on the same page with respect to critical attribution and other technical information needed for a use of effect in an operation? We all know what a tank looks like on a shared satellite image, but if you ask three cyber experts to interpret the attribution for a set of indicators, you are likely to get at least four answers.

For most U.S. allies in Europe and elsewhere, there is simply a dearth of technical know-how within the government when it comes to cyber attribution and operations. This is already a challenge for the United States, with a massive defense budget, Silicon Valley innovation and an educated workforce to pull into government service. But for many U.S. allies, tech-savvy public servants will have long fled for the private sector, nongovernmental organizations (NGOs) and academia before reaching ministerial positions.

To its credit, the U.S. National Cyber Strategy does propose capacity-building measures to support allies. This means building up law enforcement, intelligence, and military operational and investigative capability. But even with successful capacity-building programs, many nations could, in a crisis, end up in the same place the United States is—with good options stuck on the shelf while political leaders and their electorates lack a critical mass of informed voters to trust, understand and act on expert findings.

For countries weighing whether to risk their own blood and treasure in support of an ally’s cyber attribution findings, this hurdle could well prove insurmountable if not addressed well before a crisis emerges. Many such countries will no doubt recall being burned when placing too much confidence in U.S. technical and human sources without an ability to evaluate the evidence for themselves, as with the Iraq weapons of mass destruction findings.

### AT: Critical Infrastructure---1NC

#### No impact to civilian infrastructure attacks.

Lewis ’20 [James Andrew; 8/17/20; senior vice president and director of the Strategic Technologies Program at the Center for Strategic and International Studies; "Dismissing Cyber Catastrophe," https://www.csis.org/analysis/dismissing-cyber-catastrophe]

A catastrophic cyberattack was first predicted in the mid-1990s. Since then, predictions of a catastrophe have appeared regularly and have entered the popular consciousness. As a trope, a cyber catastrophe captures our imagination, but as analysis, it remains entirely imaginary and is of dubious value as a basis for policymaking. There has never been a catastrophic cyberattack.

To qualify as a catastrophe, an event must produce damaging mass effect, including casualties and destruction. The fires that swept across California last summer were a catastrophe. Covid-19 has been a catastrophe, especially in countries with inadequate responses. With man-made actions, however, a catastrophe is harder to produce than it may seem, and for cyberattacks a catastrophe requires organizational and technical skills most actors still do not possess. It requires planning, reconnaissance to find vulnerabilities, and then acquiring or building attack tools—things that require resources and experience. To achieve mass effect, either a few central targets (like an electrical grid) need to be hit or multiple targets would have to be hit simultaneously (as is the case with urban water systems), something that is itself an operational challenge.

It is easier to imagine a catastrophe than to produce it. The 2003 East Coast blackout is the archetype for an attack on the U.S. electrical grid. No one died in this blackout, and services were restored in a few days. As electric production is digitized, vulnerability increases, but many electrical companies have made cybersecurity a priority. Similarly, at water treatment plants, the chemicals used to purify water are controlled in ways that make mass releases difficult. In any case, it would take a massive amount of chemicals to poison large rivers or lakes, more than most companies keep on hand, and any release would quickly be diluted.

### AT: Cyber---1NC

#### No cyber impact – attribution, restraint, and capabilities.

Lewis ’20 [James Andrew; 8/17/20; senior vice president and director of the Strategic Technologies Program at the Center for Strategic and International Studies; "Dismissing Cyber Catastrophe," https://www.csis.org/analysis/dismissing-cyber-catastrophe]

More importantly, there are powerful strategic constraints on those who have the ability to launch catastrophe attacks. We have more than two decades of experience with the use of cyber techniques and operations for coercive and criminal purposes and have a clear understanding of motives, capabilities, and intentions. We can be guided by the methods of the Strategic Bombing Survey, which used interviews and observation (rather than hypotheses) to determine effect. These methods apply equally to cyberattacks. The conclusions we can draw from this are:

Nonstate actors and most states lack the capability to launch attacks that cause physical damage at any level, much less a catastrophe. There have been regular predictions every year for over a decade that nonstate actors will acquire these high-end cyber capabilities in two or three years in what has become a cycle of repetition. The monetary return is negligible, which dissuades the skilled cybercriminals (mostly Russian speaking) who might have the necessary skills. One mystery is why these groups have not been used as mercenaries, and this may reflect either a degree of control by the Russian state (if it has forbidden mercenary acts) or a degree of caution by criminals.

There is enough uncertainty among potential attackers about the United States’ ability to attribute that they are unwilling to risk massive retaliation in response to a catastrophic attack. (They are perfectly willing to take the risk of attribution for espionage and coercive cyber actions.)

No one has ever died from a cyberattack, and only a handful of these attacks have produced physical damage. A cyberattack is not a nuclear weapon, and it is intellectually lazy to equate them to nuclear weapons. Using a tactical nuclear weapon against an urban center would produce several hundred thousand casualties, while a strategic nuclear exchange would cause tens of millions of casualties and immense physical destruction. These are catastrophes that some hack cannot duplicate. The shadow of nuclear war distorts discussion of cyber warfare.

State use of cyber operations is consistent with their broad national strategies and interests. Their primary emphasis is on espionage and political coercion. The United States has opponents and is in conflict with them, but they have no interest in launching a catastrophic cyberattack since it would certainly produce an equally catastrophic retaliation. Their goal is to stay below the “use-of-force” threshold and undertake damaging cyber actions against the United States, not start a war.

This has implications for the discussion of inadvertent escalation, something that has also never occurred. The concern over escalation deserves a longer discussion, as there are both technological and strategic constraints that shape and limit risk in cyber operations, and the absence of inadvertent escalation suggests a high degree of control for cyber capabilities by advanced states. Attackers, particularly among the United States’ major opponents for whom cyber is just one of the tools for confrontation, seek to avoid actions that could trigger escalation.

The United States has two opponents (China and Russia) who are capable of damaging cyberattacks. Russia has demonstrated its attack skills on the Ukrainian power grid, but neither Russia nor China would be well served by a similar attack on the United States. Iran is improving and may reach the point where it could use cyberattacks to cause major damage, but it would only do so when it has decided to engage in a major armed conflict with the United States. Iran might attack targets outside the United States and its allies with less risk and continues to experiment with cyberattacks against Israeli critical infrastructure. North Korea has not yet developed this kind of capability.

### AT: Cyber---2NC

#### Resilience solves.

Lewis ’20 [James Andrew; 8/17/20; senior vice president and director of the Strategic Technologies Program at the Center for Strategic and International Studies; "Dismissing Cyber Catastrophe," https://www.csis.org/analysis/dismissing-cyber-catastrophe]

One major failing of catastrophe scenarios is that they discount the robustness and resilience of modern economies. These economies present multiple targets and configurations; they are harder to damage through cyberattack than they look, given the growing (albeit incomplete) attention to cybersecurity; and experience shows that people compensate for damage and quickly repair or rebuild. This was one of the counterintuitive lessons of the Strategic Bombing Survey. Pre-war planning assumed that civilian morale and production would crumple under aerial bombardment. In fact, the opposite occurred. Resistance hardened and production was restored.1

#### Err against catastrophe.

Lewis ’20 [James Andrew; 8/17/20; senior vice president and director of the Strategic Technologies Program at the Center for Strategic and International Studies; "Dismissing Cyber Catastrophe," https://www.csis.org/analysis/dismissing-cyber-catastrophe]

This is a short overview of why catastrophe is unlikely. Several longer CSIS reports go into the reasons in some detail. Past performance may not necessarily predict the future, but after 25 years without a single catastrophic cyberattack, we should invoke the concept cautiously, if at all. Why then, it is raised so often?

Some of the explanation for the emphasis on cyber catastrophe is hortatory. When the author of one of the first reports (in the 1990s) to sound the alarm over cyber catastrophe was asked later why he had warned of a cyber Pearl Harbor when it was clear this was not going to happen, his reply was that he hoped to scare people into action. "Catastrophe is nigh; we must act" was possibly a reasonable strategy 22 years ago, but no longer.

The resilience of historical events to remain culturally significant must be taken into account for an objective assessment of cyber warfare, and this will require the United States to discard some hypothetical scenarios. The long experience of living under the shadow of nuclear annihilation still shapes American thinking and conditions the United States to expect extreme outcomes. American thinking is also shaped by the experience of 9/11, a wrenching attack that caught the United States by surprise. Fears of another 9/11 reinforce the memory of nuclear war in driving the catastrophe trope, but when applied to cyberattack, these scenarios do not track with operational requirements or the nature of opponent strategy and planning. The contours of cyber warfare are emerging, but they are not always what we discuss. Better policy will require greater objectivity.

#### No cyber impact.

**Wirtz 18** James J. Wirtz, National Security Affairs professor at the Naval Postgraduate School, former Director of the Global Center for Security Cooperation at the Defense Security Cooperation Agency, Political Science PhD from Colombia, internally citing Cyber War versus Cyber Realities, a book by Brandon Valeriano and Ryan C. Maness. [Cyber War or Monkey Business? International Journal of Intelligence and CounterIntelligence, 31(2), Taylor and Francis]//BPS

Between 4 and 7 September 2001, I attended the First Biennial Threat Reduction Conference that was sponsored by the Defense Threat Reduction Agency in Norfolk, Virginia. One of the panels featured a debate about the likelihood of mass casualty terrorism in the United States. One panelist asserted that such an event was unlikely—the Aum Shinrikyo sarin attack being a case in point. Although well-funded and left relatively unmolested by the authorities, cultists managed to kill only 13 people when they released a nerve agent in the Tokyo subway. Thus, inflicting mass casualties, even with sarin, was not easily accomplished. The threat of mass casualty terrorism was being exaggerated by scholars and pundits alike, the panelist asserted, urging the conferees to instead focus on plausible threats. The other panelist agreed that Aum Shinrikyo was inept but offered the obvious counterpoint: just because something has not occurred in the past does not guarantee that it will not occur in the future. The next morning, I contemplated this wonderfully “academic” debate on a pleasant United Airlines flight from Dulles to San Francisco. Soon afterwards it occurred to me that when it comes to picking an itinerary or making observations about the future, timing is everything. DOUBTING THE THREAT HYPE Brandon Valeriano and Ryan Maness acknowledge the “timing” problem inherent in their well-reasoned and empirically based assessment of state cyber conflicts that occurred between 2001 and 2011. Nevertheless, in their view, cyber war is mostly hype, created by over-imaginative academics and a cyber security industry ready to profit from cyber anxieties. By contrast, their analysis reveals that, at least in the period considered, cyber conflict was limited in both scope and severity, and was largely characterized by espionage or hooliganism (defacement of government websites) that generally produced no lasting impact. They note that in the vast majority of cases the incompetence of the victim or the aid of a witting or unwitting accomplice had facilitated penetration of some system. Here the 2015 hack of the U.S. Office of Personnel Management, which compromised the personal information of just about everyone who had ever applied for or possessed a U.S. security clearance, comes to mind. The Stuxnet attack against Iranian centrifuges, an outlier in their database, is used to illustrate their fundamental point: that the use of cyber warfare to inflict real damage is a rare and extraordinarily difficult endeavor that is probably within the technical reach of only a few states. Valeriano and Maness also back up their empirical observations with some theoretical musings about why the reality of cyber warfare is out of step with the cyber hype surrounding the issue. Zero-day exploits (using heretofore unknown system vulnerabilities) are fleeting in their efficacy; once revealed, they are quickly rectified. Because they begin to lose their effectiveness soon after they are employed, the tendency is to keep one’s powder dry, so to speak. Moreover, aggressive viruses can either propagate uncontrollably across the Internet or be repackaged and returned to the sender with unpredictable consequences. Because predicting the impact of more aggressive cyber attacks is difficult, states tend to exhibit restraint in their use of cyber weapons. Put somewhat differently, weapons that are likely to produce collateral damage or even fratricide are not readily embraced by military professionals. Although the authors do not mention it, attitudes toward the use of cyber weapons seem to mirror the history of biological warfare. Unleashing contagion is highly unpredictable; weapons with unknowable effects have little military utility. They might produce their intended impact, but there is no telling how far disease might spread. Because the same can be said for cyber weapons, restraint characterizes the way states engage in cyber conflict. Another theoretical insight offered by Valeriano and Maness is that cyber conflict is both profoundly political and strategic. Conflict is centered on a set of enduring rivalries: India and Pakistan, China and Japan, Russia and member states of the former Soviet Union, the United States and China, and the United States and Iran. With the exception of Stuxnet, these incidents tend to be limited, matching the “short-of-war” levels of acrimony present in these relationships. These observations are important because some policymakers and scholars tend to focus on what might happen in cyberspace, not why it might happen. For instance, it is theoretically possible to temporarily bring down the power grid in the United States, or to disrupt the stock market, or to cripple the banking system, creating significant disruption or even loss of life. But in focusing on these scenarios observers fail to stipulate the strategic purpose or the political setting that would motivate the launch of a highly devastating cyber attack. Admittedly, for those on the front lines of cyber defense, it might appear that the world has descended into a feral state of nature as they monitor thousands of attempts daily to hack into protected networks. Nevertheless, Valeriano and Maness correctly note that no one has yet died in a cyber attack, a requirement needed to turn an incident into a “war.” In a political and strategic sense, the world has not yet witnessed cyber war.

#### Err against cyber war – media hype is based on little or faked data.

**Valeriano & Maness 18** Brandon Valeriano, PhD, Chair of Armed Politics at the Marine Corps University, Cyber Security Senior Fellow at the Atlantic Council, & Ryan Maness, an American cybersecurity expert, Defense Analysis Professor at Naval Postgraduate School. [How We Stopped Worrying about Cyber Doom and Started Collecting Data, Politics and Governance, 6(2), Cogitatio Press]//BPS

Moderate and measured takes on cyber security threats are swamped by the recent flood of research and policy positions in the cyber research field offering hyperbolic perspectives based on limited observations. This skewed perspective suggests constant cyber disasters that are confronting humanity constantly. The general tone of the debate argues that cyber war is already upon us and our future will only witness more cyber doom. However, these hyperbolic perspectives are being countered by empirical investigations that produce the opposite of what is to be expected. It is generally observed that limited cyber engagements throughout the geopolitical system are the dominant form of interaction. Our task here is to offer a different path forward. We first posit what can be known about cyber security interactions with data as well as what cannot. Where is the water's edge in cyber security research? We then examine the known works in the field that utilize data and evidence to examine cyber security processes. Finally, we conclude with an offering of what types of studies need to be done in the future to move the field forward, away from the prognostication and generalizations so typical in the discourse in this constantly changing and growing field. Keywords cyber conflict; cyber security; cyber strategy; data collection; quantitative methods Full Text: 1. The Challenge of Cyber Security Threat Data Beginning in 2014, various news organizations began reporting on a particular cyber security firm, Norse Corporation, and their active cyber threat map (Walker, 2015). Mashable noted in 2016 that "the global cyber war is raging on, and this mesmerizing map shows just how serious it has become" (Gallucci, 2016). The map is dynamic, colorful, and gets the point across quickly, a criterion for any decent visualization of data. As late of August 2017, the Defense Intelligence Agency (DIA) tweeted out a link and photo of the threat maps suggesting it represented ongoing cyber-attacks (DIA, 2017). Yet this map is not a very clear representation of any real threats that nationstates face on a daily basis. Unfortunately, the Norse cyber threat map does not represent active threat data, but attacks, likely by bots, on preset honeypots. Honeypots are a method of providing data on fake targets to either distract the opposition from the real targets or to deter an aggressor from attacking in the first place (Gartzke & Lindsay, 2015). While sometimes a useful method to gather threat intelligence if presented a sleight of hand for an attractive target, honeypots as reported in popular discourse are not exactly an accurate representation of the cyber threat landscape. In this case, the goal was to demonstrate the ability to track global attacks to gain interest in the company and promote its capabilities. Nearly all active threat maps either present data tracking honeypots and various bot networks that are devoid of human agency, simply presenting what is in fact fake data. Active representation of the threat landscape is the goal, but the reality is that the picture of the cyber security threat landscape we currently have is incomplete, misleading, or outright fake. High profile data breaches have been consuming media narratives for at least a decade. With each act of cyber disruption or espionage, pundits as well as government officials and several academics declare that cyberwar-fare is upon us, is the future of warfare, and it is only a matter of time before a "Cyber Pearl Harbor" wreaks havoc on the American homeland (Gurdus, 2016). With this new revolution in military affairs, the battlefield, according to some, is forever changed and the next big war could very well be a cyberwar (Clarke & Knake, 2010; Kello, 2013). Politicians, pundits, and practitioners have jumped on this doomsday narrative and have promoted cyber arms races, offensive advantage, and deterrence strategies to stay one step ahead of would be adversaries in order to prevent them from infiltrating networks out of fear of massive retaliation. These revolutionists point to acts such as Stuxnet, Shamoon, Sony, and the Office of Personal Management (OPM) hack as the new norm of conflict between states, and that the US is losing ground with every tolerated cyber-attack on American networks.

#### Data shows a tendency toward restraint.

**Valeriano & Maness 18** Brandon Valeriano, PhD, Chair of Armed Politics at the Marine Corps University, Cyber Security Senior Fellow at the Atlantic Council, & Ryan Maness, an American cybersecurity expert, Defense Analysis Professor at Naval Postgraduate School. [How We Stopped Worrying about Cyber Doom and Started Collecting Data, Politics and Governance, 6(2), Cogitatio Press]//BPS

6. Expanding Cyber Security Data Our team has been coding cyber incident data since 2010 and serves as a unique example of how the process of collecting cyber security data and evidence can be done. Our first peer reviewed published work appeared in 2014 in Journal of Peace Research (Valeriano & Maness, 2014). In this article we note that cyber conflict is much more restrained than generally understood by popular discourse. Threat inflation is ripe in cyber security, and the real use of cyber tools seems to be to enhance the power of strong states. The data that Valeriano and Maness (2014, 2015) have built challenges the cyber revolution perspective and does so with the tools of social science, and is a necessary turn given the general tone of the debate. We first determine that a viable data collection method in light of limited resources was to focus on states that are committed interstate rivals (Diehl & Goertz, 2001). This allows us to focus on those actors with an intense history of recent hostilities that should be the most likely users of cyber technology on the battlefield (Maness & Valeriano, 2018). In our research (Maness & Valeriano, 2016; Maness, Valeriano, & Jensen, 2017; Valeriano & Maness, 2014, 2015), we have been able to marshal a massive amount of evidence that is useful in dissecting the actual trends on the cyber battlefield in a geopolitical context. We demonstrate that while cyber-attacks are increasing in frequency, they are limited in severity, are directly connected to traditional territorial disagreements, and mostly take the shape of espionage and low-level disruptive campaigns rather than outright warfare. Given this data-based perspective, we question the dynamics of the cyber security debate and offer a countering theory where states are restrained from using more malicious cyber actions due to the limited nature of the weapons, the possibly of blowback, the connection between the digital world and civilian infrastructure, and the reality that any cyber weapon launched can be replicated and used right back against the attacker. Given all of these perspectives gleamed from the data, we must moderate our views about the transformation that is offered by cyber strategists who stress a more revolutionist tone (Lango, 2016).

### AT: Cyber Norms---1NC

#### Cyber signaling and norms are impossible.

Hurd ’19 [Ian; 2019; Political Science Professor at Northwestern University; “If I Had a Rocket Launcher: Self-Defense and Forever War in International Law,” Houston Law Review, https://houstonlawreview.org/article/7952-if-i-had-a-rocket-launcher-self-defense-and-forever-war-in-international-law]

Its history can also be told through the changing uses of law in the political practice of justification. The legal formulations that were once thought to enclose war fully within self-evident and constraining legal categories have turned inside out and now operate to disperse military action throughout the world. As national interests and military technologies have changed, the rules have adapted, both in ratione temporis and ratione materiale. The instrumental utility of expansive self-defense claims for powerful governments is great, and the power of state practice to redefine international law is well-accepted—together these two facts ensure that the operative understanding of international rules will not deviate far from the desires of strong states. As the rule has moved, so has its political effects. Today it serves to legitimize and legalize the turn to “endless war” that has characterized American foreign policy since 2001.

With self-defense now anchored on national security interests, it has released its former connections to time and to armed attack. From this new foundation, it became useful to ambitious governments who are eager to attack their enemies abroad. In self-defense defined as national security, these states found a legal justification that matched neatly with their new technologies of drones and cyber. Together, these tools encouraged those with the capabilities to engage in undeclared and perhaps never-ending military operations against those whom they see as enemies of the state.

The history of self-defense helps to show the gap between the mythology of international law and its practical life. The myth says that international law provides a stable framework of rules that enable states to act toward their objectives while limiting their capacity to engage in acts that are damaging to the entire community. The reality is that rules become tools which powerful actors aim to use to

their advantage. As Rebecca Sanders asserts, “There is nothing inherently progressive about legal culture[]” or international law.[82] The political effects of law depend on who is using it against what and against whom.

#### No one listens – interests outweigh.

Shires ’18 [James; 10-12-2018; Research Fellow with the Cyber Security Project at the Belfer Center for Science and International Affairs, Harvard Kennedy School, DPhil candidate in International Relations at the University of Oxford, MSc from Birkbeck College; “Between Multistakeholderism and Sovereignty: Cyber Norms in Egypt and the Gulf States,” War on the Rocks, https://warontherocks.com/2018/10/between-multistakeholderism-and-sovereignty-cyber-norms-in-egypt-and-the-gulf-states/]

Conclusion

Amid deep conflict over basic norms, Egypt and the GCC states have maneuvered between two poles while enjoying the tacit, if not explicit, support of both sides. This has three key implications. First, global cyber norms are much more complex — and much more entangled with traditional governance practices, diplomatic relationships, and strategic concerns — than Western officials may like to admit. However uncomfortable it may be, international policymaking on cyber norms must take into account not only the “likemindedness” of some states, but also the fact of their strategic interests and relationships with other states that are less or not at all likeminded. Without this recognition, any attempt to create global cyber norms is hampered from the start. More broadly, to understand the complexity of cyber norms we must look outside the framework of great power competition.

Second, the United States and European allies of Egypt and the Gulf states need to decide where their priorities lie: Does consistency on global cyber norms outweigh broader security considerations? If a stable, coherent set of cyber norms is the primary aim, greater attention should be given to persuading friendly states to stay within the boundaries of these norms. However, if security alliances trump cyber norms, Western democracies should recognize that the rhetorical effect of denouncing Russian or Chinese action will be limited. For the United States, effective foreign policy regarding cyber security in the Middle East requires both the identification of a clear national interest, connected to broader strategic goals concerning the kind of cyber space the United States seeks to promote, and a good understanding of the evolving landscape in which the U.S. government and U.S. companies are operating. Right now, both are lacking.

Third, although the contradictions outlined here suggest that human rights and national security are important starting points for research, we should not confine cyber security research on these states to these well-trodden paths. In the Middle East, cyber security is changing regional alliances, altering the economic calculations of businesses, and reforging fundamental relationships between individuals and their governments. There are significant differences in cyber security approaches between these states, especially in Kuwait and Qatar. And there are many new initiatives and organizations, like Saudi Arabia’s National Cyber Security Authority (al-hai’a al-watniyya lil-‘amn al-sibrani), Egypt’s High Council for Cybersecurity, the UAE’s National Electronic Security Agency, and Oman’s Arab Region Cybersecurity Centre. As our understanding of cyber security evolves and its connection to other areas of foreign policy deepens, a broader approach to cyber security research in this region is urgently needed to adequately understand these new dynamics and inform future policy choices.

### AT: NC3---1NC

#### No NC3 hacking.

Futter ’16 [Andrew; 2016; International Politics Professor at the University of Leicester; “War Games Redux? Cyberthreats, US–Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control,” European Security 25(2), p. 171-172]

It is of course highly unlikely that either the USA or Russia has plans – or perhaps more importantly, the desire – to fully undermine the other’s nuclear command and control systems as a precursor to some type of disarming first strike, but the perception that nuclear forces and associated systems could be vulnerable or compromised is persuasive. Or as Hayes (2015) puts it, “The risks of cyber disablement entering into our nuclear forces are real”. While the growing possibility of “cyber disablement” should not be overstated (notions of a “cyber-Pearl Harbor” (Panetta 2012) or “cyber 9–11” (Charles 2013) have done little to help understand the nature of the challenge), cyberthreats are nevertheless an increasingly important component of the contemporary US–Russia strategic context. This is particularly the case when they are combined with other emerging military-technical developments and programmes. The net result, especially given the current downturn in US–Russian strategic relations, and the way cyber is exacerbating the impact of other problematic strategic dynamics, is that is seems highly unlikely that either the USA or Russia will make the requisite moves to de-alert nuclear forces that the new cyber challenges appear to necessitate, or for that matter to (re)embrace the “deep nuclear cuts” agenda any time soon.

Assessing the options for arms control and enhancing mutual security

Given the new challenges presented by cyber to both US and Russian nuclear forces and to US–Russia strategic stability, it is important to consider what might be done to help mitigate and guard against these threats, and thereby help minimise the risks of unintentional launches, miscalculation, and accidents, and perhaps create the conditions for greater stability, de-alerting, and further nuclear cuts. While there is unlikely to be a panacea or “magic bullet” that will reduce the risk of cyberattacks on US and Russian nuclear forces to zero – be they designed to launch nuclear weapons or compromise the systems that support them – there are a number of options that might be considered and pursued in order to address these different types of threats and vulnerabilities. None, of these however, will be easy.

The most obvious and immediate priority for both the USA and Russia is working (potentially together) to harden and better protect nuclear systems against possible cyberattack, intrusion, or cyber-induced accidents. In fact, in October 2013 it was announced that Russian nuclear command and control networks would be protected against cyber incursion and attacks by “special units” of the Strategic Missile Forces (Russia Today 2014). Other measures will include better network defences and firewalls, more sophisticated cryptographic codes, upgraded and better protected communications systems (including cables), extra redundancy, and better training and screening for the practitioners that operate these systems (see Ullman 2015). However, and while comprehensive reviews are underway to assess the vulnerabilities of current US and Russian nuclear systems to cyberattacks, it may well be that US and Russian C2 infrastructure becomes more vulnerable to cyber as it is modernised and old analogue systems are replaced with increasingly hi-tech digital platforms. As a result, and while nuclear weapons and command and control infrastructure are likely to be the best protected of all computer systems, and “air gapped”14 from the wider Internet – this does not mean they are invulnerable or will continue to be secure in the future, particularly as systems are modernised or become more complex (Fritz 2009). Or as Peggy Morse, ICBM systems director at Boeing, put it, “while its old it’s very secure” (quoted in Reed 2012).

#### Cyber attacks can’t undermine deterrence or touch NC3.

**Caylor ’16** [Matt, Feb, Command and Staff College, “THE CYBER THREAT TO NUCLEAR DETERRENCE”, <http://warontherocks.com/2016/02/the-cyber-threat-to-nuclear-deterrence/>]

The perception that cyber threats will ultimately undermine the relevance or effectiveness of nuclear deterrence is flawed in at least three keys areas. First among these is the perception that nuclear weapons or their command and control systems are similar to a heavily defended corporate network. The critical error in this analogy is that there is an expectation of IP-based availability that simply does not exist in the case of American nuclear weapons — they are not online. Even with physical access, the proprietary nature of their control system design and redundancy of the National Command and Control System (NCCS) makes the possibility of successfully implementing an exploit against either a weapon or communications system incredibly remote. Also, whereas the cyber domain is characterized by significant levels of risk due to a combination of bias toward automated safeguards and the liability of single human failures, nuclear weapon safety and surety are predicated on balanced elements of stringent human interaction and control. From two-person integrity in physical inspections and loading, to the rigorous mechanisms and authority required for weapons release, human beings serve as a multi-factor safeguard while retaining the ultimate role to protect the integrity of nuclear deterrence against cyber threats. To a large degree, the potential vulnerabilities caused by wireless communications and physical intrusions into areas holding nuclear material are already mitigated via secure communications that are not linked to the outside and multiple layers of physical security systems. While there has been a great deal of publicity surrounding the Y-12 break-in of 2012, the truth is that the three people involved never got near any nuclear material or technology. Without state-level resourcing in the billions of dollars, the technical sophistication required to pursue a Stuxnet-like attack against nuclear weapons is most likely beyond the capability of even the most gifted group of hackers. For all intents, this excludes terrorist organizations and cyber criminals from the field of threats and restricts it to those nations that already possess nuclear weapons. Nuclear-weapon states, however, have the full-spectrum cyber threat capability referenced in the Defense Science Board report and would most likely be influenced by an understanding of the elements of classic nuclear deterrence strategy. In the case of first strike, no cyber weapon could be expected to perform at a rate higher than any conventional anti-nuclear capability (i.e., not 100 percent effective). Therefore, an adversary’s nuclear threat would be perceived to endure, thereby negating and dissuading the effort to use and employ a cyber weapon against an adversary’s nuclear force. Additionally, just as missile defense systems have been historically controversial due to perceived destabilizing effects, it is reasonable to conclude that these nuclear-weapon states would view the attempt to deploy a cyber capability against their nuclear stockpiles from a similar perspective. Finally, the very existence of nuclear weapons is often enough to alter the risk analysis of an adversary. With virtually no chance of remote or unauthorized detonation (which would be the desired results of a sabotage event), the most probable cyber threat to any nuclear stockpile is that of espionage. Attempted cyber intrusions at the U.S. National Nuclear Security Agency (NNSA) and its efforts to bolster cybersecurity initiatives provide clear evidence that this is already underway. However, theft of design information or even more robust intelligence on the location of stored nuclear weapons cannot eliminate the potential destruction that even a handful of nuclear weapons can bring to an adversary. Knowledge alone, particularly the imperfect knowledge that cyber espionage is likely to offer, is incapable of drastically altering an adversary’s risk calculus. In fact, quite the opposite is true. An adversary with greater understanding of the nuclear capabilities of a rival is forced to consider courses of action to prevent escalation, potentially increasing the credibility of a state’s nuclear deterrence. Despite the growing sophistication in cyber capabilities and the willingness to use them for espionage or in concert with kinetic attack, the strategic value of nuclear weapons has not been diminished. The insulated architecture combined with a robust and redundant command-and-control system makes the existence of any viable cyber threat of exploitation extremely low. With the list of capable adversaries limited by both funding and motivation, it is highly unlikely that any nation will possess, or even attempt to develop, a cyber weapon sufficient to undermine the credibility of nuclear weapons. In both psychological and physical terms, the threat of the megabyte will never possess the ability to overshadow the destructive force of the megaton. Although the employment of cyberspace for military effect has brought new challenges to the international community, the role of nuclear weapons and their associated deterrence against open and unconstrained global aggression are as relevant now as they were in the Cold War.

### AT: NC3 Accidents---1NC

#### No accidents impact

**Quinlan 9** [Michael, Former Permanent Under-Sec. State – UK Ministry of Defense, “Thinking about Nuclear Weapons: Principles, Problems, Prospects”, p. 63-69]

Even if initial nuclear use did not quickly end the fighting, the supposition of inexorable momentum in a developing exchange, with each side rushing to overreaction amid confusion and uncertainty, is implausible. It fails to consider what the situation of the decisionmakers would really be. Neither side could want escalatio**n**. Both would be appalled at what was going on. Both would be desperately looking for signs that the other was ready to call a halt. Both, given the capacity for evasion or concealment which modem delivery platforms and vehicles can possess, could have in reserve significant forces invulnerable enough not to entail use-or-lose pressures. (It may be more open to question, as noted earlier, whether newer nuclearweapon possessors can be immediately in that position; but it is within reach of any substantial state with advanced technological capabilities, and attaining it is certain to be a high priority in the development of forces.) As a result, neither side can have any predisposition to suppose, in an ambiguous situation of fearful risk, that the right course when in doubt is to go on copiously launching weapons. And none of this analysis rests on any presumption of highly subtle or pre-concerted rationality. The rationality required is plain. The argument is reinforced if we consider the possible reasoning of an aggressor at a more dispassionate level. Any substantial nuclear armoury can inflict destruction outweighing any possible prize that aggression could hope to seize. A state attacking the possessor of such an armoury must therefore be doing so (once given that it cannot count upon destroying the armoury pre-emptively) on a judgement that the possessor would be found lacking in the will to use it. If the attacked possessor used nuclear weapons, whether first or in response to the aggressor's own first use, this judgement would begin to look dangerously precarious. There must be at least a substantial possibility of the aggressor leaders' concluding that their initial judgement had been mistaken—that the risks were after all greater than whatever prize they had been seeking, and that for their own country's , survival they must call off the aggression. Deterrence planning such as that of NATO was directed in the first place to preventing the initial misjudgement and in the second, if it were nevertheless made, to compelling such a reappraisal. The former aim had to have primacy, because it could not be taken for granted that the latter was certain to work. But there was no ground for assuming in advance, for all possible scenarios, that the chance of its working must be negligible. An aggressor state would itself be at huge risk if nuclear war developed, as its leaders would know. It may be argued that a policy which abandons hope of physically defeating theznemy and simply hopes to get him to desist is pure gamble, a matter of who blinks first; and that the political and moral nature of most likely aggressors, almost ex hypothesi, makes them the less likely to blink. One response to this is to ask what is the alternative—it can only be surrender. But a more positive and hopeful answer lies in the fact that the criticism is posed in a political vacuum. Real-life conflict would have a political context. The context which concerned NATO during the cold war, for example, was one of defending vital interests against a postlated aggressor whose own vital interests would not be engaged, or would be less engaged. Certainty is not possible, but a clear asymmetry of vital interest is a legitimate basis for expecting an asymmetry, credible to both sides, of resolve in conflict. That places upon statesmen, as page 23 has noted, the key task in deterrence of building up in advance a clear and shared grasp of where limits lie. That was plainly achieved in cold-war Europe. If vital interests have been defined in a way that is dear, and also clearly not overlapping or incompatible with those of the adversary, a credible basis has been laid for the likelihood of greater resolve in resistance. It was also sometimes suggested by critics that whatever might be indicated by theoretical discussion of political will and interests, the military environment of nuclear warfare—particularly difficulties of communication and control—would drive escalation with overwhelming probability to the limit. But it is obscure why matters should be regarded as inevitably .so for every possible level and setting of action. Even if the history of war suggested (as it scarcely does) that military decision-makers are mostly apt to work on the principle 'When in doubt, lash out', the nuclear revolution creates an utterly new situation. The pervasive reality, always plain to both sides during the cold war, is `If this goes on to the end, we are all ruined'. Given that inexorable escalation would mean catastrophe for both, it would be perverse to suppose them permanently incapable of framing arrangements which avoid it. As page 16 has noted, NATO gave its military commanders no widespread delegated authority, in peace or war, to launch nuclear weapons without specific political direction. Many types of weapon moreover had physical safeguards such as PALs incorporated to reinforce organizational ones. There were multiple communication and control systems for passing information, orders, and prohibitions. Such systems could not be totally guaranteed against disruption if at a fairly intense level of strategic exchange—which was only one of many possible levels of conflict— an adversary judged it to be in his interest to weaken political control. It was far from clear why he necessarily should so judge. Even then, however, it remained possible to operate on a general fail-safe presumption: no authorization, no use. That was the basis on which NATO operated. If it is feared that the arrangements which 1 a nuclear-weapon possessor has in place do not meet such standards in some respects, the logical course is to continue to improve them rather than to assume escalation to be certain and uncontrollable, with all the enormous inferences that would have to flow from such an assumption. The likelihood of escalation can never be 100 per cent, and never zero. Where between those two extremes it may lie can never be precisely calculable in advance; and even were it so calculable, it would not be uniquely fixed—it would stand to vary hugely with circumstances. That there should be any risk at all of escalation to widespread nuclear war must be deeply disturbing, and decision-makers would always have to weigh it most anxiously. But a pair of key truths about it need to be recognized. The first is that the risk of escalation to large-scale nuclear war is inescapably present in any significant armed conflict between nuclear-capable powers, whoever may have started the conflict and whoever may first have used any particular category of weapon. The initiator of the conflict will always have physically available to him options for applying more force if he meets effective resistance. If the risk of escalation, whatever its degree of probability, is to be regarded as absolutely unacceptable, the necessary inference is that a state attacked by a substantial nuclear power must forgo military resistance. It must surrender, even if it has a nuclear armoury of its own. But the companion truth is that, as page 47 has noted, the risk of escalation is an inescapable burden also upon the aggressor. The exploitation of that burden is the crucial route, if conflict does break out, for managing it, to a tolerable outcome--the only route, indeed, intermediate between surrender and holocaust, and so the necessary basis for deterrence beforehand. The working out of plans to exploit escalation risk most effectively in deterring potential aggression entails further and complex issues. It is for example plainly desirable, wherever geography, politics, and available resources so permit without triggering arms races, to make provisions and dispositions that are likely to place the onus of making the bigger, and more evidently dangerous steps in escalation upon the aggressor volib wishes to maintain his attack, rather than upon the defender. (The customary shorthand for this desirable posture used to be 'escalation dominance'.) These issues are not further discussed here. But addressing them needs to start from acknowledgement that there are in any event no certainties or absolutes available, no options guaranteed to be risk-free and cost-free. Deterrence is not possible without escalation risk; and its presence can point to no automatic policy conclusion save for those who espouse outright pacifism and accept its consequences. Accident and Miscalculation Ensuring the safety and security of nuclear weapons plainly needs to be taken most seriously. Detailed information is understandably not published, but such direct evidence as there is suggests that it always has been so taken in every possessor state, with the inevitable occasional failures to follow strict procedures dealt with rigorously. Critics have nevertheless from time to time argued that the possibility of accident involving nuclear weapons is so substantial that it must weigh heavily in the entire evaluation of whether war-prevention structures entailing their existence should be tolerated at all. Two sorts of scenario are usually in question. The first is that of a single grave event involving an unintended nuclear explosion—a technical disaster at a storage site, for example, Dr the accidental or unauthorized launch of a delivery system with a live nuclear warhead. The second is that of some event—perhaps such an explosion or launch, or some other mishap such as malfunction or misinterpretation of radar signals or computer systems—initiating a sequence of response and counter-response that culminated in a nuclear exchange which no one had truly intended. No event that is physically possible can be said to be of absolutely zero probability (just as at an opposite extreme it is absurd to claim**,** as has been heard from distinguished figures, that nuclear-weapon use can be guaranteed to happen within some finite future span despite not having happened for over sixty years). But human affairs cannot be managed to the standard of either zero or total probability. We have to assess levels between those theoretical limits and weigh their reality and implications against other factors, in security planning as in everyday life. There have certainly been, across the decades since 1945, many known accidents involving nuclear weapons, from transporters skidding off roads to bomber aircraft crashing with or accidentally dropping the weapons they carried (in past days when such carriage was a frequent feature of readiness arrangements----it no longer is). A few of these accidents may have released into the nearby environment highly toxic material. None however has entailed a nuclear detonation. Some commentators suggest that this reflects bizarrely good fortune amid such massive activity and deployment over so many years. A more rational deduction from the facts of this long experience would however be that the probability of any accident triggering a nuclear explosion is extremely low. It might be further noted that the mechanisms needed to set off such an explosion are technically demanding, and that in a large number of ways the past sixty years have seen extensive improvements in safety arrangements for both the design and the handling of weapons. It is undoubtedly possible to see respects in which, after the cold war, some of the factors bearing upon risk may be new or more adverse; but some are now plainly less so. The years which the world has come through entirely without accidental or unauthorized detonation have included early decades in which knowledge was sketchier, precautions were less developed, and weapon designs were less ultra-safe than they later became, as well as substantial periods in which weapon numbers were larger, deployments more widespread and diverse, movements more frequent, and several aspects of doctrine and readiness arrangements more tense. Similar considerations apply to the hypothesis of nuclear war being mistakenly triggered by false alarm. Critics again point to the fact, as it is understood, of numerous occasions when initial steps in alert sequences for US nuclear forces were embarked upon, or at least called for, by, indicators mistaken or misconstrued. **In** none of these instances, it is accepted, did matters get at all near to nuclear launch--extraordinary good fortune again, critics have suggested. But the rival and more logical inference from hundreds of events stretching over sixty years of experience presents itself once more: that the probability of initial misinterpretation leading far towards mistaken launch is remote. Precisely because any nuclear-weapon possessor recognizes the vast gravity of any launch, release sequences have many steps, and human decision is repeatedly interposed as well as capping the sequences. To convey that because a first step was prompted the world somehow came close to accidental nuclear war is wild hyperbole, rather like asserting, when a tennis champion has lost his opening service game, that he was nearly beaten in straight sets. History anyway scarcely offers any ready example of major war started by accident even before the nuclear revolution imposed an order-of-magnitude increase in caution. It was occasionally conjectured that nuclear war might be triggered by the real but accidental or unauthorized launch of a strategic nuclear-weapon delivery system in the direction of a potential adversary. No such launch is known to have occurred in over sixty years. The probability of it is therefore very low. But even if it did happen, the further hypothesis of it initiating a general nuclear exchange is far-fetched. It fails to consider the real situation of decision-makers as pages 63-4 have brought out. The notion that cosmic holocaust might be mistakenly precipitated in this way belongs to science fiction.

### AT: NC3 Accidents---2NC

#### No accidents---BUT even if, no escalation

Steven **Pinker 18**. Johnstone Family Professor in the Department of Psychology at Harvard University. 2018. “CHAPTER 19 EXISTENTIAL THREATS.” Enlightenment Now: The Case for Reason, Science, Humanism, and Progress, Viking, an imprint of Penguin Random House LLC.

The first is to stop telling everyone they’re doomed. The fundamental fact of the nuclear age is that no atomic weapon has been used since Nagasaki. If the hands of a clock point to a few minutes to midnight for seventy-two years, something is wrong with the clock. Now, maybe the world has been blessed with a miraculous run of good luck—no one will ever know—but before resigning ourselves to that scientifically disreputable conclusion, we should at least consider the possibility that systematic features of the international system have worked against their use. Many antinuclear activists hate this way of thinking because it seems to take the heat off countries to disarm. But since the nine nuclear states won’t be scuppering their weapons tomorrow, it behooves us in the meantime to figure out what has gone right, so we can do more of whatever it is. Foremost is a historical discovery summarized by the political scientist Robert Jervis: “The Soviet archives have yet to reveal any serious plans for unprovoked aggression against Western Europe, not to mention a first strike against the United States.”89 That means that the intricate weaponry and strategic doctrines for nuclear deterrence during the Cold War—what one political scientist called “nuclear metaphysics”—were deterring an attack that the Soviets had no interest in launching in the first place.90 When the Cold War ended, the fear of massive invasions and preemptive nuclear strikes faded with it, and (as we shall see) both sides felt relaxed enough to slash their weapon stockpiles without even bothering with formal negotiations.91 Contrary to a theory of technological determinism in which nuclear weapons start a war all by themselves, the risk very much depends on the state of international relations. Much of the credit for the absence of nuclear war between great powers must go to the forces behind the decline of war between great powers (chapter 11). Anything that reduces the risk of war reduces the risk of nuclear war. The close calls, too, may not depend on a supernatural streak of good luck. Several political scientists and historians who have analyzed documents from the Cuban Missile Crisis, particularly transcripts of John F. Kennedy’s meetings with his security advisors, have argued that despite the participants’ recollections about having pulled the world back from the brink of Armageddon, “the odds that the Americans would have gone to war were next to zero.”92 The records show that Khrushchev and Kennedy remained in firm control of their governments, and that each sought a peaceful end to the crisis, ignoring provocations and leaving themselves several options for backing down. The hair-raising false alarms and brushes with accidental launches also need not imply that the gods smiled on us again and again. They might instead show that the human and technological links in the chain were predisposed to prevent catastrophes, and were strengthened after each mishap.93 In their report on nuclear close calls, the Union of Concerned Scientists summarizes the history with refreshing judiciousness: “The fact that such a launch has not occurred so far suggests that safety measures work well enough to make the chance of such an incident small. But it is not zero.”94 Thinking about our predicament in this way allows us to avoid both panic and complacency. Suppose that the chance of a catastrophic nuclear war breaking out in a single year is one percent. (This is a generous estimate: the probability must be less than that of an accidental launch, because escalation from a single accident to a full-scale war is far from automatic, and in seventytwo years the number of accidental launches has been zero.)95 That would surely be an unacceptable risk, because a little algebra shows that the probability of our going a century without such a catastrophe is less than 37 percent. But if we can reduce the annual chance of nuclear war to a tenth of a percent, the world’s odds of a catastrophe-free century increase to 90 percent; at a hundredth of a percent, the chance rises to 99 percent, and so on.

#### No miscalc or accidents---statistics, human prudence, and safety mechanisms

**Tertrais 17**—Deputy Director at the Paris-based Fondation pour la Recherche Stratégique (Foundation for Strategic Research) and a member of the editorial board of The Washington Quarterly [Bruno, Summer 2017, ““On The Brink”—Really? Revisiting Nuclear Close Calls Since 1945”, The Washington Quarterly • 40:2 pp. 51–66 <https://doi.org/10.1080/0163660X.2017.1328922>, edited for gendered language denoted by brackets]

Why have nuclear weapons not been used since 1945? The more time passes, the more the question becomes relevant and even puzzling for pessimists. Most strategists of the 1960s would be stunned to hear that as of 2017, there still has yet to be another nuclear use in anger. The prospects of a “nuclear weapons ban” or recurring proposals for “de-alerting”—instituting changes that can lengthen the time required to actually use the weapons—make the question even more relevant. Has mankind [humanity] really stood “on the brink” several times since Nagasaki, and have we avoided nuclear catastrophe mostly because of pure “luck”? 1 Recent books, articles, and reports, as well as two wide-audience documentaries, say yes.2 This is not the case. The absence of any deliberate nuclear explosion (except for testing) since 1945 can simply be explained by human prudence and the efficiency of mechanisms devoted to the guardianshipof nuclear weapons. Banning nuclear weapons may or may not be a good idea. But it should not be based on the myth of an inherently and permanently high risk of nuclear use. The analysis that follows covers the deliberate use of nuclear weapons by a legitimate authority, either by error (“false alarm”) or not (“nuclear crisis”). It does not cover the risk of an accidental nuclear explosion, an unauthorized launch, or a terrorist act.3 It covers 37 different known episodes, including 25 alleged nuclear crises and twelve technical incidents, which have been mentioned in the literature to one degree or another as potentially dangerous.4 The short answer? If we are to discard Pope John Paul II’s explanation (“Divine Providence”),5 it is that the system worked and that, with rare exceptions,those in charge of nuclear weapons have been responsible, prudent, and careful. “Close calls” have ranged in fact from “not-so-close” to “very distant.” False Alarms A number of technical incidents have taken place since 1945, all of which led to one degree or another to nuclear precautionary measures, generally involving the elevation of alert levels. Most of these incidents are well documented, but one of them does not seem to have taken place at all. It was revealed in 2015 that in the midst of the Cuban Missile Crisis, a Mace missile squadron based in Okinawa received a launch order.6 The ambassador of a Latin American country to the United Nations claimed that this incident “could have altered the course of civilization forever.” 7 One should note that according to the account—based on a single testimony—the safeguards worked: given that the procedure was not respected (the order came at DEFCON-2, whereas it was supposed to happen only at DEFCON-1), the unit commander suspended the launch.8 In any case, an in-depth inquiry by Stars & Stripes magazine at the end of 2015 did not find any confirmation of the incident; U.S. Air Force historians did not find any trace of it.9 At least a dozen real incidents took place in the United States in the 1960s, 1970s, and 1980s. (Even though there is little or no evidence that as many happened in other countries, one should assume that some also occurred in the Soviet Union or elsewhere.)10 In these cases, alert levels were elevated due to a false alarm, generally caused by the malfunction of a technical system. For instance, in 1960 a U.S. early warning radar in Greenland confused the moonrise with a missile launch.11 In 1961, a dysfunctional transmitter made the Strategic Air Command (SAC) believe that its lines of communication had been cut off.12 In 1962, a cascade of minor incidents and misinterpretation led to bombers being put on alert.13 The same year, a rare conjunction of events led a U.S. radar station to believe that a Soviet missile attack was underway.14 Something similar occurred in 1967, when a solar storm jammed three early warning radars.15 In 1980, two incidents caused by faulty computer chips led U.S. authorities to mistakenly believe that a Soviet attack could be underway.16 In the Soviet Union, a well-known 1983 incident of the same sort was recently publicized through a documentary entitled The Man Who Saved The World (2014), according to which “millions of lives were hanging by a thread,” and no less than “the end of our civilization” was at stake.17 A more sobering account of the incident casts serious doubts on whether this was actually the case. When the alarm sounded in the Soviet nuclear command center because of a U.S. missile launch, the officer in charge suspected that it was a mistake and requested visual confirmation. Such confirmation never came, and the command thus stood down.18 Some incidents involve direct human errors. This was the case for the infamous magnetic tape mistake of 1979, which went up the chain of command to the U.S. presidency. Woken up by a phone call announcing that 200 missiles were coming in the direction of U.S. territory, National Security Advisor Zbigniew Brzezinski requested a confirmation.19 He was informed a couple of minutes later that ten times that number of missiles had now been detected. The cause was the insertion of a tape used for training and exercises in SAC computers. Nobody knows what President Jimmy Carter would have done had Brzezinski told him that he only had a few minutes to decide, but can one seriously believe that he would have launched a massive counter-strike in the absence of any confirmation that an attack was underway? In a few of these incidents, a real launch caused confusion. In 1980, for instance, the Soviet Union launched four submarine-launched ballistic missiles (SLBMs) as part of an exercise, and a U.S. early warning radar wrongly judged that one of them was going in the direction of the United States. This evaluation was quickly corrected.20 The Norwegian rocket launch of 1995 belongs in the same category and has become another poster child for nuclear dangers. However, the episode should rather be taken as a testimony to Russian cool-headedness. Norwegian and American scientists launched a new type of rocket, the Black Brant XII, in order to study weather data; they had sent word of the launch to Moscow, but the information had not reached the appropriate authorities. Since Black Brant XII was new, large, and with a high-altitude trajectory, its launch was interpreted as a possible missile strike. Some in the general staff raised the hypothesis of a highaltitude electro-magnetic pulse (EMP) detonation. Yeltsin considered an interception, but it soon became clear that Russia was not a target. “After the rocket emerged onto a ballistic curve, the direction of the flight became clear, and we could see that it would in no way touch on Russian territory, but land in the Spitsbergen region—we calmed down and took no serious measures … ”21 Generals Vladimir Dvorkin, a well-known Russian expert, and Eugene Habiger, former head of STRATCOM, denied that the incident had any character of gravity.22 The System Worked Based on the above examples, one must wonder: is luck a necessary hypothesis to explain why none of these events led to nuclear war? Is it not at least equally possible that since 1945, people in charge of nuclear weapons “have taken greater care [of them] than is taken in any other situation involving human agents and complex mechanical systems”? 23 Nuclear-armed countries have set up mechanisms designed to ensure that nuclear weapons will not be used by mistake. This includes fail-safe procedures (where non-use remains the default condition up until the last possible moment) as well as dual phenomenology(the need to confirm the attack by two independent means relying on different physical principles). When The Man Who Saved The World was shown in New York City, the Russian mission to the United Nations issued a communiqué that stated: “Under no circumstances a decision to use nuclear weapons could be made or even considered in the Soviet Union (Russia) or in the United States on the basis of data from a single source or a system. For this to happen, a confirmation is necessary from several systems: ground-based radars, early-warning satellites, intelligence reports, etc.” 24 In all the incidents mentioned above, safety mechanisms worked, even in the early 1960s when they were still rudimentary. Furthermore, is it credible to imagine that the head of a State or government would order a nuclear strike without being certain that a major military attack was underway? U.S. nuclear expert Jeffrey G. Lewis rightly argues that he cannot imagine that an American president would embark in nuclear reprisals if there was the slightest doubt on the reality of the attack.25 Retired Russian General Vladimir Dvorkin thinks similarly, claiming that “No president, no matter what president it is, will ever make a decision about launch-onwarning based on information about one rocket or missile or even … two or three missiles.” 26 From the point of view of logic and complex systems analysis, it remains possible that a combination of incidents can lead to the failure of all safety mechanisms designed to prevent accidental nuclear war. Such a thesis is embodied by the classic work of Scott D. Sagan, The Limits of Safety. It would thus only be “a matter of time” due to cumulative probabilities.27 In a recent documentary about nuclear risks, author Eric Schlosser reiterates the point: “it’s also due to luck, pure luck, and the problem with luck is that eventually it runs out … Every machine ever invented eventually goes wrong.” 28 But the probability of failure increases markedly with time only if conditions do not change—and conditions do change. Safety mechanisms have been perfected (without necessarily becoming more complex) and lessons of past incidents are being learned. Sagan claimed in 1993 that the Yom Kippur war (see below), as well as the 1979 and 1980 incidents (see above), are proof that organizations fail to learn from experience. But if that was the case, why would the number of known incidents have significantly declined since 1983? We only know of one significant incident in nearly 35 years: the Black Brant XII episode. Charles Perrow, the father of “normal accidents” theory (those resulting from the complexity and interconnection of systems), wrote: “with regard to firing [nuclear weapons] after a false warning we reach a surprising conclusion, one I was not prepared for: because of the safety systems involved in a launchon-warning scenario, it is virtually impossible for wellintended actions to bring about an accidental attack.” 29

#### No accidents—safeguards and ocean targeting

**Slocombe 9** [Walter, senior advisor for the Coalition Provisional Authority in Baghdad and a former Under Secretary of Defense for Policy, he is a four-time recipient of an award for Distinguished Public Service and a member of the Council on Foreign Relations, “De-Alerting: Diagnoses, Prescriptions, and Side-Effects,” Presented at the seminar on Re-framing De-Alert: Decreasing the Operational Readiness of Nuclear Weapons Systems in the US-Russia Context in Yverdon, Switzerland, June 21-23]

Let’s start with Technical Failure – the focus of a great deal of the advocacy, or at least of stress on past incidents of failures of safety and control mechanisms.4 Much of the “de-alerting” literature points to a succession of failures to follow proper procedures and draw from that history the inference that a relatively simple procedural failure could produce a nuclear detonation. The argument is essentially that nuclear weapons systems are sufficiently susceptible of pure accident (including human error or failure at operational/field level) that it is essential to take measures that have the effect of making it necessary to undertake a prolonged reconfiguration of the elements of the nuclear weapons force for a launch or detonation to be physically possible. Specific measures said to serve this objective include separating the weapons from their launchers, burying silo doors, removal of fuzing or launching mechanisms, deliberate avoidance of maintenance measures need to permit rapid firing, and the like. . My view is that this line of action is unnecessary in its own terms and highly problematic from the point of view of other aspects of the problem and that there is a far better option that is largely already in place, at least in the US force – the requirement of external information – a code not held by the operators -- to arm the weapons Advocates of other, more “physical,” measures often describe the current arrangement as nuclear weapons being on a “hair trigger.” That is – at least with respect to US weapons – a highly misleading characterization. The “hair trigger” figure of speech confuses “alert” status – readiness to act quickly on orders -- with susceptibility to inadvertent action. The “hair trigger” image implies that a minor mistake – akin to jostling a gun – will fire the weapon. The US StratCom commander had a more accurate metaphor when he recently said that US nuclear weapons are less a pistol with a hair trigger than like a pistol in a holster with the safety turned on – and he might have added that in the case of nuclear weapons the “safety” is locked in place by a combination lock that can only be opened and firing made possible if the soldier carrying the pistol receives a message from his chain of command giving him the combination. Whatever other problems the current nuclear posture of the US nuclear force may present, it cannot reasonably be said to be on a “hair trigger.” Since the 1960s the US has taken a series of measures to insure that US nuclear weapons cannot be detonated without the receipt of both external information and properly authenticated authorization to use that information. These devices – generically Permissive Action Links or “PALs” – are in effect combination locks that keep the weapons locked and incapable of detonation unless and until the weapons’ firing mechanisms have been unlocked following receipt of a series of numbers communicated to the operators from higher authority. Equally important in the context of a military organization, launch of nuclear weapons (including insertion of the combinations) is permitted only where properly authorized by an authenticated order. This combination of reliance on discipline and procedure and on receipt of an unlocking code not held by the military personnel in charge of the launch operation is designed to insure that the system is “fail safe,” i.e., that whatever mistakes occur, the result will not be a nuclear explosion. Moreover, in recent years, both the US and Russia, as well as Britain and China, have modified their procedures so that **even if** a nuclear-armed missile were **launched**, it would go not to a “real” target in another country but – at least in the US case - to empty ocean. In addition to the basic advantage of insuring against a nuclear detonation in a populated area, the fact that a missile launched in error would be on flight path that diverged from a plausible attacking trajectory should be detectable by either the US or the Russian warning systems, reducing the possibility of the accident being perceived as a deliberate attack. De-targeting, therefore, provides a significant protection against technical error. These arrangements – PALs and their equivalents coupled with continued observance of the agreement made in the mid-90s on “de-targeting” – do not eliminate the possibility of technical or operator-level failures, but they come very close to providing absolute assurance that such errors cannot lead to a nuclear explosion or be interpreted as the start of a deliberate nuclear attack.6 The advantage of such requirements for external information to activate weapons is of course that the weapons remain available for authorized use but not susceptible of appropriation or mistaken use.

### AT: Grid---2NC

#### No blackouts

**Larson 18** Selena Larson, Cyber threat intelligence analyst at Dragos, Inc. [Threats to Electric Grid are Real; Widespread Blackouts are Not, 8-6-2018, https://dragos.com/blog/industry-news/threats-to-electric-grid-are-real-widespread-blackouts-are-not/]

The US electric grid is not about to go down. Though it’s understandable if someone believed that. Over the last few weeks, numerous media reports suggest state-backed hackers have infiltrated the US electric grid and are capable of manipulating the flow of electricity on a grand scale and cause chaos. Threats against industrial sectors including electric utilities, oil and gas, and manufacturing are growing, and it’s reasonable for people to be concerned. But to say hackers have invaded the US electric grid and are prepared to cause blackouts is false. The initial reporting stemmed from a public Department of Homeland Security (DHS) presentation in July on Russian hacking activity targeting US electric utilities. This presentation contained previously-reported information on a group known as Dragonfly by Symantec and which Dragos associates to activity labeled DYMALLOY and ALLANITE. These groups focus on information gathering from industrial control system (ICS) networks and have not demonstrated disruptive or damaging capabilities. While some news reports cite 2015 and 2016 blackouts in Ukraine as evidence of hackers’ disruptive capabilities, DYMALLOY nor ALLANITE were involved in those incidents and it is inaccurate to suggest the DHS’s public presentation and those destructive behaviors are linked. Adversaries have not placed “cyber implants” into the electric grid to cause blackouts; but they are infiltrating business networks – and in some cases, ICS networks – in an effort to steal information and intelligence to potentially gain access to operational systems. Overall, the activity is concerning and represents the prerequisites towards a potential future disruptive event – but evidence to date does not support the claim that such an attack is imminent. The US electric grid is resilient and segmented, and although it makes an interesting plot to an action movie, one or two strains of malware targeting operational networks would not cause widespread blackouts. A destructive incident at one site would require highly-tailored tools and operations and would not effectively scale. Essentially, localized impacts are possible, and asset owners and operators should work to defend their networks from intrusions such as those described by DHS. But scaling up from isolated events to widespread impacts is highly unlikely.

#### Backups solve

**IBEW 14** – (2014, International Brotherhood of Elctricial Workers, <http://www.ibew.org/IBEW/departments/utility/IBEW-Nuclear-FAQ.pdf> The International Brotherhood of Electrical Workers (IBEW) represents approximately 750,000 active members and retirees who work in a wide variety of fields, including utilities, construction, telecommunications, broadcasting, manufacturing, railroads and government. The IBEW has members in both the United States and Canada and stands out among the American unions in the AFL-CIO because it is among the largest and has members in so many skilled occupations.

Some of the units at the Japanese plants lost both off - site power and diesel generators. This is called a “station blackout.” U.S. nuclear power plants are designed to cope with station blackouts by having multiple back - up power sources at the ready. All U.S. plants are also responsible for demonstrating to the NRC that they can handle such situations in order to legally remain in operation.

### AT: Military Impact---2NC

#### Military grid access is inevitable

Michael **Aimone 12**, Director, Business Enterprise Integration, Office of the Deputy Under Secretary of Defense (Installations and Environment), 9/12/12, Statement Before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Aimone.pdf

DoD’s facility energy strategy is also focused heavily on grid security in the name of mission assurance. Although the Department’s fixed installations traditionally served largely as a platform for training and deployment of forces, in recent years they have begun to provide direct support for combat operations, such as unmanned aerial vehicles (UAVs) flown in Afghanistan from fixed installations here in the United States. Our fixed installations also serve as staging platforms for humanitarian and homeland defense missions. These installations are largely dependent on a commercial power grid that is vulnerable to disruption due to aging infrastructure, weather-related events, and potential kinetic, cyber attack. In 2008, the Defense Science Board warned that DoD’s reliance on a fragile power grid to deliver electricity to its bases places critical missions at risk.1

Standby Power Generation

Currently, DoD ensures that it can continue mission critical activities on base largely through its fleet of on-site power generation equipment. This equipment is connected to essential mission systems and automatically operates in the event of a commercial grid outage. In addition, each installation has standby generators in storage for repositioning as required. Facility power production specialists ensure that the generators are primed and ready to work, and that they are maintained and fueled during an emergency. With careful maintenance these generators can bridge the gap for even a lengthy outage. As further back up to this installed equipment, DoD maintains a strategic stockpile of electrical power generators and support equipment that is kept in operational readiness. For example, during Hurricane Katrina, the Air Force transported more than 2 megawatts of specialized diesel generators from Florida, where they were stored, to Keesler Air Force Base in Mississippi, to support base recovery.

#### Squo solves military grid dependence

Andrew **Holland 13**, American Security Project. With Nick Cunningham, Kaitlyn Huppmann, and William Joyce. July. “Powering Military Bases: DoD’s Installation Energy Efforts” https://www.americansecurityproject.org/ASP%20Reports/Ref%200128%20-%20DoD%20Installation%20Energy%20Fact%20Sheet.pdf

How Can the Military Alleviate These Threats?

• DoD plans to scale up renewable energy and energy storage on bases.

• By using distributed generation, bases will be able to “island” – or separate – bases from the commercial power grid in the event of a supply disruption.

• As of now, the “microgrids” that will allow this are not widespread, but they will mark a cornerstone of DoD’s efforts at improving energy security for its installations.

3

• By the end of FY2011, DoD had a total of 44 installations in the U.S. with plans for microgrids, or that have conducted microgrid studies or demonstrations.10

• These microgrids range from demand response and small solar PV arrays that work in conjunction with the commercial grid, to higher concentrations of solar PV with energy storage that can separate from the commercial grid when necessary.

The Role of Microgrids in Improving Energy Security

• Advanced microgrids with renewable energy can enhance energy security and help assure mission effectiveness in the event of power interruptions or demand surges.11

• Today, no bases operate using solely renewable energy. With a microgrid, renewable energy with energy storage can significantly extend islanding time in the event of a power outage.

• If power is cut off to an installation, microgrids can automatically prioritize mission critical activities, and shed less important uses of power.

• Microgrids can also improve the resiliency of the civilian power grid by allowing military bases to automatically shut down non-critical systems during commercial demand spikes. This would allow utilities greater flexibility in managing power loads.

What Has DoD Done So Far?

The Energy Independence and Security Act of 2007 requires the federal government – including DoD facilities – to reduce energy use in its buildings by 30% by FY2015.12 The John Warner National Defense Authorization Act for Fiscal Year 2007 mandates DoD obtain 25% of its electricity from renewable sources by 2025.13 In 2012, the Defense Department made a commitment to install 3 gigawatts of renewable generating capacity, one from each of the Army, Navy, and Air Force Installations by 2025.14

#### DOD’s aware of grid reliance risks and doing everything they can to resolve it

Paul **Stockton 11**, Assistant Secretary of Defense, Homeland Defense and Americas’ Security Affairs, 5/31/11, Testimony Before the Subcommittee on Energy and Power, The Committee on Energy and Commerce, United States House of Representatives, http://policy.defense.gov/portals/11/Documents/hdasa/ASD(HDASA)\_HECC-EPS\_053111.pdf

The Department of Defense fully recognizes the strategic importance of mitigating the growing risks to the commercial electric power grid, and therefore, the Department is taking affirmative steps internally and externally. Senior leaders are re-focusing some of the Department’s energy security efforts.

Although there are steps the Department can and should take on its own to improve resilience and continuity of operations, achieving more comprehensive electric grid security to ensure critical Department of Defense missions is not something the Department of Defense can do acting alone. Meeting and securing the Department of Defense’s critical electric power needs in an interdependent and increasingly complex risk environment requires a broad scope of collaborative engagement between government and industry stakeholders whose roles and responsibilities in power grid security and resiliency are distributed and shared. While there are maintenance and on-site power surety efforts that need some new focus, for the Department of Defense to succeed in this challenge, leadership and support from industry representatives and interagency partners at various levels of government are imperative.

The Department of Defense is collaborating with the Department of Energy, the Department of Homeland Security, the Federal Energy Regulatory Commission and industry representatives, namely the North American Electric Reliability Corporation, in these matters. For example, we are planning to develop a combined kinetic and cyber threat-based scenario for the U.S. electric power grid that could be applied on a regional scale throughout the country and be used to support the development of a new system "design basis" for building additional resilience in the U.S. electric power grid. We are also working with the North American Electric Reliability Corporation on planning a case study of a military installation for analysis, paired up with the local utility provider to determine what can be done in the short-term to mitigate electric power vulnerabilities and risks. The Department is also participating in exercises such as the recent National Level Exercise-11 exercise and upcoming Departments of Homeland Security, Energy and Defense sponsored Secure Grid 2011 and the North American Electric Reliability Corporation’s GridEx 2011.

These partnerships will help the Department of Defense achieve greater energy grid security and resiliency and help mitigate the risks to critical Department of Defense installations and facilities of commercial power outages.

Department of Defense Efforts Underway

The Department of Defense is making organizational changes and capability improvements that address electric power reliability and security issues and that enable better risk-informed decision-making and investments.

This year the Department of Defense submitted a report to Congress under Section 335 of the 2009 National Defense Authorization Act. Section 335 requires the Department to submit an annual report to Congress on efforts to mitigate the risks posed to Department of Defense mission critical installations, facilities, and activities by extended power outages resulting from failure of the commercial electricity supply or grid and related infrastructure. Congress enacted Section 335 of the National Defense Authorization Act in response to the publication of a 2008 Report by the Defense Science Board on the Department of Defense Energy Strategy, titled “More Fight, Less Fuel.” The report found that “critical national security and homeland defense missions are at an unacceptably high risk of extended outage from failure of the [commercial electrical power] grid” upon which Department of Defense overwhelmingly relies for its electrical power supplies.1

I would like to highlight several Department of Defense initiative that serve to foster improvements in electric grid security.

### AT: Nuclear Meltdowns---1NC

#### No meltdowns impact.

Shellenberger 19 Michael Shellenberger, author, environmental policy writer, cofounder of Breakthrough Institute and founder of Environmental Progress, Time Magazine “Hero of the Environment.” [It Sounds Crazy, But Fukushima, Chernobyl, And Three Mile Island Show Why Nuclear Is Inherently Safe, 3-11-19, https://www.forbes.com/sites/michaelshellenberger/2019/03/11/it-sounds-crazy-but-fukushima-chernobyl-and-three-mile-island-show-why-nuclear-is-inherently-safe/#5b4a65ff1688]

But now, eight years after Fukushima, the best-available science clearly shows that Caldicott’s estimate of the number of people killed by nuclear accidents was off by one million. Radiation from Chernobyl will kill, at most, 200 people, while the radiation from Fukushima and Three Mile Island will kill zero people. In other words, the main lesson that should be drawn from the worst nuclear accidents is that nuclear energy has always been inherently safe. The truth about nuclear power’s safety is so shocking that it’s worth taking a closer look at the worst accidents, starting with the worst of the worst: Chernobyl. The nuclear plant is in Ukraine which, in 1986, the year of the accident, was a Soviet Republic. Operators lost control of an unauthorized experiment that resulted in the reactor catching fire. There was no containment dome, and the fire spewed out radioactive particulate matter, which went all over the world, leading many to conclude that Chernobyl is not just the worst nuclear accident in history but is also the worst nuclear accident possible. Twenty-eight firefighters died after putting out the Chernobyl fire. While the death of any firefighter is tragic, it’s worth putting that number in perspective. Eighty-six firefighters died in the U.S. in 2018, and 343 firefighters died during the September 11, 2001 terrorist attacks. Since the Chernobyl accident, 19 first responders have died, according to the United Nations, for ”various reasons” including tuberculosis, cirrhosis of the liver, heart attacks, and trauma. The U.N. concluded that “the assignment of radiation as the cause of death has become less clear.” What about cancer? By 2065 there may be 16,000 thyroid cancers; to date there have been 6,000. Since thyroid cancer has a mortality rate of just one percent — it is an easy cancer to treat — expected deaths may be 160. The World Health Organization claims on its web site that Chernobyl could result in the premature deaths of 4,000 people, but according to Dr. Geraldine Thomas, who started and runs the Chernobyl Tissue Bank, that number is based on a disproven methodology. “That WHO number is based on LNT,” she explained, using the acronym for the “linear no-threshold” method of extrapolating deaths from radiation. LNT assumes that there is no threshold below which radiation is safe, but that assumption has been discredited over recent decades by multiple sources of data. Support for the idea that radiation is harmless at low levels comes from the fact that people who live in places with higher background radiation, like Colorado, do not suffer elevated rates of cancer. In fact, residents of Colorado, where radiation is higher because of high concentrations of uranium in the ground, enjoy some of the lowest cancer rates in the U.S. Even relatively high doses of radiation cause far less harm than most people think. Careful, large, and long-term studies of survivors of the atomic bombings of Hiroshima and Nagasaki offer compelling demonstration. Cancer rates were just 10 percent higher among atomic blast survivors, most of whom never got cancer. Even those who received a dose 1,000 times higher than today’s safety limit saw their lives cut short by an average of 16 months. But didn’t the Japanese government recently award a financial settlement to the family of a Fukushima worker who claimed his cancer was from the accident? It did, but for reasons that were clearly political, and having to do with the Japanese government’s consensus-based, conflict-averse style, as well as lingering guilt felt by elite policymakers toward Fukushima workers and residents, who felt doubly aggrieved by the tsunami and meltdowns. The worker’s cancer was highly unlikely to have come from Fukushima because, once again, the level of radiation workers received was far lower than the ones received by the Hiroshima/Nagasaki cohort that saw (modestly) higher cancer rates. What about Three Mile Island? After the accident in 1979, Time Magazine ran a cover story that superimposed a glowing headline, “Nuclear Nightmare,” over an image of the plant. Nightmare? More like a dream. What other major industrial technology can suffer a catastrophic failure and not kill anyone? Remember when the Deepwater Horizon oil drilling rig caught on fire and killed 11 people? Four months later, a Pacific Gas & Electric natural gas pipeline exploded just south of San Francisco and killed eight people sleeping in their beds. And that was just one year, 2010. The worst energy accident of all time was the 1975 collapse of the Banqiao hydroelectric dam in China. It collapsed and killed between 170,000 and 230,000 people. Nuclear’s worst accidents show that the technology has always been safe for the same, inherent reason that it has always had such a small environmental impact: the high energy density of its fuel. Splitting atoms to create heat, rather than than splitting chemical bonds through fire, requires tiny amounts of fuel. A single Coke can of uranium can provide enough energy for an entire high-energy life. When the worst occurs, and the fuel melts, the amount of particulate matter that escapes from the plant is insignificant in contrast to both the fiery explosions of fossil fuels and the daily emission of particulate matter from fossil- and biomass-burning homes, cars, and power plants, which kill seven million people a year. It's not that nuclear energy never kills. It's that nuclear's death toll is vanishingly small. Consider nuclear's global death toll in context. These are just annual deaths. - walking: 270,000 - driving: 1,350,000 - working: 2,300,000 - air pollution: 4,200,000 By contrast, nuclear's death total is likely to be around 200.

Dsa

### AT: Nuclear Meltdowns---2NC

#### No meltdowns and no impact to them

**Bradley 16** Arthur T. Bradley, PhD in electrical engineering, works at NASA. [Would a Long-Term Blackout Mean Nuclear Meltdown? The Survival Mom blog, 2-21-2016, <http://thesurvivalmom.com/long-term-blackout-nuclear-meltdown/>]//BPS

Worst-case power-loss scenario With backup systems to the backup systems, it would seem that there’s nothing to worry about, right? Under all but the direst of circumstances, I think that assessment is correct. However, one could imagine a scenario in which the grid was lost and the diesel generators ran out of fuel. Speaking of fuel, how much is actually stored onsite? It depends on the plant, but at the Watts Bar Nuclear Plant, for example, there is enough fuel to run the emergency diesel generators for at least 42 days. I say at least because it would depend on exactly what was being powered. Once the reactor was cooled down, a much smaller system, known as the Residual Heat Removal System, would be all that was required to keep the fuel assemblies cool, both in the reactor and the spent fuel rods pool. The generators and onsite fuel supply could power that smaller cooling system for significantly longer than if they were powering the larger reactor cooling system. Even if we assumed a worst case of 42 days, it’s hard to imagine a scenario in which that would not be enough time to bring in additional fuel either by land, water, or air. Nonetheless, let’s push the question a little further. What would happen in the unlikely event that the diesel fuel was exhausted? Even with the reactor having been successfully cooled, the biggest risk would continue to be overheating of the fuel rod assemblies, both in the reactor and the spent fuel rods pool. Without circulation, the heat from the fuel rod assemblies could boil the surrounding water, resulting in steam. In turn, the water levels would drop, ultimately exposing the fuel rods to air. Once exposed to air, their temperatures would rise but not to the levels that would melt the zirconium cladding. Thankfully, that means that meltdown would not occur. The steam might well carry radioactive contaminants into the air, but there would be no release of hydrogen and, thus, no subsequent explosions. The situation would certainly be dangerous to surrounding communities, but it wouldn’t be the nuclear Armageddon that many people worry about.

#### No meltdowns impact, and evacuation solves

Tiffany **Kaiser 11**, writer for Daily Tech, citing Nuclear Regulatory Commission Report, 8/2/2011, DailyTech, "NRC: Far Fewer People Would Die in a U.S. Nuclear Meltdown Than Previously Thought," http://www.dailytech.com/NRC+Far+Fewer+People+Would+Die+in+a+US+Nuclear+Meltdown+Than+Previously+Thought/article22330.htm

The nuclear crisis at Fukushima Daiichi in Japan has caused a nuclear frenzy where leaders around the world are questioning the safety of their plants. For instance, French President Nicolas Sarkozy called for global nuclear review after visiting Japan, and U.S. senators demanded that the Nuclear Regulatory Commission (NRC) repeat an expensive inspection of the country's nuclear power.¶ But now, the NRC is close to completing a large nuclear study that may ease a few worried minds.¶ The NRC has been working with Sandia National Laboratories (a Department of Energy lab) on a study that revises previous projections of how quickly and how much cesium 137, which is a radioactive material made when uranium is split, could release from a plant after a nuclear core meltdown. The NRC has been working on the study for six years, and it will not be completely finished until next spring. But the nuclear watchdog group, Union of Concerned Scientists, has obtained an early copy of the report through a Freedom of Information Act request.¶ The new study is based on how much and how quickly cesium 137 could escape an American nuclear plant if a total blackout were to occur. A total blackout means complete loss of power from the grid, and backup diesel generators and batteries have failed as well. This leads to a nuclear meltdown. NRC scientists said that a total blackout would be rare at an American plant, but it is better to be safe than sorry. In addition, the NRC wanted to update previous projections related to cesium 137.¶ The NRC focused on two different types of reactors in the U.S.: the Peach Bottom Atomic Power Station in Pennsylvania, which has boiling-water reactors like Fukushima Daiichi, and the Surry Power Station in Virginia, which has pressurized-water reactors. Over 100 different plants were studied. Through computer models and engineering analyses, the NRC has concluded that the meltdown of a typical American reactor would lead to "far fewer deaths" than previously thought.¶ According to the new study, only 1 to 2 percent of a reactor core's cesium 137 could escape during a total blackout. Previous NRC estimates concluded that 60 percent of the cesium inventory could escape.¶ In addition, the new study found that one person in every 4,348 within a 10-mile radius of a nuclear meltdown would develop a "latent cancer" from radiation exposure. In previous estimates, it was one person in every 167.¶ The NRC said that large releases of radioactive material would not be "immediate," meaning that people within a 10-mile radius would have plenty of time to evacuate the premises. It concluded that the chance of death from acute radiation exposure within a 10-mile radius would be near zero, but some would be exposed to high enough doses to experience fatal cancers decades later.¶ "Accidents progress more slowly, in some cases much more slowly, than previously assumed," said Charles G. Tinkler, a senior adviser for research on severe accidents and an author of the study. "Releases are smaller, and in some cases much smaller, of certain key radioactive materials."

### AT: Russia War---1NC

#### No Russia war.

Khramchikhin 18 – Aleksandr Khramchikhin, deputy director of the Institute for Political and Military Analysis in Moscow. [Rethinking the Danger of Escalation: The Russia-NATO Military Balance, 1-25-18, https://carnegieendowment.org/2018/01/25/rethinking-danger-of-escalation-russia-nato-military-balance-pub-75346]

In an atmosphere of crisis permeated by mutual recriminations and suspicions, both sides—NATO and Russia—have engaged in a series of military activities along the line of contact. These maneuvers in turn have triggered multiple warnings from both sides of a sharp deterioration in European security, a growing threat of a military confrontation between Russia and NATO, and an urgent need to deescalate the situation in order to avoid a catastrophic war with disastrous consequences for all. An emerging conventional wisdom maintains that the new Cold War in Europe, if allowed to continue unchecked, runs the risk of escalating into a hot war unless steps to reduce tensions are taken swiftly.

But conventional wisdom is often wrong, and so it is this time. The hysteria that has engulfed public commentary throughout Europe about this ostensibly dire military situation on the brink of getting out of hand has little, if any, basis in fact. Both sides in the standoff exaggerate the tensions and the danger of escalation, and the risks of the military moves—their own and their adversary’s—supposedly driving these tensions.

In reality, the military balance between Russia and NATO is stable, the danger of escalation is hardly approaching critical levels, and little needs to be done militarily to defuse the current tensions. The true cause of the tensions is not military, but political and diplomatic. Until those causes are resolved, tensions between Russia and the West will remain high. The likelihood of a military confrontation will remain low, however, because neither side’s posture points to a heightened state of readiness or intention to go on the offensive. Until that changes, political and diplomatic tensions will remain mere tensions.

### AT: Russia War---2NC

#### They won’t risk it.

Woolf ’20 [Amy; 2020; Specialist in Nuclear Weapons Policy in the Foreign Affairs, Defense, and Trade Division of the Congressional Research Service at the Library of Congress, received a Master’s in Public Policy from the Kennedy School of Government at Harvard University; “Russia’s Nuclear Weapons: Doctrine, Forces, and Modernization,” https://fas.org/sgp/crs/nuke/R45861.pdf]

One analyst has postulated that Russia may actually raise its nuclear threshold as it bolsters its conventional forces. According to this analyst, “It is difficult to understand why Russia would want to pursue military adventurism that would risk all-out confrontation with a technologically advanced and nuclear-armed adversary like NATO. While opportunistic, and possibly even reckless, the Putin regime does not appear to be suicidal.” 144 As a study from the RAND Corporation noted, Russia has “invested considerable sums in developing and fielding long-range conventional strike weapons since the mid-2000s to provide Russian leadership with a buffer against reaching the nuclear threshold—a set of conventional escalatory options that can achieve strategic effects without resorting to nuclear weapons.”145 Others note, however, that Russia has integrated these “conventional precision weapons and nuclear weapons into a single strategic weapon set,” lending credence to the view that Russia may be prepared to employ, or threaten to employ, nuclear weapons during a regional conflict.

#### Their impact starts at 0.38%

Rodriguez ’19 [Luisa; 2019; research fellow at the Forethought Foundation for Global Priorities Research, she also researched nuclear war at Rethink Priorities and as a visiting researcher at the Future of Humanity Institute, holds an M.A. from The Heller School for Social Policy and Management at Brandeis University; “How likely is a nuclear exchange between the US and Russia?” https://forum.effectivealtruism.org/posts/PAYa6on5gJKwAywrF/how-likely-is-a-nuclear-exchange-between-the-us-and-russia]

My previous posts address how bad a nuclear war is likely to be, conditional on there being a nuclear war (see [this post on the deaths caused directly by a US-Russia nuclear exchange](https://forum.effectivealtruism.org/posts/pMsnCieusmYqGW26W/how-bad-would-nuclear-winter-caused-by-a-us-russia-nuclear), and [this post on the deaths caused by a nuclear famine](https://forum.effectivealtruism.org/posts/dtQ5hpYjniYKWhmhx/would-us-and-russian-nuclear-forces-survive-a-first-strike)), but they don’t consider the likelihood that we actually see a US-Russia nuclear exchange unfold in the first place. In this post, I get a rough sense of how probable a nuclear war might be by looking at historical evidence, the views of experts, and predictions made by forecasters. I find that, if we aggregate those perspectives, there’s about a 1.1% chance of nuclear war each year, and that the chances of a nuclear war between the US and Russia, in particular, are around 0.38% per year.

#### They would never use nuclear force.

Veebel ’19 [Vilja; 6-1-2019; Department of Political and Strategic Studies at Baltic Defence College; “Researching Baltic Security Challenges after the Annexation of Crimea.” Journal on Baltic Security 5(1), 41–52]

3 Studies on potential nuclear escalation scenarios

The question whether Russia would use its nuclear forces in the Baltic region has also intrigued many academics and military experts recently. One of the most radical discussions in this field is a blog post by Loren B. Thompson, ‘Why the Baltic states are where nuclear war is most likely to begin’. He argues that the likelihood of nuclear war between Russia and the United States is probably growing and is the reason why it is most likely going to start is a future military confrontation over three Baltic countries. Thompson describes eight reasons why nuclear weapons could potentially be used in future warfighting scenarios with regard to the Baltics and argues that according to the bottom-line scenario, the East–West conflict escalates into the use of nuclear weapons in the Baltic area, and neither side of the conflict understands what actions might provoke nuclear use by the other. Thompson comes to a somewhat surprising conclusion -- at least in the eyes of the Baltic countries -- that the United States needs to reassess the situation, suggesting that it would make no sense to tie security of the United States to countries of ‘such modest importance that are situated in such unpromising tactical circumstances’ (Thompson, 2016).

Potential nuclear conflict escalation scenarios are in more detail discussed in another publication, a NATO playbook entitled ‘Preventing escalation in the Baltics’ by Ulrich Kühn. The author argues that the risk of escalating a wider conflict between Russia and NATO is dangerously high particularly in the case of the Baltic countries because it would be difficult for NATO to defend the region. Kühn suggest three possible escalation scenarios, i.e., deliberate escalation, inadvertent escalation, and accidental escalation. All three scenarios also involve nuclear threats; however, two of the scenarios stop short of actual Russian nuclear-weapon usage (Kühn, 2018). The analysis provides an interesting hypothetical construct for the experts at both the transatlantic and local levels, as it points to many practical issues in regard to the nuclear deterrence from the NATO’s political decision-making process to the role of domestic policies in tackling such a crisis.

Conflict escalation scenarios that involve nuclear capabilities are discussed also in other studies. For example, in a study called ‘Reducing the risk of nuclear war in the Nordic/Baltic region’ by Barry Blechman and co-authors, two scenarios of conventional war ending in the exchange of nuclear weapons are constructed (namely, ‘Escalation in Estonia’ and ‘Regional War’). Although the authors emphasize that the scenarios are purely illustrative and the probability of nuclear use is low, they argue that it is useful to reduce these risks even further and suggest two initiatives, such as a strengthening of the Alliance’s conventional military capabilities and particularly the ability to move quickly into the Baltic region, as well as to establish a Baltic nuclear weapons free zone, or at least examining the possibility to do so (for further discussion, see Blechman et at., 2015). Jüri Luik and Tomas Jermalavičius in their article ‘A plausible scenario of nuclear war in Europe, and how to deter it: A perspective from Estonia’ point to various alarming signs, e.g., Russia’s large-scale exercises incorporate limited nuclear strike scenarios against NATO as part of Russia’s ‘escalation to de-escalate’ strategy; Russia is expanding the range of its tactical delivery systems, the country’s political rhetoric includes nuclear threats toward the West, and so on. They emphasize that the Alliance’s range of response options to such threats and limited nuclear war scenarios has shrunk considerably and that the Alliance lacks a collective will to call those threats a bluff (Luik and Jermalavičius, 2017).

A large part of the research in this field more or less considers it likely that Russia could use its nuclear forces in the Baltic region. However, there are also articles that oppose this conviction. For example, Viljar Veebel and Illimar Ploom in ‘The deterrence credibility of NATO and the readiness of the Baltic states to employ the deterrence instruments’ disagree with the idea that the Baltic countries could be under potential nuclear attack, which could in turn evolve to a nuclear war. They argue that although Russia and NATO as potential conflict parties have a striking capability, it would be irrational for both of them to execute a nuclear strike even as a measure of last resort. The authors stress that it is hard to believe that Russia has any rational motivation to use nuclear weapons in the Baltic countries because a large share of the population in the Baltic countries are Russian-speaking. Likewise, in case of a potential conflict, territorial proximity of Russia and the Baltic countries, as well as Russia’s possible further ambition to legitimate the annexation comes into play. The argument of irrationality applies also to the NATO alliance as it would raise a question about morality and escalation should NATO consider using nuclear attack as a preventative measure. In addition, there are several logical gaps in the chain of arguments justifying the use of nuclear weapons against Russia if the latter has fully or partially invaded the Baltic countries. The authors hereby point to the following questions: First, how could the strategic use of nuclear weapons against Russia be believable in a regional conflict? Second, how would it help to solve the conflict which has already started? Third, what would be the possible positive outcome for NATO, having initiated mutually assured destruction with Russia to stop the occupations of Baltics? (Veebel and Ploom, 2018a).

### AT: “Only US-Russia War Extinction”

#### Even small arsenals cause extinction.

Trevithick and Rogoway ’19 [Joseph and Tyler; February 27; Military Analyst, M.A. in Conflict Resolution from Georgetown University, B.A. in the History and Policy of International Relations at Carnegie-Mellon University; Defense Journalist; The Drive, “Yes, India And Pakistan Could End The World As We Know It Through A Nuclear Exchange,” <https://www.thedrive.com/the-war-zone/26674/yes-india-and-pakistan-could-end-the-world-as-we-know-it-through-a-nuclear-exchange>]

A global threat

India and Pakistan's nuclear arsenals are tiny compared to those of the [United States and Russia](http://thedrive.com/the-war-zone/26013/russia-says-its-own-new-weapons-are-exempt-after-accusing-u-s-of-violating-nuclear-arms-deal), and these weapons are focused primarily on deterring each other, but that does not mean they're purely regional threats. Unlike conventional weapons, nuclear weapons create lasting and far-reaching effects that scientists have posited could upend life on Earth if warring parties were to use them in sufficient numbers.

[In 2012](http://climate.envsci.rutgers.edu/pdf/RobockToonSAD.pdf), Alan Robock, a distinguished professor in the Department of Environmental  Sciences and Associate Director of the Center for Environmental Prediction at Rutgers University, and Owen Brian Toon, a professor in the Department of Atmospheric and Oceanic Sciences and a research associate at  the Laboratory for Atmospheric and Space Physics at the University of Colorado, Boulder, argued that it might not take a large amount of nuclear weapons to create a scenario commonly known as "[Nuclear Winter](https://en.wikipedia.org/wiki/Nuclear_winter)."

In general, this hypothesized event occurs when smoke and soot from nuclear explosions block significant amounts of sunlight from reaching the earth's surface, leading to a precipitous drop in temperatures that results in mass crop failure and widespread famine.

Robcock and Toon summarized their findings, which were based in part on their previous work, in an article in the Bulletin of The Atomic Scientists, [writing](http://climate.envsci.rutgers.edu/pdf/RobockToonSAD.pdf):

"Even a 'small' nuclear war between India and Pakistan, with each country detonating 50 Hiroshima-size atom bombs – only about 0.03 percent of the global nuclear arsenal's explosive power – as airbursts in urban areas, could produce so much smoke that temperatures would fall below those of the [Little Ice Age](https://en.wikipedia.org/wiki/Little_Ice_Age) of the fourteenth to nineteenth centuries, shortening the growing season around the world and threatening the global food supply. Furthermore, there would be massive ozone depletion, allowing more ultraviolet radiation to reach Earth's surface. Recent studies predict that agricultural production in parts of the United States and China would decline by about 20 percent for four years, and by 10 percent for a decade.

The bomb the United States dropped on Hiroshima Japan, known as [Little Boy](https://en.wikipedia.org/wiki/Little_Boy), was an inefficient and essentially experimental design with a yield of around 15 kilotons. The reported results from [Indian](https://en.wikipedia.org/wiki/List_of_nuclear_weapons_tests_of_India) and Pakistani nuclear testing indicate that both countries can meet this threshold and both countries' weapons programs have almost certainly matured in the decades since.

In previous studies, Robcock, working with others, postulated that temperature changes could begin within 10 days of a limited nuclear exchange and the effects from the detonations of 100 nuclear weapons in the 15-kiloton class would directly result in the deaths of [at least 20 million people](http://www.nucleardarkness.org/warconsequences/fivemilliontonsofsmoke/). The second order impacts would be even worse in the years that followed.

In 2014, Michael Mills and Julia Lee-Taylor, both then working at the federally-funded National Center for Atmospheric Research's (NCAR) Earth System Laboratory, authored another paper with Robcock and Toon. This [study concluded](https://web.archive.org/web/20140308191334/http:/acd.ucar.edu/~mmills/pubs/2014_EarthsFuture_Mills_et_al.pdf) again that detonation of 100 15-kiloton yield bombs in a purely regional conflict would result in "multi-decadal global cooling" and "would put significant pressures on global food supplies and could trigger a global nuclear famine."

It is important to note that[critics have questioned](https://en.wikipedia.org/wiki/Nuclear_winter#Critical_response_to_the_more_modern_papers) whether the Nuclear Winter concept relies on too many assumptions and would ever actually occur. At the center of many of these rebuttals are debates about whether the nuclear explosions would truly create the amount of smoke and soot necessary for major climate change, as well as the specific conditions for those particles to remain in the atmosphere for a prolonged period of time.

The studies here do indicate significant impacts based on a relatively limited number of nuclear detonations of smaller yield devices, though. But even if the impacts are less pronounced than projected in this particular scenario, they could be far more severe if India and Pakistan were to use a larger number weapons and/or ones of higher yields, which both belligerents readily have.

In addition, Nuclear Winter is just one of the potential things that might happen following a nuclear exchange between the longtime foes. A detonation of dozens of nuclear weapons, even small ones, would throw hazardous nuclear fallout [into the air](http://thedrive.com/the-war-zone/19450/u-s-training-for-arctic-nuclear-satellite-disaster-amid-russian-weapons-developments) that, depending on the weather pattern, could carry that material [far and wide](https://futureoflife.org/background/us-nuclear-targets/?cn-reloaded=1#nukemap), causing both near- and short-term health impacts. The various [ground zeroes](https://nuclearsecrecy.com/nukemap/) themselves would be irritated and potentially hazardous for many years to come.

Depending on where the detonations occur, a nuclear exchange could potentially cut people off from critical water and food supplies, putting increased and potentially unsustainable strains on uncontaminated areas.  After the Chernobyl nuclear power plant, situated in Ukraine, [melted down and exploded](https://en.wikipedia.org/wiki/Chernobyl_disaster) in 1986, authorities established a 1,000 square mile restricted access "[exclusion zone](https://en.wikipedia.org/wiki/Chernobyl_Exclusion_Zone)" that remains in place today.

There would also be a major danger of second-order "spillover" effects, as individuals fled affected areas, putting economic and political strains on neighboring regions. This could inflame existing tensions not directly related to the inter-state conflict between India or Pakistan or lead to all new and potentially violent competition for what might already be limited resources. India has already threatened to [weaponize water access](https://www.nytimes.com/2019/02/21/world/asia/india-pakistan-water-kashmir.html) in its latest spat with the Pakistanis.

Any serious impacts on food and water supplies, or other economic upheavals as a direct or indirect result of the conflict, would have cascading impact across South Asia and beyond, as well. The very threat of a potential India-Pakistan war of any kind already caused [some negative reactions](https://www.cnbc.com/2019/02/27/indian-air-force-plane-crashes-in-kashmir-says-indian-police-official.html) in regional financial markets. Those markets would certainly collapse after an unprecedented nuclear exchange actually occurred, and that is before the long-term physical impacts of such an event would even manifest themselves.

Overall, we are talking about a sudden and dramatic geopolitical, financial, and environmental shift that would change our reality in a matter of hours. Even then, the darkness, both figuratively and literally, that could propagate over the weeks, months, and years would be far more damaging.

How great is the risk?

So far, India and Pakistan have not made any clear indications that the fighting is close to crossing their nuclear thresholds. Pakistan's warnings about the [risks of escalation](http://thedrive.com/the-war-zone/26642/pakistan-promises-retaliation-makes-nuclear-threats-after-indian-jets-bomb-its-territory) seem more calculated to try and prompt India to back down.

India itself has a so-called "no first use" policy, which means it has publicly pledged to use its nuclear weapons only in retaliation to a nuclear strike. However, experts have increasingly called into question whether this is truly the case and whether India might be developing delivery systems more suited to a first strike should there be a need to shift policies.

Pakistan, however, does not have a no first use policy and has insisted on its right to employ nuclear weapons to defend itself even in the face of purely conventional threat. Pakistani officials have, in the past, [specifically cited this policy](https://www.cfr.org/event/promoting-us-pakistan-relations-future-challenges-and-opportunities) as way of deterring India, which has a much larger and in some cases more advanced conventional force, and preventing larger wars.

The concern, then, is that this policy appears to have failed, at least to some degree, with India's strike on undisputed Pakistani territory on Feb. 26, 2019. India, however, did not target Pakistani forces in that instance and exchanges between the two countries have been limited, at least so far, to the disputed Jammu and Kashmir region, where violent skirmishes occur semi-regularly without precipitating a larger confrontation.

We can only hope that the two countries will find a diplomatic solution to this latest conflict and avoid any further escalation. If things were to spiral out of control and lead to the use of nuclear weapons, it would be something that would threaten all of humanity.

### AT: Undersea Cables---1NC

#### Redundancy prevents collapse

Paul Brodsky 18, Senior Analyst at TeleGeography, "Submarine Cable Redundancy, Explained," No Publication, https://blog.telegeography.com/what-is-submarine-cable-redundancy

Most cable-using companies follow a “safety in numbers” approach, spreading their networks’ capacity over multiple cables so that if one goes down, their network will run smoothly over other cables while service is restored on the damaged one. This is redundancy.

When multiple submarine cables are available between two nodes, data transmission may take multiple paths. Two cables traveling between nodes provide one level of redundancy. Three provide two levels of redundancy, and so on.

So take David Belson’s story for Dyn, which explains that “with multiple submarine cables landing in Western African countries that provide service between countries…network providers in these countries have an opportunity to take advantage of this redundancy to mitigate the potential impact of problems.”

## NATO Cohesion Adv

### NATO Cohesion Adv---1NC

#### NATO is resilient – military relations are distinct from politics

Baron 18 [Kevin, founding executive editor of Defense One, "NATO Will Outlive Trump (and Putin), Don’t Worry," Jun 27, https://www.defenseone.com/politics/2018/06/nato-will-outlive-trump-and-putin-dont-worry/149348/]

Before Trump heads back to Europe, remember that NATO isn’t the G-7 and military relations are much stronger than the political ones they often endure. Squee! What is Trump going to say this time? That’s how some of the political press in DC sound already, both giddy and worried about what President Donald Trump is going to say at the NATO Summit in two weeks. More seriously, many Americans and Europeans are worried about what Trump is going to say and do in Brussels, and how much further Trump may sink U.S. relations in general with European and North American allies. You can’t blame them. The G-7 meeting in Canada last month was a diplomatic disaster that left foreign policy pundit circles aghast yet again at how the American president treated the leaders of his nation’s closest allies. (Trump supporters loved every minute of it.) Even before that meeting, Foreign Policy had run an article headlined “Can the U.S.-Europe Alliance Survive Trump?” (They were talking about Trump pulling the U.S. out of the Iran deal.) After Vancouver, other headlines proclaimed U.S.-European relations at an all-time low. Germany’s Chancellor Angela Merkel said Europe could no longer “completely rely” on American protection, leading many to question the future of the alliance. There’s only one problem, or perhaps ray of hope. Relations between G-7 leaders are not the same as relations between their countries. And the G-7 is not NATO. NATO is not political Twitter or a TV roundtable. It’s not an economic club. NATO is a military alliance of treaty-bound governments with troops trained to kill, fight, and die to protect one another from foreign attack. NATO is a 70-year-old alliance that has withstood political winds and Cold War nuclear showdowns. It is a pact between democratic nations that their military men and women will stand that post. It outlasted Kennedy and Kruschev, Brezhnev and Reagan. It will outlast Trump and Putin and Merkel. Military relations are not like political ones. Take Turkey. Defense One ran the headline “Are U.S.-Turkey Relations Fraying?” five years ago. They are. Last week, they were “coming to a boil.” But what is happening underneath? Military leaders in constant contact, still upholding their NATO pledge. Earlier this year, I was talking with one senior military official who said he understood every American concern about President Recep Tayyip Erdoğan’s confounding moves in Syria and toward Russia, but he put it like this: military-to-military relations do and must operate on a level plane at one level (as he steadily slid his hand flat in the air, back and forth), while political relations and the sometimes-heated rhetoric of elected officials who come and go occur above them (he raised his hand above his eyes, making the same gesture). It’s true in many places. If military relations sour between the U.S. and China, it is potentially far more disastrous than any downturn in the economic, political, or trade spheres. But even when those relations are not so great, they’re often steady. In the early Obama years, when China froze communications with the U.S. military, Pentagon leaders begged the PLA to open up and talk, saying repeatedly that the U.S. wanted both sides to “avoid miscalculations” that could escalate into war. China opened up, but they also proceeded with a rapid military technological advance and created new islands to expand their power. Military relations adjusted, but they continue. At press time, Defense Secretary Jim Mattis is in Beijing discussing mutual issues like North Korean denuclearization. Or take Israel. Conservatives, liberals, and pro-Israeli and political pundits claimed U.S.-Israeli relations were at an all-time low when Obama and Netanyahu weren’t seeing eye-to-eye. But at the same moment, military and intelligence leaders of both sides were saying times were never better at their level; as mutual trust, intelligence coordination, and arms sales were flourishing. The relationships of national leaders do not always reflect the relationships of their peoples or militaries. So when you hear predictions that in two weeks Trump may pull the U.S. out of NATO, take a breath and think through what it would really take for that to happen. Think about the military. When Syria’s Bashar al-Assad was routing rebels and some U.S. leaders wanted Obama to intervene with bombs and troops, there was one group left out of the conversation who also had a vote: the military. At the time, Defense One ran the headline “Want Syria? Convince General Dempsey.” The point was that as right-left politics shouted at each other over what to do, Obama’s senior military advisor was sitting atop an officer corps that was extremely wary of leading the U.S. into another unsure military intervention in the Middle East just two years after pulling out of Iraq. Now think about the magnitude of a U.S. withdrawal from NATO. Trump so far has deferred to the generals repeatedly — on Syria, on Afghanistan, on Guantanamo, on North Korea, and, yes, on NATO. Do you really think Joint Chiefs Chairman Gen. Joseph Dunford’s “best military advice” to the commander in chief at this moment in history would be to pull out of NATO? Would any U.S. military leader’s? Would John Kelly’s? Would Congress’s? Of course not. We’ve been through this before. Trump has been dangling NATO withdrawal (or cheap disparagement) before his isolationist-but-militaristic base since early in his presidential campaign. And Trump may continue to dangle it over Europeans, the way he dangles tweets and falsehoods to manipulate his constituency, the media, and his opponents. We know that game now. Some of the NATO leaders he is going to meet in July know it more than most. They were the ones he humiliated at the G-7. The G-7 isn’t NATO. NATO will survive July. But politics is politics, and now we have a new concern. John Bolton, Trump’s still-new national security advisor, flew to Moscow and received Russian President Vladimir Putin’s assent to a meeting of the two leaders. That’s expected sometime in July, in Europe, around the time that Trump will be across the pond for the NATO Summit, the president said. “It would look like we will probably be meeting in the not too distant future and I’ve said it from day one getting along with Russia and China and with everybody is a very good thing,” Trump said Wednesday. Forget Bolton. The Trump-Putin meeting has foreign-policy pundits worried as much as when the president met North Korea’s Kim Jong-Un. Nobody knows what to expect from Trump. But there’s plenty of reason for concern. Already, the Trump-Putin meeting is left-right meat for partisans and political gamers. If you hate Trump, you hate the idea of Trump stepping over NATO and falling into Putin’s trap, and you think the outcome will be Trump getting played yet again by the master former-KGB autocrat whom nobody has yet to best. After all, if Trump halted military exercises for Kim, what will he give away to Putin? Crimea? Exercises? Nuclear stockpiles? Missile defenses? NATO? If you like Trump, you welcome the chance for the master dealmaker, the outsider, to toss out the diplomatic rulebook as in Singapore, give Putin an extra-tight manly handshake and get him on the hook to avoid a new Cold War, put an end to all this nonsense of so-called Russian interference. Either way, you’re not talking about NATO anymore. You’re talking about Trump. It’s a pickle. The data shows the United States has done nothing to back down from defending Europe. Trump’s insistence that NATO’s European members spend more on their own militaries is not a withdrawal, it is an overdue and purposefully undiplomatic attempt to level an imbalance. Merkel’s statement that Europe cannot “completely rely” on American and British support anymore is a reflection of what Trump and many American leaders have been saying for years. Europe shouldn’t. But while the new era sorts itself out at the political level, there’s been no backing away from NATO between militaries. We have seen more, not less, of U.S. and NATO-allied military exercises, troop deployments and rotations, forward-located firepower, and political attention to Europe’s eastern flank. Military relations go on. “In the last few weeks [there has] been a lot of talk about, ‘Well is the North Atlantic bond still a bond? Is it still an alliance?’ Yes, the answer is yes. We are,” said U.S. Ambassador to NATO Kay Bailey Hutchinson this month in Washington. “America is committed to NATO, to Article 5, I promise you we really are, and the president has said it publicly many times,” she continued. “I think our allies and our partners know that, but we can never say it too many times.” There’s no telling what Trump will say in the coming weeks around the NATO Summit. It will be a another leadership test for Merkel, UK’s Theresa May, France’s Emmanuel Macron, and Canada’s Justin Trudeau. No matter what they say, the press will eat it up. Except none of it matters much to NATO. The alliance will hold.

#### NATO fails -- obsolete

Walt 17 [Stephen M., P.H.D from Berkeley. Professor of international affairs at Harvard University's John F. Kennedy School of Government. “It’s Time for Europe’s Militaries to Grow Up” [http://foreignpolicy.com/2017/02/23/its-time-for-europes-militaries-to-grow-up-trump-nato]](http://foreignpolicy.com/2017/02/23/its-time-for-europes-militaries-to-grow-up-trump-nato%5d)

Finally, constantly harping about burden sharing distracts attention from the more serious challenges that threaten the transatlantic partnership. The first challenge is the lack of a compelling strategic rationale for it. Much as I hate to admit it, Trump was not entirely wrong to suggest NATO was obsolete — at least in its current form — because it was created to deal with a problem (the Soviet Union) that no longer exists. It is harder to justify an expensive U.S. commitment to defend Europe when there is no potential hegemon there and the new missions that NATO has taken on after the Cold War ended (Afghanistan, Libya, etc.) have fared rather poorly. (NATO’s other implicit purpose — “to keep the Germans down” — isn’t relevant either, despite Germany’s central role in the EU. With a declining and rapidly aging population, Germany today could never aspire to European hegemony.)

#### Complexity, conflicting interpretations, and fights over intel sharing block agreement

Arts ’18 [Sophie; December 13; senior program coordinator for security and defense policy at The German Marshall Fund; "Offense as the New Defense: New Life for NATO’s Cyber Policy," https://www.gmfus.org/publications/offense-new-defense-new-life-natos-cyber-policy]

While the United States’ announcement that it would contribute its capabilities could help lend credibility to NATO’s cyber deterrence, further clarification is needed within NATO, particularly when it comes to its command structure in the cyber domain. Without clarity on this front, it is hard to imagine that the 29 NATO allies who have different threat perceptions, and face issues of cohesion and trust, could agree on effective response scenarios in a crisis situation. This is particularly critical, because cyber operations will be subject to political approval by the NATO allies.

The new Cyber Operations Center, which should be fully operational in 2023, could play an important role in that respect, but the lack of operational authority may pose a significant challenge.37 According to NATO, the center aims to “strengthen cyber defenses and integrate cyber capabilities into NATO planning and operations.”38 But as the U.S. declaration on its potential cyber support to NATO confirms, it appears at this point that the center will serve to coordinate rather than oversee operations. This, coupled with allies’ unwillingness to share intelligence that may be critical to NATO’s strategic efforts, makes it difficult to envision the center as an effective tool in implementing a coherent top-down cyber strategy in the near future.

#### Even if diplomats agree, it’s a huge domestic fight within allies---that stops codification

Ulf Häußler 19, NATO Fellow for the U.S. National Defense University's Center for Transatlantic Security Studies, Assistant Legal Advisor for Operational Law at the Allied Command Transformation (NATO ACT, Norfolk/Va., USA), “Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO 250 Treaty”, in Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty, p. 114-115

Political Policy and Institutional Arrangements

The fact that a given cyber threat or incident crosses the threshold of political concern is without prejudice to its political and legal characterisation for the purpose of developing an appropriate response. Much will depend on political policy perceptions – are cyber threats and incidents predominantly perceived as human rights (i.e. data privacy) issues, matters of law enforcement and/or homeland security300, or matter of national security and defence – and the different roles played by the government agencies involved on the examination and assessment of cyber threats and incidents, and competent to adopt or contribute to actual responses. Accordingly, it may be for multiple reasons that NATO faces challenges in developing consensus regarding the full integration of cyber security and defence in its respective mechanisms, as well as the necessary institutional arrangements.

First, in an environment where any security and defence discourse is to a great extent predetermined by the level of political concern, there may simply have been a limited number of opportunities to actually put cyber security and defence prominently on NATO's agenda. Second, quite similar to threats arising from international terrorism, threats arising in and out of the cyber space may give rise to both internal, or homeland, and external security concerns, and thus trigger the oftentimes complex delineations of competence between the defence, law enforcement, and intelligence sectors which many NATO Nations have developed into strong checks and balances amounting to a separation of powers *en miniature* within their executive branches of government. Whilst obviously such domestic arrangements lack the capacity to affect the interpretation and application of the North Atlantic Treaty301, they may nevertheless *de facto* challenge NATO Nations' Defence Ministries' as well as Armed Forces' ability to put cyber security and defence on NATO's policy, concept, and doctrine agendas. To date, no well-entrenched method, structure or process for overcoming this *de facto* challenge – e.g. through involvement of foreign intelligence, homeland security and/or law enforcement stakeholders – exists within NATO. Third, there is a near complete lack of NATO-wide, standardised doctrine for cyber warfare. The resulting absence, amongst NATO Nations, of a militarily agreed and legally cleared (Article 36 of GP I) understanding concerning the means and methods of cyber warfare may also contribute to the lack of political policy consensus. The appetite for engaging in hostilities which might be perceived as potentially involving legally doubtful means and methods of warfare may be limited. Ultimately, the absence of consensus regarding *jus in bello* may thus have repercussions on the likelihood that consensus can be reached concerning *jus ad bellum* as well as collective security and defence.

### Say No---Allies---Unrelated Disputes---2NC

#### US leadership alone forces allies bring up unrelated disputes

Nicholas Burns 19, Goodman Family Professor of the Practice of Diplomacy and International Relations at Harvard Kennedy School, MA in International Relations from the Johns Hopkins School of Advanced International Studies, and Douglas Lute, Senior Fellow at the Project on Europe and the Transatlantic Relationship, Former United States Permanent Representative to the North Atlantic Council, Holds Degrees from the United States Military Academy at West Point and from the Kennedy School of Government at Harvard University, “NATO at Seventy: An Alliance in Crisis”, Belfer Center for Science and International Affairs, Harvard Kennedy School Report, February 2019, https://www.belfercenter.org/publication/nato-seventy-alliance-crisis

NATO needs to take a hard look at itself. Across twenty-five indicators of democracy rated by Freedom House, the downward trend among NATO allies over the past decade is stark.35 Especially in Central Europe but not exclusively, there are setbacks in the media, the judiciary and the functioning of national democratic institutions. The rate at which democracy is declining in Poland, Hungary and Turkey is particularly alarming. In 2017 and 2018, these three states’ scores represented some of the largest one-year declines in political rights and civil liberties of all 195 countries ranked by Freedom House.36 Poland—with the largest category declines in the forty-year history of the survey—is close to leaving the “consolidated democracy” category.37 Hungary is no longer rated a consolidated democracy. Turkey, whose decline in freedom over the last ten years represents the largest of any country in the world, crossed the threshold from “free” to “not free.”38

While less severe today, nationalist populism movements in other allies represent a broader, more diffuse threat to NATO and can amplify other challenges facing the Alliance. The United States is not immune, with its Freedom House rating declining in 2018 due to “Russian interference in the 2016 election, violations of basic ethical standards by the new administration and a reduction in government transparency.”39 While this slippage in the U.S. is relatively recent and still minor in scale, it nonetheless diminishes America’s standing as a standard-bearer for democracy and further erodes its leadership position within the Alliance. Further, anti-democratic policies among allies open vulnerabilities for interference by competitors outside the Alliance, especially Russia that seeks to divide NATO and the EU politically using hybrid tactics.40

The question for allies is what must the role of the Alliance be in reinforcing its core values when they are under assault from within. NATO is both a political and a military alliance. It is not enough to be bound together by a commitment only to Article 5 collective defense. The values in the Treaty and the adherence of NATO allies to those values is fundamental for Alliance cohesion. That shared commitment to values in turn makes credible the Article 5 commitment. The Washington Treaty is binding for both its political and military commitments.41 Allies cannot ignore the failure to abide by political commitments including values and expect military commitments to be unaffected. In short, NATO allies should not expect that they could violate democratic values without consequences, while resting assured that NATO cohesion is intact and other commitments in the Treaty will be upheld. The Treaty is not a menu of options from which allies can select some obligations while ignoring others.

The NATO Treaty has no provision for policing members that drift from common political values, unlike the European Union Treaty’s Chapter 7 that has been invoked recently toward several EU member states with some success.42 While it would be impossible to achieve consensus to impose penalties on wayward allies, given that the ally in question could veto any penalties, a range of escalating political initiatives on the part of the Secretary General and a coalition of the other allies could assert pressure. As a start, the Secretary General should express concern in his bilateral meetings with the anti-democratic governments, with the support of key allies and in partnership with the European Union. To increase awareness within the Alliance and among the public, foreign ministers could review annually indicators of democracy for all twenty-nine allies, perhaps prepared by an informal high-level group of experts drawing on Freedom House data. The NATO Parliamentary Assembly and coalitions of allies can amplify the message.43 To increase pressure, NATO could suspend hosting of visits, official meetings and even military exercises with these nations. In severe cases, NATO infrastructure spending and even access to military schools and information sharing could be affected. An indirect way to express concern among allies is to increase the prominence of core democratic values when considering NATO enlargement decisions in the future.44 None of these steps is without political cost and risk, even if calibrated carefully. But the costs and risks of the gradual erosion of Alliance cohesion as member states drift from the founding values are even greater. NATO cannot expect to remain coherent and relevant and able to address the full range of challenges it faces, if it ignores the internal drift from democracy within some member states. This drift is a fundamental issue for the Alliance.45

Streamlining NATO Decision-Making

Finally, the challenges facing NATO today demand more flexibility in executive decision-making. As a core principle in preserving NATO cohesion, consensus decision-making must remain the basis for major NATO actions.46 The Treaty requirements for consensus on collective defense decisions (Article 5) and enlargement decisions (Article 10) remain sensible. Major policy decisions like the Defense Investment Pledge or the creation of the Very High Readiness Joint Task Force rapid reaction capabilities require consensus. But today with NATO enlarged to twenty-nine members and facing increasingly diverse and complex challenges, it is time to consider how other, more routine, administrative decisions can be taken more efficiently. But this should be a management function, not derogation from the consensus principle.

We recommend strengthening the Secretary General’s role as the chief executive of the Alliance with broader authority to carry out routine business without seeking consensus among the twenty-nine members. For example, the Secretary General should consult allies on matters such as agendas and timings of Ministerial Council meetings, but not be required to seek consensus agreement. Today the agenda and even the dates of a Foreign Minister meeting or a NATO-Russia Council meeting can consume hours of formal Council time seeking consensus at the ambassadorial level, consuming headquarters’ bandwidth and crowding out more substantive and urgent topics, including many outlined in this paper. Further, the Secretary General’s flexibility on international staff personnel changes and NATO budget matters should be increased. Today, for example, the Secretary General is severely constrained from adapting the Alliance to emerging challenges by making meaningful shifts in personnel and budgetary resources.47 While nations will continue to want a critical role in all these decisions, criteria should be developed that will provide for more flexibility while ensuring that all allies gain a fair share of opportunities and allocation of resources.

A related problem is the tendency of some allies to bring into the Alliance bilateral issues that impede progress on collective issues of the Alliance. As an example, an ally might hold up agreement on the entire NATO military exercise program because of an unrelated bilateral dispute with a NATO partner who wishes to participate in an exercise.48 This practice erodes Alliance cohesion and should not be permitted. After appropriate consultation, we recommend the Secretary General should have the authority to exclude such external issues from consideration in the Alliance, even if it means moving forward without full consensus.

#### Greece and Turkey will bring up the Aegean---neither will back down

Yotam Gutman 20, Marketing Director at SentinelOne and Retired Lt. Commander in the Israeli Navy, “Battle for Supremacy | Hacktivists from Turkey and Greece Exchange Virtual Blows”, Sentinel One Blog, 1/21/2020, https://www.sentinelone.com/blog/battle-for-supremacy-hacktivists-from-turkey-and-greece-exchange-virtual-blows/

Tensions between Greece and its neighbor, Turkey, are nothing new. Conflict in the Aegean extends back to the days of Homer, who described how a Greek army decimated the town of Troy, located near Hisarlik in Turkey. The animosity between these nations may date centuries into the past, but the weapons and tactics used in the conflict today are cutting edge cyber tools.

Greece and Turkey are now engaged in a diplomatic conflict focused on the maritime boundaries surrounding the Greek island of Crete. The row comes after Turkey and the Libyan government agreed to seek to map out a boundary that would potentially reduce Greece’s maritime territory. This conflict raises patriotic tensions on both sides, some of which have become manifest in cyberspace.

Turkish hackers last week claimed responsibility for cyber attacks on Greek government sites, including those of the Greek National Intelligence Services (EYP), Greek Parliament, the Greek Ministry of Foreign Affairs and the Greek Ministry of Finance among others. Turkish hackers AnkaNeferler said these were in retaliation for the Greek government’s stance on the Turkish agreement with Libya (the Turkish government is providing military support and plans to send its military troops).

Meanwhile, Greece is furious at the pact between Turkey and Sarraj’s government as it threatens to skim the Greek island of Crete, which Greece and its allies say is contrary to international law.

#### That gridlocks NATO

Elisabeth Braw 20, Senior Research Fellow at the Royal United Services Institute for Defence and Security Studies, et al., “Judy Asks: Is NATO Paralyzed Over the Greece-Turkey Conflict?”, Carnegie Europe, 9/3/2020, https://carnegieeurope.eu/strategiceurope/82643 [language modified]

When Greece and Turkey joined NATO in 1952, they did so based on NATO members’ assumption that the two countries’ membership of the alliance would pacify their behavior toward each other.

China was invited to join the World Trade Organization in 2001 on the same premise.

But as every relationship counselor tells quarreling couples, you can’t change someone’s personality. Thus, NATO finds itself with two member states that are officially allies, but whose suspicion of each other is never far from the surface. How to broker between two members without taking sides? NATO seems [gridlocked] paralyzed.

But in reality, it’s not. Sure, two quarreling member states will affect an alliance, but NATO is still going strong on its main mission: defending the territorial integrity of its member states against sundry territorial threats from other countries and nonstate actors.

Here, one could in fact wish for more participation from Greece and Turkey. According to NATO’s latest Enhanced Forward Presence figures, for example, neither country contributes to the protection of the Baltic states and Poland. Solidarity goes both ways.

FRANÇOIS HEISBOURG SENIOR ADVISER AT THE INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES

NATO’s purpose as an organization is to ensure the collective defense of its members on the basis of its founding Washington Treaty. It was never designed to adjudicate disputes between its members. It should therefore not come as a surprise that NATO is [gridlocked] ~~paralyzed~~ over the current Greece-Turkey conflict.

### Say No---Allies---Flip-Flop---2NC

#### Even if they support it in the abstract, the plan’s a 180-degree flip-flop from NATO’s recently announced posture

Thomas E. Ricks 17, “NATO’s Little Noticed but Important New Aggressive Stance on Cyber Weapons”, Foreign Policy, 12/7/2017, https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/

Not many people noticed it, but last month, NATO made a dramatic change in its cyber policy announced by the NATO Secretary General that arguably was the alliance’s biggest overall policy shift in decades. Having led the policy discussions in several NATO committees for the past four years on the use of cyber capabilities and cyber weapons, I can tell you this was the most hotly debated and contentious decision during my tenure at NATO.

In short, NATO embraced the use of cyber weaponry in NATO operations. This is a marked departure from NATO’s historical stance of using cyber only defensively, mainly to ward off incursions against its own networks. The more aggressive approach was intended as a strong message, primarily to Russia, that NATO intends to use the cyber capabilities of its members to deter attacks in the same way it uses land, sea, and air weaponry.

Russia’s provocative actions during the U.S. Presidential elections, its attempts to influence the French and German elections, and its blatantly aggressive, and on-going cyberwar against Ukraine were likely key determining factors which led the NATO defense ministers to adopt a more assertive stance.

On the surface, NATO’s cyber policy shifts might seem to be little more than incremental changes to its existing policy. However, the fact the alliance is standing up a cyber operations center to integrate cyber capabilities from alliance members sends a message to the world, especially Russia, that alliance members both possess and have the will to use their cyber capabilities and weaponry during military operations.

#### That makes reversal super difficult

Dr. Jarno Limnéll 16, Professor of Cybersecurity, Aalto University, Finland, and Charly Salonius-Pasternak, Senior Research Fellow, The Finnish Institute of International Affairs, “Challenge for NATO – Cyber Article 5”, Center for Asymmetric Threat Studies, June, https://www.diva-portal.org/smash/get/diva2:1119569/FULLTEXT01.pdf

Formulating clear doctrines is frequently preferred by militaries, while politicians and diplomats prefer flexibility in message and response. The Alliance has two paths it can chose in creating the doctrine regarding cyber. It can either chose a public approach, rather similar to its approach when creating its most recent strategic concept. In such a document it could generally describe what constitutes an attack that would qualify for the invocation of Article 5, and what would be an accepted retaliatory action. The other path is to maintain strategic ambiguity, recognizing that formulating clear redlines would invite potential adversaries to push up to the red line. In this case developing the doctrine is still important, but would then be for internal use only. This non-public approach may reduce the objective of improving the Alliance´s cyber deterrence. The pace of development in the field would argue against an overly specific set of guidelines or doctrine, lest it require too frequent and politically challenging updates.

### Say No---Allies---Game Theory---2NC

#### Allies misrepresent their actual preference to gain leverage, but overshoot, producing gridlock

Dr. Ping-Kuei Chen 16, Doctor of Philosophy in Government and Politics from the University of Maryland, "Holding Hands While Parting Ways: Examining Alliance Treaty Renegotiation", Doctoral Dissertation, 2016, https://drum.lib.umd.edu/bitstream/handle/1903/18546/Chen\_umd\_0117E\_17257.pdf?sequence=1

During bargaining, alliance members interact and communicate their demands for future security cooperation. Allies not only try to determine a set of mutually acceptable solutions, but also evaluate whether the alliance is worth preserving. In the attempt to find a solution to their differences, members may encounter difficulties during negotiation, since their interests are unlikely to overlap completely.

Morrow (1994) suggests that two problems may hinder coordination in alliance politics. First, a distributional problem occurs when members have different preferences among all available solutions. The other problem is informational problem. Allies may conceal available options from each other in order to advance their own interests. These two problems intertwine. As Morrow argues, “Distributional interests prevent the honest sharing of information.” This dictum applies to intra-alliance bargaining because, even in a security alliance, members are not fully aware of each other’s intentions. Members sometimes have an incentive to misrepresent or hide their true intent in terms of maximizing their own security benefit, and so may withhold information regarding their security interests or falling short of their commitments in order to achieve unexpressed policy goals.

These distributional and informational problems give rise to three predicaments during intra-alliance bargaining: alliance members may (1) be unaware that they have an interest divergence; (2) acknowledge the existence of interest divergence, but be uncertain about a mutually acceptable solution; or (3) be unsure whether other members will keep their commitments in the future.

To overcome these difficulties, allies rely on information revealed during intraalliance bargaining when deciding on the future of an alliance. First, both sides need to recognize the existence of interest divergence and the need for a solution. Bargaining needs to focus on clarifying the problem when one or more partners fail even to see it, and sometimes this act of clarification can in fact be the most difficult discussion involved in bargaining.

Second, if both members recognize the interest divergence, they can move on to negotiate an arrangement. Successful bargaining requires allies to agree on one among a set of mutually acceptable options. A distributional problem may occur, however, when allies have uncertainties regarding each other’s updated security interests and hence regarding what arrangements might satisfy these interests. Dialogue can clarify matters, but a member may become suspicious about the claims that an ally makes if these claims differ from its own reading of the situation. Since an alliance relationship allows allies to interact more frequently, each ally is confident of its own understanding of the evolving security needs of its partners. When there is a perception gap among members concerning the security benefit that one or another enjoys or about the kind of cooperation that best furthers the alliance’s common interests, agreement may be difficult to reach. Allies must genuinely communicate their own preferences and be able to verify each other’s claims.

Finally, members naturally want to know the extent to which the other members value and are committed to the alliance. When their security interests have changed, they will not agree to negotiate unless they still consider each other reliable. When members agree to revise a treaty, a major goal is to ensure that any new obligations will induce sustained cooperation. An alliance will soon fall apart if bargaining reveals that a member has no interest in maintaining it.

When allies are consistently candid during renegotiation, their differences are likely to be resolved. However, as mentioned in the context of studies of burden sharing, allies have incentives to take advantage of their partners that are founded on the assumption that the interests of the latter in maintaining the alliance will lead them to grant concessions during negotiations as a means to salvage the imperiled relationship. In other words, some members may enter into renegotiation with the belief that abrogation would be too costly for the other members. In addition, an uncommitted partner is unlikely to engage in negotiation and more likely simply to abandon the alliance immediately. A member that is willing to renegotiate, by contrast, still values and therefore seeks to preserve the alliance. Each member thus starts bargaining under the assumption that the others are unlikely to give up easily, a situation that leaves rooms for allies to misrepresent their security interests and levels of commitment.

Even in an alliance relationship, a member’s commitment to the alliance is private information. Both the challenger and the partner have an incentive to misrepresent their true intentions in the pursuit of leverage during bargaining. Expressing discontent may gain concessions from other allies as well as testing the loyalty of each. A challenger may, in the course of renegotiation, threaten to withdraw from the alliance when it is in fact willing to accept an arrangement; a partner may misjudge a challenger’s resolve and fail to accommodate its needs; a challenger may misperceive its partner as dissatisfied and decide to withdraw from the alliance preemptively. Therefore, even though intra-alliance bargaining stands a good chance, and may represent the only chance, of resolving disagreement among members, there is no guarantee that this process will succeed.

### Say No---Negotiator Failure---2NC

#### Frontline negotiators fail---they don’t understand cyber, blocking agreement

Leuprecht 19—Class of 1965 Professor in Leadership, Department of Political Science, Royal Military College and Adjunct Research Professor at Charles Sturt University; Ph.D, Queen’s [Christian Leuprecht, Joseph Szeman (an undergraduate student in Political Studies and History in his 4th year at Queen’s University), David Skillicorn (Professor in the School of Computing at Queen’s University, and an adjunct Professor at the Royal Military College of Canada), March 2019, “The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity”, Contemporary Security Policy, Accessed through the Wake Forest Library]

Among the greatest impediments to developing a framework for the use of OCOs is that political leaders typically lack the requisite background (Kello, 2017). That is, they understand neither how they work, nor the possibilities and constraints on cyber operations. Kinetic weapons are intuitive, at least in a broad sense, in a way that cyber weapons are not, because so much of what they do is hidden in the digital environments in which they operate. At least in the West, few politicians come from a technical background that would enable them to understand the issues sufficiently deeply.

#### Only a deep understanding of the intricacies of cyber policy can create a deal

Jarno Limnéll 16, Professor of Cybersecurity, Aalto University, Finland Charly Salonius-Pasternak, Senior Research Fellow, The Finnish Institute of International Affairs. "Challenge for NATO – Cyber Article 5." http://www.diva-portal.org/smash/get/diva2:1119569/FULLTEXT01.pdf

The current ‘cyber warfare playbook’ is still a slim volume - but it is growing by the day. In order to remain a credible defence alliance, NATO must possess a credible cyber policy, including cyber deterrence. Credibility comes from a largely similar set of actions as NATO has engaged in regarding conventional military. Doing it in the cyber domain is, however, harder at the moment. For example, what is the equivalent of standing up in practice permanent battalions in member states? How do you exercise, publicly message determination to defend and counter aggression, in a serious but non-threatening way?

NATO has to find a clear way to deal with a ‘Cyber Article 5’ event. It may be necessary to reinterpret what Article 5 and an armed attack constitute in today´s world. The biggest challenges is to reach a shared understanding of the limits (physical and cyber) which could lead a member state to invoke Article 5 and delineate what proportionality in response means. The decisions are political by their nature and requires strong understanding on strategic cyber domain and its development by the political actors involved. Ultimately, success will depend on how the cyber is blended with traditional political and military power.

### AT: China Adv---1NC

#### No China rise or war.

Swaine '21 [Michael; 4/21/21; PhD in Government from Harvard University, director of the East Asia program at the Quincy Institute; "China Doesn’t Pose an Existential Threat for America," https://foreignpolicy.com/2021/04/21/china-existential-threat-america/]

There is no doubt that Beijing’s behavior in many areas challenges existing U.S. and allied interests and democratic values. Particularly under Xi Jinping, China has used its greater economic and military power to intimidate rival claimants in territorial disputes and punish nations that make statements or take what Beijing views as threatening or insulting actions. It has engaged in extensive commercial hacking and theft of technologies and favors military intimidation over dialogue in dealing with Taiwan. And it has employed draconian, repressive policies in Tibet and Xinjiang and suppressed democratic freedoms in Hong Kong.

This deeply troubling behavior certainly requires a strong, concerted response from the United States and other nations. But to be effective, such a response also requires an accurate assessment of China’s future impact on the United States and the world.

And in this regard, it is extremely counterproductive to U.S. interests to assert or even imply, as many now do, that the above Chinese actions constitute an all-of-society, existential threat to the United States, the West, and ultimately the entire world, thereby justifying a Cold War-style, zero-sum containment stance toward Beijing. Such an extreme stance stifles debate and the search for more positive-sum policy outcomes while leading to the usual calls for major increases in defense spending.

In fact, there isn’t much actual evidence to support the notion of China as an existential threat. That does not mean that China is not a threat in some areas, but Washington needs to approach this issue based on the facts, not dangerous rhetoric. Unfortunately, right-sizing the challenges that China poses seems to be an impossible task for Washington.

In the most basic, literal sense, an existential threat means a threat to the physical existence of the nation through the possession of an ability and intent to exterminate the U.S. population, presumably via the use of highly lethal nuclear, chemical, or biological weapons. A less conventional understanding of the term posits the radical erosion or ending of U.S. prosperity and freedoms through economic, political, ideational, and military pressure, thereby in essence destroying the basis for the American way of life. Any threats that fall below these two definitions do not convey what is meant by the word “existential.”

As a military power, China has no ability to destroy the United States without destroying itself. China’s nuclear capabilities are far below those of the United States, and its conventional military, while regionally potentially powerful, has a fraction of the budget of that of the United States.

Some argue that China could militarily push the United States out of Asia and dominate that region, denying the country air and naval access and hence support for critical allies. This would presumably have an existential impact by virtue of the supposedly critical importance of that region to the stability and prosperity of the United States. Yet there are no signs that Washington is losing either the will or the capacity to remain a major military actor in the region and one closely connected to major Asian allies, which are themselves opposed to China dominating the region. In reality, the greater danger in Asia is that Washington could so militarize its response to China that its actions and policies become repugnant even to U.S. allies.

This leaves the unconventional threats. Here they are presumably twofold: economic and technological, and in the realm of ideas and influence operations within the United States and other Western countries, including the export of China’s so-called “model” of authoritarian rule to the rest of the world.

The former threats would presumably consist of China attaining a level of total superiority over both economic and technological levers of influence globally and with regard to the United States (perhaps combined with a successful military blocking of U.S. sea lines of communication) that would so impoverish the country as to threaten its existence as a stable and prosperous democracy and bring it under Chinese control. Presumably, the specific basis of such leverage would consist of near-absolute global Chinese dominance over both trade and investment relations and supply chains with the United States and other countries and over all the key technologies driving future growth and military capabilities.

It is virtually inconceivable that China could achieve such a level of dominance over the United States. The United States possesses abundant energy, human, technological, and other resources; a huge and dynamic domestic market; enormous levels of accumulated wealth and capital stocks; and the globe’s financial reserve currency.

In contrast, while China boasts a highly entrepreneurial and dynamic workforce, it labors under major structural and political constraints such as insufficient arable land, a rapidly aging society, a heavy reliance on energy imports, and stifling ideological and state-centered controls across society.

Beijing has certainly used its economic leverage (such as market access) to pressure foreign companies and governments to support Chinese policies or stop what it regards as unacceptable behavior, e.g., regarding Taiwan. While such economic coercion is by no means unique to China, it certainly can erode freedom of speech, thus threatening one of democracy’s core principles. But this hardly rises to the level of an existential threat to American values, given both the limited reach of Chinese economic power and the countervailing global economic power and political influence of democratic states.

#### China’s not a cyber threat.

Jinghua ’19---Lyu Jinghua, visiting scholar with Carnegie’s Cyber Policy Initiative. Her research focuses primarily on cybersecurity and China-U.S. defense relations. [“What Are China’s Cyber Capabilities and Intentions?” *Carnegie Endowment for International Peace,* 4-1-2019, <https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734>] KS

News stories on the cyber threat that China poses appear on a regular basis. Most underscore a view that China is using cyber power to rise and ultimately win global dominance, and that the Chinese government is behind the scenes in many malicious cyber activities. Though many of the allegations focus on the tension between China and the United States on cyber espionage, these actions are unlikely to cause armed conflict since almost all capable actors conduct cyber espionage.

Suspicions of intentions and capabilities of cyber warfare, however, could drag the US and China into arms races, and even hot wars, due to the role cyber tools can play in military operations. Given the risks, it is necessary to examine China’s views on cyber warfare from a narrative that is different from what most readers are familiar with.

CONTEXT FOR CHINA’S VIEWS ON CYBER WARFARE

China’s academic discussion of cyber warfare started in the 1990s when it was called “information warfare.” Impressed by how the US military benefited from the application of high technologies in the Gulf War—and subsequent operations in Kosovo, Afghanistan, and Iraq—China began to realize that there is no way to adequately defend itself without following the changes in the forms of war in which high technologies, mainly information technologies, play more critical roles.

In 1993, two years after the Gulf War, the Chinese military adjusted its military strategic guideline which set “winning local wars in conditions of modern technology, particularly high technology” as the basic aim of preparations for military struggle (PMS). In 2004, one year after the Iraq War, the military’s PMS was changed to “winning local wars under conditions of informationization.” The basic understanding, as elaborated in China’s National Defense in 2004, is that “informationization has become the key factor in enhancing the warfighting capability of the armed forces.”

The first time that the Chinese military publicly addressed cyber warfare from a holistic point of view was in the 2013 version of “The Science of Military Strategy”—a study by the Academy of Military Science. It emphasized that cyberspace has become a new and essential domain of military struggle in today’s world. A similar tone appeared in the 2015 Ministry of National Defense paper entitled “China’s Military Strategy.”

While the latter document modified the basic point for PMS to “winning informationized local wars,” it also addressed cybersecurity for the first time in an official military document. It defined cyberspace as a “new pillar of economic and social development, and a new domain of national security,” and declared clearly that “China is confronted with grave security threats to its cyber infrastructure” as “international strategic competition in cyberspace has been turning increasingly fiercer, quite a few countries are developing their cyber military forces.”

Based on the above approach that China is taking to cyberspace and its own national security, a few conclusions can be drawn. The first is that China has not developed its cyber capabilities in a vacuum. Rather, they have developed them as a response to the changing cyber warfare approaches and practices of other countries, especially those of the US and Russia. The second is that the Chinese government’s views on cyber warfare are consistent with its military strategy, which is modified according to the national security environment, domestic situation, and activities of foreign militaries.

CORE AIMS OF CHINA’S CYBER WARFARE

Though there is no commonly accepted conception of cyber warfare, one made by a RAND Corporation study is frequently quoted by Chinese military analysts: cyber warfare is strategic warfare in the information age, just as it was nuclear warfare in the 20th century. This definition serves as the foundation to argue that cyber warfare has much broader significance to national security and involves competition in areas beyond the military, such as the economy, diplomacy, and social development.

Again, China’s Military Strategy describes the primary objectives of cyber capabilities to include: “cyberspace situation awareness, cyber defense, support for the country’s endeavors in cyberspace, and participation in international cyber cooperation.” The strategy frames these objectives within the aims of “stemming major cyber crises, ensuring national network and information security, and maintaining national security and social stability.”

Of these objectives, an essential one is national security and social stability. As shown by several incidents, such as the protests after Iran’s 2009 presidential election, the Arab Spring, as well as Occupy Wall Street and the London Riots of 2011, social media plays a vital role in helping to plan and carry out such protests and movements. The Chinese government’s monitoring of the internet and social media is based on its potential use as a platform to disseminate information that could cause similar social unrest to spread, which could lead to large-scale social and political instability.

Another essential objective, in common with all states, is defending critical information infrastructure. China is more and more dependent on information networks in all aspects, including in defense. Although it has a large-scale technology industry and possesses the potential to compete with the US in some, most of its core network technologies and key software and hardware are provided by US companies.

China uses the term “eight King Kongs” to describe the top internet companies in its domestic supply chain: Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle, and Qualcomm. Heavy dependence on these companies’ products makes it necessary to work towards developing the domestic technology industry and its capabilities, and to thereby make the country’s internal internet infrastructure more secure. It also makes China believe that its primary mission in cyberspace is to ensure information security of critical areas, which is inherently defensive and non-destructive.

Many, including the US government, have accused the Chinese government and military of cyberattacks in which intellectual property has been stolen. In this regard, there are several distinctions to make clear. The first is between those cyberattacks that aim to destroy, and cyber espionage for intelligence collection. The second is to make clear those forms of cyber espionage that are related to national security concerns and those for economic interests. And the last is between malicious cyber activities that one government or military should take responsibility for, and those that are attributed to a government or military based on less-than-reliable key indicators of where activities originate.

The implications of distinguishing clearly are great and there is a need for far lengthier analyses and studies. Looking at the issue briefly, most accusations levied at China are related to the latter distinction. Until today, there is no irrefutable evidence to show China has been involved in cyberattacks that aim to destroy or have destroyed. While cyber espionage for national security concerns is a common action conducted by most countries, cyber espionage for economic benefit is an accusation continually made against the Chinese government and military. However, there are reports indicating a notable decline in commercial cyber espionage allegedly attributed to Chinese sources, at least in the first few months following an agreement reached between Chinese President Xi Jinping and US President Barack Obama in 2015.

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

Some observers may conclude that it is more worthwhile to invest resources into cyber offense since cyberspace is offense-dominant. However, the principle that the best defense is a good offense is not applicable in cyberspace. As argued by PLA Senior Colonel Li Daguang, after the first round of a cyberattack, the targeted side can respond with a precise counter-attack as long as it has a strong defense. The attacker will then suffer unfavorable outcomes if its defense is not good enough. From this perspective, it is wiser to make efforts in building up a strong defense.

IS CHINA’S CYBER CAPABILITY AS FORMIDABLE AS IMAGINED?

As mentioned, cyber warfare encompasses far more areas than the military and intelligence gathering. It is therefore logical to measure one country’s cyber capability by a more comprehensive evaluation, which at least includes: technological research and development (R&D) and innovation capabilities; information technology industry companies; internet infrastructure scale; influences of internet websites; internet diplomacy and foreign policy capabilities; cyber military strength; and comprehensiveness of cyberspace strategy. If evaluated along all these criteria, China’s cyber power largely lags behind that of the US.

Aside from China’s disadvantages in critical technological self-sufficiency as mentioned above, it is not as advanced in other aspects as well. According to the ICT Development Index (IDI), which is based on 11 indicators to monitor and compare developments in information and communication technology across countries, China respectively ranked 80th, 81st, and 82nd among 176 states in 2017, 2016, and 2015.

Part of China’s low influence on the global internet is due to the fact that its primary languages are not widely used on the internet outside the country. Though there are a massive number of Chinese speakers throughout the world, Chinese languages are only used by 1.7 percent of all websites, while 53.9 percent use English.

China’s internet is also one of the most regularly attacked. According to a report published in February 2019 by Beijing Knownsec Information Technology, China suffered the highest rate of distributed denial of service attacks (DDOS) in the world in 2018—an average of over 800 million a day. Scanning and backdoor intrusions made up the majority of the attacks and about 97 percent were conducted by domestic hackers. However, a growing percentage came from overseas, mostly from the US, South Korea, and Japan. Among all the attacks originating overseas, those that targeted government and financial websites largely outnumbered those on other targets.

Similar statistics can be found elsewhere. However, it is not the intention here to describe how vulnerable China is, but to emphasize that a more comprehensive and objective assessment of China’s cyber power is in urgent need. As Joseph Nye argued, exaggerated fears about growing Chinese power can become a cause of conflict. The same logic applies in cyberspace, especially at a time when China-US bilateral relations are seeing sharp twists and turns.

#### No US-China cyber conflict.

Thomas ’16 (Elizabeth; 8/28/2016; professional cyberdefense expert; “US-China Relations in Cyberspace: The Benefits and Limits of a Realist Analysis,” <http://www.e-ir.info/2016/08/28/us-china-relations-in-cyberspace-the-benefits-and-limits-of-a-realist-analysis/>; Date Accessed: 9/29/2016)

However, a cyber conflict between the US and China is highly unlikely. Examples of attacks with destructive or physical consequences are still very rare (although the number may be increasing). Since the late 1980s, there have been 61 attacks conducted by states against during peacetime, and 24 during wartime.[29] Examples include Russian attacks on Georgia in 2008 and the infamous Stuxnet attack on Iranian nuclear infrastructure (usually attributed to the US and Israel).[30] No state has ever declared a ‘cyberwar’.[31] This is partly because to develop sophisticated attacks like Stuxnet is very difficult, requiring high levels of technical expertise.[32] Attribution is also notoriously difficult in cyberspace. It is extremely tough to trace attacks and states may also use proxy or non-state actors, further confusing the issue.[33] Until recently, the failure to develop an effective deterrence policy has been related to the difficulty in attributing cyberattacks. Nevertheless, the US has “reserve[d] the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law” to respond to hostile acts in cyberspace.[34] China has not used ‘force’ against the US in cyberspace but it is clear that cyberattacks would feature in any broader military clash. Difficulties arise in considering what constitutes a proportionate response to low-level attacks like hacking or cybercrime. It is very unlikely that any incident of that nature could justify a traditional military response. [35] To date, countermeasures have fallen well below the use of military force. The US has instead relied on diplomatic and law enforcement tools: attribution, indictments, and the threat of sanctions.[36]

#### War won’t occur – it’s not in the interest of either the US or China.

Lindsay ’15 (Jon; adjunct professor at the University of Munk in Toronto, Assistant Research Scientist at the University of California Institute on Global Conflict and Cooperation and Assistant, adjunct Professor at the University of California, San Diego School of International Relations and Pacific Studies; Winter 2014/2015; "The Impact of China on Cybersecurity: Fiction and Friction"; <http://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00189>; *International Security*, Vol. 39, No. 3, pp. 7-47; accessed 4/11/17) \*edited for offensive language

Exaggerated fears about the ~~paralysis~~ [shutdown] of digital infrastructure and growing concerns over competitive advantage exacerbate the spiral of mistrust. Closer consideration of domestic factors within China and China’s strategic interaction with the United States reveals a more complicated yet less worrisome situation. This article argues that for every type of purported Chinese cyber threat, there are also serious Chinese vulnerabilities and Western strengths that reinforce the political status quo. Cyberwar between the United States and China, much like U.S.-China conventional war, is highly unlikely. Nevertheless, the economically driven proliferation of information technology enables numerous instances of friction to emerge below the threshold of violence. From a technical perspective, cyber operations are often thought to be inexpensive and effective, but there are underappreciated institutional costs involved in their employment. Moreover, even if actors can overcome the operational barriers associated with ambitious cyber penetrations, they still have incentives to moderate the intensity of their exploitation in order to preserve the benefits that make exploitation worthwhile in the first place. This logic culminates in a relentlessly irritating but indefinitely tolerable stability in the cyber domain. China and the United States can look forward to chronic and ambiguous intelligence-counterintelligence contests across their networks, even as the internet facilitates productive exchange between them.

#### No liberal order collapse---it’s durable

Dr. G. John Ikenberry 18, Ph.D. in Political Science from the University of Chicago, Milbank Professor of Politics and International Affairs at Princeton University in the Department of Politics and the Woodrow Wilson School of Public and International Affairs, March 2018, “Why the Liberal World Order Will Survive,” Ethics and International Affairs, Vol. 32, No. 1, p. 19-22

But does this vision of power transition truly illuminate the struggles going on today over international order? Some might argue no—that the United States is still in a position, despite its travails, to provide hegemonic leadership. Here one would note that there is a durable infrastructure (or what Susan Strange has called “structural power”) that undergirds the existing American-led order. Far-ﬂung security alliances, market relations, liberal democratic solidarity, deeply rooted geopolitical alignments—there are many possible sources of American hegemonic power that remain intact. But there may be even deeper sources of continuity in the existing system. This would be true if the existence of a liberal-oriented international order does not in fact require hegemonic domination. It might be that the power transition theory is wrong: the stability and persistence of the existing post-war international order does not depend on the concentration of American power.

In fact, international order is not simply an artifact of concentrations of power. The rules and institutions that make up international order have a more complex and contingent relationship with the rise and fall of state power. This is true in two respects. First, international order itself is complex: multilayered, multifaceted, and not simply a political formation imposed by the leading state. International order is not “one thing” that states either join or resist. It is an aggregation of various sorts of ordering rules and institutions. There are the deep rules and norms of sovereignty. There are governing institutions, starting with the United Nations. There is a sprawling array of international institutions, regimes, treaties, agreements, protocols, and so forth. These governing arrangements cut across diverse realms, including security and arms control, the world economy, the environment and global commons, human rights, and political relations. Some of these domains of governance may have rules and institutions that narrowly reﬂect the interests of the hegemonic state, but most reﬂect negotiated outcomes based on a much broader set of interests.

As rising states continue to rise, they do not simply confront an American-led order; they face a wider conglomeration of ordering rules, institutions, and arrangements; many of which they have long embraced. By separating “American hegemony” from “the existing international order,” we can see a more complex set of relationships. The United States does not embody the international order; it has a relationship with it, as do rising states. The United States embraces many of the core global rules and institutions, such as the United Nations, International Monetary Fund (IMF), World Bank, and World Trade Organization. But it also has resisted ratiﬁcation of the Law of the Sea Convention and the Convention on the Rights of the Child (it being the only country not to have ratiﬁed the latter) as well as various arms control and disarmament agreements. China also embraces many of the same global rules and institutions, and resists ratiﬁcation of others. Generally speaking, the more fundamental or core the norms and institutions are—beginning with the Westphalian norms of sovereignty and the United Nations system—the more agreement there is between the United States and China as well as other states. Disagreements are most salient where human rights and political principles are in play, such as in the Responsibility to Protect.

Second, there is also diversity in what rising states “want” from the international order. The struggles over international order take many different forms. In some instances, what rising states want is more inﬂuence and control of territory and geopolitical space beyond their borders. One can see this in China’s efforts to expand its maritime and political inﬂuence in the South China Sea and other neighboring areas. This is an age-old type of struggle captured in realist accounts of security competition and geopolitical rivalry. Another type of struggle is over the norms and values that are enshrined in global governance rules and institutions. These may be about how open and rule-based the system should be. They may also be about the way human rights and political principles are deﬁned and brought to bear in relations among states. Finally, the struggles over international order may be focused on the distribution of authority. That is, rising states may seek a greater role in the governance of existing institutions. This is a struggle over the position of states within the global political hierarchy: voting shares, leadership rights, and authority relations.

These observations cut against the realist hegemonic perspective and cyclical theories of power transition. Rising states do not confront a single, coherent, hegemonic order. The international order offers a buffet of options and choices. They can embrace some rules and institutions and not others. Moreover, stepping back, the international orders that rising states have faced in different historical eras have not all been the same order. The British-led order that Germany faced at the turn of the twentieth century is different from the international order that China faces today. The contemporary international order is much more complex and wide-ranging than past orders. It has a much denser array of rules, institutions, and governance realms. There are also both regional and global domains of governance. This makes it hard to imagine an epic moment when the international order goes into crisis and rising states step forward—either China alone or rising states as a bloc—to reorganize and reshape its rules and institutions. Rather than a cyclical dynamic of rise and decline, change in the existing American-led order might best be captured by terms such as continuity, evolution, adaptation, and negotiation. The struggles over international order today are growing, but it is not a drama best told in terms of the rise and decline of American hegemony. If the liberal international order endures, it will be because it is based on more than American hegemonic order. To be sure, the United States did give shape to a distinctive post-war liberal hegemonic system, and many of its features— including the American-led alliance system and multilateral economic governance arrangements—are themselves quite durable. But the broader features of the modern international order are the result of centuries of struggle over its organizing principles and institutions. Rising states face an international order that is long in the making, one that presents these non-Western developing states with opportunities as well as constraints. The struggles over the existing international order will reshape the rules and institutions in the existing system in various ways. But rising states are not simply or primarily “revisionist” states seeking to overturn the order; rather, they are seeking greater access and authority over its operation. Indeed, the order creates as many safeguards and protections for rising states as it creates obstacles and constraints. For example, the World Trade Organization provides rules and mechanisms for rising states to dispute trade discrimination and protect access to markets. After all, more generally, it was this liberal-oriented international order—its openness and rules—that provided the conditions for China and other rising states to rise. Indeed, if the liberal international order survives, it will be in large part due to the fact that the constituencies for such an order that stretch across the Western and the non-Western worlds are larger than the constituencies that oppose it. We can look more closely at these sources of continuity and constituency.

### AT: Grey Zone---1NC

#### No grey-zone escalation – the entire strategy is cautiously designed to avoid retaliation.

Kakoti ’20 [Ananya Raj; 7/26/20; contributor to Modern Diplomacy, MA in International Relations from Jawaharlal Nehru University; "The Grey Zone: Understanding a Nuclear Age strategy through the South China Sea Dispute," https://moderndiplomacy.eu/2020/07/26/the-grey-zone-understanding-a-nuclear-age-strategy-through-the-south-china-sea-dispute/]

The detonation at the Trinity test site near Alamogordo, New Mexico in mid-July of 1945 marked the beginning of the ‘nuclear age’. Three weeks later, the world saw what the “Little Boy” and “Fat Man” were capable of after they were dropped on the Japanese cities of Hiroshima and Nagasaki, respectively and the Hibakusha[1] are still the proof of that. This has increased apprehension among countries towards engaging in traditional warfare, thus making it inevitable for revisionist powers to employ alternative tactics to challenge the existing world order without any major escalation. This is where one can observe an increase in the use of the grey zone strategy, which is not a novel tactic and has been present since centuries. However it has reemerged, as the need of the hour in the present political climate is unconventional stratagem. It is an identifying strategy in the nuclear age which is resistant of a full blown out war. This strategic campaign has taken a new form in the current age with the aid of cyber weapons, advanced information technology and civilian tools allowing the increase in importance of the tactic and applicability.

Understanding the Grey Zone Strategy

The new approach has been provided a fertile environment to flourish with an increase in revisionist intent, strategic gradualism and employability of unconventional tool. The revisionist intent stems from the fact that major powers may want to change the existing global order. Although there is a wide spectrum of revisionist states, the “measured revisionists” (Mazarr: 2015) are the rising powers with value for rule-based order and no intent of aggressive warfare but they do expect a transformation of the existing system and to do so they will take cautious and impactful steps to make a difference. The reason behind the tactful approach is that they want to tilt the power axis in their favour without disturbing the system altogether. The international system is being witness to the revisionist states which shall employ the grey zone strategy to cure their dilemmas of being dissatisfied of the system while being dependant on it.

### AT: Grey Zone---2NC

#### No escalation from grey-zone activity – the entire strategy is premised on a recognition of mutually assured destruction, and a prioritization of gradual change over risky disruption. Grey zone actors fear conventional escalation and are cautious to avoid conventional retaliation, much less nuclear – that’s Kakoti.

#### Economic interdependence moderates grey-zone conflict – incentives peaceful resolution with Russia.

Carment and Belo ’20 [David and Dani; 6/9/20; Professor of International Affairs at Carleton University, PhD in Political Science from McGill University; PhD Candidate and Doctoral Fellow in International Conflict Management and Resolution at Carleton University; "Gray-zone Conflict Management: Theory, Evidence, and Challenges ," https://www.airuniversity.af.edu/JEMEAA/Display/Article/2213954/gray-zone-conflict-management-theory-evidence-and-challenges/]

In the modern interconnected world, there is an incentive to employ willful blindness in relation to potential threats emanating from geostrategic opponents such as Russia. These authoritarian states provide Western liberal democracies access to both inexpensive labor and vast energy resources required to fuel economic growth. Greed for short-term economic growth, for example through reliance on comparative advantage principles, however, may have long-term security consequences. However, economic interconnectedness may also create opportunities for conflict resolution. This means, even though foreign policy of state actors in gray-zone conflicts seems to be guided by realist thinking and pursuit of maximum relative gains, liberal institutionalism should not be outright dismissed.

As we highlight in this article, the common wisdom in recent literature on gray-zone conflicts has been to treat the economic domain as an area of threat. However, for the purpose of conflict management in Ukraine, Moscow’s increasingly interconnected energy relations with the EU may also be an opportunity for peaceful conflict resolution.

Re-engagement between the EU and Russia demonstrates that complex interdependence can provide an opportunity for conflict resolution in Ukraine.26 In the contemporary interconnected world, there is no clear hierarchy between economic and military issues among states. Moreover, as the cost of engagement in conventional military operations has increased, the economic domain becomes increasingly important for exercise of power and overall interaction between states. The relationship observed is that as economic interdependence increases between nations, the cost of upsetting the mutually beneficial environment through conflict increases. Thus, states often choose to forego conflict and resolve disputes cooperatively.

#### Grey zone activity represents new peace rather than new war.

Raine ’19 [John; 4/3/19; Senior Adviser for Geopolitical Due Diligence; "War or peace? Understanding the grey zone," https://www.iiss.org/blogs/analysis/2019/04/understanding-the-grey-zone]

Policymakers shaping national security strategies attempt to apply as elastic a definition of the threat as possible, while ensuring that such strategies still meet conventional, standing defence obligations too. But given the incremental growth of designated threats, this is not sustainable. What principles might help them in navigating the grey zone?

Discipline in definition

The impulse to designate this domain as a place of conflict rather than competition is strong. After all, conflict is more likely to command attention and resources than peace. Yet much, but not all, of what we see being conducted in this space could be characterised as features of the difficult, new peace as much as the new warfare.

The range of means being used to project state power is wide and the tempo fierce, but that does not mean that a state of war exists. The contestation we are seeing through unregulated means, in particular in the field of information and subversion, might for all its bumpiness be what the new peace rather than the new war looks like.

### AT: Space War---1NC

**No space war**

**Hall 15** [Luke Penn-Hall, Analyst at The Cipher Brief, M.A. from the Johns Hopkins School for Advanced International Studies, B.A. in International Relations and Religious Studies from Claremont McKenna College, “5 Reasons “Space War” Isn’t As Scary As It Sounds”, The Cipher Brief, Aug 18, 2015, <https://www.thecipherbrief.com/article/5-reasons-%E2%80%9Cspace-war%E2%80%9D-isn%E2%80%99t-scary-it-sounds>]

The U.S. depends heavily on military and commercial satellites. If a less satellite-dependent opponent launched an anti-satellite (ASAT) attack, it would have far greater impact on the U.S. than the attacker. However, it’s not as simple as that – for the following reasons: 1. An ASAT attack would likely be **part of a larger, terrestrial attack**. An attack on space assets would be no different than an attack on territory or other assets on earth. This means that no space war would stay limited to space. An ASAT campaign would be part of a larger conventional military conflict that would play out on earth. 2. Every country with ASAT capabilities also needs **sat**ellite**s**. While the United States is the most dependent on military satellites, most other countries need satellites to participate in the global economy. All countries that have the technical ability to play in this space – the U.S., Russia, China and India - also have a **vested interest** in preventing the militarization of space and protecting their own satellites. If any of those countries were to attack U.S. satellites, it would likely **hurt them** far more than it would hurt the United States. 3. Destruction of satellites could create a damaging chain reaction. Scientists warn that the violent destruction of satellites could result in an effect called an ablation cascade. High-velocity debris from a destroyed satellite could crash into other satellites and create more high-velocity debris. If an ablation cascade were to occur, it could render certain orbital levels completely unusable for centuries. 4. Any country that threatened access to space would threaten the global economy. Even if a full-blown ablation cascade didn’t occur, an ASAT campaign would cause debris, making operating in space more hazardous. The global economy relies on satellites and any disruption of operations would be met with worldwide disapproval and severe economic ramifications. 5. International **Prohibits** the Use of ASAT Weapons. Several international treaties expressly **prohibit signatory nations** from attacking other countries’ space assets. It is generally accepted that space should be treated as a global common area, rather than a military domain. While it remains necessary for military planners to create contingency plans for a, space war it is a **highly unlikely** scenario. All involved parties are **incentivized against** attacking. However, if a space war did occur, it would be **part of** a larger conflict **on Earth**. Those concerned about the potential for war in space should be more concerned about the potential for war, period.

#### No miscalc or escalation

**Pavur 19** [James, DPhil Researcher at the Cybersecurity Centre for Doctoral Training at Oxford University, and Ivan Martinovic, Professor of Computer Science in the Department of Computer Science at Oxford University, “The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space”, 2019 11th International Conference on Cyber Conflict: Silent Battle, <https://ccdcoe.org/uploads/2019/06/Art_12_The-Cyber-ASAT.pdf>]

A. Limited Accessibility Space is difficult. Over 60 years have passed since the first Sputnik launch and only nine countries (ten including the EU) have orbital launch capabilities. Moreover, a launch programme alone does not guarantee the **resources** and **precision required** to **operate a meaningful ASAT capability**. Given this, one possible reason why **space wars have not broken out** is simply because only the US has ever had the ability to fight one [21, p. 402], [22, pp. 419–420]. Although launch technology may become cheaper and easier, it is unclear to what extent these advances will be distributed among presently non-spacefaring nations. **Limited access to orbit** necessarily reduces the scenarios which could plausibly escalate to ASAT usage. Only major conflicts between the handful of states with ‘space club’ membership could be considered possible flashpoints. Even then, the **fragility of an attacker’s own space assets** creates **de-escalatory pressures** due to the **deterrent effect of retaliation**. Since the earliest days of the space race, dominant powers have recognized this dynamic and demonstrated an inclination **towards de-escalatory space strategies** [23]. B. Attributable Norms There also exists a **long-standing normative framework** favouring the **peaceful use of space**. The effectiveness of this regime, centred around the Outer Space Treaty (**OST**), is highly contentious and many have pointed out its serious legal and political shortcomings [24]–[26]. Nevertheless, this status quo framework has somehow supported over **six decades of relative peace** in orbit. Over these six decades, **norms have become deeply ingrained** into the way states describe and perceive space weaponization. This de facto codification was dramatically demonstrated in 2005 when the US found itself on the short end of a 160-1 UN vote after opposing a non-binding resolution on space weaponization. Although states have occasionally pushed the boundaries of these norms, this has typically occurred through incremental legal re-interpretation rather than outright opposition [27]. Even the most notable incidents, such as the 2007-2008 US and Chinese ASAT demonstrations, were couched in rhetoric from both the norm violators and defenders, depicting space as a peaceful global commons [27, p. 56]. Altogether, this suggests that **states perceive real costs** to breaking this normative tradition and may even **moderate their behaviours** accordingly. One further factor supporting this norms regime is the **high degree of attributability** surrounding ASAT weapons. For kinetic ASAT technology, **plausible deniability** and **stealth** are essentially **impossible**. The literally explosive act of launching a rocket cannot evade detection and, if used offensively, retaliation. This imposes **high diplomatic costs** on ASAT usage and testing, particularly during peacetime. C. Environmental Interdependence A third stabilizing force relates to the **orbital debris consequences** of ASATs. China’s 2007 ASAT demonstration was the largest debris-generating event in history, as the targeted satellite dissipated into thousands of dangerous debris particles [28, p. 4]. Since debris particles are indiscriminate and unpredictable, they often threaten the attacker’s own space assets [22, p. 420]. This is compounded by Kessler syndrome, a phenomenon whereby orbital debris ‘breeds’ as large pieces of debris collide and disintegrate. As space debris remains in orbit for hundreds of years, the **cascade effect** of an ASAT attack can constrain the attacker’s long-term use of space [29, pp. 295– 296]. Any state with kinetic ASAT capabilities will likely also operate satellites of its own, and they are necessarily exposed to this collateral damage threat. Space debris thus acts as a strong strategic deterrent to ASAT usage.

### AT: Space War---2NC

#### No escalation---diplomacy will ramp up and head it off

Dr. Steven **Lambakis 1**, Senior Defense Analyst at the National Institute for Public Policy, Ph.D. at Catholic University, and Managing Editor of Comparative Strategy, “Space Weapons: Refuting the Critics”, Policy Review, Number 105, 2/1/2001, http://www.hoover.org/publications/policy-review/article/6612

To these examples we may add a long list of tactical blunders growing out of ambiguous circumstances and faulty intelligence, including the U.S. bombing in 1999 of the Chinese Embassy in Belgrade during Kosovo operations. Yet though these tragic actions occurred in near-war or tinderbox situations, they did not escalate or exacerbate local instability. The world also survived U.S.-Soviet "near encounters" during the 1948 Berlin crisis, the 1961 Cuban missile crisis, and the 1967 and 1973 Arab-Israeli wars. Guarded diplomacy won the day in all cases. Why would disputes affecting space be any different? In other words, it is not at all self-evident that a sudden loss of a communications satellite, for example, would precipitate a wider-scale war or make warfare termination impossible. In the context of U.S.-Russian relations, communications systems to command authorities and forces are redundant. Urgent communications may be routed through land lines or the airwaves. Other means are also available to perform special reconnaissance missions for monitoring a crisis or compliance with an armistice. While improvements are needed, our ability to know what transpires in space is growing — so we are not always in the dark. The burden is on the critics, therefore, to present convincing analogical evidence to support the notion that, in wartime or peacetime, attempts by the United States to control space or exploit orbits for defensive or offensive purposes would increase significantly the chances for crisis instability or nuclear war. In Washington and other capitals, the historical pattern is to use every available means to clarify perceptions and to consider decisions that might lead to war or escalation with care, not dispatch.

#### Space hotline solves.

Opper 15 – Chris Opper, managing editor at Bloomberg Law. [China and the U.S. Can Avoid a Space War by Making That Hotline Bling, 12-9-2015, https://science.howstuffworks.com/china-the-us-can-avoid-a-space-war-making-that-hotline-bling.htm]

The United States and China aren't 100 percent chummy these days, but that doesn't mean the two superpowers don't talk. As Uncle Sam and the world's largest Communist country look to outdo each other on the economic, military and political fronts, the two countries also recently came together to try to avoid a full-blown fight either in outer space. A new "hotline" will make it easier for officials from the States and the Middle Kingdom to share information about what they're doing up there in the final frontier, all to avoid any international dust-up.

The new communication system will allow the countries' leaders to talk directly about their space activities via secure text message. It's intended to cut through diplomatic channels and other bureaucratic middlemen so that the presidents can speak quickly to keep each other informed about operations in space. It's also meant to avoid both accidental collisions and any possible misinterpretations about space activity that could be taken as acts of aggression.

The space hotline is a first between the two countries – the U.S. and Russia already have one in place – and world leaders have been relying on similar systems to avoid hostilities on the ground and in the air for decades.

Shortly after stepping back from the ledge of World War III during the Cuban missile crisis, the U.S. and Russia established a direct telegraph system to allow them to alert each other of military and other moves. It turns out that the mythical red phone connecting the Pentagon with the Kremlin exists only on the big screen. Still, a super-secure email and audio messaging system linking the two countries has proven its worth as a way to keep leaders aware of each other's intentions when it comes to unrest in other nations.

During a 1967 skirmish between Israel and its neighbors in the Middle East, for example, President Lyndon Johnson used what was then a teletype terminal to inform Russian leader Alexei Kosygin that U.S. military planes would be flying to the Mediterranean Sea.

Richard Nixon used the hotline for similar updates during wars in Pakistan and Cyprus during the late 1960s. The goal was to keep the Russians aware of certain military movements so that they didn't think the Americans were picking a fight.

The same idea has helped build the existing war hotlines that China shares with Russian, India, Vietnam and Korea. Earlier efforts to create a direct communication line for China and the U.S. have borne little fruit. After the Tiananmen Square massacre in 1989, President George H.W. Bush tried contacting his Chinese counterpart phone only to have that call go unreturned.

This new hotline offers something for both sides: Namely, the chance to avoid orbital warfare and a space arms race.

## Solvency

### Solvency---1NC

#### Plan’s not a silver bullet---their solvency advocate

Smeets ’19 [Max; October 14; 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; Lawfareblog, “NATO Allies Need to Come to Terms With Offensive Cyber Operations,” <https://www.lawfareblog.com/nato-allies-need-come-terms-offensive-cyber-operations>]

Not a Silver Bullet

While I argue that the NATO memorandum of understanding on offensive cyber operations in systems or networks based in allied territory can greatly help in promoting stability and enhancing confidence among allies, it is not a silver bullet. It can only reduce allied concerns rather than mitigate them. Military cyber organizations may still conduct effect-based operations in allied territory without consent, leading allies to assert that their sovereignty has been violated. And there’s another crucial player involved. As Gen. Nakasone noted in the Joint Force Quarterly article, cyberspace is owned largely by the private sector. They deserve a seat at the table as well.

#### OCOs fail---cost-ineffective, and the US can’t transfer infrastructure to allies

Smeets ’22 [Max; Feb 23; 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; Security Studies, “Cyber Arms Transfer: Meaning, Limits, and Implications,” vol. 31]

An offensive cyber organization will also need attack tools to achieve a certain effect or goal. Payloads greatly vary in size. On one end of the spectrum, they can come as very lightweight files that are easy to distribute, but once executed they will trigger the download of a much larger piece of malware.43 On the other end of the spectrum, payloads can be multiple megabytes (MBs) in size. A multipurpose toolkit was discovered in 2012 by researchers from Kaspersky Lab, which they called Flame. Whereas the Stuxnet code is “only” about 1 MB in size, Flame’s malware code is about twenty times larger—and still not fully understood.44

It is difficult—and cost inefficient—to build an arsenal of tools for a more mature cyber command or intelligence agency. Although early development and stockpiling would be desirable to ensure swift deployment if the need arises, tools often must be tailored to the target and desired effect (especially if the actor desires stealth and stability), which means that in-time development is often necessary. Consider, for example, a case in which the leadership of a command decides there is a need to target a specific programmable logic controller (PLC) used to run a certain manufacturing process. The developers will likely have to build tools that can work on that particular PLC model. If leadership subsequently decides to target a different process, developers will have to deploy a new toolset.

Finally, the more features of the target you can use, the less you need yourself. Napoleon was famous for making sure his troops were living off the land through which they moved. It allowed his army to travel light and march long distances. This notion of living off the land is also commonly applied to cyber operations. The attacker may use something exotic to get into a target’s network, but it makes a lot of sense to subsequently use the target’s existing infrastructure to gain further network access. For example, existing communication lines to push out notifications can be used to move through an organization’s network. Living off the land is not merely done for cost-efficiency benefits. The practice is equally, if not more, important for remaining undetected.

Fourth, to effectively run cyber operations an organization requires infrastructure, broadly defined as the processes, structures, and facilities needed to pull off an offensive cyber operation. This element can be split into two categories: control infrastructure and preparatory infrastructure. Control infrastructure refers to processes directly used to run an operation. This is also the type of infrastructure that is generally burned down after a failed operation. It includes domain names of phishing sites, leaked email addresses, or other abused technologies.45 It also concerns C&C infrastructure used in remotely conducted operations to maintain communication with compromised systems within a target network. Depending on an operation’s goal and resources, the C&C infrastructure might be as basic as a single server operating on the external network.46 At the same time, an organization may run a whole set of operations simply to compromise legitimate web servers to use them for C&C later.

#### Refusal to specify Article 5 conditions wrecks effective cyberstrategy

Lonergan ’22 [Erica; April 15; assistant professor in the Army Cyber Institute and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University; Foreign Affairs, “The Cyber-Escalation Fallacy,” <https://www.foreignaffairs.com/articles/russian-federation/2022-04-15/cyber-escalation-fallacy>]

A one-size-fits-all approach to adversary cyber-operations may raise particular problems in the Ukraine conflict. Anticipating potential Russian cyberattacks against member states, NATO leaders have reaffirmed that Article 5, the treaty’s collective defense clause, applies to cyberspace, but they have also expressed ambiguity about what specific operations might trigger it. A lack of clarity about how thresholds and responses are defined risks undermining the credibility of this pledge and the effectiveness of NATO’s overall cyberstrategy.

#### Clarifying thresholds for invoking article V is necessary --- plan fails to restore cohesion

Robin Emmott 18, Reuters diplomatic correspondent in Brussels covering NATO, EU defence and foreign policy, while keeping a special eye on relations with China and the U.S., “NATO cyber command to be fully operational in 2023,” Reuters, 10/16/18, https://www.reuters.com/article/us-nato-cyber-idUSKCN1MQ1Z9

MONS, Belgium (Reuters) - A new NATO military command center to deter computer hackers should be fully staffed in 2023 and able to mount its own cyber attacks but the alliance is still grappling with ground rules for doing so, a senior general said on Tuesday.

While NATO does not have its own cyber weapons, the U.S.-led alliance established an operations center on Aug. 31 at its military hub in Belgium. The United States, Britain, Estonia and other allies have since offered their cyber capabilities.

“This is an emerging domain and the threat is growing,” said Major General Wolfgang Renner, a German air force commander who oversees the new cyber operations center, or CYOC, in Mons.

“We have to be prepared, to be able to execute operations in cyberspace. We have already gone beyond protection and prevention,” he told Reuters during a NATO cyber conference.

NATO communication and computer networks face hundreds of significant hacking attempts every month, according to the NATO Communication and Information Agency, while experts say Russia, North Korea and China are constantly deploying sophisticated computer hacking weapons and surveillance software.

Accusations by Western governments this month that Russia waged a global hacking campaign have raised the profile of NATO’s evolving strategy as allied governments look for a response. The European Union on Monday discussed its options, including a special economic sanctions regime to target cyber attackers.

“Our ultimate aim is to be completely aware of our cyberspace, to understand minute-by-minute the state of our networks so that commanders can rely on them,” said Ian West, chief of cyber security at the NATO communication agency.

When fully operational, the cyber center aims to coordinate NATO’s cyber deterrent through a 70-strong team of experts fed with military intelligence and real-time information about hackers ranging from Islamist militants to organized crime groups operating on behalf of hostile governments.

ARTICLE 5 DEBATE

NATO has formally recognized cyberspace as a new frontier in defense, along with land, air and sea, meaning battles could henceforth be waged on computer networks.

The center could potentially use cyber weapons that can knock out enemy missiles or air defenses, or destroy foes’ computer networks if commanders judge such a cyber attack is less harmful to human life than a traditional offensive with live weaponry.

That is now the subject of intense debate at NATO, with alliance commanders saying publicly that cyber will be an integral part of future warfare but allies unclear what would trigger NATO’s Article 5 (collective defense) clause.

“Our concept of operations, a toolbox for short-notice decisions about how to respond, is not in place yet. This is one of the challenges we face,” Renner said.

If NATO can agree cyber warfare principles, the alliance hopes to integrate individual nations’ cyber capabilities into alliance operations, coordinated through the Mons cyber operations center and under the command of NATO’s top general, the Supreme Allied Commander Europe, or SACEUR.

That could allow the top general to take quick decisions on whether to use cyber weapons, similar to existing agreements for NATO’s air defenses and its ballistic missile shield, where a commander has only minutes to decide what action to take.

### Article 5 Key---2NC

#### Clarification of article V is key

David H. Ucko 10, adjunct fellow at the Department of War Studies, King's College London"Resetting Article 5: Toward a New Understanding of NATO's Security Guarantees", World Politics Review, https://www.worldpoliticsreview.com/articles/6838/resetting-article-5-toward-a-new-understanding-of-natos-security-guarantees

For all this, the alliance badly needs a clarification of its collective security mechanism, for, though its current ambiguity may fool prospective adversaries, it really should not fool NATO itself. There is a need, in other words, to chart a middle path between traditionalists and revolutionaries, whereby NATO maintains a solidarity clause but comes to a new, narrower and shared understanding of its meaning and implications. The point would be to downgrade the expectations that come with NATO membership by talking more honestly, within NATO, about what the alliance is likely and able to commit to.

First, it would be necessary to convey, in private, to members that an Article 5 response is not automatic, but is rather the product of intensely political processes within each NATO state, and that even if a response is forthcoming, there is no way of guaranteeing that it will be timely or particularly effective. The language of an unflinching, immediate, collective and effective response may be appropriate for audiences outside of NATO, but not for internal discussion. Within the alliance, less grandstanding rhetoric and greater transparency would reduce the scope for obfuscation. The language of collective security would remain -- for symbolic reasons, for the deterrent role that Article 5 still plays and for the foundation it provides for retaliatory action. But the point would be to re-emphasize within the alliance the oft-forgotten provision of Article 5 whereby each member takes only "such action as it deems necessary" when fulfilling its security obligations.

Second, NATO would need to delineate much more clearly what types of threats it is capable of countering. No doubt a nontraditional attack can be as devastating as a military strike, but it does not follow that NATO is equally prepared to handle both. The decision regarding NATO's role in any incident must be based not only on the severity of a potential attack, but also on NATO's ability to mount an effective response. Whereas the language of solidarity following the Sept. 11 attacks was certainly appropriate, a case can be made that NATO ultimately overextended itself in invoking Article 5. The invocation established a dangerous precedent for the kinds of threats that the article might cover, many of which NATO lacks the expertise to deter, to forestall or to counter. Talking loudly about collective defense against non-traditional attacks without a concomitant ability to deliver when they occur is likely to provoke a crisis of credibility for the alliance.

Similar gaps between expectations and capabilities surround the issue of cybersecurity, which Secretary-General Rasmussen recently suggested should be covered by Article 5, as well as energy-security threats and economic warfare: NATO undoubtedly has a role to play in protecting its members from these potentially very harmful forms of attack, yet until the capability is created, it may want to interpret its security guarantees more narrowly. This also raises the question of how serious an attack in a nontraditional domain would need to be to trigger Article 5 considerations. Some informal criteria would need to be agreed upon to inform expectation, yet clearly this is also something that would need to be settled behind closed doors, so as not to invite attack and provocation under the established threshold or precisely where NATO's guarantees are the weakest.

Naturally, the prospect of agreeing within NATO to a more honest but weaker Article 5 regime will elicit much support among those who rely most on NATO's security guarantees. Nonetheless, greater transparency is preferable to false hope. A hardnosed stocktaking of what NATO can and cannot do would also provide for a more promising foundation on which progress could be made: a common appraisal of problems faced and a framework for finding limited solutions, where possible. This would also allow those nations that feel most vulnerable to make their own security arrangements, even if that means seeking relationships outside the alliance structure. In the event that such arrangements are inimical to NATO's interests, the onus would then be on the alliance itself to provide a preferable alternative. In that sense, greater transparency would make the self-interest of individual members the foundation of NATO's collective defense mechanism, rather than the need to ensure the alliance's solidarity or prove its relevance, the reasons most often used to justify Article 5 security guarantees today but whose rhetorical appeal rarely translates into action.

Upholding a security regime that is limited, patchy and short on substance is far from ideal, yet it would accurately reflect the alliance's current intentions, capabilities and political will. So long as both those making the promise of collective defense and those hoping to take it up are mutually aware of its true possibilities and very real limitations, it may be the least-bad and most-viable way out of an awkward situation.

#### Without clarifying definitions, the plan is useless

Christopher Woody 18, Washington, DC-based editor covering military and defense issues and foreign affairs.“ NATO leaders are worried about cyberattacks, but it's not clear they all agree on what that means,” Business Insider, 10/1/18, https://www.businessinsider.com/nato-leaders-agree-cyberattacks-are-threat-but-cant-agree-definition-2018-10

NATO leadership appears to be in agreement that cyberattacks and forms of hybrid warfare that involve it are a growing threat to the alliance, but it's still not totally clear how its members define and evaluate that threat, and that raises questions about how they'll respond to an attack.

In late 2014 — several months after the Russian annexation of Crimea and incursion into Ukraine — NATO leaders agreed that a large-scale cyberattack on one member could be considered an attack on the entire alliance, potentially leading to a military response.

"Today we declare that cyber defense is part of NATO's core task of collective defense" NATO's secretary general at the time, Anders Fogh Rasmussen, said of the decision.

The emphasis on the cyber realm grew considerably in 2017.

At the beginning of that year, NATO announced plans to spend more than $3 billion to upgrade its satellite and computer technology over three years, including some $900 million on computer systems that help command air and missile defenses and $80 million to improve protection against cyberattacks at NATO's 32 main locations.

At the end of that year, NATO announced plans to increase its cyber-defense capabilities, adapting its command structure to integrate cyber weapons into its military operations in what one of the alliance's former cyber-defense advisers called one of the organization's biggest policy changes in years.

Cyberattacks, along with other forms of hybrid warfare that fall short of open combat, have complicated things for NATO, current Secretary General Jens Stoltenberg said in September.

With cyber operations, Stoltenberg said, "it's very hard to tell exactly who attacked you. It's very hard to say exactly where it takes place."

"So we live in a ... completely different security environment with a more blurred line between peace and war," he added.

In an interview on the sidelines of the UN General Assembly in New York City, Spanish Prime Minister Pedro Sanchez echoed that view.

"In my opinion, cybersecurity, a fight against hybrid wars or strategies, is one of the major challenges for NATO," Sanchez said during an interview with Reuters, adding that the alliance needs to remain vigilant on its eastern and southern frontiers as well.

Despite the growing focus and increased spending, NATO's response to cyber threats appears to have a problem with definitions — namely, what constitutes an attack and how severe it is.

In late 2017, after officials from France, NATO, and the EU offered several widely varying tallies of cyberattacks in 2016, Stefan Soesanto, a former cybersecurity and defense fellow at the European Council on Foreign Relations, asked their agencies to ask what incidents were included in their totals and if their standards were public, receiving no response or no comment from each.

"But without published standards and discernable metrics, such warnings are of no real value to the public," Soesanto wrote for Defense One in September.

"We simply do not know whether 6,000 annual attacks against NATO's infrastructure is a lot or whether any of the 24,000 attacks against the French [Ministry of Defense] were serious," Soesanto added. "All we know is that something was counted by someone somehow to somewhat explain the threat environment."

Further inquiry found that even within countries, different agencies had different definitions for what constituted a cyberattack and different ways of determining their severity.

This incoherence creates several problems, according to Soesanto.

The lack of a unifying standard will lead public officials to over- and under-state such incidents, which in turn undermines the public's ability to understand the threat.

A lack of cohesion also hinders cyber-defense efforts within and between governments, and, perhaps most important, muddies the rules of engagement.

"NATO member states are embroiled in discussing cyber deterrence frameworks, offensive operations, and creating norms and rules for state behavior in cyberspace, they have still not reached consensus on how to actually count and categorize cyber incidents across the alliance," Soesanto writes.

### OCO’s Bad---1NC

#### OCOs cause positive feedback that intensify cyber conflicts and lower the nuclear threshold

**Healy ’19** [Jason Healy, School of International and Public Affairs, Columbia University, “The implications of persistent (and permanent) engagement in cyberspace” Journal of Cybersecurity, 2019, https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878#140575448]

The new strategy is a compelling assessment of cyber conflict as a state of constant contact and presents a strong case that reduced operational constraints enabling tactical friction to regain the initiative will nudge conflict back towards lower levels of aggression [9]. It is worth noting that forward defense is only one among several policies that can be termed active defense or indeed cyber deterrence: the administration of Donald Trump has continued and expanded a wide set of policy tools used by previous administrations, including sanctions and indictments [59]. It has also introduced new responses, most importantly coordinated international attribution of Russian [60] and North Korean [61] operations seen as particularly insulting to global norms and getting search warrants for computers outside of US territory in order to disrupt a North Korean botnet [62]. Still, it is no wonder that the US military has embraced an academic concept justifying its decade-long desire for reduced operational constraints and a more active posture to “take the fight to the enemy.” There remain major concerns. An overarching worry is that US Cyber Command does not appear to see this approach as fundamentally risky. The Vision asserts that the Command wants to be “not risk averse but risk aware” but it only highlights one procedural risk (an insufficient body of highly trained personnel) and one diplomatic risk (adversaries will falsely “seek to portray our strategy as ‘militarizing’ the cyberspace domain”). But those are the only risks the Command can imagine, or at least, is willing to publicly acknowledge. Indeed, because defending forward is framed as essential—“if the United States is to shape the development of international cyberspace norms, it can do so only through active cyber operations” [54], and “not a choice, but a structurally and strategically driven imperative” [57]—then the main risk is failing to adapt quickly and forcefully enough. To get to the promised land of milk and honey, superiority and stability, there is only one path: forward defense. It is technically determined that there is a single dominant strategy, one that is the best regardless of the strategies chosen by US adversaries. As in the Cold War, the military is again attempting to “pose starker alternatives and to couch them in terms of necessity rather than choice:” either remove constraints on the military or lose [63]. Imperatives are slippery things. Some are not imperatives at all, just a particularly unyielding perspective or preference presented as a dichotomy. How many US airmen died in World War Two because of the bomber-driven cult of the offensive? Other imperatives may be critical to tactical success but imperil the larger strategy, perhaps winning the battle but losing the war. The battlefield imperative to use overwhelming firepower can, for example, be fatal to a counterinsurgency strategy if it causes extensive collateral damage. Even seeming strategic imperatives can lead to catastrophic national security outcomes, as with Wilhelmine Germany’s pursuit of a grand fleet-in-being to challenge the British [64]. The dynamics here may be similar. A more thorough assessment of the risks must be rooted with the simplest one, the strategy might fail and intensify competition. Many assumptions, apparently unrecognized, underlie the belief that the USA can have both superiority and overmatch as well as stability. Yet, in a system as complex as the Internet, “we can never merely do one thing” [9, page 10].8 As Herb Lin and Max Smeets of Stanford University highlight, “neither ‘escalate’ or ‘escalation’ appear in the [Vision] document,” a significant omission which suggests US Cyber Command is downplaying, or not fully thinking through, the full dynamics of conflict [65]. A more engaged forward defense might result not in “negative” feedback—reducing conflict by bringing it back to the historical norm—but instead “positive” feedback, exacerbating the conflict and adversaries may see the new US vision as a challenge to rise to, rather than one from which to back away [9, chapter 4]. According to my colleague Robert Jervis, “a failure to anticipate positive feedback is one reason why consequences are often unintended,” [9, page 165] and sufficient positive feedback can push the system past a tipping point, at which the system resets itself into a new, and potentially far more dangerous, equilibrium. States have decided to keep their attacks below certain thresholds, but conflict and competition in cyberspace is only a few decades old. This may only be a phase, and an early one at that. As cyberspace becomes more existential for more states, the stakes continue to rise, elevating the risks along with them.

#### OCO’s cause hack-backs

Sorcher ’15 [Sara; April 6; National Security Correspondent for the National Journal and Deputy Editor of Passcode at the Christian Science Monitor; "Influencers: Companies should not be allowed to hack back," Passcode. http://passcode.csmonitor.com/influencers-hackback]

Even as companies are hit by increasingly sophisticated cyberattacks, 82 percent of Influencers say they should not be allowed to "hack back" to retrieve stolen data or shut down computers targeting their networks. There's been hot debate over companies' rights to defend themselves in cyberspace by taking offensive action. The US government has been reluctant to intervene as foreign-based hackers strike private companies – leaving this type of hacker-on-hacker retaliation a tantalizing option for some victims. But Passcode's pool of experts from across government, the private sector, and the privacy advocacy community warn the strategy, commonly known as "hacking back," could go very wrong. "Hacking back is the worst option for companies because they don't know who is on the other end of the keyboard nor what capabilities that person has. What may start as simple [intellectual property] theft could, after a 'hacking back' attempt, result in the utter destruction of the entire network," says Jeffrey Carr, president of cybersecurity firm Taia Global. "For a small to medium-sized company, that could put them out of business. For an enterprise, it could cost them hundreds of millions of dollars. People with any life experience usually understand and respect the adage 'never pick a fight with a stranger.' The same adage applies in cyberspace." It could also spark foreign policy consequences. Hackers could be backed by other nation-states, heightening the prospect of a wider digital conflict inadvertently launched by the private sector. "We should not be looking to escalate a cyberwar; we should be trying to defuse it," said one Influencer who chose to remain anonymous. Another added: "Would we let it happen in the physical world?" The Passcode Influencers Poll brings together a diverse group of more than 90 security and privacy experts from across government, the private sector, academia, and the privacy community. To preserve the candor of their responses, Influencers have the choice to keep their comments anonymous, or voice their opinions on the record. Some Influencers drew upon their own personal experiences to explain the potential perils. "I am an old Army cyber guy and I had a boss who, when I was feeling frustrated when I could not respond in kind back to a bad guy who was attacking us, would pull me aside and say, 'You know what, Rick? The enemy gets a vote,' " says Rick Howard, chief security officer for Palo Alto Networks. "Just because you are able to jab back against a cyber adversary does not mean that you should. Do you think the bad guy will just go away simply because you took a swing at him? Do you think he will say, 'Wow, these guys are tough. I guess I will hang up my hacking spurs forever?' More likely than not, you would have succeeded in poking the beehive and you may have unleashed a world of hurt on your organization that it did not need." Even government organizations where the sole purpose, Mr. Howard said, is to attribute attacks have a hard to doing it with any level of confidence that would warrant an offensive action. "The idea of turning that problem over to a commercial organization who does not have a tenth of the resources is ludicrous," he said. "The result would be to transform the Internet into the Wild Wild West; commercial organizations pointing their cyber six-shooters at any perceived slight rightfully or wrongly." Even then, Howard says, the task should be left to professionals: law enforcement and intelligence. They too "absolutely should not get carte blanche for this kind of activity. There has to be some rules put in place that all citizens understand. There has to be some oversight put in place that regularly reports back to the citizenry about what these forces are doing." A minority of 18 percent of Influencers said companies should be allowed to hack back after they're hit. "There is a significant spectrum of options for a victim to employ against a cyberattacker; 'shutting down' the computers used in an attack is at the extreme end of that spectrum," one Influencer said. "The fact is, the US government is not responding to vast majority of cyberintrusions, whether for theft or destruction; private companies are on their own, and as such, they should be able to defend themselves in cyberspace. Does the Second Amendment not extend to cyberspace?" If companies cannot get timely help and protection from law enforcement, one Influencer said, "they should be allowed to take responsible action to mitigate the impact of theft of their data. This should be done with full accountability for any damage to innocent parties." Companies should be allowed to hack back "but only under strict controls, such as using a bonded, licensed company – perhaps even deputized by an accredited law enforcement agency – which acts on their behalf," suggested Jay Healey, head of the Cyber Statecraft Initiative at the Atlantic Council think tank. "This should start as a small pilot project as the international blow back is likely to be significant." We want to hear from you. Take the readers version of the Influencers poll here. "Hacking back sounds like a great idea until you think about how easy it is to subvert. Today's attackers go to great lengths to hide the source of their attacks. How can any company know they're really hacking their attacker, and not some innocent bystander?" - Matthew Green, Johns Hopkins University "The idea that someone could 'hack back' without producing unintended consequences is absurd pipe dream promoted by businesses trying to monetize the concept. The millions of innocent people around the world whose machines are unwittingly serving as waypoints or botnet hosts would be the ones who ultimately pay the price." - Chris Finan, Manifold Security "Today the Internet is the Wild West; with hack back it moves closer to Hobbes' Leviathan." - Jacob Olcott, BitSight Technologies "Companies should be investing in actual defense mechanisms, not offensive capabilities. Actually doing defense is a far better security tactic than 'hack back.' Additionally, companies tend to have a misunderstanding of how difficult doing offense is and a misunderstanding of what can be gained. Applying the resources to being able to do 'hack back' to security would be a better use of those resources and go farther for the intended goals. Additionally, once data is gone from the network there is rarely any ability to 'retrieve' it or keep it from ending up in the adversary's hands. Executives in companies discussing 'hack back' strategies should focus efforts on empowering and training their people, breaking down cultural barriers hampering security, and aligning efforts to the threats they actually face." - Robert Lee, Dragos Security "It depends. There are so many possible unintended consequences in hacking back that unless you truly understand what you are doing, it isn't worth the risk. Remember, when you hack back, you are escalating an event with someone who may have far greater skills, resources and evil intent than you. Hacking back should only be done after consulting with legal counsel because this opens a company up to all sorts of complex legal issues – especially if you hack back and find out you’ve made a mistake. Additionally and this is a bit unfair, but if you couldn’t keep someone out of your environment in the first place, what makes you think you have the skill to up the game by attacking back?" - Mark Weatherford, Chertoff Group "Hey, I've got an idea, let's legalize vigilantism, but only for the one type of crime where people constantly talk about how difficult accurate attribution is. What could go wrong?" - Julian Sanchez, Cato Institute "This is the role of law enforcement. Allowing a safe harbor for 'hack backs' would be an invitation to abuse competitors and the like. Let's keep the job where it belongs, with law enforcement." - Influencer "We can't be taking law into our own hands as a general rule. Would need to understand the facts and circumstances. One should always contact law enforcement as fast as possible." - Influencer "Vigilantism feels good but is rarely effective (for anyone other than Liam Neeson)." - Peter Singer, New America "While we can imagine cases where it'd be satisfying for companies to do this, madness this way lies. Bad actors almost never directly tunnel into a network; they hide behind hijacked accounts and machines. To contemplate 'hacking back' puts those intermediate accounts and machines more in the crossfire. This isn't to say nothing should be done – ISPs and others can play a helpful role in quarantining the launching pads of attacks that are being used without their owners' knowledge – but hacking back should be off the table." - Jonathan Zittrain, Harvard University "The legal right to 'hack back' would incentivize an escalating spiral of attacks with almost certain collateral damage to both networks and individuals. In the most sophisticated and damaging attacks, accurately identifying the attacker has proven elusive at best." - Influencer "Hack back, retaliation, vigilantism. These words not only make for great headlines; they spark heated debate over the appropriate roles of the private sector and government in cybersecurity. Unfortunately, the 'hack-back' debate often obscures a much more fundamental debate over the future direction of US cybersecurity policy. For the past two decades, US cybersecurity has focused almost exclusively on defense – we've dedicated our time and resources to making it harder for our adversaries to penetrate our networks. But strong network fortifications are not fail-safe. Especially against nation-states and other concerted adversaries who are willing to go to almost any level of time, effort, and expense to penetrate a target's network. Defensive measures alone may delay – but are unlikely to prevent – penetration of target networks by concerted adversaries. Focusing exclusively on defense will not solve our cybersecurity problem. We need to raise the costs and risks to concerted adversaries in order to deter their activities. There are many divergent views as to the best way to do this, but one thing is clear: the time has come for a national conversation. Effective deterrence is not synonymous with hack-back, retaliation, or vigilantism. Elements of an effective deterrence strategy include: real-time detection of intrusions (a high likelihood of discovery will deter some would-be intruders) as well as identification and punishment of cyberintruders. In the absence of such consequences, cyberintruders should be expected to continue targeting our networks." - Melanie Teplinsky, American University "There is a range of activities from passive defense, through more active defense, to offensive tactics. We do need to move to where something more active than today, but perhaps less than full scale 'hack back' is acceptable and even more commonplace." - Influencer

#### Goes nuclear despite deterrence AND rationality.

Erik **Gartzke &** Jon R. **Lindsay 17**. Gartzke is at the Department of Political Science, University of California, San Diego; Lindsay is at the Munk School of Global Affairs, University of Toronto. 03/01/2017. “Thermonuclear Cyberwar.” Journal of Cybersecurity, vol. 3, no. 1, pp. 37–48.

Cyber warfare is routinely overhyped as a new weapon of mass destruction, but when used in conjunction with actual weapons of mass destruction, severe, and underappreciated, dangers emerge. One side of a stylized debate about cybersecurity in international relations argues that offensive advantages in cyberspace empower weaker nations, terrorist cells, or even lone rogue operators to paralyze vital infrastructure [4–8]. The other side argues that operational difficulties and effective deterrence restrains the severity of cyber attack, while governments and cybersecurity firms have a pecuniary interest in exaggerating the threat [9–13]. Although we have contributed to the skeptical side of this debate [14–16], \*\*\*BEGIN FOOTNOTE\*\*\* 14. Gartzke E. The myth of cyberwar: bringing war in cyberspace back down to earth. Int Security 2013;38:41–73. Google ScholarCrossRef 15 Lindsay JR. Stuxnet and the limits of cyber warfare. Security Stud 2013;22:365–404. Google ScholarCrossRef 16 Lindsay JR. The impact of China on cybersecurity: fiction and friction. Int Security 2014;39:7–47. Google ScholarCrossRef \*\*\*END FOOTNOTE\*\*\* the same strategic logic that leads us to view cyberwar as a limited political instrument in most situations also leads us to view it as incredibly destabilizing in rare situations. In a recent Israeli wargame of a regional scenario involving the United States and Russia, one participant remarked on “how quickly localized cyber events can turn dangerously kinetic when leaders are ill-prepared to deal in the cyber domain” [17]. Importantly, this sort of catalytic instability arises not from the cyber domain itself but through its interaction with forces and characteristics in other domains (land, sea, air, etc.). Further, it arises only in situations where actors possess, and are willing to use, robust traditional military forces to defend their interests. Classical deterrence theory developed to explain nuclear deterrence with nuclear weapons, but different types of weapons or combinations of operations in different domains can have differential effects on deterrence and defense [18, 19]. Nuclear weapons and cyber operations are particularly complementary (i.e. nearly complete opposites) with respect to their strategic characteristics. Theorists and practitioners have stressed the unprecedented destructiveness of nuclear weapons in explaining how nuclear deterrence works, but it is equally, if not more, important for deterrence that capabilities and intentions are clearly communicated. As quickly became apparent, public displays of their nuclear arsenals improved deterrence. At the same time, disclosing details of a nation’s nuclear capabilities did not much degrade the ability to strike or retaliate, given that defense against nuclear attack remains extremely difficult. Knowledge of nuclear capabilities is necessary to achieve a deterrent effect [20]. Cyber operations, in contrast, rely on undisclosed vulnerabilities, social engineering, and creative guile to generate indirect effects in the information systems that coordinate military, economic, and social behavior. Revelation enables crippling countermeasures, while the imperative to conceal capabilities constrains both the scope of cyber operations and their utility for coercive signaling [21, 22]. The diversity of cyber operations and confusion about their effects also contrast with the obvious destructiveness of nuclear weapons. The problem is that transparency and deception do not mix well. An attacker who hacks an adversary’s nuclear command and control apparatus, or the weapons themselves, will gain an advantage in warfighting that the attacker cannot reveal, while the adversary will continue to believe it wields a deterrent that may no longer exist. Most analyses of inadvertent escalation from cyber or conventional to nuclear war focus on “use it or lose it” pressures and fog of war created by attacks that become visible to the target [23, 24]. In a US–China conflict scenario, for example, conventional military strikes in conjunction with cyber attacks that blind sensors and confuse decision making could generate incentives for both sides to rush to preempt or escalate [25–27]. These are plausible concerns, but the revelation of information about a newly unfavorable balance of power might also cause hesitation and lead to compromise. Cyber blinding could potentially make traditional offensive operations more difficult, shifting the advantage to defenders and making conflict less likely. Clandestine attacks that remain invisible to the target potentially present a more insidious threat to crisis stability. There are empirical and theoretical reasons for taking seriously the effects of offensive cyber operations on nuclear deterrence, and we should expect the dangers to vary with the relative cyber capabilities of the actors in a crisis interaction. Nuclear command and control vulnerability General Robert Kehler, commander of US Strategic Command (STRATCOM) in 2013, stated in testimony before the Senate Armed Services Committee, “we are very concerned with the potential of a cyber-related attack on our nuclear command and control and on the weapons systems themselves” [28]. Nuclear command, control, and communications (NC3) form the nervous system of the nuclear enterprise spanning intelligence and early warning sensors located in orbit and on Earth, fixed and mobile command and control centers through which national leadership can order a launch, operational nuclear forces including strategic bombers, land-based intercontinental missiles (ICBMs), submarine-launched ballistic missiles (SLBMs), and the communication and transportation networks that tie the whole apparatus together [29, 30]. NC3 should ideally ensure that nuclear forces will always be available if authorized by the National Command Authority (to enhance deterrence) and never used without authorization (to enhance safety and reassurance). Friendly errors or enemy interference in NC3 can undermine the “always-never” criterion, weakening deterrence [31, 32]. NC3 has long been recognized as the weakest link in the US nuclear enterprise. According to a declassified official history, a Strategic Air Command (SAC) task group in 1979 “reported that tactical warning and communications systems … were ‘fragile’ and susceptible to electronic countermeasures, electromagnetic pulse, and sabotage, which could deny necessary warning and assessment to the National Command Authorities” [33]. Two years later, the Principal Deputy Under Secretary of Defense for Research and Engineering released a broad-based, multiservice report that doubled down on SAC’s findings: “the United States could not assure survivability, endurability, or connectivity of the national command authority function” due to: major command, control, and communications deficiencies: in tactical warning and attack assessment where existing systems were vulnerable to disruption and destruction from electromagnetic pulse, other high altitude nuclear effects, electronic warfare, sabotage, or physical attack; in decision making where there was inability to assure national command authority survival and connection with the nuclear forces, especially under surprise conditions; and in communications systems, which were susceptible to the same threats above and which could not guarantee availability of even minimum-essential capability during a protracted war. [33] The nuclear weapons safety literature likewise provides a number of troubling examples of NC3 glitches that illustrate some of the vulnerabilities attackers could, in principle, exploit [34–36]. The SAC history noted that NORAD has received numerous false launch indications from faulty computer components, loose circuits, and even a nuclear war training tape loaded by mistake into a live system that produced erroneous Soviet launch indications [33]. In a 1991 briefing to the STRATCOM commander, a Defense Intelligence Agency targeteer confessed, “Sir, I apologize, but we have found a problem with this target. There is a mistake in the computer code … . Sir, the error has been there for at least the life of this eighteen-month planning cycle. The nature of the error is such that the target would not have been struck” [37]. It would be a difficult operation to intentionally plant undetected errors like this, but the presence of bugs does reveal that such a hack is possible. Following many near-misses and self-audits during and after the Cold War, American NC3 improved with the addition of new safeguards and redundancies. As General Kehler pointed out in 2013, “the nuclear deterrent force was designed to operate through the most extreme circumstances we could possibly imagine” [28]. Yet vulnerabilities remain. In 2010, the US Air Force lost contact with 50 Minuteman III ICBMs for an hour because of a faulty hardware circuit at a launch control center [38]. If the accident had occurred during a crisis, or the component had been sabotaged, the USAF would have been unable to launch and unable to detect and cancel unauthorized launch attempts. As Bruce Blair, a former Minuteman missileer, points out, during a control center blackout the antennas at unmanned silos and the cables between them provide potential surreptitious access vectors [39]. The unclassified summary of a 2015 audit of US NC3 stated that “known capability gaps or deficiencies remain” [40]. Perhaps more worrisome are the unknown deficiencies. A 2013 Defense Science Board report on military cyber vulnerabilities found that while the: nuclear deterrent is regularly evaluated for reliability and readiness … , most of the systems have not been assessed (end-to-end) against a [sophisticated state] cyber attack to understand possible weak spots. A 2007 Air Force study addressed portions of this issue for the ICBM leg of the U.S. triad but was still not a complete assessment against a high-tier threat. [41] If NC3 vulnerabilities are unknown, it is also unknown whether an advanced cyber actor would be able to exploit them. As Kehler notes, “We don’t know what we don’t know” [28]. Even if NC3 of nuclear forces narrowly conceived is a hard target, cyber attacks on other critical infrastructure in preparation to or during a nuclear crisis could complicate or confuse government decision making. General Keith Alexander, Director of the NSA in the same Senate hearing with General Kehler, testified that: our infrastructure that we ride on, the power and the communications grid, are one of the things that is a source of concern … we can go to backup generators and we can have independent routes, but … our ability to communicate would be significantly reduced and it would complicate our governance … . I think what General Kehler has would be intact … [but] the cascading effect … in that kind of environment … concerns us. [28] Kehler further emphasized that “there’s a continuing need to make sure that we are protected against electromagnetic pulse and any kind of electromagnetic interference” [28]. Many NC3 components are antiquated and hard to upgrade, which is a mixed blessing. Kehler points out, “Much of the nuclear command and control system today is the legacy system that we’ve had. In some ways that helps us in terms of the cyber threat. In some cases it’s point to point, hard-wired, which makes it very difficult for an external cyber threat to emerge” [28]. The Government Accountability Office notes that the “Department of Defense uses 8-inch floppy disks in a legacy system that coordinates the operational functions of the nation’s nuclear forces” [42]. While this may limit some forms of remote access, it is also indicative of reliance on an earlier generation of software when security engineering standards were less mature. Upgrades to the digital Strategic Automated Command and Control System planned for 2017 have the potential to correct some problems, but these changes may also introduce new access vectors and vulnerabilities [43]. Admiral Cecil Haney, Kehler’s successor at STRATCOM, highlighted the challenges of NC3 modernization in 2015: Assured and reliable NC3 is fundamental to the credibility of our nuclear deterrent. The aging NC3 systems continue to meet their intended purpose, but risk to mission success is increasing as key elements of the system age. The unpredictable challenges posed by today’s complex security environment make it increasingly important to optimize our NC3 architecture while leveraging new technologies so that NC3 systems operate together as a core set of survivable and endurable capabilities that underpin a broader, national command and control system. [44] In no small irony, the internet itself owes its intellectual origin, in part, to the threat to NC3 from large-scale physical attack. A 1962 RAND report by Paul Baran considered “the problem of building digital communication networks using links with less than perfect reliability” to enable “stations surviving a physical attack and remaining in electrical connection … to operate together as a coherent entity after attack” [45]. Baran advocated as a solution decentralized packet switching protocols, not unlike those realized in the ARPANET program. The emergence of the internet was the result of many other factors that had nothing to do with managing nuclear operations, notably the meritocratic ideals of 1960s counterculture that contributed to the neglect of security in the internet’s founding architecture [46, 47]. Fears of NC3 vulnerability helped to create the internet, which then helped to create the present-day cybersecurity epidemic, which has come full circle to create new fears about NC3 vulnerability. NC3 vulnerability is not unique to the United States. The NC3 of other nuclear powers may even be easier to compromise, especially in the case of new entrants to the nuclear club like North Korea. Moreover, the United States has already demonstrated both the ability and willingness to infiltrate sensitive foreign nuclear infrastructure through operations such as Olympic Games (Stuxnet), albeit targeting Iran’s nuclear fuel cycle rather than NC3. It would be surprising to learn that the United States has failed to upgrade its Cold War NC3 attack plans to include offensive cyber operations against a wide variety of national targets. Hacking the deterrent The United States included NC3 attacks in its Cold War counterforce and damage limitation war plans, even as contemporary critics perceived these options to be destabilizing for deterrence [48]. The best known example of these activities and capabilities is a Special Access Program named Canopy Wing. East German intelligence obtained the highly classified plans from a US Army spy in Berlin, and the details began to emerge publicly after the Cold War. An East German intelligence officer, Markus Wolf, writes in his memoir that Canopy Wing “listed the types of electronic warfare that would be used to neutralize the Soviet Union and Warsaw Pact’s command centers in case of all-out war. It detailed the precise method of depriving the Soviet High Command of its high-frequency communications used to give orders to its armed forces” [49]. It is easy to see why NC3 is such an attractive target in the unlikely event of a nuclear war. If for whatever reason deterrence fails and the enemy decides to push the nuclear button, it would obviously be better to disable or destroy missiles before they launch than to rely on possibly futile efforts to shoot them down, or to accept the loss of millions of lives. American plans to disable Soviet NC3 with electronic warfare, furthermore, would have been intended to complement plans for decapitating strikes against Soviet nuclear forces. Temporary disabling of information networks in isolation would have failed to achieve any important strategic objective. A blinded adversary would eventually see again and would scramble to reconstitute its ability to launch its weapons, expecting that preemption was inevitable in any case. Reconstitution, moreover, would invalidate much of the intelligence and some of the tradecraft on which the blinding attack relied. Capabilities fielded through Canopy Wing were presumably intended to facilitate a preemptive military strike on Soviet NC3 to disable the ability to retaliate and limit the damage of any retaliatory force that survived, given credible indications that war was imminent. Canopy Wing included [50]: “Measures for short-circuiting … communications and weapons systems using, among other things, microscopic carbon-fiber particles and chemical weapons.” “Electronic blocking of communications immediately prior to an attack, thereby rendering a counterattack impossible.” “Deployment of various weapons systems for instantaneous destruction of command centers, including pin-point targeting with precision-guided weapons to destroy ‘hardened bunkers’.” “Use of deception measures, including the use of computer-simulated voices to override and substitute false commands from ground-control stations to aircraft and from regional command centers to the Soviet submarine fleet.” “Us[e of] the technical installations of ‘Radio Free Europe/Radio Liberty’ and ‘Voice of America,’ as well as the radio communications installations of the U.S. Armed Forces for creating interference and other electronic effects.” Wolf also ran a spy in the US Air Force who disclosed that the Americans had managed to penetrate the [Soviet air base at Eberswalde]’s ground-air communications and were working on a method of blocking orders before they reached the Russian pilots and substituting their own from West Berlin. Had this succeeded, the MiG pilots would have received commands from their American enemy. It sounded like science fiction, but, our experts concluded, it was in no way impossible that they could have pulled off such a trick, given the enormous spending and technical power of U.S. military air research. [49] One East German source claimed that Canopy Wing had a $14.5 billion budget for research and operational costs and a staff of 1570 people, while another claimed that it would take over 4 years and $65 million to develop “a prototype of a sophisticated electronic system for paralyzing Soviet radio traffic in the high-frequency range” [50]. Canopy Wing was not cheap, and even so, it was only a research and prototyping program. Operationalization of its capabilities and integration into NATO war plans would have been even more expensive. This is suggestive of the level of effort required to craft effective offensive cyber operations against NC3. Preparation comes to naught when a sensitive program is compromised. Canopy Wing was caught in what we describe below as the cyber commitment problem, the inability to disclose a warfighting capability for the sake of deterrence without losing it in the process. According to New York Times reporting on the counterintelligence investigation of the East German spy in the Army, Warrant Officer James Hall, “officials said that one program rendered useless cost hundreds of millions of dollars and was designed to exploit a Soviet communications vulnerability uncovered in the late 1970's” [51]. This program was probably Canopy Wing. Wolf writes, “Once we passed [Hall’s documents about Canopy Wing] on to the Soviets, they were able to install scrambling devices and other countermeasures” [49]. It is tempting to speculate that the Soviet deployment of a new NC3 system known as Signal-A to replace Signal-M (which was most likely the one targeted by Canopy Wing) was motivated in part by Hall’s betrayal [50]. Canopy Wing underscores the potential and limitations of NC3 subversion. Modern cyber methods can potentially perform many of the missions Canopy Wing addressed with electronic warfare and other means, but with even greater stealth and precision. Cyber operations might, in principle, compromise any part of the NC3 system (early warning, command centers, data transport, operational forces, etc.) by blinding sensors, injecting bogus commands or suppressing legitimate ones, monitoring or corrupting data transmissions, or interfering with the reliable launch and guidance of missiles. In practice, the operational feasibility of cyber attack against NC3 or any other target depends on the software and hardware configuration and organizational processes of the target, the intelligence and planning capacity of the attacker, and the ability and willingness to take advantage of the effects created by cyber attack [52, 53]. Cyber compromise of NC3 is technically plausible though operationally difficult, a point to which we return in a later section. To understand which threats are not only technically possible but also probable under some circumstance, we further need a political logic of cost and benefit [14]. In particular, how is it possible for a crisis to escalate to levels of destruction more costly than any conceivable political reward? Canopy Wing highlights some of the strategic dangers of NC3 exploitation. Warsaw Pact observers appear to have been deeply concerned that the program reflected an American willingness to undertake a surprise decapitation attack: they said that it “sent ice-cold shivers down our spines” [50]. The Soviets designed a system called Perimeter that, not unlike the Doomsday Device in Dr. Strangelove, was designed to detect a nuclear attack and retaliate automatically, even if cut off from Soviet high command, through an elaborate system of sensors, underground computers, and command missiles to transmit launch codes [54]. Both Canopy Wing and Perimeter show that the United States and the Soviet Union took nuclear warfighting seriously and were willing to develop secret advantages for such an event. By the same token, they were not able to reveal such capabilities to improve deterrence to avoid having to fight a nuclear war in the first place. Nuclear deterrence and credible communication Nuclear weapons have some salient political properties. They are singularly and obviously destructive. They kill in more, and more ghastly, ways than conventional munitions through electromagnetic radiation, blast, firestorms, radioactive fallout, and health effects that linger for years. Bombers, ICBMs, and SLBMs can project warheads globally without significantly mitigating their lethality, steeply attenuating the conventional loss-of-strength gradient [55]. Defense against nuclear attack is very difficult, even with modern ballistic missile defenses, given the speed of incoming warheads and use of decoys; multiple warheads and missile volleys further reduce the probability of perfect interception. If one cannot preemptively destroy all of an enemy’s missiles, then there is a nontrivial chance of getting hit by some of them. When one missed missile can incinerate millions of people, the notion of winning a nuclear war starts to seem meaningless for many politicians. As defense seemed increasingly impractical, early Cold War strategists championed the threat of assured retaliation as the chief mechanism for avoiding war [56–59]. Political actors have issued threats for millennia, but the advent of nuclear weapons brought deterrence as a strategy to center stage. The Cold War was an intense learning experience for both practitioners and students of international security, rewriting well-worn realities more than once [60–62]. A key conundrum was the practice of brinkmanship. Adversaries who could not compete by “winning” a nuclear war could still compete by manipulating the “risk” of nuclear annihilation, gambling that an opponent would have the good judgment to back down at some point short of the nuclear brink. Brinkmanship crises—conceptualized as games of Chicken where one cannot heighten tensions without increasing the hazard of the mutually undesired outcome—require that decision makers behave irrationally, or possibly that they act randomly, which is difficult to conceptualize in practical terms [63]. The chief concern in historical episodes of chicken, such as the Berlin Crisis and Cuban Missile Crisis, was not whether a certain level of harm was possible, but whether an adversary was resolved enough, possibly, to risk nuclear suicide. The logical inconsistency of the need for illogic to win led almost from the beginning of the nuclear era to elaborate deductive contortions [64–66]. Both mutually assured destruction (MAD) and successful brinksmanship depend on a less appreciated, but no less fundamental, feature of nuclear weapons: political transparency. Most elements of military power are weakened by disclosure [67]. Military plans are considerably less effective if shared with an enemy. Conventional weapons become less lethal as adversaries learn what different systems can and cannot do, where they are located, how they are operated, and how to devise countermeasures and array defenses to blunt or disarm an attack. In contrast, relatively little reduction in destruction follows from enemy knowledge of nuclear capabilities. For most of the nuclear era, no effective defense existed against a nuclear attack. Even today, with evolving ABM systems, one ICBM still might get through and annihilate the capital city. Nuclear forces are more robust to revelation than other weapons, enabling nuclear nations better to advertise the harm they can inflict. The need for transparency to achieve an effective deterrent is driven home by the satirical Cold War film, Dr. Strangelove: “the whole point of a Doomsday Machine is lost, if you keep it a secret! Why didn’t you tell the world, eh?” During the real Cold War, fortunately, Soviet leaders paraded their nuclear weapons through Red Square for the benefit of foreign military attaches and the international press corps. Satellites photographed missile, bomber, and submarine bases. While other aspects of military affairs on both sides of the Iron Curtain remained closely guarded secrets, the United States and the Soviet Union permitted observers to evaluate their nuclear capabilities. This is especially remarkable given the secrecy that pervaded Soviet society. The relative transparency of nuclear arsenals ensured that the superpowers could calculate risks and consequences within a first-order approximation, which led to a reduction in severe conflict and instability even as political competition in other arenas was fierce [61, 68]. Recent insights about the causes of war suggest that divergent expectations about the costs and consequences of war are necessary for contests to occur [69–73]. These insights are associated with rationalist theories, such as deterrence theory itself. Empirical studies and psychological critiques of the rationality assumption have helped to refine models and bring some circumspection into their application, but the formulation of sound strategy (if not the execution) still requires the articulation of some rational linkage between cause and effect [19, 62, 74]. Many supposedly nonrational factors, moreover, simply manifest as uncertainty in strategic interaction. Our focus here is on the effect of uncertainty and ignorance on the ability of states and other actors to bargain in lieu of fighting. Many wars are a product of what adversaries do not know or what they misperceive, whether as a result of bluffing, secrecy, or intrinsic uncertainty [75, 76]. If knowledge of capabilities or resolve is a prerequisite for deterrence, then one reason for deterrence failure is the inability or unwillingness to credibly communicate details of the genuine balance of power, threat, or interests. Fighting, conversely, can be understood as a costly process of discovery that informs adversaries of their actual relative strength and resolve. From this perspective, successful deterrence involves instilling in an adversary perceptions like those that result from fighting, but before fighting actually begins. Agreement about the balance of power can enable states to bargain (tacit or overt) effectively without needing to fight, forging compromises that each prefers to military confrontation or even to the bulk of possible risky brinkmanship crises. Despite other deficits, nuclear weapons have long been considered to be stabilizing with respect to rational incentives for war (the risk of nuclear accidents is another matter) [77]. If each side has a secure second strike—or even a minimal deterrent with some nonzero chance of launching a few missiles—then each side can expect to gain little and lose much by fighting a nuclear war. Whereas the costs of conventional war can be more mysterious because each side might decide to hold something back and meter out its punishment due to some internal constraint or a theory of graduated escalation, even a modest initial nuclear exchange is recognized to be extremely costly. As long as both sides understand this and understand (or believe) that the adversary understands this as well, then the relationship is stable. Countries engage nuclear powers with considerable deference, especially over issues of fundamental national or international importance. At the same time, nuclear weapons appear to be of limited value in prosecuting aggressive action, especially over issues of secondary or tertiary importance, or in response to aggression from others at lower levels of dispute intensity. Nuclear weapons are best used for signaling a willingness to run serious risks to protect or extort some issue that is considered of vital national interest. As mentioned previously, both superpowers in the Cold War considered the warfighting advantages of nuclear weapons quite apart from any deterrent effect, and the United States and Russia still do. High-altitude bursts for air defense, electromagnetic pulse for frying electronics, underwater detonations for anti-submarine warfare, hardened target penetration, area denial, and so on, have some battlefield utility. Transparency per se is less important than weapon effects for warfighting uses, and can even be deleterious for tactics that depend on stealth and mobility. Even a single tactical nuke, however, would inevitably be a political event. Survivability of the second strike deterrent can also militate against transparency, as in the case of the Soviet Perimeter system, as mobility, concealment, and deception can make it harder for an observer to track and count respective forces from space. Counterforce strategies, platform diversity and mobility, ballistic missile defense systems, and force employment doctrine can all make it more difficult for one or both sides in a crisis to know whether an attack is likely to succeed or fail. The resulting uncertainty affects not only estimates of relative capabilities but also the degree of confidence in retaliation. At the same time, there is reason to believe that platform diversity lowers the risk of nuclear or conventional contests, because increasing the number of types of delivery platforms heightens second strike survivability without increasing the lethality of an initial strike [78]. While transparency is not itself a requirement for nuclear use, stable deterrence benefits to the degree to which retaliation can be anticipated, as well as the likelihood that the consequences of a first strike are more costly than any benefit. Cyber operations, in contrast, are neither robust to revelation nor as obviously destructive. The cyber commitment problem Deterrence (and compellence) uses force or threats of force to “warn” an adversary about consequences if it takes or fails to take an action. In contrast, defense (and conquest) uses force to “win” a contest of strength and change the material distribution of power. Sometimes militaries can change the distribution of information and power at the same time. Military mobilization in a crisis signifies resolve and displays a credible warning, but it also makes it easier to attack or defend if the warning fails. Persistence in a battle of attrition not only bleeds an adversary but also reveals a willingness to pay a higher price for victory. More often, however, the informational requirements of winning and warning are in tension. Combat performance often hinges on well-kept secrets, feints, and diversions. Many military plans and capabilities degrade when revealed. National security involves trade-offs between the goals of preventing war, by advertising capabilities or interests, and improving fighting power should war break out, by concealing capabilities and surprising the enemy. The need to conceal details of the true balance of power to preserve battlefield effectiveness gives rise to the military commitment problem [79, 80]. Japan could not coerce the United States by revealing its plan to attack Pearl Harbor because the United States could not credibly promise to refrain from reorienting defenses and dispersing the Pacific Fleet. War resulted not just because of what opponents did not know but because of what they could not tell each other without paying a severe price in military advantage. The military benefits of surprise (winning) trumped the diplomatic benefits of coercion (warning). Cyber operations, whether for disruption and intelligence, are extremely constrained by the military commitment problem. Revelation of a cyber threat in advance that is specific enough to convince a target of the validity of the threat also provides enough information potentially to neutralize it. Stuxnet took years and hundreds of millions of dollars to develop but was patched within weeks of its discovery. The Snowden leaks negated a whole swath of tradecraft that the NSA took years to develop. States may use other forms of covert action, such as publicly disavowed lethal aid or aerial bombing (e.g. Nixon’s Cambodia campaign), to discretely signal their interests, but such cases can only work to the extent that revelation of operational details fails to disarm rebels or prevent airstrikes [81]. Cyber operations, especially against NC3, must be conducted in extreme secrecy as a condition of the efficacy of the attack. Cyber tradecraft relies on stealth, stratagem, and deception [21]. Operations tailored to compromise complex remote targets require extensive intelligence, planning and preparation, and testing to be effective. Actions that alert a target of an exploit allow the target to patch, reconfigure, or adopt countermeasures that invalidate the plan. As the Defense Science Board points out, competent network defenders: can also be expected to employ highly-trained system and network administrators, and this operational staff will be equipped with continuously improving network defensive tools and techniques (the same tools we advocate to improve our defenses). Should an adversary discover an implant, it is usually relatively simple to remove or disable. For this reason, offensive cyber will always be a fragile capability. [41] The world’s most advanced cyber powers, the United States, Russia, Israel, China, France, and the United Kingdom, are also nuclear states, while India, Pakistan, and North Korea also have cyber warfare programs. NC3 is likely to be an especially well defended part of their cyber infrastructures. NC3 is a hard target for offensive operations, which thus requires careful planning, detailed intelligence, and long lead-times to avoid compromise. Cyberspace is further ill-suited for signaling because cyber operations are complex, esoteric, and hard for commanders and policymakers to understand. Most targeted cyber operations have to be tailored for each unique target (a complex organization not simply a machine), quite unlike a general purpose munition tested on a range. Malware can fail in many ways and produce unintended side effects, as when the Stuxnet code was accidentally released to the public. The category of “cyber” includes tremendous diversity: irritant scams, hacktivist and propaganda operations, intelligence collection, critical infrastructure disruption, etc. Few intrusions create consequences that rise to the level of attacks such as Stuxnet or BlackEnergy, and even they pale beside the harm imposed by a small war. Vague threats are less credible because they are indistinguishable from casual bluffing. Ambiguity can be useful for concealing a lack of capability or resolve, allowing an actor to pool with more capable or resolved states and acquiring some deterrence success by association. But this works by discounting the costliness of the threat. Nuclear threats, for example, are usually somewhat veiled because one cannot credibly threaten nuclear suicide. The consistently ambiguous phrasing of US cyber declaratory policy (e.g. “we will respond to cyber-attacks in a manner and at a time and place of our choosing using appropriate instruments of U.S. power” [82]) seeks to operate across domains to mobilize credibility in one area to compensate for a lack of credibility elsewhere, specifically by leveraging the greater robustness to revelation of military capabilities other than cyber. This does not mean that cyberspace is categorically useless for signaling, just as nuclear weapons are not categorically useless for warfighting. Ransomware attacks work when the money extorted to unlock the compromised host is priced below the cost of an investigation or replacing the system. The United States probably gained some benefits in general deterrence (i.e. discouraging the emergence of challenges as opposed to immediate deterrence in response to a challenge) through the disclosure of Stuxnet and the Snowden leaks. Both revelations compromised tradecraft, but they also advertised that the NSA probably had more exploits and tradecraft where they came from. Some cyber operations may actually be hard to mitigate within tactically meaningful timelines (e.g. hardware implants installed in hard-to-reach locations). Such operations might be revealed to coerce concessions within the tactical window created by a given operation, if the attacker can coordinate the window with the application of coercion in other domains. As a general rule, however, the cyber domain on its own is better suited for winning than warning [83]. Cyber and nuclear weapons fall on extreme opposite sides of this spectrum. Dangerous complements Nuclear weapons have been used in anger twice—against the Japanese cities Hiroshima and Nagasaki—but cyberspace is abused daily. Considered separately, the nuclear domain is stable and the cyber domain is unstable. In combination, the results are ambiguous. The nuclear domain can bound the intensity of destruction that a cyber attacker is willing to inflict on an adversary. US declaratory policy states that unacceptable cyber attacks may prompt a military response; while nuclear weapons are not explicitly threatened, neither are they withheld. Nuclear threats have no credibility at the low end, where the bulk of cyber attacks occur. This produces a cross-domain version of the stability–instability paradox, where deterrence works at the high end but is not credible, and thus encourages provocation, at low intensities. Nuclear weapons, and military power generally, create an upper bound on cyber aggression to the degree that retaliation is anticipated and feared [22, 83, 84]. In the other direction, the unstable cyber domain can undermine the stability of nuclear deterrence. Most analysts who argue that the cyber–nuclear combination is a recipe for danger focus on the fog of crisis decision making [85–87]. Stephen Cimbala points out that today’s relatively smaller nuclear arsenals may perversely magnify the attractiveness of NC3 exploitation in a crisis: “Ironically, the downsizing of U.S. and post-Soviet Russian strategic nuclear arsenals since the end of the Cold War, while a positive development from the perspectives of nuclear arms control and nonproliferation, makes the concurrence of cyber and nuclear attack capabilities more alarming” [88]. Cimbala focuses mainly on the risks of misperception and miscalculation that emerge when a cyber attack muddies the transparent communication required for opponents to understand one another’s interests, redlines, and willingness to use force, and to ensure reliable control over subordinate commanders. Thus a nuclear actor “faced with a sudden burst of holes in its vital warning and response systems might, for example, press the preemption button instead of waiting to ride out the attack and then retaliate” [85]. The outcome of fog of decision scenarios such as these depend on how humans react to risk and uncertainty, which in turn depends on bounded rationality and organizational frameworks that might confuse rational decision making [89, 90]. These factors exacerbate a hard problem. Yet within a rationalist framework, cyber attacks that have already created their effects need not trigger an escalatory spiral. While being handed a fait accompli may trigger an aggressive reaction, it is also plausible that the target’s awareness that its NC3 has been compromised in some way would help to convey new information that the balance of power is not as favorable as previously thought. This in turn could encourage the target to accommodate, rather than escalate. While defects in rational decision making are a serious concern in any cyber–nuclear scenario, the situation becomes even more hazardous when there are rational incentives to escalate. Although “known unknowns” can create confusion, to paraphrase Donald Rumsfeld, the “unknown unknowns” are perhaps more dangerous. A successful clandestine penetration of NC3 can defeat the informational symmetry that stabilizes nuclear relationships. Nuclear weapons are useful for deterrence because they impose a degree of consensus about the distribution of power; each side knows the other can inflict prohibitive levels of damage, even if they may disagree about the precise extent of this damage. Cyber operations are attractive precisely because they can secretly revise the distribution of power. NC3 neutralization may be an expensive and rarified capability in the reach of only a few states with mature signals intelligence agencies, but it is much cheaper than nuclear attack. Yet the very usefulness of cyber operations for nuclear warfighting ensure that deterrence failure during brinksmanship crises is more likely. Nuclear states may initiate crises of risk and resolve to see who will back down first, which is not always clear in advance. Chicken appears viable, ironically, because each player understands that a nuclear war would be a disaster for all, and thus all can agree that someone can be expected swerve. Nuclear deterrence should ultimately make dealing with an adversary diplomatically more attractive than fighting, provided that fighting is costly—as would seem evident for the prospect of nuclear war—and assuming that bargains are available to states willing to accept compromise rather than annihilation. If, however, one side knows, but the other does not, that the attacker has disabled the target’s ability to perceive an impending military attack, or to react to one when it is underway, then they will not have a shared understanding of the probable outcome of war, even in broad terms. Consider a brinksmanship crisis between two nuclear states where only one has realized a successful penetration of the rival’s NC3. The cyber attacker knows that it has a military advantage, but it cannot reveal the advantage to the target, lest the advantage be lost. The target does not know that it is at a disadvantage, and it cannot be told by the attacker for the same reason. The attacker perceives an imbalance of power while the target perceives a balance. A dangerous competition in risk taking ensues. The first side knows that it does not need to back down. The second side feels confident that it can stand fast and raise the stakes far beyond what it would be willing to if it understood the true balance of power. Each side is willing to escalate to create more risk for the other side, making it more likely that one or the other will conclude that deterrence has failed and move into warfighting mode to attempt to limit the damage the other can inflict. The targeted nature and uncertain effects of offensive cyber operations put additional pressure on decision makers. An intrusion will probably disable only part of the enemy’s NC3 architecture, not all of it (which is not only operationally formidable to achieve but also more likely to be noticed by the target). Thus the target may retain control over some nuclear forces, or conventional forces. The target may be tempted to use some of them piecemeal to signal a willingness to escalate further, even though it cannot actually escalate because of the cyber operation. The cyber attacker knows that it has escalation dominance, but when even a minor demonstration by the target can cause great damage, it is tempting to preempt this move or others like it. This situation would be especially unstable if only second strike but not primary strike NC3 was incapacitated. Uncertainty in the efficacy of the clandestine penetration would discount the attacker’s confidence in its escalation dominance, with a range of possible outcomes. Enough uncertainty would discount the cyber attack to nothing, which would have a stabilizing effect by returning the crisis to the pure nuclear domain. A little bit of uncertainty about cyber effectiveness would heighten risk acceptance while also raising the incentives to preempt as an insurance measure. Adding allies into the mix introduces additional instability. An ally emboldened by its nuclear umbrella might run provocative risks that it would be much more reluctant to embrace if it was aware that the umbrella was actually full of holes. Conversely, if the clandestine advantage is held by the state extending the umbrella, allies could become unnerved by the willingness of their defender to run what appear to be outsize risks, oblivious of the reasons for the defender’s confidence, creating discord in the alliance and incentives for self-protective action, leading to greater uncertainty about alliance solidarity. The direction of influence between the cyber and nuclear realms depends to large degree on which domain is the main arena of action. Planning and conducting cyber operations will be bounded by the ability of aggressors to convince themselves that attacks will remain secret, and by the confidence of nuclear nations in their invulnerability. Fears of cross-domain escalation will tend to keep instability in cyberspace bounded. However, if a crisis has risen to the point where nuclear threats are being seriously considered or made, then NC3 exploitation will be destabilizing. Brinksmanship crises seem to have receded in frequency since the Cuban Missile Crisis but may be more likely than is generally believed. President Vladimir Putin of Russia has insinuated more than once in recent years that his government is willing to use tactical nuclear weapons if necessary to support his policies. Cyber power and nuclear stability Not all crises are the same. Indeed, their very idiosyncrasies create the uncertainties that make bargaining failure more likely [75]. So far our analysis would be at home in the Cold War, with the technological novelty of cyber operations. Yet not every state has the same cyber capabilities or vulnerabilities. Variation in cyber power relations across dyads should be expected to affect the strategic stability of nuclear states. The so-called second nuclear age differs from superpower rivalry in important ways [91]. There are fewer absolute numbers of warheads in the world, down from a peak of over 70 000 in the 1980s to about 15 000 today (less than 5000 deployed), but they are distributed very unevenly [92]. The United States and Russia have comparably sized arsenals, each with a fully diversified triad of delivery platforms, while North Korea only has a dozen or so bombs and no meaningful delivery system (for now). China, India, Pakistan, Britain, France, and Israel have modest arsenals in the range of several dozen to a couple hundred weapons, but they have very different doctrines, conventional force complements, domestic political institutions, and alliance relationships. The recent nuclear powers lack the hard-won experience and shared norms of the Cold War to guide them through crises, and even the United States and Russia have much to relearn. Cyber warfare capacity also varies considerably across contemporary nuclear nations. The United States, Russia, Israel, and Britain are in the top tier, able to run sophisticated, persistent, clandestine penetrations. China is a uniquely active cyber power with ambitious cyber warfare doctrine, but its operational focus is on economic espionage and political censorship, resulting in less refined tradecraft and more porous defenses for military purposes [16]. France, India, and Pakistan also have active cyber warfare programs, while North Korea is the least developed cyber nation, depending on China for its expertise [93]. It is beyond the scope of this article to assess crisis dyads in detail, and data on nuclear and cyber power for these countries are shrouded in secrecy. Here, as a way of summing up the arguments above, we offer a few conjectures about how stylized aspects of cyber power affect crisis stability through incentives and key aspects of decision making. We do not stress relative nuclear weapon capabilities on the admittedly strong (and contestable) assumption that nuclear transparency in the absence of cyber operations would render nuclear asymmetry irrelevant for crisis bargaining because both sides would agree about the terrible consequences of conflict [94]. We also omit domestic or psychological variables that affect relative power assessments, although these are obviously important. Even if neither India nor Pakistan have viable cyber–nuclear capabilities, brinksmanship between them is dangerous for many other reasons, notably compressed decision timelines, Pakistan’s willingness to shoot first, and domestic regime instability. Our focus is on the impact of offensive and defensive cyber power on nuclear deterrence above and beyond the other factors that certainly play a role in real-world outcomes. First, does the cyber attacker have the organizational capacity, technical expertise, and intelligence support to “compromise” the target’s NC3? Can hackers access critical networks, exploit technical vulnerabilities, and confidently execute a payload to disrupt or exploit strategic sensing, command, forces, or transport capacity? The result would be some tangible advantage for warfighting, such as tactical warning or control paralysis, but one that cannot be exercised in bargaining. Second, is the target able to “detect” the compromise of its NC3? The more complicated and sensitive the target, the more likely cyber attackers are to make a mistake that undermines the intrusion. Attribution is not likely to be difficult given the constricted pool of potential attackers, but at the same time the consequences of misattributing “false flag” operations could be severe [95]. At a minimum, detection is assumed to provide information to the target that the balance of power is perhaps not as favorable as imagined previously. We assume that detection without an actual compromise is possible because of false positives or deceptive information operations designed to create pessimism or paranoia. Third, is the target able to “mitigate” the compromise it detects? Revelation can prompt patching or network reconfiguration to block an attack, but this assumption is not always realistic. The attacker may have multiple pathways open or may have implanted malware that is difficult to remove in tactically meaningful timelines. In such cases the cyber commitment problem is not absolute, since the discovery of the power to hurt does not automatically disarm it. Successful mitigation here is assumed to restore mutual assessments of the balance of power to what they would be absent the cyber attack. Table 1 shows how these factors combine to produce different deterrence outcomes in a brinksmanship (chicken) crisis. If there is no cyber compromise and the target detects nothing (no false positives) then we have the optimistic ideal case where nuclear transparency affords stable “deterrence.” Transparency about the nuclear balance, including the viability of secure second strike forces, provides strategic stability. We also expect this box to describe situations where the target has excellent network defense capabilities and thus the prospect of defense, denial or deception successfully deters any attempts to penetrate NC3. This may resemble the Cold War situation (with electronic warfare in lieu of cyber), or even the present day US–Russia dyad, where the odds of either side pulling off a successful compromise against a highly capable defender are not favorable. Alternately the attack may be deemed risky enough to encourage serious circumspection. However, the existence of Canopy Wing does not encourage optimism in this regard. [[TABLE 1 OMITTED]] Conversely, if there is a compromise that goes undetected, then there is a heightened risk of “war” because of the cyber commitment problem. This box may be particularly relevant for asymmetric dyads such as the United States and North Korea, where one side has real cyber power but the other side is willing to go to the brink where it believes, falsely, that it has the capability to compel its counterpart to back down. Cyber disruption of NC3 is attractive for damage limitation should deterrence fail, given that the weaker state’s diminutive arsenal makes damage limitation by the stronger state more likely to succeed. The dilemma for the stronger state is that the clandestine counterforce hedge, which makes warfighting success more likely, is precisely what makes deterrence more likely to fail. The United States would face similar counterforce dilemmas with other dyads like China or even Russia, although even a strong cyber power should be more circumspect when confronted with an adversary with a larger/more capable nuclear and conventional arsenal. More complex and cyber savvy targets, moreover, are more likely to detect a breach in NC3, leading to more ambiguous outcomes depending on how actors cope with risk and uncertainty. Paradoxically, confidence in cyber security may be a major contributor to failure; believing one is safe from attack increases the chance that an attack is successful. If the successful compromise is detected but not mitigated, then the target learns that the balance of power is not as favorable as thought. This possibility suggests fleeting opportunities for “coercion” by revealing the cyber coup to the target in the midst of a crisis while the cyber attacker maintains or develops a favorable military advantage before the target has the opportunity to reverse or compensate the NC3 disruption. Recognizing the newly transparent costs of war, a risk neutral or risk averse target should prefer compromise. The coercive advantages (deterrence or compellence) of a detected but unmitigated NC3 compromise will likely be fleeting. This suggests a logical possibility for creating a window of opportunity for using particular cyber operations that are more robust to revelation as a credible signal of superior capability in the midst of a crisis. It would be important to exploit this fleeting advantage via other credible military threats (e.g. forces mobilized on visible alert or deployed into the crisis area) before the window closes. One side may be able gain an unearned advantage, an opportunity for coercion via a “bluff,” by the same window-of-opportunity logic. A target concerned about NC3 compromise will probably have some network monitoring system and other protections in place. Defensive systems can produce false positives as a result of internal errors or a deception operation by the attacker to encourage paranoia. It is logically possible that some false positives would appear to the target to be difficult to mitigate. In this situation, the target could believe it is at a disadvantage, even though this is not in fact the case. This gambit would be operationally very difficult to pull off with any reliability in a real nuclear crisis. Cyber–nuclear coercion and bluffing strategies are fraught with danger. Detection without mitigation might put a risk-acceptant or loss-averse target into a “use-lose” situation, creating pressures to preempt or escalate. The muddling of decision-making heightens the risk of accidents or irrational choices in a crisis scenario. Worry about preemption or accident then heightens the likelihood that the initiator will exercise counterforce options while they remain available. These pressures can be expected to be particularly intense if the target’s detection is only partial or has not revealed the true extent of damage to its NC3 (i.e. the target does not realize it has already lost some or all of what it hopes to use). These types of scenarios are most usually invoked in analyses of inadvertent escalation [23–27]. The essential distinction between “use-lose” risks and “war” in this typology is the target’s knowledge of some degree of NC3 compromise. Use-lose and other cognitive pressures can certainly result in nuclear war, since the breakdown of deterrence leads to the release of nuclear weapons, but we distinguish these outcomes to highlight the different decision making processes or rational incentives at work. A “spiral” of mistrust may emerge if one side attempts a compromise but the defender detects and mitigates it. Both sides again have common mutual estimates of the relative balance of power, which superficially resembles the “deterrence” case because the NC3 compromise is negated. Unfortunately, the detection of the compromise will provide the target with information about the hostile intentions of the cyber attacker. This in turn is likely to exacerbate other political or psychological factors in the crisis itself or in the crisis-proneness of the broader relationship. The strange logical case where there is no compromise but one is detected and mitigated could result from a false positive misperception (including a third-party false flag operation) that could conflict spiraling [96, 97]. The bluff and coercion outcomes are also likely to encourage spiraling behavior once the fleeting bargaining advantage dissipates or is dispelled (provided anyone survives the interaction). The risk of crisis instability is not the same for all dyads. It is harder to compromise the NC3 of strong states because of the redundancy and active defenses in their arsenal. Likewise, strong states are better able to compromise the NC3 of any states but especially of weaker states, because of strong states’ greater organizational capacity and expertise in cyber operations. Stable deterrence or MAD is most likely to hold in mutually strong dyads (e.g. the United States and the Soviet Union in the Cold War or Russia today to a lesser extent). Deterrence is slightly less likely in other equally matched dyads (India–Pakistan) where defensive vulnerabilities create temptations but offensive capabilities may not be sufficient to exploit them. Most states can be expected to refrain from targeting American NC3 given a US reputation for cyber power (a general deterrence benefit enhanced by Stuxnet and Snowden). The situation is less stable if the United States is the attacker. The most dangerous dyad is a stronger and a weaker state (United States and North Korea or Israel and Iran). Dyads involving strong and middle powers are also dangerous (United States and China). The stronger side is tempted to disrupt NC3 as a warfighting hedge in case deterrence breaks down, while the weaker but still formidable side has a reasonable chance at detection. The marginally weaker may also be tempted to subvert NC3, particularly for reconnaissance; the stronger side is more likely to detect and correct the intrusion but will be alarmed by the ambiguity in distinguishing intelligence collection from attack planning [98]. In a brinksmanship crisis between them, windows for coercion may be available yet fleeting, with real risks of spiral and war.

### OCO’s Bad---2NC

#### OCOs escalate cyber conflict – vulnerabilities, complexity, and kinetic effects.

Slayton ’17 (Rebecca; 2/2017; PhD in chemical biology from Harvard University, Masters in chemistry and chemical biology from Harvard University, Bachelor’s in chemistry from Westmont College, author of Arguments that Count: Physics, Computing, and Missile Defense, winner of the Computer History Museum Prize, author of Shadowing Cybersecurity, winner of a 5-year National Science Foundation CAREER award, project lead on research funded by the Department of Homeland Security Center of Excellence’s Critical Infrastructure Resilience Institute; “Why Cyber Operations Do Not Always Favor the Offense,” <https://www.belfercenter.org/sites/default/files/files/publication/Cyber%20Ops%20Offense%20-%20final.pdf>; Date Accessed: 7/10/2017; DS)

Creating Unnecessary Vulnerabilities Prioritizing offensive operations can **increase adversaries’ fears**, suspicions, and **readiness to take offensive action**. Cyber offenses include cyber exploitation (intelligence gathering) and cyberattack (disrupting, destroying, or subverting an adversary’s computer systems). An adversary can easily mistake defensive cyber exploitation for offensive operations because the distinction is a matter of intent, not technical operation. The difficulty of distinguishing between offensive and defensive tactics makes mistrustful adversaries **more reactive**, and repeatedly conducting offensive cyber operations only **increases distrust**. A focus on offensive operations can also **increase vulnerabilities**; for example, secretly stockpiling information about vulnerabilities in computers for later exploitation, rather than publicizing and helping civil society to mitigate those vulnerabilities, leaves critical infrastructure vulnerable to attack. The skills and organizational capabilities for offense and defense are very similar. Defense requires understanding how to compromise computer systems; one of the best ways to protect computer systems is to engage in penetration testing (i.e., controlled offensive operations on one’s own systems). The similarity between offensive and defensive skills makes it **unnecessary to conduct offensive operations** against adversaries to maintain offensive capability. Thus, rather than stockpiling technologies in the hope of gaining offensive advantage, states should develop the skills and organizational capabilities required to innovate and maintain information and communications technologies. Managing Complexity The complexity of information systems gives the offense certain advantages for purely probabilistic reasons. Imagine a race: offense and defense go hunting for randomly distributed vulnerabilities, with the offense attempting to exploit those vulnerabilities and the defense aiming to patch them. The number of vulnerabilities grows with the **size and complexity** of the computer system, as do the technological advantages of offense—at least in principle. With a vast number of vulnerabilities, it is **unlikely** that the defense will be able to find and patch every vulnerability before the offense finds and exploits it. Technology is, however, embedded in social organizations, and organizations can help the defense better manage complexity. Those that develop software can check for common errors before making hardware-software systems available for use. The defender has complete access to its computer system, whereas the attacker has a more limited set of attack vectors. Organizations can help skilled defenders by establishing good cybersecurity processes, such as continually scanning for vulnerabilities and updating software. Assessing Kinetic Effects To date, failures of cyber defense have largely been failures of management, and the successes of offense are a result of its relatively simpler goals. Offense, like defense, becomes more difficult as its goals become more complex. In particular, the advantages that complexity offers the offense in cyberspace diminish in the physical world. Computers controlling physical machinery can be hacked, but achieving particular physical effects, such as covertly sabotaging nuclear enrichment facilities, requires knowledge of the physical processes that the computers control, not merely knowledge of the computers. Much of the detailed knowledge needed to run an industrial control system is tacit, passed from one engineer to another but never written down, let alone stored on a computer. Gathering such information requires traditional espionage by humans on the ground, which is both expensive and risky. A cost-benefit analysis of Stuxnet for both the offense and the defense demonstrates why damaging physical infrastructure is **more costly** than simply infiltrating information networks. The costs of Stuxnet were likely far greater for the offense (the United States and Israel) than for the defense (Iran), and Stuxnet was relatively ineffective, setting back Iran’s nuclear program by fewer than three months. The great expense of Stuxnet was intelligence; though digital espionage can be used to obtain some kinds of information, the knowledge needed to disrupt a physical control system, such as the detailed methods and settings used to control pressure in Iran’s nuclear centrifuges, is not generally held in computers. The costs for both sides are dominated not by technology but by skilled labor—for example, hackers who identify and exploit zero-day vulnerabilities, systems administrators who manage and defend computer systems, and the nuclear engineers who understand enrichment processes and the means of disrupting them. In addition, assessing costs alone is misguided: the perceived benefits of attacking with and defending from Stuxnet (i.e., the value of Iran’s nuclear weapons program) greatly exceeded the costs for both the offense and the defense. This is one reason not to be complacent about the need to secure industrial control systems and critical infrastructure: though cyberattacks on such systems will be costly, a determined adversary may be **willing to pay the cost** to achieve its aims. Conclusion The common assumption that the offense dominates cyberspace is dangerous and deeply misguided. The offense-defense balance can be assessed only for specific operations, not for all of cyberspace, as it is shaped by the capabilities of adversaries and the complexity of their goals in any conflict. When it comes to exerting precise physical effects, cyberspace **does not offer overwhelming advantages** to the offense. Because the capabilities of offense and defense are similar, improving defensive operations allows preparation for cyber offense without **risking geopolitical instability** or increasing vulnerability to attack.

#### OCOs cause overconfidence and arms races – that escalates.

Slayton ’17 (Rebecca; 2/1/2017; PhD in chemical biology from Harvard University, Masters in chemistry and chemical biology from Harvard University, Bachelor’s in chemistry from Westmont College, author of Arguments that Count: Physics, Computing, and Missile Defense, winner of the Computer History Museum Prize, author of Shadowing Cybersecurity, winner of a 5-year National Science Foundation CAREER award, project lead on research funded by the Department of Homeland Security Center of Excellence’s Critical Infrastructure Resilience Institute; “What is the Cyber Offense-Defense Balance?” What Is the Cyber Offense-Defense Balance?” <https://cornell.app.box.com/s/58xm5d4xwbdjq549vx5xnwc3qu1dqybk>; Date Accessed: 7/10/2017; DS)

“In cyberspace, the offense has the upper hand.” 1 These words, written in 2010 by Deputy Secretary of Defense William Lynn, reflect conventional wisdom among military officers, policymakers, and scholars. 2 A minority of scholars disagree. 3 Nonetheless, the prevalent belief that cyberspace favors the offense has major consequences for **international security**. According to offense-defense theory, state perceptions that technology favors the offense increase fears of attack **encourage arms races**, and through interactions between fears and capabilities, **increase the likelihood and consequences of war**. 4 Overconfidence in the advantages of offense can create a “cult of the offensive” with potentially **tragic results**. 5 Many of these dynamics appear to be at work with cyber conflict. Military leaders perceive cyberspace as favoring the offense and are seeking more discretion to conduct offensive cyber operations. 6 Cyberattack features prominently in the U.S. intelligence community’s list of global threats. 7 In 2012 Defense Secretary Leon Panetta warned of a potential “cyber-Pearl Harbor.” 8 Fears of being hacked, optimism about hacking others, or both have spurred massive investments in military cyber operations around the world, suggesting a cyber arms race. 9 Because cyber operations can **blur lines** between espionage (or “cyber exploitation”) and use of force (or “cyberattack”), they create a “cybersecurity dilemma,” wherein network intrusions undertaken for defensive purposes are easily misunderstood as preparation for an attack, **creating the risk of escalation** and use of force. 10

#### Undermines norms and causes kinetic warfare.

Gompert and Libicki ’15 (David and Martin; 7/22/2015; researcher @ RAND and Principal Deputy Director of National Intelligence from 2009 to 2010, PhD in economics from the University of California Berkeley and Master’s in city and regional planning from the University of California Berkeley; “Waging Cyber War the American Way,” <http://www.tandfonline.com/doi/pdf/10.1080/00396338.2015.1068551>; Date Accessed: 7/10/2017; DS)

US ambivalence toward cyber war is both strategic and normative, the implication being that what is bad for the United States is also bad for the world. Washington insists that any cyber operations it might conduct would be ‘in a manner **consistent with US and international law’**.5 Perceiving cyber war as war implies the applicability of the laws of war, specifically the principles of non-aggression, non-intervention, proportionality, discrimination and respect for neutrality.6 Compliance with all these norms could be **challenging** when initiating and conducting offensive cyber war. Case in point: the United States and Israel are said to have created and inserted the Stuxnet worm to interfere with the control of centrifuges used by Iran to enrich uranium. However justified by the imperative of preventing Iran from building nuclear weapons, it is fair to ask if this act of cyber war was lawful, especially in light of the unintended collateral effects it reportedly had. More broadly, harming non-combatants and civilian life, which can occur when infecting non-military computer systems, raises especially vexing issues, at least for the United States – thus its defensive posture. There are **several obvious reasons** for US wariness about offensive cyber war. Firstly, US military, intelligence, economic, governmental and societal functions are **highly dependent on computer systems**, and vulnerable to their disruption and degradation. Put starkly, having led and benefited enormously from the ‘digital revolution’, the United States regards cyber war as counter-revolutionary. Moreover, once begun, the course a cyber war might take would be **hard to predict, control or contain**. It could trigger **kinetic hostilities**, visit indiscriminate harm on non-combatants, escalate far beyond what the belligerents intended, and cause grave economic damage.7 Finally, US superiority in conventional military capabilities limits the need for cyber war, whereas enemies could use cyber war as an asymmetric answer to such superiority. In other words, cyber war could level the battlefield to the US disadvantage.

#### Our ev is comparative – risks of OCOs outweigh the benefits.

Lindsay and Gartzke ’16 (Jon and Erik; 8/25/2016; assistant professor of digital media and international affairs at the Univesrity of Toronto and PhD in political science form the Massachusetts Institute of Technology and wrote China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, professor of political science at the University of California San Diego and Director of cPASS; “Coercion through Cyberspace: The Stability-Instability Paradox Revisited,” <http://deterrence.ucsd.edu/_files/LindsayGartzke_CoercionThroughCyberspace_DraftPublic1.pdf>; Date Accessed: 7/10/2017; DS)

In contemporary defense policy discourse there are three **influential narratives** of mounting cyber peril, corresponding roughly to the three operational modes of attack, exploitation, and defense. The most dangerous scenarios envision the paralysis of industrial control systems or military command and control through surprise attack by anonymous hackers. The imagined aggressor may be a **revisionist state** like China or Iran or a non-state anarchist or terrorist empowered by the information revolution. A second narrative offers an alternative to the shock of sudden catastrophe, warning instead of the long term erosion of economic and military competitiveness drained away through persistent computer espionage. The relentless theft of vital secrets stored on corporate and government networks produces a “death by a thousand cuts” as states give their firms an unfair commercial advantage and equip their military forces with potent countermeasures to U.S. strengths. In both of these scenarios, commercial hacking tools and ubiquitous connectivity give weaker states and terrorists provide a **potent means** to exploit and attack the expanding attack surface of digitally-dependent advanced industrial states. A third threat narrative concerns the transformation of internet architecture to decisively benefit one political group at the expense of the other. At one extreme, the growth of flexible social media enables connected protesters to overwhelm and overthrow authoritarian regimes.15 At the other extreme, authoritarian governments censor internet content and reconfigure internet governance to undermine the internet’s potential for innovation and freedom. State paranoia about the threats of paralysis and erosion thus leads to digital lockout or “the end of the internet” as we know it.16 Threats of catastrophic attack, omniscient exploitation, and unassailable defense are myths because they imagine major rewards for little cost. The actual rewards of any given cyber campaign are **rarely so great** and the costs are rarely so trivial. Potential benefits of attack are **discounted by uncertainty** about the true value of the target to the adversary and the ability for the attacker to take advantage of it. **Operative costs** include the bureaucratic resources, development and testing requirements, human capital, and intelligence experience required to plan and run an effective covert cyber campaign. Setting aside the myths of low costs and high rewards (no free lunch), there are a variety of more realistic cyber operations with significant variation in their operative costs and benefits. A set of higher cost, and, potentially, higher reward complements enhance the capabilities of stronger actors who can master them. A much larger set of low cost, low reward irritants are available to weaker actors or even solitary individuals, but they provide only a small marginal return on a small investment.

### AT: Plan Secret---2NC

#### Secrecy magnifies not diminishes the link

Kuo, PhD Princeton, 19

(Raymond, Secrecy among Friends: Covert Military Alliances and Portfolio Consistency Journal of Conflict Resolution 1-27 ª The Author(s) 2019)

This literature provides little analytical traction because secret alliances are conceptually distinct from covert communication. Most obviously, mutual hostility—a prerequisite for Carson (2016), Carson and Yarhi-Milo (2017), and Yarhi-Milo (2013)—does not exist among “friendly” partners. The private diplomacy literature focuses on short-term engagements of limited coordination, where adversaries seek to avoid revelation and escalation to lend credibility to their signals. But revelation and escalation are typically the goals of secret alliances, which formalize and codify cooperative and often lasting relationships. As Bas and Schub (2016) highlight, a significant proportion of hidden pacts are offensive: they are designed to spread conflict. Even defensive pacts, as Ritter (2004) discusses, generate strategic uncertainty and surprise, causing allies to take less compromising positions. Indeed, the hidden nature of covert pacts undermines deterrence, potentially making conflict more likely, in contrast to much of secret diplomacy.

#### Resolve leaks in favor of the negative- everyone knows about the plan within 30 minutes

Glaze 16

(Ben, deputy political editor, https://www.mirror.co.uk/news/uk-news/vital-nato-secrets-being-leaked-8449680, 7-19)

Vital military secrets are being leaked to the Russians, Defence Secretary Michael Fallon sensationally admitted today. Nato intelligence files only for the eyes of the 28-member alliance are being slipped to President Vladimir Putin's regime, he told MPs. Allies have launched a huge crackdown to prevent even more secrets being passed to the Kremlin, the top Tory minister said. The revelation came after Conservative MP Colonel Bob Stewart, who commanded UN forces in Bosnia, accused Nato members of colluding with Moscow in the 1990s. “When something says 'Nato: secret', that's the last bloody thing it is,” he said. “When I served in Nato we reckoned anything with 'Nato: secret, classified' on it took half an hour before the Russians had it.

#### NATO doesn’t prohibit disclosure

Roberts, PhD, 03

(Alasdair Roberts is Director of the Campbell Public Affairs Institute at the Maxwell School of Citizenship and Public Affairs, Syracuse University, United States. Professor Roberts is a specialist on government information policy. https://www.aip-bg.org/library/press/dnev\_151003\_eng.htm, 10-15)

The United States does have narrow laws that punish the disclosure of certain kinds of very sensitive classified information, such as information about CIA agents. However, these laws apply mainly to government officials. In the current controversy, no one has suggested that the journalist Robert Novak should be sent to prison for publishing information he received from senior government officials. Under American law, there is no way that Mr. Novak could be sent to prison. The United States is a powerful country, and perhaps it is in a position to ignore NATO rules about Penal Code provisions for unauthorized disclosure of classified information. A more likely explanation is that NATO has no specific rules.

#### Turkey will leak to spite NATO

Ya Libnan 17

(Ya Libnan Oh Lebanon, is a Lebanese media outlet that delivers English-language news from Beirut to an international audience. https://yalibnan.com/2017/07/21/turkey-leaks-secret-locations-of-us-french-troops-in-syria/, 7-21)

Turkey’s state news agency on Tuesday published the locations of secret US military bases in Syria as well as details on the numbers of US and French troops stationed there, sparking the ire of fellow NATO member states. In the latest display of tensions between Turkey and other NATO member nations, Turkey’s state-run Anadolu news agency earlier this week published a detailed report of the secret locations of US military bases, operational posts and military posts inside Syria. The 620-word news report also included the numbers of US soldiers and French special forces stationed at these locations. The unprecedented leaking of sensitive battlefield information by the state-run news agency obviously had official Turkish backing, according to Jasper Mortimer, FRANCE 24’s Turkey correspondent. “It certainly was intentional. Anadolu agency is the hand-servant of the [Turkish] government. It would not have published this report without the green light from the top of government,” explained Mortimer, reporting from Ankara, adding that the revelation of troop numbers was particularly serious. “War correspondents do not give the number of troops in the unit to which they are attached. That is seen as giving information to the enemy. But here, Anadolu agency appears to have done exactly that.”

#### Secrecy is the link, not a turn -psychological research proves leaks inevitable and will be more damaging

Kuo, PhD Princeton, 19

(Raymond, Secrecy among Friends: Covert Military Alliances and Portfolio Consistency Journal of Conflict Resolution 1-27 ª The Author(s) 2019)

Furthermore, portfolio consistency is a form of network effect. The pressure to maintain secrecy scales with the number of hidden partners or obligations. A state may face only small costs from reneging on one secret ally. But when a state is embedded within overlapping covert alliances, it faces significant social pressure from several different actors to maintain secrecy in subsequent partnerships. Even a small number of hidden allies can constrain defection by raising the risk of wider network damage. Revelation of one set of obligations allows other partners and adversaries to identify that alliance’s conditions, reducing its strategic utility and potentially disclosing the wider limits on an actor’s foreign policy. Similarly, the extensiveness of hidden provisions can result in the same network effect. Assuming that states hope to avoid conflicting commitments, they must shape additional obligations around existing ones, creating an “interlocking” set of provisions exclusive to each partner. Revelation of one allows partners and adversaries better insight into additional limits on the alliance’s commitments or the conditions of other secret treaties. Of course, some states may want contradictory obligations, as Nazi Germany did. But maintaining secrecy then is even more important. Countries with conflicting commitments will suffer strategic, reputational, policy, and other costs whenever any of their pacts are invoked. Avoiding these costs for as long as possible requires keeping all these obligations hidden. However, contradictory commitments should be relatively rare. The gains from “fooling” other countries would have be substantial to offset the reputational and strategic damage caused. In addition, extensive research in psychology finds that lying is cognitively more taxing than telling the truth, particularly if lies must also be mixed with truthful statements (Caso et al. 2005; DePaulo et al. 2003; Gilbert 1991; Granhag and Strmwall 2002; Hartwig et al. 2006; Spence et al. 2001, 2004; Strmwall, Hartwig; Granhag 2006; Vrij and Mann 2001; White and Burgoon 2001; Vrij et al. 2008). As secret policy contradictions proliferate, as the situations they apply to become more complex, and as the number of hidden partners increases, the cognitive load increases as well, making it much easier for diplomats to inadvertently disclose confidential information.

## Turf Wars DA

### Turf Wars DA---1NC

#### The plan’s expansion of OCO’s under Title 10 ignites legal turf wars

Smeets ’20 [Max; February 15; senior researcher at the Center for Security Studies (CSS) and Affiliate at Stanford University Center for International Security and Cooperation and Research Associate at the Centre for Technology and Global Affairs, University of Oxford; Intelligence and National Security, “U.S. cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection,” 35:3]

This means that if U.S. Cyber Command seeks to operate only in ‘red space,’ its activities will still have global reach. It also suggests that red space grows as adversaries expand their operational activity. Most importantly, this implies that if U.S. Cyber Command seeks to achieve ‘effects’ in gray space, this will involve operating infrastructure that adversaries do not control – which is to say those systems or networks on which adversaries merely have a presence or are not active at all.

What is really new here? The United States has long operated in networks ‘close to the adversary.’ As Ben Buchanan’s book, ‘The Cybersecurity Dilemma,’ demonstrates, the U.S. has long acted as an observer outside of its own networks, gathering intelligence of adversarial activity in those others’ networks.21 In fact, information has become public concerning a case in which the Five Eyes collected intelligence about an espionage platform (dubbed ‘Snowglobe’ by the Canadian Intelligence Agency CSEC and ‘Animal Farm’ by Kaspersky Lab) of an allied country, France, likely operating in adversarial networks in the Middle East.22 In other words, the practice of fourth-party collection is nothing new.23 Furthermore, the U.S. has long acted in foreign non-adversarial networks as a passerby, transiting through allied’ networks to access an adversarial network.

Yet, the new Cyber Command and Defense Department strategy changes the nature of the U.S. military’s behavior within those systems and networks. Under the new strategy, Cyber Command wants to be an active disrupter on those networks. It wants to achieve effects – that is to disrupt, deny, degrade, and/or destroy. The only known precedent is U.S. Cyber Command operators wiping Islamic State propaganda material off a server located in Germany.24 The German government was notified in some fashion but not asked for advance consent, causing much frustration.25 This will likely lead to a systematic scaling up: U.S. Cyber Command now also seeks to be an active disrupter on those networks ‘globally, continuously and seamlessly’ – not regionally and sporadically.26

Out of network operations in allied networks also affect the turf war between the NSA and Cyber Command – mostly critically Title 10 and Title 50 concerns.27 As Chesney summarizes:

From a legal perspective, the issue this [case of Germany] highlights is that operations abroad implicate the UN Charter and related claims about international law protection of sovereignty. […] Intelligence agencies can more easily act in this setting when operating under Title 50 authority, as covert action status carries with it a statutory obligation to comply with the U.S. Constitution and U.S. statutes – but no more than that. Title 10, in contrast, carries with it no such implicit statutory shield against international law objections, and of course there is a general Defense Department policy of international law compliance. Thus CYBERCOM operating under Title 10 would run into the full thicket of international law concerns.28

Overall, it is expected that operating in allied networks under Title 10 is likely to cause more legal friction than operating under Title 50.

#### Turf battles over cyber authority spill over---decking domestic law enforcement of financial crime

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

As James Q. Wilson notes in his study of bureaucracy, government agencies "view any interagency agreement as a threat to their autonomy." James Q. Wilson, Bureaucracy: What Government Agencies Do and Why They Do It 192 (2000). He points out that the "chief result of the [bureaucratic] concern for turf … is that it is extraordinarily difficult to coordinate the work of different agencies." Id. Wilson notes that business bureaucracies "coordinate their actions by responding to market signals" and, where appropriate, by "entering into explicit agreements … in which mutual material gain is the criterion for cooperation." Id. "Government agencies, by contrast, view any interagency agreement as a threat to their autonomy." Id. They also "resist being regulated by other agencies." Id. at 193.

[END FOOTNOTE]

Before Cyber Command was created, some members of the military argued that branch-specific commands could not provide an effective cyberwar response system. They claimed the "cultures of today's military services are fundamentally incompatible with the culture required to conduct cyberwarfare." And they contended that the "core skills" needed to wage cyberwar differ radically from those needed for conventional war. Those who subscribed to this view believed the better approach was to create a new, cyber-specific branch of the military and assign it overall responsibility for cyber operations, just as the Air Force was assigned responsibility for air operations.

I suspect that view did not prevail because it would have required the various branches to give up their cyber commands. Since it has for some time been apparent that cyberspace can be used for military purposes, I suspect the five branches were reluctant to give up the opportunity to play a role in this new theatre of combat. I also suspect that the proposal to create a new, cyber-specific branch of the U.S. military may not have prevailed because it would have been difficult, if not impossible, to implement. As we saw above, the rationale for the different branches is that each is responsible for military activity in a specific spatial domain in the physical world. While the divisions are not precise, it is far easier to parse response authority in a spatial context than it is with regard to cyberspace.

Cyberspace operations do not take place in a physical [\*183] place; instead, they involve activity that occurs in and through computer technology, which is pervasive in today's world. If the Department of Defense had chosen to create a distinct branch with exclusive combat authority in cyberspace, it would presumably mean this branch would take command of any and all of the other branches' activities that involved cyberspace. It is difficult to see how this could be a viable strategy. It would presumably mean, for example, that members of the cyberbranch would monitor, and probably control, the other branches' computers and online activities (i) to ensure a baseline of security and (ii) to be in a position to respond if and when the cyberbranch believed it necessary to deter or respond to cyberwarfare attacks. That seems to be the only way to functionally allocate operational responsibility in cyberspace to a new, cyber-specific branch of the U.S. military.

If that is, indeed, the only way to accomplish this, then instead of participating in a carefully-defined, complementary division of responsibility, such as the one the existing branches currently represent, the hypothesized cyberbranch would essentially subsume the other branches as to its distinct area of responsibility. That could be problematic. It might, for example, create clashes of authority that could have negative consequences for the United States' ability to respond to cyber-attacks.

This might be one of the reasons the Department of Defense apparently opted, instead, to create a distinct command that unified the cyberspace components of the five traditional branches of the military. This approach is fraught with its own problems, the most obvious of which is coordinating the activities [\*184] of the five branch cyber commands. If cyberspace were divisible into spatial operational domains, Cyber Command could function in a fashion analogous to that of one of the United States military's conventional Unified Combatant Commands. These Commands incorporate personnel from the five military branches into a unified command with responsibility for a specific geographical area. The personnel assigned to such a Command respectively carry out the functions that are within their branch's unique expertise, e.g., the Navy carries out operations at sea, the Air Force conducts aerial activities, and so forth.

As we saw above, cyberspace, unlike real space, cannot be parsed into spatial domains. Unless that changes, Cyber Command faces the unenviable task of trying to sort out what, precisely, should be the respective responsibility of the Air Force, Army, Marine, and Navy cyber commands. At the moment, it appears that at least these four cyber commands have essentially the same mission, i.e., to conduct offensive and defensive military operations in cyberspace. This is not only pointless, it is likely to be counterproductive. Unfortunately, as we also saw above, this state of affairs seems likely to continue for some time.

There is yet another issue Cyber Command must resolve. Since the task list cited earlier focuses exclusively on (i) defending the military's assets in cyberspace and (ii) directing and conducting military operations in cyberspace, many wondered if the new Cyber Command was only going to be responsible for [\*185] protecting military assets and networks. In other words, would Cyber Command also be responsible for protecting civilians and civilian-owned assets?

In the fall of 2010, the newly-appointed head of Cyber Command, General Keith Alexander, told reporters the new unit did "not have a role" in protecting civilian networks and cyber-assets. This caused controversy because, as Part II noted, the military's role has historically been to protect a state, its citizens, and their assets from external threats. If General Alexander's comment was transposed to the context of kinetic warfare, it would become a declaration that in the event of nuclear war the U.S. military will protect itself but not civilians. Since that proposition is completely inconsistent with the military's role in society, it is not surprising that the General, at least to some extent, retreated from that position in a statement he made the next day.

In testifying before the House Armed Services Committee, General Alexander prosposed that Cyber Command "could also have a broader role in the civilian sector through protecting US critical infrastructure networks and systems." He noted, though, that the White House "was examining the legal authority needed for Cyber Command to take responsibility for protecting civilians and civilian-owned assets." A few days later, the Department of Defense and the Department of Homeland Security perhaps sought to address this issue, at least in [\*186] part, by signing a memorandum of understanding that (i) gives Homeland Security "lead responsibility for protecting the United States government's civilian networks and critical infrastructure," (ii) makes the Defense Department responsible for "protecting some 15,000 military networks," and (iii) provides that the two will collaborate to "safeguard cyberspace against state as well as non-state actors."

General Alexander's comments and the memorandum of understanding executed by the Departments of Defense and Homeland Security demonstrate the doctrinal and institutional constraints that impede the U.S.'s ability to mount a unified response to cyber-threats. The primary constraint is the bifurcation described in Part II: the military (Defense) deals with war, while law enforcement (Homeland Security) deals with crime and terrorism. Due to historical circumstance, the bifurcation [\*187] implicitly assumes attacks from abroad target nation-state assets and/or personnel while crime and terrorism target civilian assets and/or personnel.

As we saw in Part II, that is not necessarily true as threats migrate into cyberspace. Civilians and civilian-owned assets are already a target of cybercrime and cyberterrorism, and it has for some time been apparent that they will also be targets in cyberwarfare. The bifurcation, though, does not allow (i) law enforcement officers to retaliate against cyberwarfare attacks or (ii) members of the military to retaliate against cybercrime and cyberterrorism. That is why General Alexander could not assert that Cyber Command would protect civilians, and that is why the Departments of Defense and Homeland Security found it necessary to execute the memorandum of understanding noted above.

As matters currently stand, Cyber Command will have to utilize the attribution processes described in Part II to determine, with the necessary level of confidence, that a given attack was state-sponsored before it can reciprocate in kind. Civilians and civilian assets have been targets of conventional warfare, even though the law of armed conflict calls for minimizing attacks on noncombatants. But those attacks have come from an identified, nation-state enemy, which allowed the targeted nation-state to respond in kind, even if the attack occurred on its territory.

General Alexander's primary problem, therefore, is that it may be impossible for the military to make such a determination for a cyber-attack quickly enough for a timely response because [\*188] the "markers" traditionally used to distinguish between internal and external attacks are of little utility in the cyber context. This is essentially a doctrinal problem, as it arises from the practice of dividing threats into these two categories and categorically parsing threat response authority between them. But as we saw earlier, General Alexander also confronts an institutional problem: fusing six distinct cyber commands into a coordinated, coherent cyber-response effort. We will return to this issue in Part IV.

As we will see below, United States law enforcement confronts a correlate doctrinal problem and operates in a far more complex institutional structure.

B. Law Enforcement

As we saw in Part II, law enforcement is charged with controlling the "other" threat: the threat to internal order that arises from antisocial conduct on the part of individuals who are "in" the territory of the state under whose authority law enforcement officers operate. Some countries have a national penal code and a national police agency that enforces that code. But because it is a federal state, the United States has an essentially two-tiered system of penal laws and a two-tiered law enforcement structure.

As to the former, the United States has fifty-two distinct [\*189] criminal codes (one for each state, one for the District of Columbia and a federal criminal code). These codes require a corresponding, two-tiered law enforcement structure: one tier consists of the over 15,000 state and local agencies that respectively enforce state criminal codes. Their geographical jurisdiction is generally linked to the nature of the agency in which they serve: state police have jurisdiction throughout the state, a county sheriff has jurisdiction in that county, and municipal police have jurisdiction within the territorial boundaries of their municipality.

The other tier is composed of agencies that enforce federal law. Five of them - the Federal Bureau of Investigation, the [\*190] U.S. Secret Service, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the Drug Enforcement Administration, and U.S. Immigration and Customs Enforcement - are primarily responsible for pursing those who violate the federal criminal code. And because these agencies operate under the authority of the federal government, they have national jurisdiction, i.e., their agents can pursue investigations anywhere that is within the "maritime and territorial jurisdiction of the U.S." and, under certain circumstances, abroad.

It may seem that this complex enforcement structure, with its often-overlapping federal and state jurisdiction, must inevitably generate turf wars that impede the efficient enforcement of the law. The likelihood that rivalry will occur between state and local law enforcement agencies is mitigated, at least to some extent, by the fact that each has a clearly defined geographical jurisdiction within which it operates. This reduces, but does not eliminate, the potential for inter-agency conflicts. Instances can and do arise in which, say, the State Police [\*191] and the County Sheriff both have jurisdiction in a given matter, which can create conflicts as to who should take the lead. Over the last few years, state and local agencies have used multi-jurisdictional task forces to reduce, if not eliminate, such conflicts.

Historically, the more serious conflicts arose between state and local agencies and their federal counterparts. There appears to have been a corresponding reduction in these conflicts as well, a phenomenon many attribute to a spirit of greater cooperation brought on by the 9/11 attacks.

That leaves the federal agencies, which have certainly not [\*192] been immune to turf wars. And according to recent reports, turf battles continue to be a problem for federal law enforcement agencies, despite their use of task forces and other, similar efforts. One reason why such conflicts persist among federal agencies is that, unlike their state and local counterparts, federal agencies' jurisdictional authority is predicated not on geographical turf, but on what a recent report refers to as "operational turf."

In situations like the hypothetical noted earlier, in which a crime scene falls within the State Police's and the local Sheriff's geographical turf, the State Police may defer to the Sheriff, because his office has stronger ties to that location and the victim. That calculus does not come into play at the federal level because, as I noted earlier, the federal law enforcement agencies listed above all have national jurisdiction. This, as noted above, means their turf is not linked to a specific state, county, city, or other area. The agents employed by these agencies operate out of specific, geographically located offices, but this is a matter of operational efficiency and, as such, does not define the legitimate scope of an agency's operations. That is a function of "operational turf," that is, of the statutes that define a given agency's investigative authority.

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

Salvador ’15 [W. Joseph; 2015; 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.

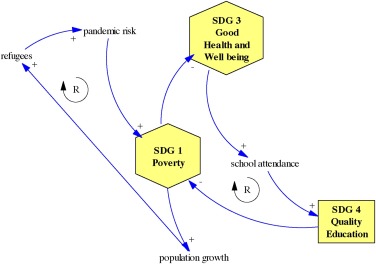
### Impact---2NC

#### They dropped that it wrecks development---extinction

Cernev ’20 [Tom; January; MPhil in Engineering for Sustainable Development from the University of Cambridge, BA in Mechanical Engineering from the University of Adelaide, Winter School Attendee at the Australian National University, and Dr. Richard Fenner, Reader at the University of Cambridge and Director of the MPhil in Engineering for Sustainable Development; Futures, “The Importance of Achieving Foundational Sustainable Development Goals in Reducing Global Risk,” https://doi.org/10.1016/j.futures.2019.102492

4.3. Linking risks with progress in the SDGs

Generally it is the Outcome/Foundational and Human input SDGs that are most directly related. For example as the movement of refugees increases pandemic risk, poverty levels in low and middle income countries increase reducing the health of the population, and so restricting access to education which further enhances poverty and birth rates rise as family sizes increases generating unsustainable population growth which furthers the migration of refugees (Fig. 5). Fig. 3 shows that leverage points to reduce refugees lies in SDG 16 (Peace Justice and Strong Institutions), reducing malnutrition through alleviating SDG 2 (Zero Hunger) and taking SDG 13 (Climate Action) to avoid the mass movement of people to avoid the impacts of global warming.



Global warming itself will drive disruptive changes in both terrestial and aquatic ecosystems affecting SDG 15 (Life on Land) and SDG 14 (Life Below Water) adding to their vulnerability to increases in pollution driven by a growing economy. Loop B (in Fig. 4)shows the constraints associated with SDG 13 (Climate Action) may slow the economic investment in industry and infrastructure reducing the pollution generated, encouraging adoption of SDG 7 (Affordable and Clean Energy) whilst stimulating carbon reduction and measures such as afforestation, which will also improve the foundational environmental goals.

Depletion of resources and biodiversity are strongly linked to SDG 12 (Responsible Consumption and Production) through measures such as halving global waste, reducing waste generation through recycling reuse and reduction schemes, and striving for more efficient industrial processes. The more resources that are used, the less responsible is Consumption and Production which may thus reduce biodiversity (Fig. 3) and increase the amounts of wastes accumulating in the environment.

The final driver of Global Catastrophic Risk is an agricultural shortfall which will increase global Hunger (SDG 2) and widen the Inequality (SDG 10) between rich and poor nations and individuals. Quality Education (SDG 4) is important as a key leverage point to stimulate the generation and adoption of new technologies to improve energy (SDG 7) and water supplies (6) which can enhance agricultural production. Such linkages are convincingly examined and demonstrated in the recent film “The Boy Who Harnessed the Wind” (2019), based on a factual story of water shortages in Malawi in the mid 2000s.

These examples may appear self evident, but it is the connections between the goals and how they adjust together that is important to consider so the consequence of policy actions in one area can be fully understood. Because of the underlying system structures global threats can quickly transmit through the system. Water Crises will limit the water available for agriculture and basic needs which in turn will stimulate a decline in Gender Equality (SDG 5). Technology disruption from cyber attacks will restrict the ability to operate Sustainable Cities and Communities (SDG 11) and potentially expose populations to extreme events by disrupting transport, health services, and the ability to pay for adaptation and mitigation of climate related threats from a weakened economy. Conflict (in all forms) will increase refugees and climate change provides the backdrop against which all these interactions will play out.

Whilst it is possible that general catastrophic risk or existential risk scenarios may eventuate from the non-achievement of the Sustainable Development Goals, there are certain aspects within the causal loop diagram which if prioritised will reduce this risk. For example, to reduce the risk of pandemic, ensuring that the number of Refugees is minimised, and is a leverage point. Similarly, prioritising SDG 3 (Good Health and Well-being) is essential and is enabled by many of the other goals. However, a feature missing from the SDGs is a recognition of the precautionary principle, with an implicit assumption that technological innovation alone may create improvements in many of the goals.

#### It destabilizes every region---nuclear war

Dobriansky ‘1 [Paula, Under Secretary for Global Affairs at the State Department, “The Explosive Growth of Globalized Crime,”<http://www.iwar.org.uk/ecoespionage/resources/transnational-crime/gj01.htm>]

Certain types of international crime -- terrorism, human trafficking, drug trafficking, and contraband smuggling -- involve serious violence and physical harm. Other forms -- fraud, extortion, money laundering, bribery, economic espionage, intellectual property theft, and counterfeiting -- don't require guns to cause major damage. Moreover, the spread of information technology has created new categories of cybercrime. For the United States, international crime poses threats on three broad, interrelated fronts. First, the impact is felt directly on the streets of American communities. Hundreds of thousands of individuals enter the U.S. illegally each year, and smuggling of drugs, firearms, stolen cars, child pornography, and other contraband occurs on a wide scale across our borders. Second, the expansion of American business worldwide has opened new opportunities for foreign-based criminals. When an American enterprise abroad is victimized, the consequences may include the loss of profits, productivity, and jobs for Americans at home. Third, international criminals engage in a variety of activities that pose a grave threat to the national security of the United States and the stability and values of the entire world community. Examples include the acquisition of weapons of mass destruction, trade in banned or dangerous substances, and trafficking in women and children. Corruption and the enormous flow of unregulated, crime-generated profits are serious threats to the stability of democratic institutions and free market economies around the world.

#### That’s the single largest threat to global security – convergence of terrorism with cybercrime requires effective enforcement

Stavridis ’13 [James G.; May 31; dean of the Fletcher School at Tufts University and former supreme allied commander at NATO; Washington Post, “The dark side of globalization,” <http://www.washingtonpost.com/opinions/how-terrorists-can-exploit-globalization/2013/05/31/a91b8f64-c93a-11e2-9245-773c0123c027_story.html>]

I am often asked what keeps me awake at night after nearly 40 years as a Navy officer, including four years as supreme allied commander for global operations at NATO. There is no shortage of frightening issues: Iran, North Korea, the insurgency in Afghanistan, civil war in Syria , cyberthreats , chemical weapons, terrorism. But my one-word answer may surprise: convergence. Convergence may be thought of as the dark side of globalization. It is the merger of a wide variety of mobile human activities, each of which is individually dangerous and whose sum represents a far greater threat. The most obvious example of this kind of convergence is narco-terrorism. Drug cartels use sophisticated trafficking routes to move huge amounts of heroin, cocaine and methamphetamines. Terrorists can in effect “rent” these routes by co-opting the drug cartels through money, coercion or ideological persuasion. These organizations can then move personnel, cash or arms — **possibly even a w**eapon of **m**ass **d**estruction— clandestinely to the United States. Other globally trafficked illicit goods can also be found constantly moving on these routes: stolen and counterfeit intellectual property, illegal migrants, human slaves, laundered cash, sophisticated armaments. Meanwhile, in laboratories in North Korea, Iran and Syria, sophisticated weapons of mass destruction are in production or being researched. When global trafficking routes and weapons of mass destruction merge, the result will be catastrophic**.** A special case of this kind of convergence is emerging in the cyberworld, where the greatest mismatch between the level of threat to our country (high) and our level of preparation (low) is evident. High-threat packages move through the world’s servers, fiber-optic cables and routers in the service of nations, anarchic organizations and garden-variety hackers. Trillions of dollars’ worth of cybercrime occurs each year; if the cyber-capability and the resultant cash converge with terrorist groups or pariah states such as Iran and North Korea, the potential for catastrophe is high. So, what can be done? First and foremost, the United States and the international community must recognize the threat this kind of deviant globalization poses. Convergence of these mobile illicit activities can rapidly undermine global security norms. Too often the focus is on single-point threats — drugs, money laundering, human trafficking, weapons trading, production of weapons of mass destruction — while the true threat lies in their convergence. The Obama administration’s Strategy to Combat Transnational Organized Crime, published in 2011, is a step in the right direction.

#### It turns cyber---failing private sector defense causes offensive hack-backs---those escalate

Gen. Martin **Dempsey 13**.Graduate of the U.S. Military Academy; he also holds Masters’ degrees from West Point and Duke; his career in the nation's service has taken him around the world during both war and peacetime, from places that ranged from Germany to Iraq, from platoon leader to Chief of Staff of the Army, became the 18th Chairman of the Joint Chiefs of Staff, where he currently serves as the nation's highest ranking military officer, and principal military adviser to the President and Secretary of Defense and the National Security Council. 07-23-13. “Gen. Dempsey's Remarks and Q&A on Cyber Security at the Brookings Institute.” JCS. http://www.jcs.mil/Media/Speeches/tabid/3890/Article/571864/gen-dempseys-remarks-and-qa-on-cyber-security-at-the-brookings-institute.aspx

MR. SINGER: Great. This is from V. Eric McCann. What can private sector do to help the government with learning more about and defending against cyber attacks?

GEN DEMPSEY: Information sharing. Right now, information sharing is actually disincentivized, and we need to incentivize it.

MR. SINGER: Let me ask a follow up to this, a link to a prior topic you mentioned. Private security, we've got it maybe growing equivalent in the cyber realm and the hack back companies that are, right now, I was talking with someone, if you want a couple million dollars in venture capital, say you're exploring offensive cyber, what is your view of this growing potential industry of companies that do hack back?

GEN DEMPSEY: I'm very concerned about that. In fact, I have raised it [is] as all the more reason for us to come together as a whole of government, because we don't want private cyber organizations conducting operations that could be perceived as hostile acts. And if they're perceived as hostile acts, it could lead us into conflict.

### Uniqueness---2NC

#### Biden’s providing the NSA with authority

Dark Reading ’22 [Dark Reading; Jan 20; long one of the most widely read cybersecurity news sites, Dark Reading is also the most trusted online community for security professionals; Dark Reading “Biden Broadens NSA Oversight of National Security Systems,” https://www.darkreading.com/vulnerabilities-threats/biden-broadens-nsa-oversight-of-national-security-systems]

President Biden yesterday signed a memorandum that effectively expands the National Security Agency's role in overseeing the cybersecurity of intelligence, military, and other US government networks that handle classified or sensitive military or intel activities and data.

"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," said General Paul M. Nakasone, chief of the NSA and director of the US Commander Cyber Command, in a statement about the NSA's enhanced role.

Agencies with national security systems now report to Nakasone any cyber incidents of their systems, how they are mitigating cybersecurity incidents, and assessments of threats to their systems. The memorandum also requires them to adopt more modern encryption and zero-trust security strategies, among other cybersecurity practices.

"The new authorities will provide us with the necessary cybersecurity visibility into our most important systems," said Rob Joyce, NSA cybersecurity director and deputy national manager for national security systems. "This new insight will allow us to identify vulnerabilities, detect malicious threat activity and drive mitigations to better secure all national security systems."

#### NSA SIGINT authority enables them to be the globe’s most effective cybersecurity agent

**Economist ’20** [“A new global ranking of cyber-power throws up some surprises,” The Economist, September 19, 2020, https://www.economist.com/science-and-technology/2020/09/19/a-new-global-ranking-of-cyber-power-throws-up-some-surprises]

America rules digital national security, China is not far behind

China has the world’s largest army. Russia wields the most tanks. America owns the fanciest satellites. But who has the most cyber-power? A new National Cyber Power Index by the Belfer Centre at Harvard University ranks 30 countries on their level of ambition and capability. Offensive cyber-power—the ability to do harm in or through computer networks—is one measure. But so too are the strength of a country’s defences, the sophistication of its cyber-security industry and its ability to spread and counter propaganda (see chart).

That America stands at the top of the list is not surprising. Its cyber-security budget for fiscal year 2020 stood at over $17bn and the National Security Agency (nsa), its signals-intelligence (sigint) agency, probably gets well over $10bn. The awesome scale of America’s digital espionage was laid bare in leaks by Edward Snowden, a former nsa contractor, in 2013, which showed the agency hoovering up vast amounts of the world’s internet traffic and trying to weaken encryption standards.

China, in second place, has demonstrated a voracious appetite for commercial cyber-espionage abroad and an iron grip on the internet at home. Britain, whose National Cyber Security Centre has parried over 1,800 cyber-attacks since its creation in 2016, is third. Britain is currently setting up an offensive National Cyber Force staffed jointly by spies and soldiers. Russia, whose spies interfered with America’s last election, is in fourth place.

The big surprise is the Netherlands in fifth place, ahead of France, Germany and Canada. Dutch expertise in analysing malware is particularly sharp, says a Dutch insider, who points out that this is handy both for spotting attacks and mounting them. The cybercrime team of the Dutch police has proved adept at apprehending online criminals. And in 2014 the small but world-class group of hackers working for Dutch intelligence managed to penetrate a computer network used by the svr, Russia’s foreign intelligence service—including cctv cameras in the building—allowing them to watch as the Russians hacked America’s State Department.

Measuring cyber-power is fraught with difficulty, warns Marcus Willett, a former deputy director of gchq, Britain’s sigint agency. Many experts are puzzled by Israel’s relatively low ranking on the Belfer index, despite its hacking prowess; its secrecy may be one reason for this. “Warships in the Antarctic can easily be seen,” says Mr Willett, “yet a piece of code inserted into a power plant is hard to detect.” Though some states acknowledge their offensive capabilities—America and Britain boast of smashing Islamic State networks in Iraq and Syria, partly as a signal to Russia and China—most shy away from doing so.

Many countries outsource the dirtiest work to deniable proxies, like “hacktivists” and criminals. And whereas procuring a warship or missile is expensive and time-consuming, potent malware can be stolen or bought online. WannaCry, a ransomware attack mounted by North Korea in 2017, used a hacking tool, EternalBlue, which had leaked out of the nsa.

### Link---2NC

#### The plan disrupts domestic and global intel collection---the military is a cyber neophyte, which ensures backlash

Smeets ’19 [Max; October 14; 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; Lawfareblog, “NATO Allies Need to Come to Terms With Offensive Cyber Operations,” <https://www.lawfareblog.com/nato-allies-need-come-terms-offensive-cyber-operations>]

Second, it is not just about cyber effect operations taking place in systems or networks in allied territory. There could also be a negative impact on allied intelligence operations and capabilities beyond these systems and networks. The U.S Cyber Command – and other military cyber organizations – are operating in a global environment historically dominated by intelligence agencies, and the Five Eyes has always been the most dominant actor in cyberspace.39 But the Anglophone intelligence alliance is not the only intelligence actor operating across the world. Recent cases – such as the infiltration of the Dutch General Intelligence and Security Service into the Russia-based network of the infamous hacking group Cozy Bear – have illustrated the continued global prevalence and value of allies’ intelligence operations beyond the Five Eyes alliance.40 If U.S. Cyber Command increasingly take up the role of ‘disrupter’ it may negatively impact global intelligence collection of allies – particularly those countries that favor long-term access over immediate effect. It will also more likely uncover and burn allied capabilities.

The risks of occurring are higher than one may think as intelligence agencies have a tendency and incentive to target and track the same entities. For example, in late 2014, cybersecurity company Kaspersky Lab reported on the so-called ‘Magnet of Threats’. The cybersecurity company discovered a server belonging to a research organization in the Middle East that simultaneously hosted implants for at least five Advanced Persistent Threat (APT) actors: Regin and the Equation Group, Turla and ItaDuke, Animal Farm, and Careto.41 All of these APTs have been associated with prominent national security and intelligence agencies. Equation group and Regin are connected to the Five-Eyes. As said, Animal Farm has been attributed to France’s external intelligence agency. Turla Group has been associated with the Russian federal security service (FSB). ItaDuke is said to be linked to the Russian government too. Finally, it is theorized that Spain is behind Careto, also known as ‘The Mask’.

Consider what would have happened if one of those five APT groups had sought to cause a disruptive effect – rather than collect intelligence – against the target in the Middle East. It likely would have resulted in much earlier discovery and analysis by threat intelligence companies (or other actors) exposing the tactics, techniques and procedures (TTPs) of each actor group.

#### Expanding security cooperation for cybersecurity is exclusively Title 10---that leaves the NSA behind

Thaler et al. ’16 [David E., Michael J. McNerney, Beth Grill, Jefferson P. Marquis, Amanda Kadlec; 2016; Senior International/Defense Researcher at the RAND Institute, M.I.A. in International Security Policy from Columbia; Acting Director, International Security and Defense Policy Center; Senior International/Defense Researcher and Affiliate Faculty, Pardee RAND Graduate School; RAND Institute, “From Patchwork to Framework: A Review of Title 10 Authorities for Security Cooperation,” <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1438/RAND_RR1438.pdf>]

We refer to lack of flexibility in authorities in a previous section; this has led to "gaming" behavior—even embarrassment in relationships— as SC personnel need to stretch the intent of the authorities to fill perceived gaps in their ability to achieve SC objectives. In one case, discussants spoke of two seminars held recently in Poland and Estonia to share ideas and best practices and gain "intellectual interoperability" with allies with regard to Russian activities. These seminars took months of preparation and required considerable funding by the host nations, but at the last minute there was a cost increase because U.S. statute did not allow DoD to fund the coffee because the forums were not CT-related. Emerging threats (e.g., to cyber operations or maritime security) create some of these gaps, but there are also gaps that emerge from other needs, such as the need to sustain equipment that has been provided to partners through Title 10 authorities.

In the case of cybersecurity, some CCMDs are getting requests from partners to help them improve their capabilities but note that they "can't do it." While the belief may not yet be widespread that a relative lack of authorities for cyber security is a problem, there is growing recognition of the importance of this domain and that partners' weakness in cyber security is also U.S. weakness given that U.S. strategy depends on the support and competence of those partners. Some DoD stakeholders with whom we engaged indicated that they found no reasonable authority for building cyber capacity and thus could not conduct exchanges or training with a range of partners in this area, especially in the case of countries that cannot afford to send their personnel to relevant schools. There have been attempts to apply Section 1206 to cyber BPC activities, but this is one of those "gaming" situations mentioned above and is suboptimal. Stakeholders note that cyber should be more integrated into engagements with partners, and that they would like broader authority to work with them. They point out that the SC community can be slow to respond to a dynamic and changing security environment, and that greater focus on building cyber capacity is warranted. This appears to be a critical need, as U.S.

forces overseas "rely on our partners for critical infrastructure [in their countries]: energy, power, telecommunications, and water."

#### That undermines the “dual-hatting” unified command structure crucial to NSA effectiveness

**Alexander ’13** [Keith; June 12; COMMANDER, UNITED STATES CYBER COMMAND DIRECTOR, NATIONAL SECURITY AGENCY CHIEF, CENTRAL SECURITY SERVICE (Keith, “CYBERSECURITY: PREPARING FOR AND RESPONDING TO THE ENDURING THREAT” Congressional Testimony, <http://www.defense.gov/home/features/2013/0713_cyberdomain/docs/Alexander,_General_Keith_Testimony_6.12.13_Cybersecurity_Hearing.pdf>]

Due to the intersecting responsibilities of the two organizations, USCYBERCOM was placed at the headquarters of NSA/CSS at Fort Meade. NSA/CSS collects signals intelligence on our cyber adversaries; and provides information assurance strategies and technologies to protect our national security systems. The conduct of these two missions is critical to enabling cyber operations. NSA/CSS also has multiple, technical capabilities critical to the cyber mission area, such as high-performance computing and large-scale, distributed processing and data storage. These are just some of the components of what we call the cryptologic platform; it constitutes the collection of signals intelligence and communications security capabilities that since 1952 have served users ranging from national customers, to departmental analysts, to battlefield commanders. The defense of U.S. military networks depends on knowing what those who would harm us are doing in cyberspace, which in turn depends on intelligence produced by NSA and other members of the Intelligence Community regarding adversary intentions and capabilities.

Cyberspace is characterized by high levels of convergence of separate and different networks and technology that have come together to form something greater than the sum of the parts. In this regard, USCYBERCOM’s co-location with NSA/CSS mirrors the convergence in cyberspace and is a direct result of that technological shift. What we have learned is that if convergence is the reality of the cyber environment, then integration must be the reality of our response. Co-location promotes intense and mutually beneficial collaboration in an operational environment in which USCYBERCOM’s success relies on net-speed intelligence. Although they are separate and distinct organizations with their own missions and authorities, NSA/CSS is a major force multiplier for USCYBERCOM, pairing the Command’s operators, planners, and analysts with the expertise and assistance of NSA/CSS’ cryptographers, analysts, access developers, on-net operators, language analysts, and support personnel. These are close working relationships that enable seamless, deconflicted operations that are vital to the success of the cyber mission. Co-location also improves the deconfliction of operations; physical proximity enhances mutual understanding and awareness of mission areas and helps forge effective partnerships that serve both organizations and the nation well. Only a tightly integrated team, and tightly integrated solutions, can do what is required to address cyber threats at net speed.

I serve as the dual-hatted Commander, USCYBERCOM, and Director, NSA/Chief, CSS. The dual-hatting unifies the capabilities for full-spectrum cyber operations under a single official, maximizes the leverage of NSA/CSS cyber capabilities, capacities, and authorities, and establishes unity of effort in cyberspace for the Department of Defense. It allows deconfliction of the use of the cryptologic platform to occur with full knowledge of the needs of both organizations on a timely basis. Together, the people under my command and direction at USCYBERCOM and NSA/CSS work in concert but always under their respective authorities. They direct the operation of the Department’s information networks, detect threats in foreign cyberspace, attribute threats, secure national security information systems, and help ensure freedom of action for the United States military and its allies in cyberspace—and, when directed, defend the nation against a cyber attack.

#### The NSA conducts most info sharing with foreign partners---expanding that process ensures further relegation of the NSA and sparks turf wars

West ’21 [Laura; 2021; Major, Judge Advocate, U.S. Army, Deputy Chief of National Security Law, U.S. Cyber Command, Fort Meade, Maryland, LL.M and J.D.; Military Law Review, “The Rise of the “Fifth Fight” in Cyberspace: A New Legal Framework and Implications for Great Power Competition,” Volume 229 Issue 3]

To that end, Congress should consider improving the military’s ability to share cyberspace capabilities, information, and related data with international partners. Intelligence agencies, such as the NSA and the National Geospatial-Intelligence Agency, have special authorities that allow for more permissive capability or information sharing and support with foreign partners. [341] But no such authority exists—outside perhaps the long, arduous, and unclear process of arms control and foreign military sales— for the military (i.e., U.S. Cyber Command and subordinate units), the entity now primarily conducting operations with foreign partners in cyberspace. If one legal framework has changed to account for the speed and changing nature of cyberspace, then others should follow suit. Otherwise, the United States stands to lose the benefits of those newly granted military authorities.

#### The plan requires micromanaging civilian regulations that shred the effectiveness of CYBERCOM

Zehtab ’18 [Sean; June 13; JD from the University of Nebraska College Of Law, BS from University Of Nebraska-Lincoln, Judge Advocate in the United States Army; Harvard National Security Journal, “Overseeing or Interfering? A Functional Alternative to Congressional Oversight in Intelligence and Operations,” https://harvardnsj.org/2018/06/overseeing-or-interfering-a-functional-alternative-to-congressional-oversight-in-intelligence-and-operations]

Recently, the Army has incorporated cyber and electromagnetic capabilities at the Brigade level.[6] Moreover, there is interest in empowering conventional commands to deploy capabilities such as special forces and cyber in tactical operations.[7] Finally, gathering open source intelligence has become both easier and more useful at the operational level.[8] All these developments in Multi-Domain Operations raise oversight concerns, since conventional units do not currently have the kind of oversight systems designed to ensure respect for the civil liberties of U.S. Persons,[9] and congress and high-level actors are too far removed from day-to-day tactical operations to provide effective oversight.

Oversight of military decision making is vital to preserving the civilian control of the military, safeguarding democratic accountability, and ensuring compliance with international law. Excessive or poorly structured oversight, however, can inhibit flexible and timely responses to national security threats and can needlessly interfere with the effective use of expertise by military professionals. Good oversight, then, is a structural balance that both ensures compliance and accountability and permits flexibility and the effective use of expertise by military professionals.[10] Achieving this balance has been an ongoing challenge, subject to extensive scholarly debate and practical evolution over the past decade.[11]

Unfortunately, the current oversight regime in tactical cyber and other clandestine operations is in many ways the worst of both worlds: it chills aggressive action and is not effective at ensuring respect for civil liberties. Over the past decade, oversight has tended towards being concentrated in various high-level entities and individuals, increasingly far-removed from the realities and necessities of the modern operational environment. Moreover, Congress has directly involved itself in military oversight, while important operational decisions are made by field commanders who lack the resources, expertise, and priorities to ensure the protection of the civil liberties of U.S. Persons. The result is, predictably, violations—scarcely deterred by a highly bureaucratic, far-removed, and overly politicized system of oversight.

For instance, a single cyber operation could require oversight from intelligence and intelligence-related entities and agencies, congressional reporting and interagency concurrence, and ordinary operational approval from the military approval authority. In addition to ineffectively ensuring compliance with domestic and international law, the bureaucratic work generated by the current oversight regime takes valuable time and attention away from focusing on the planning and execution of a mission.[12]

This article argues that the Command Operations Review Board (CORB) of the United States Special Operations Command (USSOCOM) provides a model of effective oversight that should be applied to the operational and intelligence contexts. The CORB, independent but with military experience, leanly staffed and closer to the action, effectively balances ensuring compliance with the need for flexible, timely operations, and has provided effective oversight of special operations. This model, if applied more generally in operations and intelligence, could mitigate the problems, measured in blood, treasure, and legal violations, associated with the trend towards redundant and ineffective oversight of these operations by high-level executive and legislative organizations.

The core concern of this article is oversight mechanisms of contemporary cyber and special operations. More traditional intelligence activities, such as counterintelligence, signals intelligence and human intelligence, conducted by DOD under the Secretary of Defense authorities colloquially referred to as “Title 50,” already have multi-layered, robust statutory and agency regulation, whereas operational activities, such as operational preparation of the environment,[13] information operations, and cyber operations, do not have the same robust oversight framework. Cyber and special operations are often conducted in a clandestine manner, facing similar oversight challenges as intelligence.[14] But while oversight is necessary, the trend towards greater congressional involvement[15] reflects a misplaced locus of oversight. It should take place at the operational, not legislative, level.

### AT: Plan Not Title 10---2NC

#### SC isn’t Title 10---it’s either Title 22 or Title 10---either way that strips NSA authority

Hooper ’19 [Lt. General Charles and Michael O’Hanlon; June 4; Director of the Defense Security Cooperation Agency; Senior Fellow and Director of Research, Foreign Policy, Brookings; “How Security Cooperation Advances U.S. Interests,” Brookings Institute Foreign Policy Studies Program event]

Well, thank you, Mike, and thanks very much for having me. And good morning, everybody. I am the director of the Defense Security Cooperation Agency and it's the agency that does more and is known by less people than anybody else in Washington, so I always welcome the opportunity to tell everybody about it.

The Defense Security Cooperation Agency is mandated by Congress to execute all security cooperation, some on behalf of the State Department, much on behalf of the Department of Defense, writ large and worldwide. It is most known for being the executive agent for foreign military sales, and that's what most people know about us. But we're also responsible for excess defense articles. We are the executive agent for all five Department of Defense regional centers, so the Marshall Center in Germany; the Inouye Center, Asia-Pacific Center for Security Studies, in Hawaii.

We're also responsible, and we'll talk a little bit about this later, for what I call institutional capacity-building. That is the complement to foreign military sales that ensures that our partners have the human resources and the defense institutional development to properly utilize the equipment we buy for them in the interest of national security.

Our headquarters is here in Crystal City, in Washington. We also work with the Security Cooperation's officers worldwide. We work with the COCOMs. And we're under actually, and this is unique for the United States, we work for the Under Secretary of Defense for Policy. So we work for Mr. John Rood. And the reason I say that is in many countries, the acquisitions and the arms sales come under the acquisitions or the logistics directorates or work directly in some of our competitors, for those companies, those state-owned companies. But here in the United States security cooperation and arms sales is a policy tool and not a tool for anything else. So that's basically kind of a snapshot of what DSCA does.

MR. O'HANLON: So, great. That's very helpful. And let me ask a couple more follow-up questions just to continue to refine our understanding.

So a command like Africa Command, where you spent three years, which does a lot of training in the field, is all of that training essentially under your purview? Or the parts that do not involve U.S. weapons transfers or sales, are they potentially separate and you coordinate, but you're not in charge of that? Is that correct?

GENERAL HOOPER: Well, that's a very good question. The geographic combatant commands still have the responsibility for executing security cooperation in their respective commands. We work by, with, and through those commands. The weapons sales portion of it, or the defense articles and services portion of it, comes directly under DSCA's supervision. Some of the training exercises and other things we work collaboratively with the combatant commands. And then in some cases, for example, in institutional capacity-building, we work together in a synergistic fashion to effect that security cooperation.

So it's equal parts. Some things we're principally responsible for, some things the combatant commands are responsible for, and some things we work jointly together.

MR. O'HANLON: And as we start to paint this picture of your responsibilities and how you work with others, I also wanted to bring in foreign military assistance and financing. And my understanding is that there are parts of foreign military assistance of various types that we give through the State Department and other types we give through DOD. It depends a little bit on the recipient and the nature of the aid. Could you help us understand that a little bit, too? Because I'm sure some of that money is what's being used to buy the weapons that you're overseeing the transfer of.

GENERAL HOOPER: Absolutely. And that's also a very good question. So let's start on what we call the Title 22 on the State Department side.

We are the executive agent. The State Department has responsibility for foreign military sales and we are, in effect, the executive agent for the State Department in foreign military sales. Now, there are two real big components of security cooperation. One is what we call Title 22, which is the State Department supervised element for which we are the executive agent. The other half of it is the Title 10 piece.

So, for example, as a result of the Fiscal Year '17 NDAA, we had several different authorities and a disparate group of authorities that were all consolidated into one, the majority into one authority, 333, Section 333, that many of you may be familiar with. And this constitutes the Title 10 security cooperation piece.

The biggest way to distinguish between the two is our State Department responsibilities are principally focused to a great extent on defense articles and services, whereas our Title 10 responsibilities fall, in many cases, more into the realm of institutional capacity-building, exercises, and other types of things like that.

MR. O'HANLON: That's interesting. So you could think of it the hardware, sort of the weapons, the hardcore stuff, that's through State. The people side, the softer side, the software side is through DOD.

#### The plan expands Title 10 authority

Thaler et al. ’16 [David E., Michael J. McNerney, Beth Grill, Jefferson P. Marquis, Amanda Kadlec; 2016; Senior International/Defense Researcher at the RAND Institute, M.I.A. in International Security Policy from Columbia; Acting Director, International Security and Defense Policy Center; Senior International/Defense Researcher and Affiliate Faculty, Pardee RAND Graduate School; RAND Institute, “From Patchwork to Framework: A Review of Title 10 Authorities for Security Cooperation,” <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1438/RAND_RR1438.pdf>]

Only one existing Title 10 authority addresses the issue of cyber- security (see Table 4.10). Section 1051c in U.S. Code, introduced by Public Law 112-81, Section 951, allows foreign military personnel to be assigned to DoD to obtain education and training on threats to information security. There are no statutes that specifically authorize

Table 4.10

Changes to Cybersecurity Authorities

Authority and Purpose Suggested Change (Consolidate, Revise, Clarify, New Authority)

10 U.S.C. Sec. 1051c— Personnel Assignments for Information Security Education and Training • Revise to allow exchange of military personnel and limited training and equipment to military and nonmilitary foreign personnel

• Clarify what cyber capabilities could be shared by partner-type

the DoD to engage more broadly in information sharing and training on cybersecurity threats.

As indicated in Chapter Two, cybersecurity deserves greater focus in SC planning and implementation, and changes in statutes can help raise the priority of this emerging mission and give expression to congressional intent. It may be advisable to revise and substantially broaden the current statute to enable DoD to engage in more comprehensive cybersecurity activities with partners. The authority to assign personnel to DoD in Section 1051c could be expanded to allow for the exchange of defense personnel with foreign countries (similar to Public Law 104-201, Section 1082, and Public Law 111-84, Section 1207). This would allow DoD personnel to engage with a greater number of foreign personnel and gain a better understanding of partners' information security needs. Such exchanges would likely be restricted to certain countries with limits on the types of information that could be shared. Section 1051c also might be broadened beyond the authority to provide information security education and to include limited training and equipment for both military and nonmilitary foreign agencies. Such an authority would require Congress to clarify what specific cyber capabilities could be shared by partner-type. It also would require close monitoring and further revision as the cybersecurity mission area continues to evolve.

### AT: Aff Solves Cyber---2NC

#### Organized crime has gone digital---robust U.S. enforcement is key

Marker ’20 [Maxwell D; 2020; Section Chief, Transnational Organized Crime – Eastern Hemisphere, FBI, “Organized Crime Has Gone High Tech”, Police Chief Magazine, https://www.policechiefmagazine.org/organized-crime-has-gone-high-tech]

As the world has become increasingly wired, and now wireless, it is only natural that transnational organized crime (TOC) has moved into the digital age. The use of sophisticated information systems is no longer solely the realm of the hacker and the coder, it is now also the realm of the drug dealer, the extortionist, and the illegal gambler. Currency is no longer sponsored solely by governments, but exists in a digital realm. The Internet of Things is a reality. Computer skills are in high demand, and those skills can be developed independently and online.

The Internet provides a sense of anonymity to users. Anonymity, in turn, breeds vice. Vice inevitably lures organized crime, which is only too happy to capitalize on it. This article will look at how organized criminals are utilizing technology, what that means for law enforcement, and suggest ways TOC investigators need to be positioned for success in this new era.

On February 9, 2017, U.S. President Donald Trump issued Presidential Executive Order 13773 on Enforcing Federal Law with Respect to Transnational Criminal Organizations and Preventing International Trafficking (E.O. 13773). That order reaffirms the commitment of the U.S. government to address the scourge of TOC and protect communities and individuals from its influence. That order specifically calls for the investigation of

criminal gangs, cartels, racketeering organizations, and other groups engaged in illicit activities that present a threat to public safety and national security and that are related to, for example: (i) the illegal smuggling and trafficking of humans, drugs or other substances, wildlife, and weapons; (ii) corruption, cybercrime, fraud, financial crimes, and intellectual-property theft; or the illegal concealment or transfer of proceeds derived from such illicit activities.1

All of those significant criminal activities have in common the fact that they become easier to accomplish and more efficient when technology is leveraged to facilitate them. A rapidly emerging criminal threat lies in the gap between traditional criminal investigations and core intrusion-focused cyber investigations, where criminals are utilizing high tech tools developed by others and taking advantage of particularly sophisticated functionality available via the Internet. These tools and technologies are determining the future of organized crime investigations. Nowhere does this future become clearer than when one looks at how illicit items are being trafficked on the dark web.

#### Cyber crime is a key method to enhance their resource base

Roderic Broadhurst 14, Peter Grabosky, Mamoun Alazab & Steve Chon, ANU Cybercrime Observatory, Australian National University, “Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime”, International Journal of Cyber Criminology, Volume 8, Issue 1, January – June 2014, https://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf

Governments, law enforcement agencies, academic researchers, and the cyber-security industry speculate that ‘conventional’ organized crime groups have become increasingly involved in digital crime. The available empirical data suggest that criminals, operating online or on the ground, are more likely to be involved in loosely associated illicit networks rather than formal organizations (Décary-Hétu & Dupont, 2012). In recent years, insurgent and extremist groups have used Internet technology as an instrument of theft in order to enhance their resource base. Imam Samudra, convicted architect of the 2002 Bali bombings, reportedly called upon his followers to commit credit card fraud in order to finance militant activities (Sipress, 2004).

Cyber criminals may operate as loose networks, but evidence suggests that members are still located in close geographic proximity even when their attacks are cross-national. For example, small local networks, as well as groups centred on relatives and friends, remain significant actors. Cybercrime hot spots with potential links to organized crime groups are found in countries of Eastern Europe and the former Soviet Union (Kshetri, 2013a; see also Jones, 2010). Hackers from Russia and Ukraine are regarded as skilful innovators. For example, the cyber crime hub in the small town of Râmnicu Vâlcea in Romania is one of a number of such hubs widely reported in Eastern Europe (Bhattacharjee, 2011). There is also increasing concern about cyber crime in China (China Daily, 2010; Pauli, 2012). The source and extent of malware attacks (whether of domestic or foreign origin) and the scale of malware-botnet activity remain unclear, but a substantial proportion of Chinese computers are compromised and it is likely that local crime groups play a crucial role (Kshetri, 2013a; Chang, 2012; Kshetri, 2013b; Broadhurst & Chang, 2013). A recent study of spam and phishing sources found that these originated from a small number of ISPs (20 of 42,201 observed), which the author dubbed ‘Internet bad neighbourhoods.’ One in particular, Spectranet (Nigeria), was host to 62% of IP addresses that were spam related. Phishing hosts were mostly located in the United States, while spam originated from ISPs located in India, Brazil and Vietnam (Moura, 2013).

### Pharma Impact---2NC

#### Cybercrime decks the pharmaceutical industry

Mitsuhiko Maruyama 14, Partner and Cyber Risk Services Unit Leader at Deloitte, et al., “Cyber & Insider Risk at a Glance: The Pharmaceutical Industry”, <https://www2.deloitte.com/content/dam/Deloitte/jp/Documents/life-sciences-health-care/ls/jp-ls-cyber-insider-risk-en.pdf>

Abstract

Nothing is more valuable to a pharmaceutical company than the formula for one of its new drugs. Reports of hackers breaking into all sorts of firms and stealing their trade secrets is of enormous concern. Equally troubling, experts warn that theft of trade secrets by company insiders is a larger problem. This article looks at some recent cases of corporate cyber-espionage and insider trade secret theft. It discusses the use of spear phishing and zero-day exploits by sophisticated criminal gangs targeting corporations as well as more traditional, but hard to detect cases of outsiders paying employees to steal secrets. Many of the victims of cyber theft find themselves the target of class action lawsuits and regulatory actions. A quick look at data breach shows a rapidly changing regulatory environment, growing risks of litigation, and some important insurance implications for companies and their top management. This article ends with some areas that companies should consider in tightening up their safeguards against intellectual property theft.

Introduction

In 2011, the UK government estimates its pharmaceutical, biotechnology and healthcare sector suffered ₤1.8b in losses arising from theft of intellectual property (IP)2. The same year, the US government reportedly estimated its economy suffered $500b in harm from intellectual property and trade secret theft3. The Obama administration has publicly accused China of orchestrating many of these attacks against US organizations and even took the extraordinary step of indicting alleged members of the Chinese government’s elite military hacking team4.

One Chinese gang allegedly behind attacks on Boston Scientific and other US pharmaceutical companies also developed an exploit deployed specifically against Japanese targets5. According to FireEye, in 2013, Japan was the fourth largest target of such sophisticated cyber gangs that it tracks 6. If Japan’s pharmaceutical industry incurred damages on a level similar to the UK (whose market is about half the size), this would amount to something on the scale of ¥300b per year7.

The global market for pharmaceuticals is estimated to hit USD $1.1 trillion this year8. Strong demand for new cures and high profits associated with marketing new, patent-protected drugs drive fierce competition in product development1. It is not surprising then that criminal elements have increasingly targeted the intellectual property of pharmaceutical companies. The cost of IP falling into a competitor’s hands, however, is difficult to calculate9. For its 2014 estimate of the global cost of cybercrime, CSIS presented a wide range of $375-575m and specifically noted the difficulty of calculating damages caused by IP theft, adding this difficulty likely produced an artificially low estimate10.

Despite this challenge, some hard costs are identifiable. Cyber damages expert, the Ponemon Institute, estimates that globally the cost of recovering from a breach averaged $3.5m in 201411. Ponemon’s 2014 review of cyber incidents reported by 26 Japanese companies in 10 sectors showed that the average cost of remediation in Japan is approximately ¥241m12. In addition, the firm found that the adage, “an ounce of prevention is worth a pound of cure”, applies to a robust cyber defense. On average, Ponemon found a strong security posture to be the single most important factor in decreasing the cost of cleaning up after a cyber-incident2.

#### Extinction

Dr. Hugo Engelhardt 8, PhD, MD, Professor of Philosophy at Rice University, “Innovation and the Pharmaceutical Industry: Critical Reflections on the Virtues of Profit,” EBrary

Many are suspicious of, or indeed jealous of, the good fortune of others. Even when profit is gained in the market without fraud and with the consent of all buying and selling goods and services, there is a sense on the part of some that something is wrong if considerable profit is secured. There is even a sense that good fortune in the market, especially if it is very good fortune, is unfair. One might think of such rhetorically disparaging terms as "wind-fall profits". There is also a suspicion of the pursuit of profit because it is often embraced not just because of the material benefits it sought, but because of the hierarchical satisfaction of being more affluent than others. The pursuit of profit in the pharmaceutical and medical-device industries is tor many in particular morally dubious because it is acquired from those who have the bad fortune to be diseased or disabled. Although the suspicion of profit is not well-founded, this suspicion is a major moral and public-policy challenge. Profit in the market for the pharmaceutical and medical-device industries is to be celebrated. This is the case, in that if one is of the view (1) that the presence of additional resources for research and development spurs innovation in the development of pharmaceuticals and med-ical devices (i.e., if one is of the view that the allure of profit is one of the most effective ways not only to acquire resources but productively to direct human energies in their use), (2) that given the limits of altruism and of the willingness of persons to be taxed, the possibility of profits is necessary to secure such resources, (3) that the allure of profits also tends to enhance the creative use of available resources in the pursuit of phar-maceutical and medical-device innovation, and (4) if one judges it to be the case that such innovation is both necessary to maintain the human species in an ever-changing and always dangerous environment in which new microbial and other threats may at any time emerge to threaten human well-being, if not survival (i.e., that such innovation is necessary to prevent increases in morbidity and mortality risks), as well as (5) in order generally to decrease morbidity and mortality risks in the future, it then follows (6) that one should be concerned regarding any policies that decrease the amount of resources and energies available to encourage such innovation. One should indeed be of the view that the possibilities for profit, all things being equal, should be highest in the pharmaceutical and medical-device industries. Yet, there is a suspicion regarding the pursuit of profit in medicine and especially in the pharmaceutical and medical-device industries.

## Dedev

### Dedev---1NC

#### The aff prevents a short-term crisis that causes a transition away from growth, which is unsustainable and otherwise causes extinction

Kirk ’18 [Martin, co-founder and Director of Strategy for The Rules, former Head of Campaigns at Oxfam UK and Head of Global Advocacy for Save the Children, citing a study by Rodolfo Dirzo and Paul Ehrlich from the Stanford Woods Institute for the Environment and Gerardo Ceballos of the National Autonomous University of Mexico, “What if economic growth isn’t as positive as you think?,” <https://www.fastcompany.com/90202203/what-if-economic-growth-isnt-as-positive-as-you-think>]

But there are some new strains of thought that take a more nuanced and sophisticated view of growth. That say, yes, all other things being equal, economic growth is a positive thing. But all other things are not equal. There’s no such thing as a free lunch, and, for all its positives, economic growth has a dark side; its ecological impact. The impacts of our ever-growing economy have become so stark and so widespread that they are by any sane measure portents to catastrophe. Whether it’s the fact that Antarctic ice is now melting three times faster than we thought, or the unfolding “biological annihilation” that has already wiped out 50% of all animals and up to 75% of all insects, or the fact that, in spite of all this, we are pumping out CO2 at record levels, it takes willful ignorance or a blinding ideology to deny the severity of the crisis.

This creates a terrible paradox: Economic growth keeps economies stable today, but threatens not just future growth but medium-term social and civilizational cohesion, and ultimately the very capacity of this biosphere to sustain life. A paper published in the Proceedings of the National Academy of Sciences last year suggested that “the window for effective action is very short, probably two or three decades at most.” And that even this dire prediction is considered “conservative” by the authors, “given the increasing trajectories of the drivers of extinction.” In terms of practical politics, that means acting immediately, preferably yesterday.

Most politicians deal with this paradox by ignoring it. It’s by far the easiest option; one afforded every incentive and reward by this political economy and the beliefs that underpin it. This belief system has been dominant for a long time now. We are, as a society, deeply comfortable with it, which means many of its core assumptions are considered unassailable–too obvious to question. The most profound being this idea that growth is always good. Questioning this amounts to political suicide for any politician.

Or, at least, it used to. We are starting to see some movement in interesting corners of the global political landscape that suggest that some leaders are showing the sort of political courage needed to shift established norms. It may well be starting to become something of a bonafide political movement. It’s young and small, still, but so were all movements at one time.

A little thought experiment shows how growth can be a problem: Insert the word “a” before it. “A growth.” That feels very different from just “growth,” right? Growth is a big part of what we all understand happens in a healthy life. Children grow, knowledge grows, love grows. But “a growth” is what happens when life gets corrupted. “A growth” is when the growth is unchecked, and thus a symptom not of health but disease; when it takes on the character of an invader, attacking its host. The word for growth that gets out of control in this way, such that it becomes “a growth,” is, of course, cancer.

But wait, I hear you cry, technological progress will save us! We can just grow meat in test tubes rather than needing so much land and clean air space for cows and their methane-laden farts, or we can all switch to renewable energy, or recycle more and better, and then we can get back to the promise of infinite growth. Unfortunately, the evidence is clear that this is simply not possible. Yes, we can make dents in our impact with such measures, and we should with all possible speed, but the way the global economy is currently programmed means such things are important–but also entirely insufficient.

So, once we discard the vain hope of being able to grow the economy infinitely and indefinitely, what are we looking at? This is where the innovation and bravery come in.

A new alliance was formed in 2017, called the Wellbeing Economy Alliance. What they are shooting for is one–or many different–economic model(s) that have, “the fundamental goal of achieving sustainable well-being with dignity and fairness for humans and the rest of Nature.” Which means they cannot just reach for socialism or any other historical model–socialism, like capitalism, relies on growth, as does communism. They have recognized that we can’t rely on past thinking; we must genuinely put our best brains forward and innovate.

We’re not talking about a bunch of random, dreamy utopians here, but real politicians who have won real elections and are exercising real power. So far, the roster of governments signing up to the Alliance includes Scotland, Costa Rica, Slovenia, and New Zealand. Other governments that are actively looking at the issue include Italy, and there are political parties emerging, like the Alternative Party in Denmark, which is also embracing the innovation challenge. These are not what are often referred to as Tier 1 countries in the international order, but neither are they so small they are irrelevant.

Scotland, for example, provides a direct line into both the U.K. and (at least for the time being) the EU. Costa Rica has long been a pioneer of innovative economic and social thinking, with impressive results: It is routinely in the top three countries in the world when measured for the well-being and happiness of their people. New Zealand is, perhaps, the most newly bold. Its prime minster has not only called growth-at-all-costs capitalism “a “blatant failure” but also has said her government would no longer accept GDP as the sole, supreme measure of progress. “The measures for us have to change,” she said in October last year. “We need to make sure we are looking at people’s ability to actually have a meaningful life, an enjoyable life, where their work is enough to survive and support their families.”

And this is where social and economic forces start to align in very interesting and potentially powerful ways. And open the door for seeing electoral strategies in an agenda based on innovations to take us beyond traditional growth-at-all-costs economics.

Consider a few facts: More than 50% of millennials say they would take a pay cut to find work that matches their values, while 90% want to use their skills for good. And these trends are on the up. Deloitte’s 7th Annual Millennial Survey of 12,000 young people, for example–both millennials and gen Z–reports record low opinions of businesses. Fewer than half now believe that businesses behave ethically, and this directly affects how loyal they feel to their employers; 43% of millennials and a whopping 61% of gen-Zers expect to stay in a job no more than two years. And all this against a backdrop of general public opinion that is also looking increasingly unkindly on the economic paradigm we have.

These are conditions that can be worked with. They show that there is a large and growing instinct out there that thinks that we need fundamental change to the way we do economics. Not tweaking around the edges, but fundamental change at the very roots of the global economy. There is no neat or reliable evidence to suggest that challenging infinite growth is at the top of peoples’ minds, or likely to be a particularly easy sell. But there is significant doubt in growth-at-all-costs capitalism, and that is an opportunity for innovation. Combine that with the new thinking coming out of places like the Wellbeing Alliance, and you can start to sense the causes and conditions may well be aligning in favor of the emergence of wholly new, post-growth economies. It cannot come soon enough.

#### Growth-oriented AI ensures extinction---degrowth solves

Pueyo ’18 [Salvador; 8 Department of Evolutionary Biology, Ecology, and Environmental Sciences, Universitat de Barcelona; Oct 1; “Growth, Degrowth, and the Challenge of Artificial Superintelligence.” Journal of Cleaner Production, vol. 197, pp. 1731–1736]

The challenges of sustainability and of superintelligence are not independent. The changing 84 fluxes of energy, matter, and information can be interpreted as different faces of a general acceleration2 85 . More directly, it is argued below that superintelligence would deeply affect 86 production technologies and also economic decisions, and could in turn be affected by the 87 socioeconomic and ecological context in which it develops. Along the lines of Pueyo (2014, p. 88 3454), this paper presents an approach that integrates these topics. It employs insights from a 89 variety of sources, such as ecological theory and several schools of economic theory. 90 The next section presents a thought experiment, in which superintelligence emerges after the 91 technical aspects of goal alignment have been resolved, and this occurs specifically in a neoliberal 92 scenario. Neoliberalism is a major force shaping current policies on a global level, which urges 93 governments to assume as their main role the creation and support of capitalist markets, and to 94 avoid interfering in their functioning (Mirowski, 2009). Neoliberal policies stand in sharp contrast 95 to degrowth views: the first are largely rationalized as a way to enhance efficiency and production 96 (Plehwe, 2009), and represent the maximum expression of capitalist values. 97 The thought experiment illustrates how superintelligence perfectly aligned with capitalist 98 markets could have very undesirable consequences for humanity and the whole biosphere. It also 99 suggests that there is little reason to expect that the wealthiest and most powerful people would be 100 exempt from these consequences, which, as argued below, gives reason for hope. Section 3 raises 101 the possibility of a broad social consensus to respond to this challenge along the lines of degrowth, 102 thus tackling major technological, environmental, and social problems simultaneously. The 103 uncertainty involved in these scenarios is vast, but, if a non-negligible probability is assigned to 104 these two futures, little room is left for either complacency or resignation. 105 106 2. Thought experiment: Superintelligence in a neoliberal scenario 107 108 Neoliberalism is creating a very special breeding ground for superintelligence, because it strives 109 to reduce the role of human agency in collective affairs. The neoliberal pioneer Friedrich Hayek 110 argued that the spontaneous order of markets was preferable over conscious plans, because markets, 111 he thought, have more capacity than humans to process information (Mirowski, 2009). Neoliberal 112 policies are actively transferring decisions to markets (Mirowski, 2009), while firms' automated 113 decision systems become an integral part of the market's information processing machinery 114 (Davenport and Harris, 2005). Neoliberal globalization is locking governments in the role of mere 115 players competing in the global market (Swank, 2016). Furthermore, automated governance is a 116 foundational tenet of neoliberal ideology (Plehwe, 2009, p. 23). 117 In the neoliberal scenario, most technological development can be expected to take place either in the context of firms or in support of firms3 118 . A number of institutionalist (Galbraith, 1985), post119 Keynesian (Lavoie, 2014; and references therein) and evolutionary (Metcalfe, 2008) economists 120 concur that, in capitalist markets, firms tend to maximize their growth rates (this principle is related 121 but not identical to the neoclassical assumption that firms maximize profits; Lavoie, 2014). Growth 122 maximization might be interpreted as expressing the goals of people in key positions, but, from an 123 evolutionary perspective, it is thought to result from a mechanism akin to natural selection 124 (Metcalfe, 2008). The first interpretation is insufficient if we accept that: (1) in big corporations, the 125 managerial bureaucracy is a coherent social-psychological system with motives and preferences of 126 its own (Gordon, 1968, p. 639; for an insider view, see Nace, 2005, pp. 1-10), (2) this system is 127 becoming techno-social-psychological with the progressive incorporation of decision-making 128 algorithms and the increasing opacity of such algorithms (Danaher, 2016), and (3) human mentality 129 and goals are partly shaped by firms themselves (Galbraith, 1985). 130 The type of AI best suited to participate in firms' decisions in this context is described in a 131 recent review in Science: AI researchers aim to construct a synthetic homo economicus, the 132 mythical perfectly rational agent of neoclassical economics. We review progress toward creating 133 this new species of machine, machina economicus (Parkes and Wellman, 2015, p. 267; a more 134 orthodox denomination would be Machina oeconomica). 135 Firm growth is thought to rely critically on retained earnings (Galbraith, 1985; Lavoie, 2014, p. 136 134-141). Therefore, economic selection can be generally expected to favor firms in which these are greater. The aggregate retained earnings4 137 RE of all firms in an economy can be expressed as: 138 RE=FE(R,L,K)-w⋅L-(i+δ)⋅K-g. (1) 139 Bold symbols represent vectors (to indicate multidimensionality). F is an aggregate production 140 function, relying on inputs of various types of natural resources R, labor L and capital K (including intelligent machines), and being affected by environmental factors5 141 E; w are wages, i are returns to 142 capital (dividends, interests) paid to households, δ is depreciation and g are the net taxes paid to 143 governments. 144 Increases in retained earnings face constraints, such as trade-offs among different parameters of 145 Eq. 1. The present thought experiment explores the consequences of economic selection in a 146 scenario in which two sets of constraints are nearly absent: sociopolitical constraints on market 147 dynamics are averted by a neoliberal institutional setting, while technical constraints are overcome 148 by asymptotically advanced technology (with extreme AI allowing for extreme technological 149 development also in other fields). The environmental and the social implications are discussed in 150 turn. Note that this scenario is not defined by some contingent choice of AIs' goals by their 151 programmers: The goals of maximizing each firm's growth and retained earnings are assumed to 152 emerge from the collective dynamics of large sets of entities subject to capitalistic rules of 153 interaction and, therefore, to economic selection.

#### Decline doesn’t cause war

Clary 15 – Christopher Clary, PhD in Political Science from MIT, M.A. in National Security Affairs, Postdoctoral Fellow, Watson Institute for International Studies, Brown University, 2015 (“Economic Stress and International Cooperation: Evidence from International Rivalries,” April 25th, Available Online via SSRN Subscription, AIvackovic)

Do economic downturns generate pressure for diversionary conflict?

Or might downturns encourage austerity and economizing behavior in foreign policy? This paper provides new evidence that economic stress is associated with conciliatory policies between strategic rivals. For states that view each other as military threats, the biggest step possible toward bilateral cooperation is to terminate the rivalry by taking political steps to manage the competition. Drawing on data from 109 distinct rival dyads since 19i9 50, 67 of which terminated, the evidence suggests rivalries were approximately twice as likely to terminate during economic downturns than they were during periods of economic normalcy. This is true controlling for all of the main alternative explanations for peaceful relations between foes (democratic status, nuclear weapons possession, capability imbalance, common enemies, and international systemic changes), as well as many other possible confounding variables. This research questions existing theories claiming that economic downturns are associated with diversionary war, and instead argues that in certain circumstances peace may result from economic troubles. I define a rivalry as the perception by national elites of two states that the other state possesses conflicting interests and presents a military threat of sufficient severity that future military conflict is likely. Rivalry termination is the transition from a state of rivalry to one where conflicts of interest are not viewed as being so severe as to provoke interstate conflict and/or where a mutual recognition of the imbalance in military capabilities makes conflict-causing bargaining failures unlikely. In other words, rivalries terminate when the elites assess that the risks of military conflict between rivals has been reduced dramatically. This definition draws on a growing quantitative literature most closely associated with the research programs of William Thompson, J. Joseph Hewitt, and James P. Klein, Gary Goertz, and Paul F. Diehl.1 My definition conforms to that of William Thompson. In work with Karen Rasler, they define rivalries as situations in which “[b]oth actors view each other as a significant political-military threat and, therefore, an enemy.”2 In other work, Thompson writing with Michael Colaresi, explains further: The presumption is that decisionmakers explicitly identify who they think are their foreign enemies. They orient their military preparations and foreign policies toward meeting their threats. They assure their constituents that they will not let their adversaries take advantage. Usually, these activities are done in public. Hence, we should be able to follow the explicit cues in decisionmaker utterances and writings, as well as in the descriptive political histories written about the foreign policies of specific countries.3 Drawing from available records and histories, Thompson and David Dreyer have generated a universe of strategic rivalries from 1494 to 2010 that serves as the basis for this project’s empirical analysis.4 This project measures rivalry termination as occurring on the last year that Thompson and Dreyer record the existence of a rivalry.

Economic crises lead to conciliatory behavior through five primary channels. (1) Economic crises lead to austerity pressures, which in turn incent leaders to search for ways to cut defense expenditures. (2) Economic crises also encourage strategic reassessment, so that leaders can argue to their peers and their publics that defense spending can be arrested without endangering the state. This can lead to threat deflation, where elites attempt to downplay the seriousness of the threat posed by a former rival. (3) If a state faces multiple threats, economic crises provoke elites to consider threat prioritization, a process that is postponed during periods of economic normalcy. (4) Economic crises increase the political and economic benefit from international economic cooperation. Leaders seek foreign aid, enhanced trade, and increased investment from abroad during periods of economic trouble. This search is made easier if tensions are reduced with historic rivals. (5) Finally, during crises, elites are more prone to select leaders who are perceived as capable of resolving economic difficulties, permitting the emergence of leaders who hold heterodox foreign policy views. Collectively, these mechanisms make it much more likely that a leader will prefer conciliatory policies compared to during periods of economic normalcy. This section reviews this causal logic in greater detail, while also providing historical examples that these mechanisms recur in practice.

### AI Impact---2NC

#### Outweighs on probability

**Turchin & Denkenberger ‘18** (Alexey Turchin & David Denkenberger 18. Turchin is a researcher at the Science for Life Extension Foundation; Denkenberger is with the Global Catastrophic Risk Institute (GCRI) @ Tennessee State University, Alliance to Feed the Earth in Disasters (ALLFED). 05/03/2018. “Classification of Global Catastrophic Risks Connected with Artificial Intelligence.” AI & SOCIETY, pp. 1–17.)

According to Yampolskiy and Spellchecker (2016), the probability and seriousness of AI failures will increase with time. We estimate that they will reach their peak between the appearance of the first self-improving AI and the moment that an AI or group of AIs reach global power, and will later diminish, as late-stage AI halting seems to be a low-probability event. AI is an extremely powerful and completely unpredictable technology, millions of times more powerful than nuclear weapons. Its existence could create multiple individual global risks, most of which we can not currently imagine. We present several dozen separate global risk scenarios connected with AI in this article, but it is likely that some of the most serious are not included. The sheer number of possible failure modes suggests that there are more to come.

#### And magnitude

Milan M. **Ćirković 19**. Future of Humanity Institute, Faculty of Philosophy, University of Oxford. 01/01/2019. “Space Colonization Remains the Only Long-Term Option for Humanity: A Reply to Torres.” Futures, vol. 105, pp. 166–173.

Perhaps a skeptic wants to believe (as a kind of anti-agent Moulder, of the X-Files’ fame) that extraterrestrial intelligence is nonexistent or vanishingly rare? To begin with, it would be strange to bet the long-term future of humanity on such a technical astrobiological issue, on which we can exert no influence whatsoever. Extraterrestrial life either exists or it does not, irrespectively of any amount of our ethical or political hand-wringing. So, lacking specific information for one or the other, we should certainly make strategies for both options. Further, the advances of astrobiology over the last quarter century offer many reasons for cautious belief in the conclusion that life and intelligence are reasonably abundant in astrophysically and astrochemically permissible ecosystems. Some of the arguments to that effect are summarized in Ćirković (2012).11 Even if, by some quirk of astrobiological evolution, humanity is the first intelligent species to arise in the Milky Way (as, for instance, per the well-known argument of Carter, 1983, 2008), following Torres’s advice and relinquishing space colonization will simply ensure that the second, third, or 275th intelligent species to evolve will indeed colonize the Galaxy instead of humans. If, on the other hand, Torres is wrong and it is possible to colonize the Galaxy in a peaceful and prosperous manner, humanity might survive on Earth in a kind of zoo or preserve, surrounded by friendly and considerate interstellar aliens – but obviously failing to realize its creative potential (which would also count as an existential catastrophe in Bostrom’s taxonomy).12 There is simply no way out of that quandary, unless one is a creationist who believes that humanity originated by Divine supernatural act and there is exactly zero probability of abiogenesis/noogenesis occurring elsewhere. In general, no naturalistic utilitarian calculus of various scenarios for the future of humanity could be complete if it does not take extraterrestrial intelligence into account.

### AI Internal link---2NC

#### Slow growth prevents unfriendly AI

Yudkowsky, 13—co-founder and research fellow at the Machine Intelligence Research Institute, celebrated Harry Potter fanfiction author (Eliezer, “Do Earths with slower economic growth have a better chance at FAI?,” <http://lesswrong.com/lw/hoz/do_earths_with_slower_economic_growth_have_a/>, dml) [(U)FAI=(Un)Friendly AI]

But suppose my main-line projection is correct and the "probability of an OK outcome" / "astronomical benefit" scenario essentially comes down to a race between Friendly AI and unFriendly AI. So far as I can tell, the most likely reason we wouldn't get Friendly AI is the total serial research depth required to develop and implement a strong-enough theory of stable self-improvement with a possible side order of failing to solve the goal transfer problem. Relative to UFAI, FAI work seems like it would be mathier and more insight-based, where UFAI can more easily cobble together lots of pieces. This means that UFAI parallelizes better than FAI. UFAI also probably benefits from brute-force computing power more than FAI. Both of these imply, so far as I can tell, that slower economic growth is good news for FAI; it lengthens the deadline to UFAI and gives us more time to get the job done. I have sometimes thought half-jokingly and half-anthropically that I ought to try to find investment scenarios based on a continued Great Stagnation and an indefinite Great Recession where the whole developed world slowly goes the way of Spain, because these scenarios would account for a majority of surviving Everett branches. Roughly, it seems to me like higher economic growth speeds up time and this is not a good thing. I wish I had more time, not less, in which to work on FAI; I would prefer worlds in which this research can proceed at a relatively less frenzied pace and still succeed, worlds in which the default timelines to UFAI terminate in 2055 instead of 2035.

#### Uniqueness goes neg---we haven’t built UFAI yet---slowing growth is the best way to keep it that way

Nordhaus, 15—Sterling Professor of Economics; Cowles Foundation, Yale University (William, “Are We Approaching an Economic Singularity? Information Technology and the Future of Economic Growth,” Cowles Foundation Discussion Paper No. 2021, dml)

f. Competition among the superintelligent If superintelligent agents develop, we must contemplate the prospect of competition among rival powers. The parallel here is to the game-theoretic dynamics of weaponry. Even though the innovators (of bows and arrows, machine guns, tanks, nuclear weapons, and drones) had an initial advantage over their adversaries, their advantage was temporary. Even the most closely held technological secrets diffuse slowly around the world. We must therefore assume that those who develop the engines of superintelligence will eventually find they are soon shadowed by their military, commercial, and political adversaries. Moreover, to the list of adversaries will be added the superintelligent machines themselves. We might take comfort in Asimov’s Three Laws of Robotics, of which the First Law is, “A robot may not injure a human being or, through inaction, allow a human being to come to harm.” But to take refuge here would surely be super-naïve. It would only take one unethical designer to launch a superintelligent agent who did not incorporate the Laws of Robotics. This would probably launch an arms race among rival superintelligent powers. So the point here is that the approaching Singularity is not one of unambiguous economic and social improvement. This was appreciated by nuclear-weapons developer John von Neumann (1955): Useful and harmful techniques lie everywhere so close together that it is never possible to separate the lions from the lambs. This is known to all who have so laboriously tried to separate secret, classified science or technology (military) from the open kind; success is never more nor intended to be more than transient, lasting perhaps half a decade. Similarly, a separation into useful and harmful subjects in any technological sphere would probably diffuse into nothing in a decade. XI. Concluding Comments on Singularity So the conclusion as of today is that “the Singularity is not near.” This conclusion is based on several tests that place the theory of the Singularity within the context of economic growth theory. Much of the computer science literature on the Singularity examines the growth in specific sectors or processes (such as flops or storage), but the economic perspective insists that the growth must be weighted by the economic valuation of the good or service. The major insight of economics is to emphasize the heterogeneity of both inputs and outputs of the economic system. It is surely true that technological change in the production of raw computation has been phenomenal over the last century. We can process information at a speed that is millions of billions times faster and cheaper than was possible for the fastest lightning calculators of the nineteenth century. Suppose that trend continues indefinitely, including the ability to devise ever more ingenious software and artificial intelligence (AI). For increasing capabilities of computers to lead to the Singularity would require that AI could encompass all human activities, not just add numbers, solve equations, play chess, and interpret speech; but also lay hands on patients, read bedtime stories to children, and select presidential candidates. Whereas computerized AI might do many routine tasks, the non-routine tasks are less easily programmed, and they evolve over time in response to the economic environment, including the environment of artificial intelligence itself. Particularly if we view the world with potential superintelligence as a competition between humans and machines, then we definitely would need a team of humans to consider how to protect humans from machines. We routinely spend 5% of output on defense, and this might rise to a much larger number when faced with a more potential enemies like superintelligent machines. So one occupation at least would survive into the Era of Singularity. Whether other sectors and tasks would be immune to the rise of superintelligence is an open question. The empirical question is the degree of substitutability between information and human efforts. Given the complexity of both humans and jobs, it is unlikely that the question can be decided a priori. The analysis above indicates that information and computers will come to dominate the economy only if the informational capital takes a rising share of inputs. This requires that the expenditure shares or input cost shares of information rise over time, which in turn requires that the volume of inputs rises more rapidly than the relative prices fall. We can call these the “substitution tests” to be concise. There are six tests on the supply side. The conclusions from the empirical tests proposed here is that the substitution tests fail or are ambiguous for four of six tests and succeed barely for two of the six tests. However, the growth trajectories of the variables which pass the test (the share of capital in total income and the share of informational capital in total capital) are extremely slow. Projecting the trends of the last decade or more, it would be in the order of a century before these variables would reach the level associated with the growth Singularity. The conclusion is therefore that the economic Singularity is not near.

### AT: No AI---2NC

#### Overwhelming consensus of AI experts is that AI is inevitable.

Allan **Dafoe &** Stuart **Russell 16**. Dafoe is an assistant professor of political science at Yale University; Russell is a professor of computer science at the University of California, Berkeley. 11-02-16. “Yes, We Are Worried About the Existential Risk of Artificial Intelligence.” MIT Technology Review. https://www.technologyreview.com/s/602776/yes-we-are-worried-about-the-existential-risk-of-artificial-intelligence/.

Oren Etzioni, a well-known AI researcher, complains about news coverage of potential long-term risks arising from future success in AI research (see “No, Experts Don't Think Superintelligent AI is a Threat to Humanity”). After pointing the finger squarely at Oxford philosopher Nick Bostrom and his recent book, Superintelligence, Etzioni complains that Bostrom’s “main source of data on the advent of human-level intelligence” consists of surveys on the opinions of AI researchers. He then surveys the opinions of AI researchers, arguing that his results refute Bostrom’s. It’s important to understand that Etzioni is not even addressing the reason Superintelligence has had the impact he decries: its clear explanation of why superintelligent AI may have arbitrarily negative consequences and why it’s important to begin addressing the issue well in advance. Bostrom does not base his case on predictions that superhuman AI systems are imminent. He writes, “It is no part of the argument in this book that we are on the threshold of a big breakthrough in artificial intelligence, or that we can predict with any precision when such a development might occur.” Thus, in our view, Etzioni’s article distracts the reader from the core argument of the book and directs an ad hominem attack against Bostrom under the pretext of disputing his survey results. We feel it is necessary to correct the record. One of us (Russell) even contributed to Etzioni’s survey, only to see his response being completely misconstrued. In fact, as our detailed analysis shows, Etzioni’s survey results are entirely consistent with the ones Bostrom cites. How, then, does Etzioni reach his novel conclusion? By designing a survey instrument that is inferior to Bostrom’s and then misinterpreting the results. The subtitle of the article reads, “If you ask the people who should really know, you’ll find that few believe AI is a threat to humanity.” So the reader is led to believe that Etzioni asked this question of the people who should really know, while Bostrom did not. In fact, the opposite is true: Bostrom did ask people who should really know, but Etzioni did not ask anyone at all. Bostrom surveyed the top 100 most cited AI researchers. More than half of the respondents said they believe there is a substantial (at least 15 percent) chance that the effect of human-level machine intelligence on humanity will be “on balance bad” or “extremely bad (existential catastrophe).” Etzioni’s survey, unlike Bostrom’s, did not ask any questions about a threat to humanity. Instead, he simply asks one question about when we will achieve superintelligence. As Bostrom’s data would have already predicted, somewhat more than half (67.5 percent) of Etzioni’s respondents plumped for “more than 25 years” to achieve superintelligence—after all, more than half of Bostrom’s respondents gave dates beyond 25 years for a mere 50 percent probability of achieving mere human-level intelligence. One of us (Russell) responded to Etzioni’s survey with “more than 25 years,” and Bostrom himself writes, of his own surveys, “My own view is that the median numbers reported in the expert survey do not have enough probability mass on later arrival dates.” Now, having designed a survey where respondents could be expected to choose “more than 25 years,” Etzioni springs his trap: he asserts that 25 years is “beyond the foreseeable horizon” and thereby deduces that neither Russell nor indeed Bostrom himself believes that superintelligent AI is a threat to humanity. This will come as a surprise to Russell and Bostrom, and presumably to many other respondents in the survey. (Indeed, Etzioni’s headline could just as easily have been “75 percent of experts think superintelligent AI is inevitable.”) Should we ignore catastrophic risks simply because most experts think they are more than 25 years away? By Etzioni’s logic, we should also ignore the catastrophic risks of climate change and castigate those who bring them up. Contrary to the views of Etzioni and some others in the AI community, pointing to long-term risks from AI is not equivalent to claiming that superintelligent AI and its accompanying risks are “imminent.” The list of those who have pointed to the risks includes such luminaries as Alan Turing, Norbert Wiener, I.J. Good, and Marvin Minsky. Even Oren Etzioni has acknowledged these challenges. To our knowledge, none of these ever asserted that superintelligent AI was imminent. Nor, as noted above, did Bostrom in Superintelligence.

#### The transition to superintelligence is rapid, opaque, and would cause universal extinction

James Daniel **Miller 18**. Based at Smith College, South Deerfield, Massachusetts. 10/11/2018. “When Two Existential Risks Are Better than One.” Foresight. Crossref, doi:10.1108/FS-04-2018-0038.

2. The dangers of unfriendly powerful artificial general intelligence Unlike with whatever wetware runs the human brain, it would be relatively easy to make changes to a PAGI’s software. PAGI could even make changes to itself. Such selfmodification could possibly allow PAGI to undergo an intelligence explosion where it figures out how to improve its own intelligence, then, as it gets smarter, it figures out new ways to improve its intelligence. It has been theorized that through recursive self-improvement a PAGI could go from being a bit smarter than humans to becoming a computer superintelligence in a matter of days (Good, 1965; Yudkowsky, 2008). If our understanding of the laws of physics is correct, the universe contains a limited amount of free energy, and this free energy is necessary to do any kind of work and most types of computing. Consequently, it has been theorized that most types of computer superintelligences would have an instrumental goal of gathering as much free energy as possible to further whatever ultimate goals they had (Omohundro, 2008). Humanity’s continued existence uses free energy. Consequently, if a PAGI did not have promoting human welfare as a goal, it would likely see humanity’s continuing existence as rival to its terminal values. A PAGI that wanted to maximize its understanding of, say, chess would further this end by exterminating mankind and using the atoms in our bodies to make chess computing hardware. A PAGI that wanted to maximize the number of paperclips in the universe would likewise kill us, not out of malice, but to align the atoms in our bodies with its objective. The term “paperclip maximizer” has come to mean a PAGI that seeks to use all the resources it can get for an objective that most humans would not consider worthwhile (Arbital Contributors, 2017). A PAGI that was smarter than humans, but not yet smart enough to take over the world, would have an incentive to hide its abilities and intentions from us if it predicted that we would turn the PAGI off if it scared us. Consequently, the PAGI might appear friendly weak, and unambitious right until it launches a surprise devastating attack on us, by taking what has been called a “treacherous turn” (Bostrom, 2014, pp. 116-119).

### AT: Adaptation—2NC

#### A confluence of crises will overwhelm our ability to adapt

Wallace-Wells 17 - climate writer @ nymag (David, <http://nymag.com/intelligencer/2017/07/climate-change-earth-too-hot-for-humans.html>, EM)

I. ‘Doomsday’ Peering beyond scientific reticence. It is, I promise, worse than you think. If your anxiety about global warming is dominated by fears of sea-level rise, you are barely scratching the surface of what terrors are possible, even within the lifetime of a teenager today. And yet the swelling seas — and the cities they will drown — have so dominated the picture of global warming, and so overwhelmed our capacity for climate panic, that they have occluded our perception of other threats, many much closer at hand. Rising oceans are bad, in fact very bad; but fleeing the coastline will not be enough. Indeed, absent a significant adjustment to how billions of humans conduct their lives, parts of the Earth will likely become close to uninhabitable, and other parts horrifically inhospitable, as soon as the end of this century. Even when we train our eyes on climate change, we are unable to comprehend its scope. This past winter, a string of days 60 and 70 degrees warmer than normal baked the North Pole, melting the permafrost that encased Norway’s Svalbard seed vault — a global food bank nicknamed “Doomsday,” designed to ensure that our agriculture survives any catastrophe, and which appeared to have been flooded by climate change less than ten years after being built. The Doomsday vault is fine, for now: The structure has been secured and the seeds are safe. But treating the episode as a parable of impending flooding missed the more important news. Until recently, permafrost was not a major concern of climate scientists, because, as the name suggests, it was soil that stayed permanently frozen. But Arctic permafrost contains 1.8 trillion tons of carbon, more than twice as much as is currently suspended in the Earth’s atmosphere. When it thaws and is released, that carbon may evaporate as methane, which is 34 times as powerful a greenhouse-gas warming blanket as carbon dioxide when judged on the timescale of a century; when judged on the timescale of two decades, it is 86 times as powerful. In other words, we have, trapped in Arctic permafrost, twice as much carbon as is currently wrecking the atmosphere of the planet, all of it scheduled to be released at a date that keeps getting moved up, partially in the form of a gas that multiplies its warming power 86 times over. Maybe you know that already — there are alarming stories in the news every day, like those, last month, that seemed to suggest satellite data [showed](https://www.carbonbrief.org/major-correction-to-satellite-data-shows-140-faster-warming-since-1998) the globe warming since 1998 more than twice as fast as scientists had thought (in fact, the underlying story was considerably less alarming than the headlines). Or the news from Antarctica this past May, when a [crack](http://www.newsweek.com/antarctica-ice-shelf-larsen-c-crack-grown-618676) in an ice shelf grew 11 miles in six days, then kept going; the break now has just three miles to go — by the time you read this, [it may already have met the open water](http://nymag.com/daily/intelligencer/2017/07/trillion-ton-iceberg-breaks-off-antarctic-ice-shelf.html), where it will drop into the sea one of the biggest icebergs ever, a process known poetically as “calving.” But no matter how well-informed you are, you are surely not alarmed enough. Over the past decades, our culture has gone apocalyptic with zombie movies and [Mad Max dystopias](http://www.vulture.com/2016/07/the-present-worse-than-fictional-dystopias.html), perhaps the collective result of displaced climate anxiety, and yet when it comes to contemplating real-world warming dangers, we suffer from an incredible failure of imagination. The reasons for that are many: the timid language of scientific probabilities, which the climatologist James Hansen once called “scientific reticence” in a paper chastising scientists for editing their own observations so conscientiously that they failed to communicate how dire the threat really was; the fact that the country is dominated by a group of technocrats who believe any problem can be solved and an opposing culture that doesn’t even see warming as a problem worth addressing; the way that climate denialism has made scientists even more cautious in offering speculative warnings; the simple speed of change and, also, its slowness, such that we are only seeing effects now of warming from decades past; our uncertainty about uncertainty, which the climate writer Naomi Oreskes in particular has suggested stops us from preparing as though anything worse than a median outcome were even possible; the way we assume climate change will hit hardest elsewhere, not everywhere; the smallness (two degrees) and largeness (1.8 trillion tons) and abstractness (400 parts per million) of the numbers; the discomfort of considering a problem that is very difficult, if not impossible, to solve; the altogether incomprehensible scale of that problem, which amounts to the prospect of our own annihilation; simple fear. But aversion arising from fear is a form of denial, too. In between scientific reticence and science fiction is science itself. This article is the result of dozens of interviews and exchanges with climatologists and researchers in related fields and reflects hundreds of scientific papers on the subject of climate change. What follows is not a series of predictions of what will happen — that will be determined in large part by the much-less-certain science of human response. Instead, it is a portrait of our best understanding of where the planet is heading absent aggressive action. It is unlikely that all of these warming scenarios will be fully realized, largely because the devastation along the way will shake our complacency. But those scenarios, and not the present climate, are the baseline. In fact, they are our schedule. The present tense of climate change — the destruction we’ve already baked into our future — is horrifying enough. Most people talk as if Miami and Bangladesh still have a chance of surviving; most of the scientists I spoke with assume we’ll lose them within the century, even if we stop burning fossil fuel in the next decade. Two degrees of warming used to be considered the threshold of catastrophe: tens of millions of climate refugees unleashed upon an unprepared world. Now two degrees is our goal, per the Paris climate accords, and experts give us only slim odds of hitting it. The U.N. Intergovernmental Panel on Climate Change issues serial reports, often called the “gold standard” of climate research; the most recent one projects us to hit four degrees of warming by the beginning of the next century, should we stay the present course. But that’s just a median projection. The upper end of the probability curve runs as high as eight degrees — and the authors still haven’t figured out how to deal with that permafrost melt. The IPCC reports also don’t fully account for the albedo effect (less ice means less reflected and more absorbed sunlight, hence more warming); more cloud cover (which traps heat); or the dieback of forests and other flora (which extract carbon from the atmosphere). Each of these promises to accelerate warming, and the history of the planet shows that temperature can shift as much as five degrees Celsius within thirteen years. The last time the planet was even four degrees warmer, Peter Brannen points out in [The Ends of the World](https://www.amazon.com/Ends-World-Apocalypses-Understand-Extinctions/dp/0062364804?ascsubtag=%5b%5din%5bp%5dcj4u5jzvo0000osy64knayino%5bi%5dAbwfZQ%5bz%5dm%5bd%5dD%5br%5dgoogle.com), his new history of the planet’s major extinction events, the oceans were hundreds of feet higher.\* The Earth has experienced five mass extinctions before the one we are living through now, each so complete a slate-wiping of the evolutionary record it functioned as a resetting of the planetary clock, and many climate scientists will tell you they are the best analog for the ecological future we are diving headlong into. Unless you are a teenager, you probably read in your high-school textbooks that these extinctions were the result of asteroids. In fact, all but the one that killed the dinosaurs were caused by climate change produced by greenhouse gas. The most notorious was 252 million years ago; it began when carbon warmed the planet by five degrees, accelerated when that warming triggered the release of methane in the Arctic, and ended with 97 percent of all life on Earth dead. We are currently adding carbon to the atmosphere at a considerably faster rate; by most estimates, at least ten times faster. The rate is accelerating. This is what Stephen Hawking had in mind when [he said](http://www.telegraph.co.uk/science/2017/05/02/tomorrows-world-returns-bbc-startling-warning-stephen-hawking/), this spring, that the species needs to colonize other planets in the next century to survive, and what drove Elon Musk, last month, to [unveil](http://www.newsweek.com/elon-musk-mars-spacex-martian-city-625994) his plans to build a Mars habitat in 40 to 100 years. These are nonspecialists, of course, and probably as inclined to irrational panic as you or I. But the many sober-minded scientists I interviewed over the past several months — the most credentialed and tenured in the field, few of them inclined to alarmism and many advisers to the IPCC who nevertheless criticize its conservatism — have quietly reached an apocalyptic conclusion, too: No plausible program of emissions reductions alone can prevent climate disaster. Over the past few decades, the term [“Anthropocene” has climbed out of academic discourse and into the popular imagination](http://nymag.com/scienceofus/2015/06/anthropocene-debate.html) — a name given to the geologic era we live in now, and a way to signal that it is a new era, defined on the wall chart of deep history by human intervention. One problem with the term is that it implies a conquest of nature (and even echoes the biblical “dominion”). And however sanguine you might be about the proposition that we have already ravaged the natural world, which we surely have, it is another thing entirely to consider the possibility that we have only provoked it, engineering first in ignorance and then in denial a climate system that will now go to war with us for many centuries, perhaps until it destroys us. That is what Wallace Smith Broecker, the avuncular oceanographer who coined the term “global warming,” means when he calls the planet an “angry beast.” You could also go with “war machine.” Each day we arm it more. II. Heat Death The bahraining of New York. Humans, like all mammals, are heat engines; surviving means having to continually cool off, like panting dogs. For that, the temperature needs to be low enough for the air to act as a kind of refrigerant, drawing heat off the skin so the engine can keep pumping. At seven degrees of warming, that would become impossible for large portions of the planet’s equatorial band, and especially the tropics, where humidity adds to the problem; in the jungles of Costa Rica, for instance, where humidity routinely tops 90 percent, simply moving around outside when it’s over 105 degrees Fahrenheit would be lethal. And the effect would be fast: Within a few hours, a human body would be cooked to death from both inside and out. Climate-change skeptics point out that the planet has warmed and cooled many times before, but the climate window that has allowed for human life is very narrow, even by the standards of planetary history. At 11 or 12 degrees of warming, more than half the world’s population, as distributed today, would die of direct heat. Things almost certainly won’t get that hot this century, though models of unabated emissions do bring us that far eventually. This century, and especially in the tropics, the pain points will pinch much more quickly even than an increase of seven degrees. The key factor is something called wet-bulb temperature, which is a term of measurement as home-laboratory-kit as it sounds: the heat registered on a thermometer wrapped in a damp sock as it’s swung around in the air (since the moisture evaporates from a sock more quickly in dry air, this single number reflects both heat and humidity). At present, most regions reach a wet-bulb maximum of 26 or 27 degrees Celsius; the true red line for habitability is 35 degrees. What is called heat stress comes much sooner. Actually, we’re about there already. Since 1980, the planet has experienced a 50-fold increase in the number of places experiencing dangerous or extreme heat; a bigger increase is to come. The five warmest summers in Europe since 1500 have all occurred since 2002, and soon, the IPCC warns, simply being outdoors that time of year will be unhealthy for much of the globe. Even if we meet the Paris goals of two degrees warming, cities like Karachi and Kolkata will become close to uninhabitable, annually encountering deadly heat waves like those that crippled them in 2015. At four degrees, the deadly European heat wave of 2003, which killed as many as 2,000 people a day, will be a normal summer. At six, according to an assessment focused only on effects within the U.S. from the National Oceanic and Atmospheric Administration, summer labor of any kind would become impossible in the lower Mississippi Valley, and everybody in the country east of the Rockies would be under more heat stress than anyone, anywhere, in the world today. As Joseph Romm has put it in his authoritative primer [Climate Change: What Everyone Needs to Know](https://www.amazon.com/Climate-Change-Everyone-Needs-Know%C2%AE/dp/0190250178?ascsubtag=%5b%5din%5bp%5dcj4u5jzvo0000osy64knayino%5bi%5dkpnStB%5bz%5dm%5bd%5dD%5br%5dgoogle.com), heat stress in New York City would exceed that of present-day Bahrain, one of the planet’s hottest spots, and the temperature in Bahrain “would induce hyperthermia in even sleeping humans.” The high-end IPCC estimate, remember, is two degrees warmer still. By the end of the century, the World Bank has estimated, the coolest months in tropical South America, Africa, and the Pacific are likely to be warmer than the warmest months at the end of the 20th century. Air-conditioning can help but will ultimately only add to the carbon problem; plus, the climate-controlled malls of the Arab emirates aside, it is not remotely plausible to wholesale air-condition all the hottest parts of the world, many of them also the poorest. And indeed, the crisis will be most dramatic across the Middle East and Persian Gulf, where in 2015 the heat index registered temperatures as high as 163 degrees Fahrenheit. As soon as several decades from now, the hajj will become physically impossible for the 2 million Muslims who make the pilgrimage each year. It is not just the hajj, and it is not just Mecca; heat is already killing us. In the sugarcane region of El Salvador, as much as one-fifth of the population has chronic kidney disease, including over a quarter of the men, the presumed result of dehydration from working the fields they were able to comfortably harvest as recently as two decades ago. With dialysis, which is expensive, those with kidney failure can expect to live five years; without it, life expectancy is in the weeks. Of course, heat stress promises to pummel us in places other than our kidneys, too. As I type that sentence, in the California desert in mid-June, it is 121 degrees outside my door. It is not a record high. III. The End of Food Praying for cornfields in the tundra. Climates differ and plants vary, but the basic rule for staple cereal crops grown at optimal temperature is that for every degree of warming, yields decline by 10 percent. Some estimates run as high as 15 or even 17 percent. Which means that if the planet is five degrees warmer at the end of the century, we may have as many as 50 percent more people to feed and 50 percent less grain to give them. And proteins are worse: It takes 16 calories of grain to produce just a single calorie of hamburger meat, butchered from a cow that spent its life polluting the climate with methane farts. Pollyannaish plant physiologists will point out that the cereal-crop math applies only to those regions already at peak growing temperature, and they are right — theoretically, a warmer climate will make it easier to grow corn in Greenland. But as the pathbreaking work by Rosamond Naylor and David Battisti has shown, the tropics are already too hot to efficiently grow grain, and those places where grain is produced today are already at optimal growing temperature — which means even a small warming will push them down the slope of declining productivity. And you can’t easily move croplands north a few hundred miles, because yields in places like remote Canada and Russia are limited by the quality of soil there; it takes many centuries for the planet to produce optimally fertile dirt. Drought might be an even bigger problem than heat, with some of the world’s most arable land turning quickly to desert. Precipitation is notoriously hard to model, yet predictions for later this century are basically unanimous: unprecedented droughts nearly everywhere food is today produced. By 2080, without dramatic reductions in emissions, southern Europe will be in permanent extreme drought, much worse than the American dust bowl ever was. The same will be true in Iraq and Syria and much of the rest of the Middle East; some of the most densely populated parts of Australia, Africa, and South America; and the breadbasket regions of China. None of these places, which today supply much of the world’s food, will be reliable sources of any. As for the original dust bowl: The droughts in the American plains and Southwest would not just be worse than in the 1930s, a 2015 NASA study [predicted](https://www.nasa.gov/press/2015/february/nasa-study-finds-carbon-emissions-could-dramatically-increase-risk-of-us), but worse than any droughts in a thousand years — and that includes those that struck between 1100 and 1300, which “dried up all the rivers East of the Sierra Nevada mountains” and may have been responsible for the death of the Anasazi civilization. Remember, we do not live in a world without hunger as it is. Far from it: Most estimates put the number of undernourished at 800 million globally. In case you haven’t heard, this spring has already brought an unprecedented quadruple famine to Africa and the Middle East; the U.N. has warned that separate starvation events in Somalia, South Sudan, Nigeria, and Yemen could kill 20 million this year alone. IV. Climate Plagues What happens when the bubonic ice melts? Rock, in the right spot, is a record of planetary history, eras as long as millions of years flattened by the forces of geological time into strata with amplitudes of just inches, or just an inch, or even less. Ice works that way, too, as a climate ledger, but it is also frozen history, some of which can be reanimated when unfrozen. There are now, trapped in Arctic ice, diseases that have not circulated in the air for millions of years — in some cases, since before humans were around to encounter them. Which means our immune systems would have no idea how to fight back when those prehistoric plagues emerge from the ice. The Arctic also stores terrifying bugs from more recent times. In Alaska, already, researchers have discovered remnants of the 1918 flu that infected as many as 500 million and killed as many as 100 million — about 5 percent of the world’s population and almost six times as many as had died in the world war for which the pandemic served as a kind of gruesome capstone. As the BBC [reported](http://www.bbc.com/earth/story/20170504-there-are-diseases-hidden-in-ice-and-they-are-waking-up) in May, scientists suspect smallpox and the bubonic plague are trapped in Siberian ice, too — an abridged history of devastating human sickness, left out like egg salad in the Arctic sun. Experts caution that many of these organisms won’t actually survive the thaw and point to the fastidious lab conditions under which they have already reanimated several of them — the 32,000-year-old “extremophile” bacteria revived in 2005, an 8 million-year-old bug brought back to life in 2007, the 3.5 million–year–old one a Russian scientist [self-injected](https://www.youtube.com/watch?v=lv0_Cu0FcPA) just out of curiosity — to suggest that those are necessary conditions for the return of such ancient plagues. But already last year, a boy was killed and 20 others infected by anthrax released when retreating permafrost exposed the frozen carcass of a reindeer killed by the bacteria at least 75 years earlier; 2,000 present-day reindeer were infected, too, carrying and spreading the disease beyond the tundra. What concerns epidemiologists more than ancient diseases are existing scourges relocated, rewired, or even re-evolved by warming. The first effect is geographical. Before the early-modern period, when adventuring sailboats accelerated the mixing of peoples and their bugs, human provinciality was a guard against pandemic. Today, even with globalization and the enormous intermingling of human populations, our ecosystems are mostly stable, and this functions as another limit, but global warming will scramble those ecosystems and help disease trespass those limits as surely as Cortés did. You don’t worry much about dengue or malaria if you are living in Maine or France. But as the tropics creep northward and mosquitoes migrate with them, you will. You didn’t much worry about Zika a couple of years ago, either. As it happens, [Zika may also be a good model](http://nymag.com/scienceofus/2016/02/zika-virus-gmo-mosquitoes.html) of the second worrying effect — disease mutation. One reason you hadn’t heard about Zika until recently is that it had been trapped in Uganda; another is that it did not, until recently, appear to cause birth defects. Scientists still don’t entirely understand what happened, or what they missed. But there are things we do know for sure about how climate affects some diseases: Malaria, for instance, thrives in hotter regions not just because the mosquitoes that carry it do, too, but because for every degree increase in temperature, the parasite reproduces ten times faster. Which is one reason that the World Bank estimates that by 2050, 5.2 billion people will be reckoning with it. V. Unbreathable Air A rolling death smog that suffocates millions. Our lungs need oxygen, but that is only a fraction of what we breathe. The fraction of carbon dioxide is growing: It just crossed 400 parts per million, and high-end estimates extrapolating from current trends suggest it will hit 1,000 ppm by 2100. At that concentration, compared to the air we breathe now, human cognitive ability declines by 21 percent. Other stuff in the hotter air is even scarier, with small increases in pollution capable of shortening life spans by ten years. The warmer the planet gets, the more ozone forms, and by mid-century, Americans will likely suffer a 70 percent increase in unhealthy ozone smog, the National Center for Atmospheric Research has projected. By 2090, as many as 2 billion people globally will be breathing air above the WHO “safe” level; one paper last month showed that, among other effects, a pregnant mother’s exposure to ozone raises the child’s risk of autism (as much as tenfold, combined with other environmental factors). Which does make you think again about the autism epidemic in West Hollywood. Already, more than 10,000 people die each day from the small particles emitted from fossil-fuel burning; each year, 339,000 people die from wildfire smoke, in part because climate change has extended forest-fire season (in the U.S., it’s increased by 78 days since 1970). By 2050, according to the [U.S. Forest Service](https://www.usda.gov/oce/climate_change/effects_2012/FS_Climate1114%20opt.pdf), wildfires will be twice as destructive as they are today; in some places, the area burned could grow fivefold. What worries people even more is the effect that would have on emissions, especially when the fires ravage forests arising out of peat. Peatland fires in Indonesia in 1997, for instance, added to the global CO2 release by up to 40 percent, and more burning only means more warming only means more burning. There is also the terrifying possibility that rain forests like the Amazon, which in 2010 suffered its second “hundred-year drought” in the space of five years, could dry out enough to become vulnerable to these kinds of devastating, rolling forest fires — which would not only expel enormous amounts of carbon into the atmosphere but also shrink the size of the forest. That is especially bad because the Amazon alone provides 20 percent of our oxygen. Then there are the more familiar forms of pollution. In 2013, melting Arctic ice remodeled Asian weather patterns, depriving industrial China of the natural ventilation systems it had come to depend on, which blanketed much of the country’s north in an unbreathable smog. Literally unbreathable. A metric called the Air Quality Index categorizes the risks and tops out at the 301-to-500 range, warning of “serious aggravation of heart or lung disease and premature mortality in persons with cardiopulmonary disease and the elderly” and, for all others, “serious risk of respiratory effects”; at that level, “everyone should avoid all outdoor exertion.” The Chinese “airpocalypse” of 2013 peaked at what would have been an Air Quality Index of over 800. That year, smog was responsible for a third of all deaths in the country. VI. Perpetual War The violence baked into heat. Climatologists are very careful when talking about Syria. They want you to know that while climate change did produce a drought that contributed to civil war, it is not exactly fair to saythat the conflict is the result of warming; next door, for instance, Lebanon suffered the same crop failures. But researchers like Marshall Burke and Solomon Hsiang have managed to quantify some of the non-obvious relationships between temperature and violence: For every half-degree of warming, they say, societies will see between a 10 and 20 percent increase in the likelihood of armed conflict. In climate science, nothing is simple, but the arithmetic is harrowing: A planet five degrees warmer would have at least half again as many wars as we do today. Overall, social conflict could more than double this century. This is one reason that, as nearly every climate scientist I spoke to pointed out, the U.S. military is obsessed with climate change: The drowning of all American Navy bases by sea-level rise is trouble enough, but being the world’s policeman is quite a bit harder when the crime rate doubles. Of course, it’s not just Syria where climate has contributed to conflict. Some speculate that the elevated level of strife across the Middle East over the past generation reflects the pressures of global warming — a hypothesis all the more cruel considering that warming began accelerating when the industrialized world extracted and then burned the region’s oil. What accounts for the relationship between climate and conflict? Some of it comes down to agriculture and economics; a lot has to do with forced migration, already at a record high, with at least 65 million displaced people wandering the planet right now. But there is also the simple fact of individual irritability. Heat increases municipal crime rates, and swearing on social media, and the likelihood that a major-league pitcher, coming to the mound after his teammate has been hit by a pitch, will hit an opposing batter in retaliation. And the arrival of air-conditioning in the developed world, in the middle of the past century, did little to solve the problem of the summer crime wave. VII. Permanent Economic Collapse Dismal capitalism in a half-poorer world. The murmuring mantra of global neoliberalism, which prevailed between the end of the Cold War and the onset of the Great Recession, is that economic growth would save us from anything and everything. But in the aftermath of the 2008 crash, a growing number of historians studying what they call “fossil capitalism” have begun to suggest that the entire history of swift economic growth, which began somewhat suddenly in the 18th century, is not the result of innovation or trade or the dynamics of global capitalism but simply our discovery of fossil fuels and all their raw power — a onetime injection of new “value” into a system that had previously been characterized by global subsistence living. Before fossil fuels, nobody lived better than their parents or grandparents or ancestors from 500 years before, except in the immediate aftermath of a great plague like the Black Death, which allowed the lucky survivors to gobble up the resources liberated by mass graves. After we’ve burned all the fossil fuels, these scholars suggest, perhaps we will return to a “steady state” global economy. Of course, that onetime injection has a devastating long-term cost: climate change. The most exciting research on the economics of warming has also come from Hsiang and his colleagues, who are not historians of fossil capitalism but who offer some very bleak analysis of their own: Every degree Celsius of warming costs, on average, 1.2 percent of GDP (an enormous number, considering we count growth in the low single digits as “strong”). This is the sterling work in the field, and their median projection is for a 23 percent loss in per capita earning globally by the end of this century (resulting from changes in agriculture, crime, storms, energy, mortality, and labor). Tracing the shape of the probability curve is even scarier: There is a 12 percent chance that climate change will reduce global output by more than 50 percent by 2100, they say, and a 51 percent chance that it lowers per capita GDP by 20 percent or more by then, unless emissions decline. By comparison, the Great Recession lowered global GDP by about 6 percent, in a onetime shock; Hsiang and his colleagues estimate a one-in-eight chance of an ongoing and irreversible effect by the end of the century that is eight times worse. The scale of that economic devastation is hard to comprehend, but you can start by imagining what the world would look like today with an economy half as big, which would produce only half as much value, generating only half as much to offer the workers of the world. It makes the grounding of flights out of heat-stricken Phoenix last month seem like pathetically small economic potatoes. And, among other things, it makes the idea of postponing government action on reducing emissions and relying solely on growth and technology to solve the problem an absurd business calculation. of ice. VIII. Poisoned Oceans Sulfide burps off the skeleton coast. That the sea will become a killer is a given. Barring a radical reduction of emissions, we will see at least four feet of sea-level rise and possibly ten by the end of the century. A third of the world’s major cities are on the coast, not to mention its power plants, ports, navy bases, farmlands, fisheries, river deltas, marshlands, and rice-paddy empires, and even those above ten feet will flood much more easily, and much more regularly, if the water gets that high. At least 600 million people live within ten meters of sea level today. But the drowning of those homelands is just the start. At present, more than a third of the world’s carbon is sucked up by the oceans — thank God, or else we’d have that much more warming already. But the result is what’s called “ocean acidification,” which, on its own, may add a half a degree to warming this century. It is also already burning through the planet’s water basins — you may remember these as the place where life arose in the first place. You have probably heard of “coral bleaching” — that is, coral dying — which is very bad news, because reefs support as much as a quarter of all marine life and supply food for half a billion people. Ocean acidification will fry fish populations directly, too, though scientists aren’t yet sure how to predict the effects on the stuff we haul out of the ocean to eat; they do know that in acid waters, oysters and mussels will struggle to grow their shells, and that when the pH of human blood drops as much as the oceans’ pH has over the past generation, it induces seizures, comas, and sudden death. That isn’t all that ocean acidification can do. Carbon absorption can initiate a feedback loop in which underoxygenated waters breed different kinds of microbes that turn the water still more “anoxic,” first in deep ocean “dead zones,” then gradually up toward the surface. There, the small fish die out, unable to breathe, which means oxygen-eating bacteria thrive, and the feedback loop doubles back. This process, in which dead zones grow like cancers, choking off marine life and wiping out fisheries, is already quite advanced in parts of the Gulf of Mexico and just off Namibia, where hydrogen sulfide is bubbling out of the sea along a thousand-mile stretch of land known as the “Skeleton Coast.” The name originally referred to the detritus of the whaling industry, but today it’s more apt than ever. Hydrogen sulfide is so toxic that evolution has trained us to recognize the tiniest, safest traces of it, which is why our noses are so exquisitely skilled at registering flatulence. Hydrogen sulfide is also the thing that finally did us in that time 97 percent of all life on Earth died, once all the feedback loops had been triggered and the circulating jet streams of a warmed ocean ground to a halt — it’s the planet’s preferred gas for a natural holocaust. Gradually, the ocean’s dead zones spread, killing off marine species that had dominated the oceans for hundreds of millions of years, and the gas the inert waters gave off into the atmosphere poisoned everything on land. Plants, too. It was millions of years before the oceans recovered.

#### Climate change causes extinction – their defense is based on inaccurate models.

Specktor ‘6/4 (Brandon Specktor, Senior Writer, "Human Civilization Will Crumble by 2050 If We Don't Stop Climate Change Now, New Paper Claims," Live Science, 6-4-2019, https://www.livescience.com/65633-climate-change-dooms-humans-by-2050.html, SB).

It seems every week there's a scary new report about how man-made climate change is going to cause the collapse of the world's ice sheets, result in the extinction of up to 1 million animal species and — if that wasn't bad enough — make our beer very, very expensive. This week, a new policy paper from an Australian think tank claims that those other reports are slightly off; the risks of climate change are actually much, much worse than anyone can imagine. According to the paper, climate change poses a "near- to mid-term existential threat to human civilization," and there's a good chance society could collapse as soon as 2050 if serious mitigation actions aren't taken in the next decade. Published by the Breakthrough National Centre for Climate Restoration in Melbourne (an independent think tank focused on climate policy) and authored by a climate researcher and a former fossil fuel executive, the paper's central thesis is that climate scientists are too restrained in their predictions of how climate change will affect the planet in the near future. [Top 9 Ways the World Could End] The current climate crisis, they say, is larger and more complex than any humans have ever dealt with before. General climate models — like the one that the United Nations' Panel on Climate Change (IPCC) used in 2018 to predict that a global temperature increase of 3.6 degrees Fahrenheit (2 degrees Celsius) could put hundreds of millions of people at risk — fail to account for the sheer complexity of Earth's many interlinked geological processes; as such, they fail to adequately predict the scale of the potential consequences. The truth, the authors wrote, is probably far worse than any models can fathom. How the world ends What might an accurate worst-case picture of the planet's climate-addled future actually look like, then? The authors provide one particularly grim scenario that begins with world governments "politely ignoring" the advice of scientists and the will of the public to decarbonize the economy (finding alternative energy sources), resulting in a global temperature increase 5.4 F (3 C) by the year 2050. At this point, the world's ice sheets vanish; brutal droughts kill many of the trees in the Amazon rainforest (removing one of the world's largest carbon offsets); and the planet plunges into a feedback loop of ever-hotter, ever-deadlier conditions. "Thirty-five percent of the global land area, and 55 percent of the global population, are subject to more than 20 days a year of lethal heat conditions, beyond the threshold of human survivability," the authors hypothesized. Meanwhile, droughts, floods and wildfires regularly ravage the land. Nearly one-third of the world's land surface turns to desert. Entire ecosystems collapse, beginning with the planet's coral reefs, the rainforest and the Arctic ice sheets. The world's tropics are hit hardest by these new climate extremes, destroying the region's agriculture and turning more than 1 billion people into refugees. This mass movement of refugees — coupled with shrinking coastlines and severe drops in food and water availability — begin to stress the fabric of the world's largest nations, including the United States. Armed conflicts over resources, perhaps culminating in nuclear war, are likely. The result, according to the new paper, is "outright chaos" and perhaps "the end of human global civilization as we know it."

### Environment Impact---2NC

#### Dedev outweighs---its try or die---land, overfishing, deforestation, food and water shortages have cascading effects on bio-d that’s key to survival

Richard Smith 14, economic historian, has written on capitalism and the environment for The Ecologist, the International Journal of Ecological Economics and Statistics, Real-World Economics Review, and others, and has a PhD in economic history from UCLA. Green Capitalism: The God That Failed, truth-out.org/news/item/21060-green-capitalism-the-god-that-failed

Given the enormous dangers that such a high target implies, critics have asked why Stern is so reluctant to aim for a safer target? Marxist ecologist John Bellamy Foster and his colleagues suggest that the answer is to be found in Stern's economics, not the science: The Stern Review is very explicit, however, that such a radical mitigation of the problem should not be attempted. The costs to the world economy of ensuring that atmospheric CO₂e stabilized at present levels or below would be prohibitive, destabilizing capitalism itself. "Paths requiring very rapid emissions cuts," we are told, "are unlikely to be economically viable." If global greenhouse gas emissions peaked in 2010, the annual emissions reduction rate necessary to stabilize CO2e at 450 ppm, the Stern Review suggests, would be 7 percent, with emissions dropping by about 70 percent below 2005 levels by 2050. This is viewed as economically insupportable.(39) Stern asserted that "the world does not have to choose between averting climate change and promoting growth and development."(40) But if the science is right that we need to keep emissions below 400 ppm, or even get them back below 350 ppm, then more growth is out of the question. Indeed, we would have to make radically deeper cuts in GDP than even the 7 percent reduction per year that Stern calculates would be necessary just to get us down to 450 ppm. Because, under capitalism, a contraction of economic output on anything like that scale would mean economic collapse and depression, it is difficult to see how we can make the reductions in greenhouse gases we have to make to avoid climate catastrophe unless we abandon capitalism. This is the dilemma. So far most scientists have tended to avoid getting into the contentious economic side of the question. But with respect to the issue of growth, the science is unequivocal: Never-ending growth means the end of civilization, if not humanity itself - and in the not-so-distant future. For a summary of the peer-reviewed science on this subject, read a few chapters of Mark Lynas' harrowing Six Degrees.(41) Global warming is surely the most urgent threat we face, but it is far from the only driver of global ecological collapse. For even if we switched to clean renewable electric power tomorrow, this would not stop the overconsumption of forests, fish, minerals, fresh water. It would not stop pollution or solve the garbage crisis or stop the changes in ocean chemistry. Indeed, the advent of cheap, clean energy could even accelerate these trends.(42) Numerous credible scientific and environmental researchers back up what the climate scientists have been telling us, to demonstrate why perpetual growth is the road to collective social suicide. For example: In 2005 the United Nations Millennium Ecosystem Assessment team of 1,300 scientists from 95 countries issued a landmark report on humanity's overconsumption of "nature's services." The scientists reported that 60 percent (15 of 24) of the ecosystems examined that are critical for human survival are being "degraded or used unsustainably," including fresh water, capture fisheries, coral reefs, wetlands, drylands and forests. Around the world, many of these are deteriorating or on the verge of collapse. Thus nature's ability to provide the resources for growing future populations is very much in doubt unless radical steps are taken soon. In its Living Planet Report 2010, the World Wide Fund for Nature (WWF) similarly concluded that people are plundering the world's resources at a rate that far outstrips the planet's capacity to sustain life. As of 2007, the world's 6 billion-plus people were using up 50 percent more natural resources per year than can be naturally regenerated (and many resources, like oil, cannot be replenished at all). Put another way, humanity's current "global footprint" is equal to 1.5 planets. Under a business-as-usual scenario, even with modest projections for population growth, consumption and climate change, the UN predicts that by 2030 humanity will need the capacity of two Earths to absorb CO2 waste and support natural resource consumption. Of course we don't all consume equally: The footprint of high-income countries is three times that of middle-income countries and five times that of low-income countries. Americans have the biggest footprint of all, consuming the most energy and producing the most waste. If everyone lived like Americans do, we would need 5.3 planets to support all this. James Leape, director general of WWF, says, "The implications are clear. Rich nations must find ways to live much more lightly on the Earth - to sharply reduce their footprint, in particular their reliance on fossil fuels. The rapidly growing emerging economies must also find a new model for growth - one that allows for them to improve the well-being of their citizens in ways the Earth can actually sustain."(43) And in its own 2010 State of the World Report, the World Watch Institute says that: As consumerism has taken root in culture upon culture over the past half-century, it has become a powerful driver of the inexorable increase in demand for resources and production of waste that marks our age. ... More than 6.8 billion human beings are now demanding ever greater quantities of material resources, decimating the world's richest ecosystems, and dumping billions of tons of heat-trapping gases into the atmosphere each year. Despite a 30-percent increase in resource efficiency, global resource use has expanded 50 percent over the past three decades. And those numbers could continue to soar for decades to come as more than 5 billion people who currently consume one tenth as many resources per person as the average European try to follow the trail blazed by the world's affluent.(44)

### Chemicals Impact---2NC

#### Growth causes chemical emissions which cause extinction

**Cribb, 17**—principal of JCA, Fellow of the Australian Academy of Technological Sciences and Engineering, former Director, National Awareness, CSIRO (Julian, “The Poisoner,” *Surviving the 21st Century* Chapter 6)

There are two essential points about the Earthwide chemical flood. First it is quite new. It began with the industrial revolution of the late nineteenth century, but expanded dramatically in the wake of the two world wars—where chemicals were extensively used in munitions—and has exploded in deadly earnest in the past 50 years, attaining a new crescendo in the early twenty-first century. It is something our ancestors never faced—and to which we, in consequence, lack any protective adaptations which might otherwise have evolved due to constant exposure to poisons.

Second, the toxic flood is, for the most part, preventable. It is not compulsory—but is an unwanted by-product of economic growth. Though driven by powerful industries and interests, it still lies within the powers and rights of citizens, consumers and their governments to demand it be curtailed or ended and to encourage industry to safer, healthier products and production systems.

The issue is whether, or not, a wise humanity would choose to continue poisoning our children, ourselves and our world.

Regulatory Failure

Despite the fact that around 2000 new chemicals are released onto world markets annually, most have not received proper health, safety or environmental screening—especially in terms of their impact on babies and small children. Regulation has so far failed to make any serious curtailment of this flood: only 21 out of 144,000 known chemicals have been banned internationally, and this has not eliminated their use. At such a rate of progress it will take us more than 50,000 years to identify and prohibit or restrict all the chemicals which do us harm. Even then, bans will only apply in a handful of well-regulated countries, and will not protect the Earth system nor humanity at large. Clearly, national regulation holds few answers to what is now an out-of-control global problem.

Furthermore, the chemical industry is relocating from the developed world (where it is quite well regulated and observes its own ethical standards) and into developing countries, mainly in Asia, where it is largely beyond the reach of either ethics or the law. However, its toxic emissions return to citizens in well-regulated countries via wind, water, food, wildlife, consumer goods, industrial products and people. The bottom line is that it doesn’t matter how good your country’s regulations are: you and your family are still exposed to a growing global flood of toxins from which even a careful diet and sensible consumer choices cannot fully protect you.

The wake-up call to the world about the risks of chemical contamination was issued by American biologist Rachel Carson when she published Silent Spring in 1962, in which she warned specifically about the impact of certain persistent pesticides used in agriculture. Since her book came out, the volume of pesticide use worldwide has increased 30-fold, to around four million tonnes a year in the mid-2010s. Since the modern chemical age began there has been a string of high-profile chemical disasters: Minamata, the Love Canal, Seveso, Bhopal, Flixborough, Oppau, Toulouse, Hinkley, Texas City, Jilin, Tianjin. Most of these display a familiar pattern of unproductive confrontation between angry citizens, industry and regulators, involving drawn-out legal battles that deliver justice to nobody. By their spectacular and local nature, such events serve to distract from the far larger, more insidious and ubiquitous, universal toxic flood.

Chemists and chemical makers often claim that their products are ‘safe’ because individual exposure (e.g. in a given product, like a serve of food) is too low to result in a toxic dose, a theory first put forward by the mediaeval scholar Paracelsus in the sixteenth century. This ‘dose related’ argument is disingenuous, if not dishonest—as modern chemists well know—for the following reasons:

Most chemicals target a receptor or receptors on certain of your body cells, to cause harm. There may be not one, but hundreds or even thousands of different chemicals all targeting the same receptor, so a particular substance may contribute an unknowable fraction to an overall toxic dose. That does not make it ‘safe’.

Chemicals not known to be poisonous in small doses on their own can combine with other substances in water, air, food or your body to create a toxin. No manufacturer can truthfully assert this will not happen to their products.

Chemical toxicity is a function of both dose and the length of time you are exposed to it. In the case of persistent chemicals and heavy metals, this exposure may occur over days, months, years, even a lifetime in some cases. Tiny doses may thus accumulate into toxic ones.

Most chemical toxicity is still measured on the basis of an exposed adult male. Babies and children being smaller and using much more water, food and air for their bodyweight, are therefore more at risk of receiving a poisonous dose than are adults.

Chemicals and minerals are valuable and extremely useful. They do great good, save many lives and much money. No-one is suggesting they should all be banned. But their value may be for nothing if the current uncontrolled, unmonitored, unregulated and unconscionable mass release and planetary saturation continues.

Chemical Extinction

Two billion years ago, excessive production of one particular poisonous chemical by the inhabitants of Earth caused a colossal die-off and threatened the extermination of all life. That chemical was oxygen and it was excreted by the blue-green algae which then dominated the planet, as part of their photosynthetic processes. After several hundred million of years, the planet’s physical ability to soak up the surplus O2 in iron formations, oceans and sediments had reached saturation and the gas began to poison the existing life. This event was known as the ‘oxygen holocaust’, and is probably the nearest life on Earth has ever come to complete disaster before the present (Margulis and Sagan 1986). Since it developed slowly, over tens of millions of years, the poisonous atmosphere permitted some of these primitive organisms to evolve a tolerance to O2—and this in time led to the rise of oxygen-dependent species such as fish, mammals and eventually, us. The takehome learning from this brush with total annihilation is that it is possible for living creatures to pollute themselves into oblivion, if they don’t take care to avoid it or rapidly adapt to the new, toxic environment. It’s a message that humans, with our colossal planetary chemical impact, would do well to ponder.

While it is unlikely that human chemical emissions alone could reach such a volume and toxic state as to directly threaten our entire species with extinction (other than through carbon emissions in a runaway global warming event) or even the collapse of civilisation, it is likely they will emerge as a serious contributing factor during the twenty-first century in combination with other factors such as war, climate change, pandemic disease and ecosystem breakdown. Credible ways in which man-made chemicals might imperil the human future include:

Undermining the immune systems, physical and mental health of the population through growing exposure to toxins

Reducing the intelligence of current and future generations through the action of nerve poisons on the developing brains and central nervous systems of children, rendering humanity less able to solve its problems and adapt to major changes; and by increasing the level of violent crime and conflict in society, which is closely linked to lower IQ.

Bringing down the economy through the massive healthcare costs of having to nurse, treat and maintain a growing proportion of the population disabled by lifelong chronic chemical exposure.

By poisoning the ecosystem services—clean air, water, soil, plants, insects and wildlife—on which humanity depends for its own survival and thereby contributing to potential global ecosystem breakdown

By augmenting the global arsenal of weapons of mass destruction and hence the risk of their use by nations or uncontrollable fanatics.

### Phosphorous Impact---2NC

#### Phosphorous depletion

Charly Faradji 16, Doctor of Philosophy Student, Chemistry, University of Bristol, “How the great phosphorus shortage could leave us short of food,” 2/17/16, https://phys.org/news/2016-02-great-phosphorus-shortage-short-food.html

It's not as well-known as the other issues, but phosphorus depletion is no less significant. After all, we could live without cars or unusual species, but if phosphorus ran out we'd have to live without food.¶ Phosphorus is an essential nutrient for all forms of life. It is a key element in our DNA and all living organisms require daily phosphorus intake to produce energy. It cannot be replaced and there is no synthetic substitute: without phosphorus, there is no life.¶ Our dependence began in the mid-19th century, after farmers noticed spreading phosphorus-rich guano (bird excrement) on their fields led to impressive improvements in crop yields. Soon after, mines opened up in the US and China to extract phosphate ore – rocks which contain the useful mineral. This triggered the current use of mineral fertilisers and, without this industrial breakthrough, humanity could only produce half the food that it does today.¶ Fertiliser use has quadrupled over the past half century and will continue rising as the population expands. The growing wealth of developing countries allows people to afford more meat which has a "phosphorus footprint" 50 times higher than most vegetables. This, together with the increasing usage of biofuels, is estimated to double the demand for phosphorus fertilisers by 2050.¶ Today phosphorus is also used in pharmaceuticals, personal care products, flame retardants, catalysts for chemical industries, building materials, cleaners, detergents and food preservatives.¶ Phosphorus is not a renewable resource¶ Reserves are limited and not equally spread over the planet. The only large mines are located in Morocco, Russia, China and the US. Depending on which scientists you ask, the world's phosphate rock reserves will last for another 35 to 400 years – though the more optimistic assessments rely on the discovery of new deposits.¶ It's a big concern for the EU and other countries without their own reserves, and phosphorus depletion could lead to geopolitical tensions. Back in 2008, when fertiliser prices sharply increased by 600% and directly influenced food prices, there were violent riots in 40 different developing countries.¶ Phosphorus also harms the environment. Excessive fertiliser use means it leaches from agricultural lands into rivers and eventually the sea, leading to so-called dead zones where most fish can't survive. Uninhibited algae growth caused by high levels of phosphorus in water has already created more than 400 coastal death zones worldwide. Related human poisoning costs US$2.2 billion dollars annually in the US alone.¶ With the increasing demand for phosphorus leading to massive social and environmental issues, it's time we looked towards more sustainable and responsible use.¶ There is still hope¶ In the past, the phosphorus cycle was closed: crops were eaten by humans and livestock while their faeces were used as natural fertilisers to grow crops again.¶ These days, the cycle is broken. Each year 220m tonnes of phosphate rocks are mined, but only a negligible amount makes it back into the soil. Crops are transported to cities and the waste is not returned to the fields but to the sewage system, which mainly ends up in the sea. A cycle has become a linear process.¶ We could reinvent a modern phosphorus cycle simply by dramatically reducing our consumption. After all, less than a third of the phosphorus in fertilisers is actually taken up by plants; the rest accumulates in the soil or is washed away. To take one example, in the Netherlands there is enough phosphorus in the soil today to supply the country with fertiliser for the next 40 years.

### AT: CCS

#### CCS can’t solve warming

Kole 16 (Allison Kole, Senior legal fellow with the Climate Investigations Center, “It’s Too Late for Expensive Capture Technology to Help Climate,” The New York Times, July 7, 2016, http://www.nytimes.com/roomfordebate/2016/07/07/clean-coal-or-a-dirty-shame/its-too-late-for-expensive-carbon-capture-technology-to-help-the-climate)

Despite decades of effort, carbon capture and storage for coal­fired power plants has yet to come close to offsetting the damage caused by coal and has created new hazards of its own. The term “clean coal” has always seemed like an oxymoron, and so it is no wonder that carbon capture, a technology touted by industry, has done little to clean up coal. We cannot afford further investment in a pipe dream that distracts us from developing real solutions and technologies for climate change. Yet policymakers, prodded by the coal industry, continue to invest money and precious time to try to develop carbon capture for coal­fired plants. The Department of Energy began developing carbon capture in 1997, and since 2008, Congress has allocated $7 billion for carbon capture programs. Still, no commercial­scale carbon capture power plant has gone online in the United States, and the long list of abandoned projects in the United States and abroad grows. Carbon capture is an expensive technology requiring expansive new infrastructure. This includes potentially thousands of miles of pipeline for transporting captured carbon dioxide and maintenance and monitoring of storage sites to prevent leakage. Assuming such obstacles can be overcome, it is likely too late for carbon capture to be scaled up as needed to be an effective tool for combating climate change. To achieve meaningful carbon dioxide reductions, approximately 100 carbon capture projects must be online by 2020 and 3,000 by 2050. No carbon capture project has been able to capture the quantities of carbon dioxide promised. Also, carbon capture investment is not a smart strategy for reducing carbon emissions. To recoup costs, some carbon capture power plant operators plan to sell carbon dioxide to oil companies to help them extract more oil. Also, because carbon capture reduces a coal plant’s efficiency, using carbon capture actually requires the use of more coal to produce the same amount of energy than a plant without carbon capture. Putting costs, infrastructure issues and efficiency problems aside, the use of carbon capture to reduce carbon emissions ignores the harmful effects of coal on the environment and communities. Regardless of any reduction in carbon achieved, plants with carbon capture still release harmful air pollutants and produce polluting coal ash ponds. With or without carbon capture, the burning, storage and extraction of coal disproportionately affects poor communities and communities of color. We cannot afford further investment in the carbon capture pipe dream that distracts the nation from developing real solutions and adaptive technologies for climate change. Our energy and environmental future should not be dictated by the narrow vision of the fading coal industry.

#### Leakage thumps

Chu 15 – writer for MIT News, (Jennifer, “Sequestration on shaky ground,” MIT News, Jan 20, 2015, <http://news.mit.edu/2015/carbon-dioxide-sequestration-doubts-0120>, jwg)

Carbon sequestration promises to address greenhouse-gas emissions by capturing carbon dioxide from the atmosphere and injecting it deep below the Earth’s surface, where it would permanently solidify into rock. The U.S. Environmental Protection Agency estimates that current carbon-sequestration technologies may eliminate up to 90 percent of carbon dioxide emissions from coal-fired power plants. While such technologies may successfully remove greenhouse gases from the atmosphere, researchers in the Department of Earth, Atmospheric and Planetary Sciences at MIT have found that once injected into the ground, less carbon dioxide is converted to rock than previously imagined. The team studied the chemical reactions between carbon dioxide and its surroundings once the gas is injected into the Earth — finding that as carbon dioxide works its way underground, only a small fraction of the gas turns to rock. The remainder of the gas stays in a more tenuous form. “If it turns into rock, it’s stable and will remain there permanently,” says postdoc Yossi Cohen. “However, if it stays in its gaseous or liquid phase, it remains mobile and it can possibly return back to the atmosphere.” Cohen and Daniel Rothman, a professor of geophysics in MIT’s Department of Earth, Atmospheric, and Planetary Sciences, detail the results this week in the journal Proceedings of the Royal Society A. Current geologic carbon-sequestration techniques aim to inject carbon dioxide into the subsurface some 7,000 feet below the Earth’s surface, a depth equivalent to more than five Empire State Buildings stacked end-to-end. At such depths, carbon dioxide may be stored in deep-saline aquifers: large pockets of brine that can chemically react with carbon dioxide to solidify the gas. Cohen and Rothman sought to model the chemical reactions that take place after carbon dioxide is injected into a briny, rocky environment. When carbon dioxide is pumped into the ground, it rushes into open pockets within rock, displacing any existing fluid, such as brine. What remains are bubbles of carbon dioxide, along with carbon dioxide dissolved in water. The dissolved carbon dioxide takes the form of bicarbonate and carbonic acid, which create an acidic environment. To precipitate, or solidify into rock, carbon dioxide requires a basic environment, such as brine. The researchers modeled the chemical reactions between two main regions: an acidic, low-pH region with a high concentration of carbon dioxide, and a higher-pH region filled with brine, or salty water. As each carbonate species reacts differently when diffusing or flowing through water, the researchers characterized each reaction, then worked each reaction into a reactive diffusion model — a simulation of chemical reactions as carbon dioxide flows through a briny, rocky environment. When the team analyzed the chemical reactions between regions rich in carbon dioxide and regions of brine, they found that the carbon dioxide solidifies — but only at the interface. The reaction essentially creates a solid wall at the point where carbon dioxide meets brine, keeping the bulk of the carbon dioxide from reacting with the brine. “This can basically close the channel, and no more material can move farther into the brine, because as soon as it touches the brine, it will become solid,” Cohen says. “The expectation was that most of the carbon dioxide would become solid mineral. Our work suggests that significantly less will precipitate.”

### AT: Eco-Modernist Manifesto

#### Dedev solves better than they can

Brook, et al, 15—professor of environmental sustainability at the University of Tasmania (Barry, with John Asafu-Adjaye, University of Queensland, Linus Blomqvist, Breakthrough Institute, Stewart Brand, Long Now Foundation, Ruth DeFries, Columbia Univeristy, Erle Ellis, University of Maryland, Baltimore County, Christopher Foreman, University of Maryland School of Public Policy, David Keith, Harvard University School of Engineering and Applied Sciences, Martin Lewis, Stanford University, Mark Lynas, Cornell University, Ted Nordhaus, Breakthrough Institute, Roger Pielke, Jr., University of Colorado, Boulder, Rachel Pritzker, Pritzker Innovation Fund, Joyashree Roy, Jadavpur University, Mark Sagoff, George Mason University, Michael Shellenberger, Breakthrough Institute, Robert Stone, Filmmaker, and Peter Teague, Breakthrough Institute, “AN ECOMODERNIST MANIFESTO,” <http://www.ecomodernism.org/manifesto/>, dml)//JM

We affirm the need and human capacity for accelerated, active, and conscious decoupling. Technological progress is not inevitable. Decoupling environmental impacts from economic outputs is not simply a function of market-driven innovation and efficient response to scarcity. The long arc of human transformation of natural environments through technologies began well before there existed anything resembling a market or a price signal. Thanks to rising demand, scarcity, inspiration, and serendipity, humans have remade the world for millennia. Technological solutions to environmental problems must also be considered within a broader social, economic, and political context. We think it is counterproductive for nations like Germany and Japan, and states like California, to shutter nuclear power plants, recarbonize their energy sectors, and recouple their economies to fossil fuels and biomass. However, such examples underscore clearly that technological choices will not be determined by remote international bodies but rather by national and local institutions and cultures. Too often, modernization is conflated, both by its defenders and critics, with capitalism, corporate power, and laissez-faire economic policies. We reject such reductions. What we refer to when we speak of modernization is the long-term evolution of social, economic, political, and technological arrangements in human societies toward vastly improved material well-being, public health ,resource productivity, economic integration, shared infrastructure, and personal freedom.

#### Ecomodernist Manifesto is wrong

Caradonna 15 (Jeremy Cardonna, PhD in the history of scientific, environmental, and political thought and teach Environmental Studies and Human Dimensions of Climate Change at the University of Victoria; Iris Borowy, Shanghai University, College of Liberal Arts, Faculty Member; Tom Green; Peter A. Victor; Maurie Cohen; Andrew Gow; Anna Ignatyeva; Matthias Schmelzer; Philip Vergragt; Josefin Wangel; Jessica Dempsey; Robert Orzanna; Sylvia Lorek; Julian Axmann; Rob Duncan; Richard B. Norgaard; Halina S. Brown; Richard Heinberg; “A Call to Look Past An Ecomodernist Manifesto: A Degrowth Critique”, <http://www.resilience.org/wp-content/uploads/articles/General/2015/05_May/A-Degrowth-Response-to-An-Ecomodernist-Manifesto.pdf>, 5/5/15)//NRG

The manifesto, which does not include sources or references, is divided into seven sections (The Communist Manifesto, by contrast, had only four) that puts forth a vision of a future society, or a pathway to that society, that is driven by the creation of new technologies, as well as the “intensification” of human activities, that together would “decouple[e] human development from environmental impacts (7). xv In short, the manifesto rehashes the fantastical goal, long pursued by neoclassical economists, of separating out the apparently desirable stuff (morepeople, more affluence, more consumption) from the undesirable stuff (waste, pollution, environmental degradation, and declines in energy stocks). Key to the ecomodernist argument is the narrative of modernity, or in more technocratic language, “modernization.” The ecomodernists do not romanticize low-impact indigenous or pre-industrial societies, and do not seem to value anything about global societies that existed before, say, 1750, or those in the present that retain non-industrial practices. These people are simply and backwardly “undeveloped.”xvi At times, the manifesto reads like a chapter from a Herbert Spencer tract; the love, admiration, and faith in science and technology borders on the Victorian, and the mythos of Progress, so essential to industrialism since the 19th century, is bizarrely juxtaposed against more sober acknowledgements of humankind’s toll on the planet. Here’s one example of this rather saccharine metanarrative of Progress: “Personal, economic, and political liberties have spread worldwide and are today largely accepted as universal values. Modernization liberates women from traditional gender roles, increasing their control of their fertility. Historically large numbers of humans—both in percentage and in absolute terms—are free from insecurity, penury, and servitude” (8-9). The ecomodernists view the Industrial Revolution as a largely positive phase of human history that increased life expectancy, allowed for technologies that increased human wellbeing, produced modern medicine and the ability to more effectively fight disease, and created systems that mitigated the effects of natural disasters (8).

One does not need a degrowth perspective to understand that this statement is highly questionable and that the effects of “modernization” have been more complex than this liberationist narrative would suggest. The “liberation” of women from “traditional gender roles” was due in large part to the work of twentiethcentury suffragettes and feminists, and had relatively little to do with industrialism in the narrow sense. (And what about women in the non-Western industrialized world?) It is important to acknowledge, moreover, that child labor and 16-hour days for adults fuelled the Industrial Revolution and were ended only by strike action taken by trade unions in the face of strong opposition by industrialists. In thesecases, technology and industrial production were the problem, for which collective, grass-roots action and resistance was the solution. Further, the idea that there are fewer people in “servitude” in 2015 than there were in the past is also a debatable point. New research sponsored by the United Nations suggests that over 20 million people are currently working as modern-day slaves. xviii xvii The total number of African slaves brought to the Americas by Europeans between 1500 and 1850 was 12 million, although many millions more died in waiting or in transit. At no single point, however, did the population of African (or aboriginal) slaves come close to 20 million. Slaves and subjugation certainly existed in other parts of the world, too, but the notion that servitude has declined in real numbers over time ultimately rests on the subjective interpretation on the word “servitude.” But the raw numbers are, here, beside the point. The point is that ecomodernism offers a peculiarly whitewashed and sugary interpretation of industrial modernism, and fails to acknowledge that the interrelated problems of overconsumption and environmental decline were not coincidental byproducts of those modern industrial processes. Industrial modernity has certainly brought numerous benefits to humankind, but it has come at a heavy toll, and one that jeopardizes the possibility of creating a sustainable society.

The technology-will-save-us thesis of the ecomodernists merely restates the optimism of industrialists and many futurists going back two centuries or more, but also borrows from the technocratic school of thought within sustainability that is often associated with Amory Lovins.xx The ecomodernists paper over the highly destructive nature of modern technologies throughout the manifesto, or else exaggerate the benefits of emergent technologies, such as the dubious and largely untested systems for carbon capture and storage (24). “Given that humans are completely dependent on the living biosphere, how is it possible that people are doing so much damage to natural systems without doing more harm to themselves?”(9). It comes as news to us that humans are not doing harm to themselves. The World Health Organization reported recently that in 2012 around 7 million people died—that is, one in eight of total global deaths—“as a result of air pollution exposure,” the vast majority of which was emitted via “modern” technologies. xxiii xxi In the 1970s, Paul Ehrlich developed the metric I = PAT, in which the overall impact of a society is determined by the factors of population, affluence, and technology. xxii This metric was invented as a caution toward overly simplistic acceptance of technologies, but the ecomodernists set aside this concern (28) and assume that more technology is necessarily the solution. The Manifesto is silent on the topic of geoengineering, but one worries that the ecomodernists support this fraught and highly risky response to climate change.

The ecomodernists scoff at the idea of “limits to growth,” arguing that technology will always find a way to overcome those limits. “Despite frequent assertions starting in the 1970s of fundamental ‘limits to growth,’ there is still remarkably little evidence that human populations and economic expansion will outstrip the capacity to grow food or procure critical material resources in the foreseeable future” (9).xxiv Here is one of the first clues that the ecomodernists agree with George H. W. Bush that the limits to growth are, in the words of the former president, “contrary to human nature.”xxv Graham Turner, Ugo Bardi, and numerous others have shown through empirical research that many of the modeled scenarios, and the fundamental thesis, of the Club of Rome remain as relevant as ever—that is, that the human endeavor is bumping up against natural limits. xxvii xxviii But what additional evidence do the ecomodernists need to appreciate that the limits to growth are being reached?

Richard Heinberg has demonstrated that the production of conventional oil, natural gas, and heavy oil all peaked around 2010, despite, but also due to, continued global reliance on fossil fuels, which still comprise over 80% of the world’s primary source of energy. The so-called Green Revolution and chemically intensive conventional farming has polluted many of the world’s waterways and lakes, and has caused a New Jersey-sized dead zone in the Gulf of Mexico. In North America, the vast majority of the original humus content on arable land has been lost to agriculture and monocultures. There are 7 million tons of accumulated non-biodegradable plastic debris caught in the eastern and western gyres of the Pacific Ocean, and half of the fish biomass in the world’s oceans show traces of microplastic contamination.xxix Copper will be in short supply by as early as the 2030s, and a number of rare Earth minerals will not be far behind.xxx Perhaps the absolute limits to growth have not yet been reached, but mounting evidence suggests that they are not far off, and it behooves ecomodernists to consider that yet more growth might not be the answer. The history of industrialism to date suggests that more growth will be coupled with increasing environmental costs. xxxii xxxi It is also worth realizing that many once-thriving societies, from the Anasazi to the Maya, collapsed due to demographic, ecological, and social pressures. The limits to growth are real, even if their exact nature differs over time and space.

Moreover, the ecomodernists’ disregard for ecology and natural systems is disturbingly anthropocentric. That is, they ignore or externalize the non-human casualties of growth. Even if technology and human ingenuity enabled miraculously the endless growth of “human populations and economic expansion”—why would we want this, again?—this Biggering would still generate manifold environmental impacts. The collapse of the Atlantic northwest cod fishery in the 1980s and early 1990s is merely one example of ecological ruin that was facilitated by industrial technologies (refrigeration, new kinds of ships, new harvesting materiel, and so forth) and the naïve contempt for natural limits. When the Canadian Federal Minister of Fisheries and Oceans declared a much-belated moratorium on the cod fishery in 1992, it brought to an end 500 years of intensive cod harvesting, destroyed many Canadian maritime communities, and put paid to the debate on natural limits. It is true that humanity survived the decline of the Northern cod, but does the precipitous decline of this fishery matter in the Story of Modern Progress?

One of the central arguments of the Manifesto is that human-induced environmental impacts could one day become “decoupled” from economic growth. As noted, this has long been the fantasy of neoclassical economists, who want to have their cake and eat it, too. But rather than addressing the fundamental flaws of a growth-obsessed economy, the ecomodernists assume that economic growth is both necessary and possible in the long term and that, therefore, technology will have to do the work of decoupling. “Decoupling of human welfare from environmental impacts will require a sustained commitment to technological progress and the continuing evolution of social, economic, and political institutionsalongside those changes” (29). The authors argue that the relative environmental impact of humans has decreased in some domains, even though there has not been an absolute decoupling of these aggregated impacts (11). They cite as evidence the fact that many countries have reduced their carbon intensity over the past few decades, meaning that they get more economic bang for their energy buck (20), partly because of increases in energy efficiency. However, to hold aggregate ecological impact over time constant with growth, eco-efficiency would need to improve at the same rate as the economy grows, which places a heavy burden on engineers and inventors. More troublingly, the ecomodernists fail to address the deeper problem that absolute, aggregated impacts have continued to climb—the concentration of GHGs in the atmosphere is increasing, the extinction of species chugs along at an alarming rate, the Human Appropriation of Net Primary Production (HANPP) remains staggeringly high, and the world’s major ecosystems have only become more degraded since the middle of the last century. Moreover, there is no hint of the Jevons Paradox—the long-recognized enigma that increases in technological and energy efficiency almost always increase consumption, not decrease it, due to various rebound effects. But the more profound dilemma is that ecomodernism is still locked inside the business-as-usual, growth paradigm. It is certainly true that a growing global economy will mean greater impacts on the natural world and human health, which is why we question the necessity of this growth.

Even the most anti-growth and pro-steady-state economists, from Herman Daly to Daniel O’Neil, argue that some parts of the world, namely Sub-Saharan Africa, could benefit from more economic growth. Many other parts of the planet would benefit from less growth, or in any case, will have to make do with a less busy economy. The point is that there needs to be a more critical and qualitative approach to growth, and one that jettisons GDP as a meaningful measure of economic well-being. But the ecomodernists seem to assume that all growth is good, in contradistinction to the degrowthists, who recognize that much of the growth in the developed world, with its high levels of material throughput and energy consumption, is “uneconomic” and leads to long-term costs and environmental impacts. In other words, growth backfires. Rather than leaving the developing world to play an impossible game of catch-up with levels of energy and material consumption in the developed world, what is needed is for the high-consumption countries to cease treating the present growth model as a limitless aspiration for others to follow.

One of the most unfortunate results of this technophilism and Biggering-Is-Better attitude is the ecomodernists’ adoration of nuclear power. The environmental thinkers behind the Manifesto seem to have followed James Lovelock into the misguided belief that nuclear power is the only hope for humanity. xl Some passages rival H. G. Wells’ Anticipations (1901) in their gushing optimism in Scientific Progress. Consider the following: “Human civilization can flourish for centuries and millennia on energy delivered from a closed uranium or thorium fuel cycle, or from hydrogen-deuterium fusion” (10). “Nuclear fission presents the only present-day zero-carbon technology with the demonstrated ability to meet most, if not all, of the energy demands of a modern economy.” (23) “We think it is counterproductive for nations like Germany and Japan, and states like California, to shutter nuclear power plants, recarbonize their energy sectors, and recouple their economies to fossil fuels and biomass.” (28) The reality is that nuclear power has never played a major role in meeting the world’s energy demands, despite the fact that it was touted throughout much of the middle and late twentieth century as a panacea for our energy woes. According to the Intergovernmental Panel on Climate Change (IPCC), nuclear provides only 2 percent of the world’s energy, although the International Energy Association puts the number at 5.7 percent. xli These numbers are still well below those of renewables, which are pushing 15 percent of global energy consumption.x Indeed, there are at least eight reasons that nuclear power should not be seen as a positive contribution from the standpoint of sustainable development, and it is worth dwelling on them in detail, since ecomodernism places so much emphasis on nuclear. First, nuclear power has never lived up to its expectations as a major energy source, especially when compared to its immense impacts and costs. Second, the building of nuclear power plants is hugely capital intensive, which seems to contradict the Manifesto’s call for “cheap, clean, dense, and abundant” energy sources (24). Third, nuclear power is a nonrenewable resource since uranium is finite, and some energy analysts project that low-cost and accessible stocks could become quite scarce by 2080. Fourth, most countries do not possess uranium deposits, and therefore nuclear power prevents many countries from achieving energy independence. Fifth, most countries do not currently have (or want, or could even consider) a nuclear power plant. As of 2013, only 31 countries had this capacity. Sixth, nuclear power and nuclear weapons are inherently linked since the ability to produce nuclear power also establishes the material basis and expertise for making nuclear weapons. It is not an energy source that creates the conditions for long-term peace, as we have learned recently, once again, in the standoff between Iran and the West. Seventh, nuclear waste is dangerously radioactive and essentially impossible to store safely in the long term, since the waste takes thousands of years to lose its radioactivity. The 440 or so nuclear power plants that function today generate enormous amounts of waste, much of which is still sitting on the grounds of the power plants, while some has been stored in caves or dumped in the ocean. Eighth, and finally, nuclear power plants are prone to catastrophic disasters—that is, environmental impacts—such as the ones that occurred in 1986 at Chernobyl, and in 2011 at the Fukushima Daiichi plant in Japan.xliii As a result of these disasters, and these concerns, public confidence in nuclear power has waned considerably in most countries around the world, and Even with future breakthroughs in nuclear technology, the reality is that a nuclear power will always remain an ecologically reckless endeavor. As a result of these disasters, and these concerns, public confidence in nuclear power has waned considerably in most countries around the world, and some governments, such as in Germany, have begun phasing out their remaining facilities. As seen above, the ecomodernists do not like that citizens in Germany or Japan are questioning nuclear power. Yet this indignation is insensitive in the extreme. For starters, Japan is still coping with a major power plant calamity, and one that has led to much soul-searching over the future of energy in Japan. In Germany, the effects of the Chernobyl disaster were direct and impactful. In West Berlin, for instance, the prevalence of Down syndrome rose dramatically in the nine months following the incident, which blanketed much of Western Europe in radioactive fallout. It may very well be true, as the Manifesto notes, that nuclear power is a low-carbon technology (at least, in the direct production phases of the energy), but there are many other health and environmental impacts to consider, not to mention the political and economic ramifications of this technology. More nuclear power plants will almost inevitably mean more disasters and more longterm storage headaches. The ecomodernists seem particularly miffed that Germans want to “recarbonize” their economy, since reducing nuclear will, according to the Manifesto, require filling the void with coal (along with wind, biomass, and solar), although this, too, is a complicated matter. Renewable energy production has, so far, overcompensated for the decline in production in nuclear energy, and there is every indication that it could continue to do so. It is true that Germany, along with many other countries, is still powered in part by coal. But Germany, unlike national governments in Canada or the United States, has a long-term energy plan to wean itself from fossil fuels.xliv Why abandon those gains in favor of nuclear power (a proven liability) and carbon capture and storage (which reinforces the fossil-fueled status quo)?

Rather than ramping up on dangerous forms of energy production to meet increased economic activity, the world needs less (and also different) economic activity and a sustainable population, which could then create the possibility of powering the world via renewable resources. That is, degrowthists and ecomodernists agree that economic growth creates energy problems, but the two camps differ starkly in their response to this dilemma. For the ecomodernists, population and economic growth are taken as givens, and thus governments are forced into making difficult decisions about energy, including support for conventional, hard energies, from coal and gas to nuclear power. For degrowthists, population growth and continued economic expansion are seen as undesirable and essentially impossible in the medium term, and thus the solution is to live within biophysical limits, and reduce global energy demands to a level that could be safely met by renewables. To borrow a book title from Ted Trainer, Renewable Energy Cannot Sustain a Consumer Society.

The ecomodernists also assume that the increasing urbanization of the planet is fundamentally positive. Dehli now counts 25 million people. Beijing has over 21 million smog-chocked inhabitants. Mexico City, 20 million. Cities now occupy an astounding three percent of the Earth’s surface and house around four billion people (12), leading to historically unprecedented densities of human clusterings. While urban dwellers tend to have higher incomes and better access to societal services than their rural counterparts, looking only at the average number hides the deep inequalities within and across cities worldwide. A city such as Mumbai has stunning inequalities, human suffering, public health crises, slums, and dilapidated infrastructure. The relative affluence of urban dwellers comes at a cost for the environment. Cities are home to about half of the global population, but contribute about 80 percent of global GHG emissions. xlvii xlvi It is hard to see how yet more urbanization will necessarily increase human wellbeing, as the ecomodernists credulously contend. Economic growth has been accompanied by mounting income inequalities in urban areas and beyond. In contrast to the three decades of rapid growth following World War II, the little growth that has been squeezed out of the economic system in recent years has largely benefitted the richer strata of society, while cramming the world’s poor into densely packed cities, from China to Brazil. The bright and powerful vision of economic growth—to provide the material basis for a better life for all—bears little resemblance to the current prospects of only accumulating the wealth of the richest while destroying the environment and livelihoods of future generations and the poorest and most vulnerable today.

Further, ecomodernism is patently condescending toward peasants, farmers, and those who support agrarian values. This Manifesto is not for Wendell Berry. The authors note that only two percent of Americans are today engaged in farming, whereas half the population lived and worked on farms in the 1880s (12)—a demographic shift, it should be noted, that was facilitated by access to cheap and abundant fossil fuels. The authors go so far as to say that humans need to be “liberated” from agricultural labor, as though the production of food were not an essential good in and of itself. This very westernized and industrialized snobbery toward agrarianism is redolent of Nicholas Kristof and Sheryl WuDunn’s infamous and repugnant New York Times article, entitled “Two Cheers for Sweatshops,” which assumed that working in a wretched factory in industrial China was perforce a better fate than working in a rice paddy, as farmers in China have done for “forty centuries.” From the point of view of degrowth, a lower impact and less consumerist world will require an increase in farming (and gardening) and greater reconnections to the natural world. A sustainable global society will need more than two percent of the population engaged in food production. More generally, the Manifesto has literally nothing to say about the impacts of conventional farming, monoculture, pesticide-resistant insects, genetically modified organisms (GMOs), and the increasing privatization of seeds and genetic material. It implicitly implies that the Green Revolution was an unqualified positive for humankind. The CEOs of Monsanto and Nestlé would no doubt endorse this manifesto.

The issue of condescension toward indigenous cultures is particularly stark in the Manifesto. There is not a word about religion, spirituality, or indigenous ecological practices, even though the authors throw a bone to the “cultural preferences” for development (26). But the core assumption is that “development” has only one true trajectory, and that is to “modernize” along the lines of Western, industrialized countries. The conceit that technological modernity is Progress is hugely favorable to the development path of the Global North, but also quasi-imperialist in its assumption that the rest of the world needs to reproduce, in fast forward, the European and Neo-European Industrial Revolution. How is it simultaneously true that industrial modernity is both the problem and the solution? If the authors acknowledge, as they do, that industrialism has produced manifold negative impacts on the natural world, then why assume that yet more industrialism will magically reverse this trend? Furthermore, the ecomodernists do not seem to believe that the “developed” North has anything to learn from the “less developed” Global South. Is it possible that indigenous societies that lived sustainably for long periods of time might have important lessons to teach the rest of the world? The ecomodernists do not seem to think so.

Finally, the Manifesto often uses misleading (if not downright false) language in making its case. The passages on deforestation are especially greenwashed. For instance, the ecomodernists claim that three quarters of deforestation occurred before the Industrial Revolution (16). This may be true, but as Williams (2002) has shown, this is not really saying much.xlix Anatomically modern homo sapiens have been around for 200,000 years, and it has taken only 250 years to produce one quarter of all recorded deforestation. This fact does not strike us as particularly laudable, nor is it laudable that pollutive fossil fuels replaced forest resources as the world’s primary form of energy. Also, on page 13, the Manifesto manages to imply that there is currently “net reforestation” occurring on the globe, but since the text has no sources, it is hard to know the origin or particulars of this claim. The 2014 Millennium Development Report shows that a combination of afforestation and reforestation efforts has slowed deforestation rates, but that the world still suffered a net loss of forested land between 2000 and 2010 by many millions of hectares.l Certainly, the vast majority of those who study deforestation, including the World Wide Fund for Nature and the United Nations, contend unequivocally that deforestation is an ongoing concern. “For example, in the Amazon around 17 percent of the forest has been lost in the last 50 years.”li The United Nations Food and Agriculture Organization’s 2005 Forest Resources Assessment paints a pretty bleak picture for the world’s tropical forests, and many of the temperate ones, too, noting that loss of woodland jeopardizes essential ecosystem services, a concept that never appears in the Manifesto. lii

### AT: Geoengineering

#### At best it would take 160 years

Lieberman, Yale Climate Connections, citing Harvard researcher Gernot Wagner, 10/2/16

(Bruce, “Geoengineering: Crazy for sure, but with big but”, http://www.yaleclimateconnections.org/2016/11/geoengineering-crazy-for-sure-but-with-a-big-but/)

We’ll need more than solar geoengineering In September, the National Center for Atmospheric Research released [a study](http://www2.ucar.edu/atmosnews/just-published/122687/2-degree-goal-and-question-geoengineering) that found that geoengineering with sulfate particles will require a sustained effort of artificially pumping 18 megatons of sulfate particles into the stratosphere every year for 160 years – 160 years! – to slow the rate of warming. And geoengineering alone won’t do it. The NCAR study assumes that the globe will also drastically cut carbon emissions beginning in 2040. But even in that best-case scenario, we’ll still see the consequences of elevated levels of CO2 already built into the climate system: more episodes of extreme heat in North America, more retreating sea ice in the Arctic, changing patterns of precipitation globally, and more. It just won’t be as severe as doing nothing. Wagner says he is an optimist and also a realist. “Solar geoengineering is not a replacement for cutting emissions,” he says. “Whatever analogy you prefer — a Band-Aid, a fire extinguisher, chemotherapy for the planet, etc. – all point to the fact that we must treat the underlying condition. That means cutting CO2 and other greenhouse gases.”

#### It makes warming worse, causes Africa water wars, and kills the ozone

Renee **Cho 12** – Renee Cho is a staff blogger for the Earth Institute and a freelance environmental writer who has written for www.insideclimatenews.com, E Magazine and On Earth. Previously, Renee was Communications Coordinator for Riverkeeper, the Hudson River environmental organization. She received the Executive Education Certificate in Conservation and Sustainability from the Earth Institute Center for Environmental Sustainability (Renee Cho, 5-1-2012, "The Double-Edged Sword of Geoengineering," No Publication, accessed 8-20-2016, http://blogs.ei.columbia.edu/2012/05/01/the-double-edged-sword-of-geoengineering/)

Shooting sulfur particles into the stratosphere to reflect the sun? Dumping iron into the ocean to boost the absorption of carbon dioxide? Could these far-fetched and dangerous-sounding schemes help avert potentially catastrophic effects of climate change, or would they exacerbate conditions on our ever warming planet? These strategies, which involve the deliberate and large-scale intervention in our climate system to moderate global warming, are known as geoengineering. Fantastical as they seem, billionaires Bill Gates, Sir Richard Branson and others, are investing millions of dollars into the geoengineering research of a few leading climate scientists like Ken Caldeira at Stanford. At first, Caldeira thought geoengineering sounded crazy too, but his research showed that it would basically work. If global warming exceeds 2˚ C, it would be “a prescription for disaster,” said NASA scientist James Hansen. To prevent this from happening, we need to cap atmospheric carbon dioxide levels at 350 parts per million; but in March 2012, we reached almost 394.5 ppm and global greenhouse gas emissions continue to rise. Even if we were able to immediately cut greenhouse gas emissions to zero, however, global warming would continue for the foreseeable future because carbon dioxide remains in the atmosphere for several hundred years. Moreover, the international community has failed to reach an agreement that tackles the fundamental problem of controlling carbon emissions and prospects for doing so don’t look good. As a result, geoengineering is beginning to sound less like science fiction to some, and more like a possible Plan B. Geoengineering strategies fall into two main categories: Solar radiation management, which seeks to reduce the amount of sunlight that reaches earth by deflecting it or increasing Earth’s reflectivity (albedo). Carbon dioxide removal, which tries to take carbon dioxide out of the atmosphere. Solar radiation management includes efforts like white roofs that deflect sunlight, brightening clouds by shooting seawater into them to increase their albedo (salt provides the nuclei that seed the clouds), and controversial strategies based on the cooling effect that can follow major volcanic eruptions. In 1991, Mt. Pinatubo in the Philippines erupted, sending 22 million tons of sulfur dioxide into the stratosphere. The sulfur particles scattered around the globe, deflected sunlight, and cooled Earth by 0.4 to 0.5˚ C. Solar radiation management would recreate this effect by using balloons, aircraft or cannons to shoot tiny reflective particles like sulfates into the stratosphere to temporarily block sunlight. The 1992 Panel on Policy Implications of Greenhouse Warming calculated that this strategy would cost just pennies per ton of carbon dioxide mitigated. It would also be fast-acting, capable of quickly reducing the impacts of heat stress on crops, resulting in increased productivity since carbon dioxide levels, which boost growth, would remain high. Other solar radiation management ideas include the use of engineered nanoparticles, which could be constructed to ascend high into the atmosphere and keep their shiny side to the sun, and sunshades in space made of mirrors. Solar radiation management would do nothing to address the root cause of global warming—carbon dioxide emissions—or ocean acidification caused by the sea’s absorption of excess carbon dioxide. And while stratospheric aerosols could theoretically produce cooling on a local or global level, they might also create regional problems by affecting rain and snowfall patterns and causing drought. According to Caldeira, a year or two after Mt. Pinatubo, when aerosols dropped from the stratosphere, both the Amazon River and the Ganges had very low flows and droughts occurred. A 2010 study by ETC (Erosion, Technology and Concentration), an international group that opposes geoengineering, states that solar radiation management climate models show a risk of increased drought over Africa, Asia and the Amazon jungle. Putting sulfate particles into the stratosphere could also damage the ozone layer, lead to acid rain and increased ocean acidification, and interfere with solar cells, astronomy and satellites. In addition, solar radiation management techniques carry the risk of a rapid rise in temperature if the program were started then stopped, which would be more dangerous to life on Earth than a gradual temperature rise.

### AT: Nuclear

#### Nuclear energy fails

**Caradonna et al 15** (Jeremey, <http://www.ecomodernism.org/responses/2015/5/7/a-degrowth-response-to-an-ecomodernist-manifesto>, EM)

One of the most unfortunate results of this technophilism and Biggering-Is-Better attitude is the ecomodernists’ adoration of nuclear power. The environmental thinkers behind the Manifesto seem to have followed James Lovelock into the misguided belief that nuclear power is the only hope for humanity. xl Some passages rival H. G. Wells’ Anticipations (1901) in their gushing optimism in Scientific Progress. Consider the following: “Human civilization can flourish for centuries and millennia on energy delivered from a closed uranium or thorium fuel cycle, or from hydrogen-deuterium fusion” (10). “Nuclear fission presents the only present-day zero-carbon technology with the demonstrated ability to meet most, if not all, of the energy demands of a modern economy.” (23) “We think it is counterproductive for nations like Germany and Japan, and states like California, to shutter nuclear power plants, recarbonize their energy sectors, and recouple their economies to fossil fuels and biomass.” (28) The reality is that nuclear power has never played a major role in meeting the world’s energy demands, despite the fact that it was touted throughout much of the middle and late twentieth century as a panacea for our energy woes. According to the Intergovernmental Panel on Climate Change (IPCC), nuclear provides only 2 percent of the world’s energy, although the International Energy Association puts the number at 5.7 percent. xli These numbers are still well below those of renewables, which are pushing 15 percent of global energy consumption.x Indeed, there are at least eight reasons that nuclear power should not be seen as a positive contribution from the standpoint of sustainable development, and it is worth dwelling on them in detail, since ecomodernism places so much emphasis on nuclear. First, nuclear power has never lived up to its expectations as a major energy source, especially when compared to its immense impacts and costs. Second, the building of nuclear power plants is hugely capital intensive, which seems to contradict the Manifesto’s call for “cheap, clean, dense, and abundant” energy sources (24). Third, nuclear power is a nonrenewable resource since uranium is finite, and some energy analysts project that low-cost and accessible stocks could become quite scarce by 2080. Fourth, most countries do not possess uranium deposits, and therefore nuclear power prevents many countries from achieving energy independence. Fifth, most countries do not currently have (or want, or could even consider) a nuclear power plant. As of 2013, only 31 countries had this capacity. Sixth, nuclear power and nuclear weapons are inherently linked since the ability to produce nuclear power also establishes the material basis and expertise for making nuclear weapons. It is not an energy source that creates the conditions for long-term peace, as we have learned recently, once again, in the standoff between Iran and the West. Seventh, nuclear waste is dangerously radioactive and essentially impossible to store safely in the long term, since the waste takes thousands of years to lose its radioactivity. The 440 or so nuclear power plants that function today generate enormous amounts of waste, much of which is still sitting on the grounds of the power plants, while some has been stored in caves or dumped in the ocean. Eighth, and finally, nuclear power plants are prone to catastrophic disasters—that is, environmental impacts—such as the ones that occurred in 1986 at Chernobyl, and in 2011 at the Fukushima Daiichi plant in Japan.xliii As a result of these disasters, and these concerns, public confidence in nuclear power has waned considerably in most countries around the world, and Even with future breakthroughs in nuclear technology, the reality is that a nuclear power will always remain an ecologically reckless endeavor. As a result of these disasters, and these concerns, public confidence in nuclear power has waned considerably in most countries around the world, and some governments, such as in Germany, have begun phasing out their remaining facilities. As seen above, the ecomodernists do not like that citizens in Germany or Japan are questioning nuclear power. Yet this indignation is insensitive in the extreme. For starters, Japan is still coping with a major power plant calamity, and one that has led to much soul-searching over the future of energy in Japan. In Germany, the effects of the Chernobyl disaster were direct and impactful. In West Berlin, for instance, the prevalence of Down syndrome rose dramatically in the nine months following the incident, which blanketed much of Western Europe in radioactive fallout. It may very well be true, as the Manifesto notes, that nuclear power is a low-carbon technology (at least, in the direct production phases of the energy), but there are many other health and environmental impacts to consider, not to mention the political and economic ramifications of this technology. More nuclear power plants will almost inevitably mean more disasters and more longterm storage headaches. The ecomodernists seem particularly miffed that Germans want to “recarbonize” their economy, since reducing nuclear will, according to the Manifesto, require filling the void with coal (along with wind, biomass, and solar), although this, too, is a complicated matter. Renewable energy production has, so far, overcompensated for the decline in production in nuclear energy, and there is every indication that it could continue to do so. It is true that Germany, along with many other countries, is still powered in part by coal. But Germany, unlike national governments in Canada or the United States, has a long-term energy plan to wean itself from fossil fuels.xliv Why abandon those gains in favor of nuclear power (a proven liability) and carbon capture and storage (which reinforces the fossil-fueled status quo)?

### AT: Industrial Ag

#### Localized ag works and industrial ag is unsustainable

Alexander 16 (Samuel Alexander - lecturer at the Office for Environmental Programs, University of Melbourne, Australia, PhD from Melborne, 12-29-2016 “Frugal Abundance in an Age of Limits: Envisioning a Degrowth Economy” <https://link.springer.com/chapter/10.1057/978-1-349-95176-5_7>) //bp

2.2 Food A foundational issue for any economy is how it sources and produces its food, and this issue sits next to water on the list of essential needs. The globalised, industrial food production system currently in existence is highly unsustainable for various reasons. Not only are industrial farming techniques causing the severe and widespread erosion of nutrient-rich topsoil (which takes many hundreds of years to rejuvenate), but also the industrialised system is extremely fossil fuel dependent (see generally, Brown, 2011). Natural gas is needed to produce commercial fertilisers, and oil is needed to produce commercial pesticides, to fuel farm machinery, and to create the plastics used in packaging. Furthermore, there are extremely long supply chains that reach all around the world and which are dependent therefore on oil for transport. In Australia, for example, a basket of food from the supermarket typically travels 70,000 kilometres from producer to consumer, if the distance each item travels is aggregated (Salleh, 2007). With respect to the UK, one study has the figure at 241,000 kilometres (Sustain, 2001). This fossil fuel dependency is highly problematic not only due to its link to climate change, but also because it may not be economically sustainable as oil continues to get more expensive (Rubin, 2009; Alexander, 2014a). In a degrowth economy, food production may need to be highly localised, organic, and based on permaculture (Holmgren, 2002) or ‘biointensive’ (Jeavons, 2012) principles, in order to decarbonise industrial methods. One of the most significant, but often overlooked, implications of the transition away from industrial food production is the increased human labour needed for organic food production. The increased labour requirements arise primarily from the reduced reliance on energy-intensive, mechanised farm machinery, but organic fertiliser production and pest control are also typically more time intensive than industrialised techniques. Organic food production is entirely capable of feeding the world (United Nations, 2013; Jeavons, 2012), but to do so will require a huge increase in the provision of agricultural labour. This transition, however, will have many benefits, including reconnecting communities with the local land base upon which they depend for subsistence, and the health benefits associated with moving away from sedentary office or factory work toward the more active and outdoor work of farming (Mansen et al, 2004; Tremblay et al, 2010). Governments should do everything they can to support localised, organic agriculture, starting by putting a price on carbon. If they do not, grassroots movements should localise food production as best they can without state support. To begin with, a degrowth economy should aim to maximise organic food production within the urban boundary. This would involve digging up lawns and turning them into productive vegetable gardens, and planting fruit trees in all available spaces. Nature strips could be cultivated; parks could be turned into small farms or community gardens; suitable roofs could become productive, herbs could grow on balconies and windowsills, and generally all food producing potential would be realised. Suburban backyards could keep chickens for eggs, and perhaps even small livestock, such as goats for milk and cheese. Animals are also a great source of manure for compost, and many permaculturalists build animals into their organic systems (Holmgren, 2002). There is also great potential for building raised garden beds on driveways, some footpaths or roads, and redundant car parks. Mushrooms could be cultivated on the shady side of the house for protein and household or neighbourhood aquaculture systems could provide urban centres with some of their fish supply. Even in a degrowth economy, however, we can expect our urban households to ‘import’ various foods in various forms, if not always from around the world, then certainly from rural or peri-urban contexts. This, in fact, would be an absolute necessity in dense urban contexts, because growing space simply does not permit anywhere near strict self-sufficiency (see McCrae et al, 2010). Even inspiring examples of urban agriculture, like Havana, in Cuba (see Friedrichs, 2013; Percy et al, 2010), still require the importation of food – not only portions of its fruit and vegetables, but also its meat, minerals, and other foodstuffs, such as salt. The mainly local and organic food production would also drastically change our consumption habits. Food would be eaten ‘in season’ in order to avoid having to import non-seasonal foods from the other side of the world. Preserving foods would be the most appropriate way to access those foods out of season. Generally, food would be unprocessed and require no disposable packaging. A robust carbon tax would significantly increase the relative price of meat (especially red meat) and consequently relative demand would significantly reduce, which is a necessary part of low-carbon living. This transition to low- or no-meat diets would open up huge tracts of land for human food production or ‘rewilding’ (Monbiot, 2013) that are currently used to produce grain for animals.

### AT: Renewables

#### Renewables take too long

Harold Wilhite 16, Research Director at the University of Oslo’s Centre for Development and Environment and Academic Director of a program entitled Environmental Change and Sustainable Energy, *The Political Economy of Low Carbon Transformation: Breaking the habits of capitalism*, 2016, no page numbers

The main within-capitalism solution for reducing energy-related climate emissions is the replacement of fossil fuels with other energy sources that do not emit carbon, such as sun, wind, geothermal and nuclear power. As I have argued in several recent publications, the transformation to renewable energies, while important, will not happen fast enough, nor assume a large enough share of global energy production over the next couple of centuries to make a significant dent in carbon reductions (Wilhite 2012). In the highest carbon-emitting country, the USA, even the latest and most ambitious plan for reducing carbon emissions assumes that 70 percent of primary energy use in 2030 will be from fossil fuels (compared to 72 percent in 1990) and 15 percent from renewable energy sources (CSE 2015). The most lucrative alternative source of energy, solar, has disadvantages relative to fossil fuels regarding storage and production at scale which limit its uses in industrial production and large-scale electricity production (Altvater 2007). In Chapter 4 1 will argue that mainstream 'green' economy approaches to reducing carbon are overoptimistic in their assumptions about the capacity for renewable energies to achieve urgently needed rapid and significant decreases in carbon emissions. I will also argue that the consumption of the things that use energy will have to be reduced in numbers and size, including reductions in the sizes of the houses in which we live and in the energy used to produce essential in-home services such as thermal comfort, clean bodies, food and transport. Achieving these reductions will demand challenging the cornerstones of capitalist political economy — growth, individualism and consumerism — and reforming the habits that this economic system have fostered.

#### Logistic growth thumps scalability

J.P. Hansen 17, Department of Physics and Technology, University of Bergen, “Limits to growth in the renewable energy sector,” *Renewable and Sustainable Energy Reviews*, Volume 70, April 2017, pp. 769-774

Which mechanisms have led to the apparent logistic behavior in wind and solar energy production? This cannot be assessed from the present data, but we comment on four potential saturation mechanisms that have been pointed at in previously published studies: First, despite becoming increasingly competitive against other technologies, some studies [18,19] suggest that unsubsidized renewable energy, in spite of high annual learning rates [20], is presently more expensive than alternatives on a direct cost basis. Comparisons of this type are often made without taking into account all costs associated with deployment of intermittent renewable energy sources. It is well documented in the literature that these intermittent technologies have different values for the system [21,22] in the sense that they do not always lower system costs (grid + generation costs) if deployed [23], everything else being equal. If this was not the case, there would be little investment in conventional technologies today. A second potential mechanism related to energy return on energy invested (EROI) has been thoroughly discussed in several studies [10–12]: In considering the ratio of energy produced vs. energy invested in the build-up of large renewable energy systems these studies forecast an optimum level in global renewable energy production well below what is needed to satisfy the global demand. The origin of this limit was considered to be limited area and increased expenses to build energy production at increasingly more remote locations. A third saturation mechanism is finite material life times which implies that there will be an increasing need to renew existing power production sites [11]. This mechanism, however, has hardly been important so far due to the early stage, but will certainly increase with the aging of current installations in coming years. A final saturation mechanism that applies to intermittent sources of energy, like wind and solar, is that they tend to cannibalize their own revenue streams [24]. Assuming a constant price over a 24-h period, the deployment of a limited capacity of solar PV can already make a dip in the market price for electricity in hours when solar radiation is at its strongest. Once installed, solar energy delivery has marginal costs close to zero and assuming a well-functioning market, not distorted by subsidies, an owner of solar PV will bid at a price down towards zero in order to enter the market. This drags the price down during hours with solar capacity [25]. Hence, the more solar capacity installed, the lower the price in these hours. At some stage, when the average market price is lower than the long-run marginal cost of producing solar power during hours with solar production, investors will lose interest in installing more capacity since they cannot expect positive returns on their investment. Current market designs thus limit how much solar power can be deployed in a system. Consequently, regional plans [26] for ruling out subsidies towards renewable energy without compensating with other marked changing strategies are likely to strengthen the marked contribution to a logistic pattern. 5. Conclusions In this paper we have shown that at present wind and solar power shows early signs of logistic growth despite high learning rates and energy return on energy invested particularly within the photovoltaics section [27]. Extrapolation of the logistic time development for sun and wind combined suggests saturation of about 1.6 TW (Fig. 3) around 2030. For the most optimistic scenario in our analyses, where stakeholders prognosis are included in separate analyses for wind and sun, a saturation of 1.8 TW is indicated (sum of upper confidence limits of Pmax for wind and sun in Table 1). This is likely much less than 10% of the global energy mix in 2030. This alarmingly low fraction will make the COP 21 ambitions on climate gas reductions hard to achieve. We are well aware of the uncertainties [8] with the logistic forecast: Technology development, e.g. in ocean wind energy, and unforeseen breakthroughs of competing energy resources, e.g. nuclear fusion, may cause the development to take a completely new route [28]. In absence of such developments, however, the present data are an early warning of a growing gap between expressed ambitions and an actual growth.

### War---2NC

#### Growth causes war-

#### 1---Both funds AND motivates aggression

Lucas **Hahn 16**. Bryant University. April, 2016. Global Economic Expansion and the Prevalence of Militarized Interstate Disputes.

Economic Factors Leading to Increased Militarized Interstate Disputes Running counter to the arguments that global economic expansion has led to a decline in MIDs throughout the world, there is a large body of literature that claims the exact opposite. In particular, some authors argue that the recent declines that have been observed are a direct result of a decline in conflict after major spikes during the World Wars and the Cold War. The following section will highlight four different economic factors that are potentially leading to an increase in MIDs. These four factors include: (1) imperialism and resources, (2) the “War-Chest Proposition”, (3) Neo-Marxist views on asymmetrical trade, and (4) interdependence versus interconnectedness. 1. Imperialism and Resources The presence of imperialism between the 17th and early 20th centuries was, in a way, a precursor to globalization today. During this period of time the most developed nations worked to expand their empires and in doing so, began to connect the people of the world for the first time. However, while there were many positive benefits of this expansion, there were also many negative happenings that led to violent conflict. As Arquilla (2009, 73) frames it imperialism involved commercial practices (often supported by military force) that took advantage of the colonized people and ultimately destroyed their way of life. Thus, the increased economic expansion that was brought about in order to build the empire, often led to violent encounters. More specifically, imperialism and the conquest of particular regions was often done in an effort to gain access to that region’s natural resources. Authors such as Schneider (2014) state that undeveloped nations or regions are often subject to what he refers to as the “domestic resource curse”. Basically, during the times of imperialism, the more powerful nations would go to undeveloped areas and take whatever they wanted or needed from areas that were rich with resources5. This often involved a great deal of conflict and the native people were often exploited. In modern times, the presence of significant caches of national resources, particularly in Africa, has been shown to lead to violence as corrupt governments and warlords take advantage of those native to the area. Additionally, as Barbieri (1996) points out, conflict over resources may not be limited to an imperialist nation’s encounter with the undeveloped region. Violent conflict can also exist between the multiple nations that are competing to gain access or control over natural resources in a given area. 2. The “War Chest Proposition” Building on the previous discussion, Boehmer (2010) proposes something that he calls the “War-Chest Proposition”. He states that economic growth can lead to increased military/defense spending and that this buildup of a nation’s “war chest” may be used to pay for new or continuing military engagements (251). In other words, increased economic power often leads to greater capabilities of the nation-state as a whole. This is particularly true in terms of military capabilities and in this way, nations may thus be able to engage in more conflict. Furthermore, he argues that positive economic expansion builds up the confidence of the nation to a point where they may feel invincible and thus, engage in violent conflict that will help them to continue to expand. 3. Neo-Marxist Views on Asymmetrical Trade One of the most supported arguments against the notion that economic expansion promotes peace is that trade, brought about by economic expansion, actually increases MIDs. Many authors have in fact argued that increased economic interdependence and increased trade may have, in some ways, “cheapened war”, and thus made it easier to wage war more frequently (Harrison and Nikolaus 2012).

#### 2---Asymmetry

Levy & Thompson 10 (Jack S & William R; Levy is Board of Governors' Professor of Political Science at Rutgers University, former president of the International Studies Association, Affiliate at the Saltzman Institute of War and Peace Studies at Columbia University; Thompson is Distinguished Professor and the Donald A. Rogers Professor of Political Science at Indiana University; 2010; “The Dyadic Interactions of States”; *Causes of War*; pp. 72-75, published by Wiley-Blackwell)

Realist and rationalist critiques Realists, who share the economic nationalism and statist orientation of the old mercantilists, criticize the liberal economic theory of peace on a number of grounds. First of all, they argue (as do some non-realists) that even if it were true that trade has a pacifying effect, the magnitude of the impact of trade on decisions for war and peace issmall relative tothat of military and diplomatic considerations (Buzan, 1984 ; Levy, 1989b ). Realists, like mercantilists, argue that states are motivated primarily by power and that economic opportunity costs of war are minor in the context of the long-term struggle for power. Were the Western liberal democracies seriously concerned about the short-term loss of trade when they made decisions to go to war against the hegemonic threats posed by Germany in 1914 and again in 1939? Realists also argue that trade and other forms of economic interdependence can actually increase the level of militarized conflict rather than reduce it (Barbieri, 2002 ). As Rousseau (cited in Hoffmann, 1963 :319) argued, “…interdependence breeds not accommodation and harmony, but suspicion and incompatibility. ”Among other things, interdependence creates increased opportunities for conflict. The greater the interdependence between states, the greater the number of things to argue about. In addition, whereas liberals argue that economic interdependence creates mutual dependence and incentives to avoid war, realists argue that interdependence may also be asymmetrical. Each is dependent on the other, but the degree of dependence is uneven. The less dependent party may be tempted to use economic coercion to exploit the adversary’s vulnerabilities and influence its behavior relating to security as well as economic issues. 32 These can lead to retaliatory actions, conflict spirals, and war. 33

#### Wars are inevitable, BUT growth makes them bloodier.

Laio 19 – Jianan Liao, Shenzhen Nanshan Foreign Language School. [Business Cycle and War: A Literature Review and Evaluation, Advances in Economics, Business and Management Research, Volume 68, International Symposium on Social Science and Management Innovation, https://download.atlantis-press.com/article/55913122.pdf]//BPS

Through the comparison of the two views, it can be found that both sides are too vague in the description of the concept of business cycle. According to economists such as Joseph Schumpeter, the business cycle is divided into four phases: expansion, crisis, recession, recovery. [12] Although there are discords in the division and naming of business cycle, it is certain that they are not simply divided into two stages of rise and recession. However, as mentioned above, scholars who discussed the relationship between business cycle and war often failed to divide the business cycle into four stages in detail to analyze the relationship.

First, war can occur at any stage of expansion, crisis, recession, recovery, so it is unrealistic to assume that wars occur at any particular stage of the business cycle. On the one hand, although the domestic economic problems in the crisis/recession/depression period break out and become prominent in a short time, in fact, such challenge exists at all stages of the business cycle. When countries cannot manage to solve these problems through conventional approaches, including fiscal and monetary policies, they may resort to military expansion to achieve their goals, a theory known as Lateral Pressure. [13] Under such circumstances, even countries in the period of economic expansion are facing downward pressure on the economy and may try to solve the problem through expansion. On the other hand, although the resources required for foreign wars are huge for countries in economic depression, the decision to wage wars depends largely on the consideration of the gain and loss of wars. Even during depression, governments can raise funding for war by issuing bonds. Argentina, for example, was mired in economic stagflation before the war on the Malvinas islands (also known as the Falkland islands in the UK). In fact, many governments would dramatically increase their expenditure to stimulate the economy during the recession, and economically war is the same as these policies, so the claim that a depressed economy cannot support a war is unfounded. In addition, during the crisis period of the business cycle, which is the early stage of the economic downturn, despite the economic crisis and potential depression, the country still retains the ability to start wars based on its economic and military power. Based on the above understanding, war has the conditions and reasons for its outbreak in all stages of the business cycle.

Second, the economic origin for the outbreak of war is downward pressure on the economy rather than optimism or competition for monopoly capital, which may exist during economic recession or economic prosperity. This is due to a fact that during economic prosperity, people are also worried about a potential economic recession. Blainey pointed out that wars often occur in the economic upturn, which is caused by the optimism in people's mind [14], that is, the confidence to prevail. This interpretation linking optimism and war ignores the strength contrast between the warring parties. Not all wars are equally comprehensive, and there have always been wars of unequal strength. In such a war, one of the parties tends to have an absolute advantage, so the expectation of the outcome of the war is not directly related to the economic situation of the country. Optimism is not a major factor leading to war, but may somewhat serve as stimulation. In addition, Lenin attributed the war to competition between monopoly capital. This theory may seem plausible, but its scope of application is obviously too narrow. Lenin's theory of imperialism is only applicable to developed capitalist countries in the late stage of the development capitalism, but in reality, many wars take place among developing countries whose economies are still at their beginning stages. Therefore, the theory centered on competition among monopoly capital cannot explain most foreign wars. Moreover, even wars that occur during periods of economic expansion are likely to result from the potential expectation of economic recession, the "limits of growth" [15] faced during prosperity -- a potential deficiency of market demand. So the downward pressure on the economy is the cause of war.

Third, the business cycle may be related with the intensity, instead of the outbreak, of the war. Scholars who supported the first two views did not pay attention to the underlying relationship between business cycle and the intensity of war. Some scholars, such as Nikolai Kondratieff and Joshua Goldstein, believes that the business cycle is not directly related to the outbreak of war, but the outbreak of war during the economic upswing appears to be more intense and persistent. In their analysis of the business cycle and war, Kondratieff and Goldstein discovered that the most dramatic and deadly wars occurred during periods of economic upswing. This finding may provide some clues on the relationship between war and the business cycle. Although the relationship between the outbreak of war and the business cycle is unclear, the scale of the war is likely to be influenced by the exact phase of the business cycle in which the belligerents are engaged. Such a phenomenon might make sense, since countries in economic upturn have better fiscal capacity, making them more likely to wage large-scale wars. Moreover, such relationship may also stem from the optimism pointed out by Blainey. While optimism may not directly lead to wars, it may have an impact on the choice of rivals. This is because optimism about national strength and the outcome of the war may drive countries to choose stronger rivals. The resulting war is likely to be far more massive and bloody. Nevertheless, more research is needed to specifically reveal this relationship.

From this point of view, it is not clear whether there is a direct causal relationship between the outbreak of war and the business cycle, but the existence of periodic economic crises in capitalist countries renders war a tool to promote expansionary economic policies. The economic performance of the war is the expansion of government expenditure and possession of overseas resources and markets, which is in some ways consistent with the goal of expansionary fiscal policy. Therefore, war may be used by governments as a political means to stimulate the economy, although the relationship between the use of such means and the specific stages of business cycle remains to be explored.

### AT: Diversionary War---2NC

#### Diversionary wars are small and don’t escalate

Dominic **Tierney 17**, associate professor of political science at Swarthmore College and contributing editor at The Atlantic, latest book is The Right Way to Lose a War: America in an Age of Unwinnable Conflicts, “The Risks of Foreign Policy as Political Distraction,” The Atlantic, 6/15/2017, https://www.theatlantic.com/international/archive/2017/06/trump-diversionary-foreign-policy/530079/

But what about military force? To be clear, there is little cause to speculate that Trump plans to launch a full-scale war solely to distract attention. For one thing, as president, the worst possible time to start a major military campaign is when you’re deeply unpopular. And the political upside is shaky at best. Recent big wars in Afghanistan and Iraq were politically damaging to George W. Bush. Even victory doesn’t guarantee a pay-off, as George H. W. Bush discovered when he won the 1991 Gulf War and then lost his bid for reelection in 1992. A crisis may arise where there are real national-security rationales for fighting, along with potential domestic gains. Here, the payoff at home would likely enter Trump’s calculus, and even push him over the edge to fight, with the legitimate casus belli providing a shield of plausible deniability. The most tempting use of force may be a seemingly manageable, but still dazzling, kinetic operation, like a missile strike or a raid to kill terrorist leaders. Another option would be to escalate a crisis where an easy win seems available: The key is to find the right enemy, one that’s both widely hated and too weak to fight back. After all, there’s a well-established “rally ‘round the flag” effect, where almost any military crisis temporarily juices the president’s approval ratings. In the wake of Clinton’s airstrikes in 1998, one poll found that 68 percent of Americans approved of his foreign policy. Republican House Speaker Newt Gingrich said, “it was the right thing to do at the right time.”

### Sustainability---2NC

#### Structural factors

Haggith ’17 (David; economic analyst who predicted The Great Recession half a year before it hit, editor of The Great Recession Blog; 2/11/17; “The Inevitability of Economic Collapse”; <http://www.philstockworld.com/2017/02/11/the-inevitability-of-economic-collapse/>; Phil’s Stock World; accessed 7/7/17)

While I haven't had the privilege of divine revelation, I do try to look at the forces that are in play that have the power to move nations economically. Two dominant countervailing forces right now are those who have George Soros nearly in tears -- who make up the anti-global revolution -- and then all the globalists like Soros who are panicking that their new world order is being shredded accompanied by all the raging anarchists that Soros can sponsor as his mercenaries. There is some certainty here: globalists will not give up after decades of massaging and manipulating and cajoling the world in their pluralistic, globalist direction and so will wage battles everywhere they find people or candidates resisting their agenda. At the same time, those who are sick of globalism have risen up in Brexit and with Trump as their champion, and are not about to lie back down. So, conflict is certain for several years to come. That was an easy prediction for me to make earlier, and we're seeing it play out daily now that Trump is in 0ffice as president. Internal conflict tends to get in the way of commerce and so is likely to have economic impact. Within this milieu of daily conflict we have an economic structure in the US (and similarly in most of the rest of the world) that is so riddled with flaws that have not been fixed (and have even been made far worse) that it's collapse is inevitable even without conflict knocking up against it. A list of economic flaws that are too big not to fail Banks that were too big to fail are now much bigger than they were in 2008 and 2009. While banks may be a little more solvent at the moment, if failure comes, the risk to the overall economy is far worse than in 2008 and 2009. Banksters who destroyed the global economy were almost all rewarded with much larger bonuses, instead of thrown in jail, so they remain at large to wreck things again and even are enticed to strike again because it all worked out so well the first time; but we don't know where and at what time their corruption will cause their failure. What we do know, is that corruption drifts that way. Bailing out banks created exactly the "moral hazard" that many people warned about in 2009. As a result, one thing we do know is that bailed-out banks continued their derivative investments that caused many of the 2008 and 2009 failures. In fact, they increased their involvement in this perilous and poorly understood area of investment to such new heights that the number of derivatives in 2009 looks like an large city seen from earth-orbiting altitude -- a mere spot compared to all that can be seen now. Goldman Sachs, the most evil of all the companies that helped cause the global economic collapse, now has three high-level positions in the Trump administration, versus the one that it had in the Obama admin. It, in essence now oversees the whole US financial system -- the Fed, the National Economic Council, and the Treasury. Thanks to the revoking of Glass-Steagall, Banks are still allowed to invest in risky assets like stocks, and the Federal Reserve has even talked about investing directly in stocks as its next recovery plan, even though the revoking of Glass-Steagall played a major role in setting the US up for the Great Recession. Trump plans to roll back Dodd-Frank (Glass-Steagall's half-hearted replacement). That means there will be no correction to this serious economic aberration for a long time. Because the Fed can print infinite amounts of money at its own discretion and give it to banks or maybe even start investing it directly, there is no legal limit to how much the Fed and its member bank's can manipulate the stock market ... so long as the keep overall inflation (which doesn't count stocks) and jobs under control. So, for economic recovery, we're returning to the old tricks of banking deregulation to loosen up credit; we've all seen how beautifully banks policed themselves, as Alan Greenspan assured us they would. Likewise, we are returning to trickle-down economics, and are about to trump it up higher than under Reagan or GW Bush. We've had many years of trickle-down economics over the past thirty years, and clearly it has diminished the middle class and shifted wealth to the top one percent to where our market economy is now weaker because it was a well-off middle class that constituted that market. We've learned nothing! The national debt, which was completely absurd at $10,000,000,000,000 by the end of the Bush administration, has now doubled to $20,000,000,000,000, thanks to the Obama administration. Trump's infrastructure stimulus plan and military buildup are, so far, estimated to add somewhere between $5 trillion and $10 trillion to that debt over a decade. That means we'll likely continue Obama's $1 trillion annual deficit. Thus, we fully plan to keep continue the immoral game of spending all of the next generation's money to buy the things we need, build up our military and to fund our generous welfare to immigrants and other nations. We've learned nothing! Corporate debt has also increased to stratospheric levels, and that debt was a big part of what was keeping stock prices rising as companies created market demand for their own shares by buying them back, which also reduces supply to drive up prices. The stock market, which I believe is already a bubble, is ballooning in speculation of Trump's grand credit card (not because earnings have greatly improved, for those calculations look more jury-rigged than ever). Housing prices are back up to the same insane levels they reached in 2007 in most of the US, which could only be supported by loose terms of credit back then. The move back up to those prices has mostly been accomplished by resorting again to looser terms of credit. So, we're back in a housing bubble because real wages are no better now than they were then. (We learned nothing!) Banks continued to issue adjustable-rate mortgages, which we experienced as being safe when home values are rising, but devastating time bombs if home values fall so that people cannot refinance their way out of them when the interest increase hits. Home values have just started declining in several key markets, particularly at the top end, meaning some of those adjustable-rate mortgages bombs may be nearing their final ticks. Interest on all of that debt (housing, corporate, government) remains at historically low levels, but started rising at an historically rapid rate in the last few months, even without the Fed moving its targets, due in part to anticipation of the financing Trump will have to do to carry out his infrastructure plans. That's just domestically. Internationally, two of the oldest and largest banks in Europe keep teetering on the edge of collapse. All of Italy's banks are structurally unsound because they continue to carry the bad debt from the 2008-2009 financial collapse because they cannot afford to write it off. Greece is still walking the fine edge of bankruptcy. Spain, Portugal and Ireland look marginal at best. Trends determine ends These are all problems that are major trends. They are also all structural economic flaws that existed prior to 2007 and that contributed to the economic collapse that started in 2007 and became known by 2008 as the Great Recession. Nothing (or, at best, very little) has been done about them. Nothing is even being talked about being done about them in any serious way. Therefore, nothing is going to be done about them. In fact, all of these flaws are worse today than they were in 2008! That means they will continue to grow until they erupt in turmoil again. Exactly when I'm not as certain because the election changed things. Trumps stimulus plans on the national credit are so huge they are bound to create some temporary lift, but Trump and his cabinetful of bankster-barons are not going to be able to stop these numerous trends from crushing us. For one thing, Trump has expressed no plans to solve any of these overwhelming structural flaws that are trending against us, some of which are past solving (like the national debt). It is questionable he and his cabinet even believe they are important. Ultimately, his short-term stimulus will make some of the items on this list worse in the long term. Huge tax breaks for the rich will give some temporary economic boost if they ever make it through congress, but they will also create more economic disparity as the cost. That means more political conflict as the gap between the rich and the poor widens more quickly than we've ever seen before. The boost, if it happens, will also come at the cost of much more national debt. So, the longterm economic damage will be significant as it has been after all previous periods of trickle-down economics, marching us toward more debt and decline. The cabinetful of bankster-barons will not likely start putting banksters in jail. They will even less likely break up banks that are too big to fail. They will not put the Fed out of business or the nation back onto the gold standard. They will not likely put Hillary in jail. None of that is going to happen. Or, at least, very little of it. As it turns out, the first major wave of the Epocalypse that I predicted for 2016 turned out to be political -- a revolt against the establishment -- rather than economic. Now, the counter-revolution has begun as liberals start fighting back. While I certainly don't want the non-globalists to back down, you can be certain the globalist establishment isn't about to back down either. Efforts will intensify on both sides as the pressures above continue to build unabated, making 2017 a year of intensifying battles while the economic time bomb keeps ticking away because no one is paying attention to these structural flaws. We're too busy fighting over other things. If anyone doesn't think this is the Epocalypse, that's only because they started thinking too certainly that it would happen in a particular way and didn't note the caveats I gave along the way that said the exact order of events is unpredictable -- that an election year could change the timing -- but economic failure is assured, and the timing would not be long delayed.

#### Inevitable, unpredictable shocks

**Lechner et al. 16**. European Commission, Joint Research Centre (JRC), Institute for the Protection and the Security of the Citizen (IPSC). 10/01/2016. “Resilience in a Complex World – Avoiding Cross-Sector Collapse.” International Journal of Disaster Risk Reduction, vol. 19, pp. 84–91.

In a more and more globalized world we have created unprecedented connectivity, mainly by striving for better business opportunities. But with such a strong global connectivity, the risks associated have also changed: formerly local issues can now have global impact, and systems are often too complex to fully understand their interdependencies. In addition, the speed of change is increasing in many sectors of society and the economy. So we are building a future world with more and more interdependencies of which we understand less and less, and this process is accelerating sharply. This means that we are mixing together the typical ingredients for an upcoming crash, which in the worst case could mean the collapse of society as we know it. To avoid such a scenario, a coordinated effort of public authorities, civil society, industry, and academia will be required. 1. Introduction Predictions about the collapse of society are probably as old as society itself, but only in the last decades has mankind managed to approach – and sometimes even overstep – the planetary boundaries [1,2] in several dimensions, often irreversibly. The scientific approach of modeling human societies on the basis predator (mankind) and prey (planetary resources) [3], also points to the possibility of a large-scale collapse. We often reassure ourselves by noting that all the models used are based on assumptions, that they have many uncertainties, that they only approximate our highly complex reality. Critical analyses of the limits of modeling seem to confirm this [4], and we know that technical models clearly do not take into account our human ingenuity at getting ourselves out of difficulties – but is this reassurance reasonable? Even the assumption that we can define our own future within the planetary boundaries is questioned by critical voices like Russell [5], warning us against the belief in unlimited growth of exponential curves, and drawing drastic conclusions about the future of mankind. Nevertheless, our economic strategies seem to assume continuously greater efficiency in the future and even faster economic growth with literally no limit. This method of forecasting future development by extrapolation from the past is risky in two different ways. Firstly, it does not respect natural limits to growth. These may arise from the limited availability of resources, or from physical boundaries which seemed far away in the past, but now have come into reach. A good example for the latter is Moore's law [6], predicting in 1965 a doubling of the maximum number of transistors in integrated circuits every 12 months. This “law”, adjusted to 24 months in 1975 and confirmed as ‘not going to stop soon’ in 1995 [7,8], remained valid for some 50 years, but it is now at or near its limits [9], imposed by several paradigms of fundamental physics. Although completely new approaches might one day circumvent some of these limits [10], Moore's law simply cannot remain valid for another 50 years for integrated circuits as we currently know them. Secondly, a prediction based solely on experience from the past does not foresee unexpected and potentially disruptive events. The Fukushima nuclear disaster of 2011 and the global financial crisis of 2007–08 are prominent examples of sudden events ending high-flying hopes for controlled risk in energy supply or ever-increasing economic profits, respectively. Looking at the large number of fascinating growth stories from sources like digital industries, Chinese GDP, or investment banking profits, we tend to forget about the fate of the stars from the past when they reached their limits: US automotive industries, Canadian and European cell phone producers or Japanese efficiency champions all have in common that they could not maintain their excellent growth rates for eternity. We need to pay attention to the limits of growth very carefully when looking at the long-term resilience of our global society. 2. Objectives We will show that globalization and the digital revolution have led to more interdependencies, higher complexity and rapid acceleration of change in most sectors of our societies and economies. For this reason, the long-term resilience of a nation, a region or an industry cannot be considered any more as a confined matter that has little to do with the global environment. We will demonstrate by several examples from the recent years that interconnection, complexity and acceleration thereof as ingredients of globalization and digitization have increased the risk of major shocks, propagating not only inside but also across individual sectors, and to society as a whole. We will show that there are strategies to limit this risk but also show that these strategies could not have been implemented successfully so far in our current economically driven environment. During the discussion we will look at two important concepts which are relevant to resilience, but are not at the center of the attention of our growth-oriented efforts today: fairness, which is important to avoid tensions within societies, and risk transfer, which in many examples seems to flow from the better-informed expert stakeholders to the less-informed parts of our society. We make a number of suggestions as to how science can support policy decisions in a highly complex world. We also propose a radically different pattern of business incentives, aimed at taking some steps towards improving fairness, at decoupling economic growth from consumption and above all at making risk-taking at someone else's expense less attractive. 3. Methods Although there is abundant literature about resilience, sustainability and risk, there are very few scientific discussions of hyper-complex issues spanning multiple sectors of our societies, policies and economies. The notion of so-called post-normal science, introduced by Funtowicz and Ravetz [11], is a step in the direction of understanding complex systems at the borderline between science and policy, but it only gives theoretical backing rather than direct guidance. More on the practical side, Taleb [12] provides many important examples, including valuable considerations on the human inability to assess risks correctly in complex environments. The issue of the human mind often being misled is also underlined by Spiegelhalter [13], showcasing several disruptive events with economic or health impact. Because resilience and sustainability are typically discussed in communities focused on the business perspective (such as re-insurance companies), at the national level (governments), or in a particular community (e.g. the civil protection community), there is no obvious forum for a broader scale discussion at supranational level, connecting economic, political and societal dimensions. We started such a dialog on the work of the European Commission's Joint Research Centre (JRC), when around 2012 we realized that the typical crisis management activities are related to civil protection, but the predominant crisis of these years was the financial crisis, in which the JRC was performing completely different activities such as modeling the probabilities of bank failure or assessing the trends and issues in public finances of Eurozone Member States. From the idea of resilience cutting across sectors and being relevant in many places, we identified many sectors in society, policy and economy where resilience matters, and documented them in an overview report [14]. In a series of related workshops and conferences we discussed the facets of resilience with the stakeholder community and gathered valuable insights. In a 2014 workshop on 'Thinking the impossible' at the JRC in Ispra, Italy, we looked at risks that sound highly unlikely but could be devastating. At the Global Risk Forum 2014 in Davos we ran a dedicated session on risks across sectors of society. At the European Climate Foundation in Brussels early 2015 we followed up on the matter, and at a big conference of the European Commission in September 2015 (also in Brussels) we had a plenary presentation on resilience, complexity and risk across sectors of society. Finally, in joint session of the International Council of Science (ICSU) and the JRC at the World Science Forum of November 2015 in Budapest we discussed resilience in a changing world. The findings and conclusions of these workshops and conferences are presented in this article. 4. Results 4.1. Increased dependencies across sectors Crises can spread globally, and in our modern world they can easily also impact business sectors that at first glance do not seem exposed. In the following section we will show examples of how effects can hop from the digital world into the finance sector, from finance to government, on to geopolitics, to energy and finally to societal stability. The related damage in each hop amounts to several billions. Although the examples listed are not connected, in the future we might see cross-sector cascading effects. 4.1.1. From digital to finance In the digital world, computer viruses can cause damages in the millions, but these damages are usually distributed over a very large number of users and businesses. Other digital risks strike more centrally: high-speed trading algorithms, making autonomous decisions at the stock exchanges in milliseconds, caused the so-called flash crashes at the New York Stock exchange in 2010 and at the Singapore stock exchange in October 2013, with the latter reportedly wiping out 6.9bn USD [15]. It took more than four months to analyze the reasons behind the 15-min New York crash, and the report by the US authorities came to the conclusion that there was no clearly identifiable root cause that sparked the crash. They considered the events 'an important reminder of the inter-connectedness of our derivatives and securities markets' and stated that they 'clearly demonstrate the importance of data in today's world of fully-automated trading strategies and systems'[16]. Although many stocks rebounded right after the dip, the reaction of software algorithms could easily have ruined companies, and in Singapore some stocks lost 87% of their value. Safeguards were consequently installed in the systems of the stock exchanges, but other unpleasant and new surprises might come from different directions: high-frequency trading, for instance, can be vulnerable to the effects of solar storms [17], but not all financial institutions are aware of these very indirect effects: originating on the surface of the sun, solar outbreaks can create electromagnetic disturbances strong enough to take out the GPS signal, which is widely used for time synchronization in financial trading. 4.1.2. Financial to economic After the collapse of Lehman Brothers in 2008, a major shock went through the US banking system. Not only the US housing market had gone sour, but credit default swaps had been spread all over the globe – and a cascade of repackaged and distributed risk started, jumping the Atlantic Ocean easily and hitting EU banks. Some of these were hit so hard that they had to be bailed out by their governments, so the risk continued in the governments. Some EU governments needed central support, and the EU used the opportunity to overhaul its financial system. Nevertheless, the governments of eleven EU Member States resigned or were ousted over the crisis, some of them several times (Latvia and the Czech Republic in 2009, Ireland, Portugal, Greece, Italy and Spain, in 2011, Romania, the Netherlands, and Italy again in 2012, Slovenia in 2013, Italy a third time and France in 2014 and Portugal in 2015). The link between the US banking sector and EU government stability is obvious in hindsight, but very few if any observers had noted it before 2007. More obvious is the link from government to geopolitics. The Arab Spring gave rise to unstructured power relations and laid the ground for extremism and radicalism. Ukraine's attempt to sign an association agreement with the EU led to massive demonstrations and a regional political crisis, including a (civil) war. The civil war in Syria, ongoing since more than five years, has destroyed stability and economy in the region. And we recently saw in the gas supply discussions between Russia, Ukraine and the EU that geopolitics links to energy. It took a well-prepared last-minute effort to conclude a gas supply deal, which finally was agreed only shortly before winter, during the last days of October 2014. 4.1.3. Energy to society Energy is at the core of the economic development of many countries, and the power grid has become an indispensable critical infrastructure. A fictional but well-researched scenario on what the world would look like after a widespread collapse of the power grid is available in the book by Elsberg [18]. Elsberg considers an IT-based collapse, but that is not the only hazard to the power grid: several reports and studies on severe space weather suggest that this too could cause major damage, up to USD 2.6 trillion in the first year in the US alone [19,20]. In addition, energy has an obvious relation to climate policies, to the real economy and even to digital processes: modern computing centers depend on energy availability, and new digital concepts like the blockchain [21] of the bitcoin currency even exploit the obstacle of not being able to calculate highly complex matters without consuming significant energy [22]. There are numerous other examples where sectors that were reasonably independent in the past are now coupled across the globe. E. coli contaminated food traveled all across Europe. Pandemics like SARS or bird flu spread through intercontinental travelers. Ebola cases were spread by infected passengers from Africa to Europe and to the US; the disease was only contained through a major international initiative. All these examples show clearly that not only has the interrelation between sectors increased, but also the complexity of interdependencies in financial markets, of energy grids, of high-speed trading algorithms, of the food chains, of environmental changes and of global travel has grown hugely. Indeed, in many cases we only perceive these interdependencies after a major perturbation, and there is no agreement on what body or institution has the responsibility for identifying, monitoring, and controlling the risks created. The context of change is formally given a global perspective by the Global Risks Report 2016[23], which draws attention to ways global risks could evolve and interact in the next decade. The top five global risks in terms of likelihood are ranked to be: 1. large-scale involuntary migration; 2. extreme weather events; 3. failure of climate change mitigation and adaptation; 4. interstate conflict with regional consequences; and 5. major natural catastrophes. The report's Global Risks Interconnectedness Map 2016 shows strong interconnections across sectors, e.g. between environmental and societal risks (failure on climate change and water crises), but also across societal, geopolitical and economic risks (with strong links from state collapse to migration and between social instability and unemployment). 4.2. Increased complexity of systems and processes The financial crisis has brought to our attention that the lending relations in the interbanking market have become highly complex [24], which decreases systemic resilience. Haldane and May [25] identify modularity as a key feature for the topology of a stable financial system, as it helps limit contagion. Typically, one would expect that a good connectivity in financial networks allows for a sound distribution of risk, but Battiston et al. [26] have shown that in the presence of a financial accelerator (which we clearly had in the financial crisis, where the robustness of an entity was strongly assessed on the basis of its past trend) this only holds until a certain threshold is reached. Over the threshold, additional connectivity turns counterproductive and creates a pernicious feedback loop, increasing individual and systemic risk. The situation during the financial crisis was even worse than that depicted by the theoretical approaches. Little was known about the real connectivity in the banking system. Rumors about new candidates for bankruptcy were traveling fast, and the biggest unanswered question about the distribution of debt was literally: 'Where is the money?' In addition, banks were rushing to pass on questionable debt for as long as it was still possible, creating a dynamism which could not be controlled easily. The failure to understand the complexity of the market is perhaps depicted most prominently by the fact that the German KfW Bank transferred 320 million Euros to Lehman on Monday, September 15th, 2008, the very day Lehman collapsed. Luckily for the KfW, the majority of the sum was recovered later [27]. But the financial markets are just one example of a sector that has become so complex that we simply do not understand it anymore. The fact that we have also lost track of the details of our food chain became obvious when in 2011 the European E. coli bacteria outbreak caused several fatalities in Germany and beyond, and a frantic search for the origin started. Due to the precautionary principle, also suspect traces had to be addressed, resulting in Spanish cucumbers being wrongly identified as contaminated with E. coli. This led to reported weekly Spanish losses of 200 million Euros [28] due to the decline in consumer trust, whereas finally bean sprouts of completely different origin were identified as the root cause for the E. coli outbreak, although even this was contested. The issue showed how little we know about the origin and stopovers of our food. Another less damaging but unexpected complexity could be observed after the Fukushima nuclear disaster, when Ford Motors in the US and other international car makers could no longer produce models in a particular metallized black [29] due to a shortage in the Xirallic® pigment, produced by Merck plant near Fukushima, which had been affected by the catastrophe. (Note that strong impact from Fukushima also arrived on the other side of the planet, when the German government issued its Energiewende policy to abandon nuclear power as a consequence of the disaster in Japan.) This example shows that it is not only in the food sector that the complexity of supply chains has grown beyond our comprehension. The power grid is another infrastructure which has become so complex that we do not fully understand it anymore. On 4 November 2006, the cruise ship Norwegian Pearl was planned to make its way on the German river Ems to the North Sea, requiring a shutdown of a 380 kV power line across the river for safety reasons. Although a routine operation, this shutdown resulted in cascading effects all across Europe, leaving an estimated 15 million households in Germany, France, Italy, Belgium, Spain, and Portugal without power for more than an hour [30]. These examples show that our technologically driven world has developed structures and processes that cannot be fully understood or easily modeled anymore. Even if we had the time to carefully analyze this, it would not be very helpful: reality is moving on, and complexity is added on a daily basis. In a competitive world with tightly fought margins we cannot expect the complex processes to be stable over time. The opposite is true: the speed of change is even increasing in many domains. 4.3. Acceleration of interconnectedness and complexity The exponential growth of Moore's law has boosted performance and minimized the size of microelectronics. The availability of ever smaller and more powerful digital technologies has also accelerated other areas such as climate modeling, agriculture, industry automation, material sciences, genetics, economic assessment, finance, transport, construction and many other sectors. In addition, modern information technology has created a wealth of business opportunities for the digital economy. Smartphones put the information of the internet at our fingertips, social networks arose, satellite navigation systems helped with orientation and timing, digital imaging and new sensors gave us a better picture of the world, and all of these results can be joined into what we call big data. In December 2015 the international science community, Science International, published a joint statement, on Open Data in a Big Data World: An international accord[31]. They identified the opportunities and challenges of the data revolution as today's predominant issue for global science policy and proposed some fundamental principles, noting that the scientific community has a distinctive voice. The acceleration of all of these sectors has also changed many business models, which has two negative consequences for the resilience of modern society. Firstly, there is a stronger dependency of almost all of the processes of our daily life on very few players, and secondly – though associated to the first effect – we can observe a more and more uneven distribution of profits, leading to tensions in societies. Dependency has been created by new concepts such as Information as a Service (IaaS) or Software as a Service (SaaS), binding customers to suppliers in a far stronger way than the traditional model of producing and selling. Ten years ago we would buy a CD and own it, whereas today we need to sign up to music platforms which provide us with the desired content – and monitor our behavior continuously. The associated business models are pushing into other sectors of industry. Traditional companies in the automotive sector have to face competition from IT companies developing autonomous driving, thereby harvesting even more data. E-books are so convenient that hardcover and paperback revenues are sharply declining, non-digital photography has almost disappeared and smart phone apps are replacing travel agencies and taxi companies. This digital acceleration might be creating more choices for the customer, but comes at the price of dependency on very few digital players. In addition to this dependency, which is detrimental to resilience, there is a mid-term issue with wealth distribution: the agreed measure for macroeconomic growth is still GDP, which does not contain any fairness component. So we are striving for economic growth, sometimes also for inclusive growth, but not necessarily for a fair distribution of growth. An example illustrates the differences: from 2007–2015, a period covering the financial crisis, the OECD countries on average experienced moderate growth in terms of GDP [32], but the general aggregate is not telling a lot. The GDP per capita of different countries developed quite differently, and in 2015 Germany and Greece were at 107.65% and 76.75% of their 2007 values, respectively. This created significant political tensions, and is not expressed in monitoring the aggregate OECD total (which is 106.45%). But the problem also exists at national level: the majority of EU households might not agree on having experienced any economic growth since 2007, but would rather recall austerity measures, income cuts, and tax increases. The growth measured must therefore have arrived in other places – but we do not have detailed, up-to-date statistics on this. Some evidence originates from a study [33] of the European Central Bank (ECB) in 2013, comparing the mean and the median values of household wealth in the Eurozone and coming to the conclusion that fairness has suffered. Germany's households, for example, are on average (mean) comparably well-off, but the difference between the mean household wealth and the median one is the largest in Europe, indicating significant unfairness in the detailed distribution. A very clear analysis of the ECB study can be found in [34]. In addition to potential tensions in society, the risky business models leading to uneven distribution are undermining resilience even further. We were reminded during the financial crisis that our modern world is targeted at short-term profit, possibly at the expense of the system, and that governments have to intervene if society is not to end up paying the price of excessive risk taking by comparably few market players.. This strategy of leaving behind the risk for the bank (or afterwards for the government and for society) should have been known well since February 1995, when Barings Bank, the oldest UK merchant bank, was brought down by a single rogue trader [35]. But in a fierce global competition every penny counts, and we cannot expect our job-creating entrepreneurs to give way to competitors for fairness's sake. Production lines of companies are transferred for profitability reasons from Central Europe to Eastern Europe, later to China and from there to Vietnam. Domestic jobs are lost and costs are being saved, while dependencies rise and unfairness increases. So a certain share of the digital revolution may just be a silent conversion of thousands of jobs into an enormous cash flow towards the few big digital shareholders. The evolution of wealth distribution in the US is very telling, and the perceived rule of billionaires has even been exploited with some success by Bernie Sanders in his 2016 US presidential candidature campaign for the Democrats. Europe also needs to monitor its trends very carefully. The situation of many young Greek graduates without a job, in combination with loopholes for the wealthy in the national tax regime (or its enforcement) has already created massive tensions, led to government changes and to discussions with EU partners, put pressure on EU solidarity and weakened EU resilience during the financial crisis. 5. Discussion 5.1. Current situation When analyzing the resilience of our modern and complex society, we start from the UNISDR Terminology on Disaster Risk Reduction [36], defining resilience as 'The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions.' The United Nations’ definition has an important addendum, expressed by the following note: 'Resilience means the ability to “resile from” or “spring back from” a shock. The resilience of a community in respect to potential hazard events is determined by the degree to which the community has the necessary resources and is capable of organizing itself both prior to and during times of need'. This notion of springing back from a shock is nicely expressed as 'Why things bounce back' by Zolli and Healy [37], who formally define resilience as 'the capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances'. For a resilience assessment we therefore need to understand both the change we are exposed to and our capability to cope with it. Are we already living in dramatically changed circumstances, are dramatic changes just ahead of us, or will there be a dramatic change only at a more distant point in the future? Comparing the world of today with the world in the late 1980s, we can see huge differences, e.g. in globalization and in digitization, but there are also many areas that have remained comparably stable, such as peace in Central Europe, the economically strong position of the US, the mechanisms of the United Nations, or the simple fact that the majority of our cars still run on four wheels and are fueled by hydrocarbons. Dramatic changes there have been, but often not arriving with a big bang, but silently inserting themselves into our daily lives (e.g. the internet). The process is continuing and accelerating. Our capacity to 'bounce back' – or more formally to cope with dramatic change – is also difficult to assess. There is no formally agreed measure for resilience that could serve as a benchmark, but we have created powerful political processes to cope with change globally, such as the Sustainable Development Goals [38], the Paris Climate Agreement [39], or the global Sendai Framework for Disaster Risk Reduction 2015–2030 [40]. The latter includes in its Priorities for Disaster Risk Reduction, the statement 'Enhancing disaster preparedness for effective response, and to ‘Build Back Better’ in recovery, rehabilitation and reconstruction'. The Sendai Conference included a session on Disaster Risk in the Financial System which concluded that, by 2020, 1-in-100 and 1-in-20 risk analyses should be developed to enable the understanding of levels of resilience across all capital and support the adoption of standards by global regulators. These international agreements were all made in 2015 but it is notable that all of these instruments and procedures were the culmination of decades of work. The Paris agreement (called COP21 because it was signed at the 21st annual meeting of the Conference of the Parties of the UNFCCC) was preceded by the Kyoto [41] climate agreement of 1997 and its Doha amendment [42] of 2012. The Sendai Framework was preceded by the 2005 Hyogo Framework for Action [43]. The sustainable development goals were preceded by the original Millennium Development Goals [44] of 2000. Altogether, the international community has been working on resilience for at least 20 years in quite a determined way. Nevertheless, while global agreements on resilience and sustainability have been concluded over the last 20 years, the exploitation of resources has continued, and our remaining planetary reserve has been depleted more and more. Significant economic development took place and growth was achieved in many regions of the world, including places like China, Brazil, India and South Africa, the OPEC countries, Southeast Asia, but also in Europe, Australia and in North America. However, much of this growth was accompanied by massive exploitation of natural resources, often associated with major catastrophes. Offshore drilling created disasters like the Deepwater Horizon incident with an estimated settlement of approximately $7.8bn [45]. Massive irrigation caused a significant loss of natural water reservoirs and dried out the Aral Sea [46], and biodiversity is decreasing at a speed that made Chapin et al. [47] request the establishment of a new international body to assess changes in biodiversity already in 2000. Our complex technology has created nuclear incidents with global impact, such as the Fukushima meltdown in 2011. Even our technological progress in successfully exploring space has left so much space debris behind that it will jeopardize the success of future missions, and Hall states in [48]'… the space community is realizing that the failure to solve the problem would be disastrous.'. The role of media in these changes is complex, but important. On the one hand the mass media, often powered by an explicit political agenda, can choose to sensationalise some aspects of global risks while concealing others, thereby aggravating the problem and making it more difficult for society to find solutions; on the other hand the media – especially modern social media – can create awareness and encourage solutions. In modern democracies there should be no compromise with the principles of free speech, even where the effect may be destructive; but responsible media leaders, journalists and other commentators can be encouraged to understand the risks and help towards mitigating them. Other important factors are known but cannot be reliably predicted: the geopolitical power balance, the strength of the influence of supranational organizations and institutions, or the power of the civil society play an important role when assessing the risk of societal collapse. The authors acknowledge that these factors – as well as other drivers such as cultural, religious or historical developments – should be considered in a comprehensive assessment but go beyond the scope of this article. 5.2. Key questions Starting from the above definitions, the key questions when looking at the resilience of our current societies are (i) how much flexibility do we have left, and (ii) how can we carry on from today. It seems particularly with regards to global energy needs that whatever coping capacity is left on our planet (e.g. shale gas or nuclear fusion energy) will either be exhausted very soon or contribute to a further acceleration of the negative effects. Therefore, unless we can decouple growth from the use of resources, we are heading for, at worst, a crash, or at best an unpleasant downward spiral, even though currently the slope is still pointing up. Ehrlich [49] concludes that our modern society has a different risk of collapse than former societies which collapsed locally or regionally only. He claims that complex, multi-level systems may be better able to cope with complex, multi-level problems, but we fear that this statement only holds up to a point where the complexity of systems itself becomes an additional risk. Carrying on from today is even more difficult. Our short-term thinking often limits our vision to the next few years, and although we could still change course, we rather exercise ourselves in denial and promises of continuous and never-ending growth, missing the point that even the growth we are experiencing today is more and more unfair and therefore already eroding our social solidarity and, as a consequence, our resilience. Diamond [50] has analyzed the differences between today's dangers and the dangers that past societies faced, and identified twelve main problems specific to the world of today, including inequality. He also researched why many of the formerly ruling societies failed to recognize that big problems were looming up before they fell, and concludes that this reflex of denial has not changed over the centuries. We enjoy the speed and acceleration – but can we distinguish between the thrust of the engine and the free fall as we go over the cliff? Currently we simply try to outperform each other on speed, and leave it at that. The interconnectedness, complexity and acceleration of our modern society have brought us to the limits of exponential growth and have simultaneously exhausted the resources of the planet in several dimensions, weakening our resilience. To capitalize on what is left of it, a major rethink in society is required. In a fierce global competition such reconsideration will clearly not happen on its own, but needs to be accomplished by the right incentives to avoid unnecessary interconnectedness, reduce systemic complexity and slow down an acceleration that cannot be maintained forever anyway. But how can we achieve this? Key elements for accomplishing this challenge will be decoupling growth from consumption, introducing more fairness into the system and identifying and mastering risk. Especially this last requires a better understanding of risk in our complex systems, especially if there is a risk of major systemic failure. In addition, we need to prevent the transfer of systemic risk to less knowledgeable stakeholders (the general public, the taxpayer, etc.) not connected with the original transaction in which the risk was created. 5.3. Suggestions for a way ahead We therefore suggest three initiatives to lay the ground for an economy and society aiming at sustainable wealth rather than chasing for unrealistic never-ending growth, turning from a continued depletion of resources to a resilient continuum. The initiatives are not meant to suffocate or kill the economy but to move it rapidly from a destructive and short-term mode to a long-term healthy equilibrium. This might sound ambitious, and might be perceived as threatening by the homo economicus of our modern days, but any profit-oriented activity has long had to consider political side constraints, and moving the incentives to different objectives will only regulate markets in the desired direction, not abolish them or move to socialism. History shows that with the right incentives a single human generation is sufficient not only to turn the mindset of modern society but also to create a highly competitive technology position in the markets. Between 1970 and 2000, environmental thinking in Europe and in the US was fostered by regulators, civil society and industry altogether, and created new markets and green growth to the benefit of nature. Another example, still ongoing, is the global effort on CO2-reduction and climate change agreements, which started roughly 15 years ago and has made significant progress with the COP21 agreement of 2015. Science will have to play an important role in this respect, and a number of international initiatives with scientific involvement have already been started in the related area of sustainability. The International Council for Science (ICSU), UN agency partners and other non-governmental organizations including the International Social Sciences Council, Sustainable Development Solutions Network and Science and Technology in Society Forum, with the World Business Council for Sustainable Development (WBCSD) as an observer, have created a new global research program Future Earth: Research for Global Sustainability[51]. The goal is to provide the knowledge required for societies in the world to face risks posed by global environmental change and to seize opportunities in a transition to global sustainability. The Integrated Research on Disaster Risk Programme (IRDR) [52] (focusing on 'natural' hazards) is another approach to research on disaster risk through an international, multidisciplinary (natural, health, engineering and social sciences) collaborative programme. The Program has created IRDR International Centres of Excellence such as one on Vulnerability and Resilience Metrics and another on Disaster Resilient Homes, Buildings and Public Infrastructure. Another newly-started research programme, recognizing the importance of the urban scene and health is Urban Health and Wellbeing[53], which is an interdisciplinary research effort whose overall aim is to generate policy-relevant knowledge that will improve health status, reduce health inequalities and enhance the well-being of urban dwellers. It will focus on systems approaches to address the complexity of urban issues and their influence on health. The International Council for Science is working with UN agencies to bring together the science from these three international research programs in an integrated way to provide advice to the Climate Convention, the Sendai Agreement, the Sustainable Development Goals and other international issues. The next thirty years should be sufficient time to instill a sustainability and resilience philosophy into policies, civil society and the economy – turning from unfair growth to healthy growth. The start of any such initiative could even bring direct economic benefits: The World Business Council for Sustainable Development identified significant business opportunities in sustainability, and underlines the importance of being first in the green race [54], and first business models in creating a sustainable future have already emerged [55]. This means we have arrived at a point where not acting might make us fall behind. With the right political, economic and societal incentives, resilience will pay off, whereby it will no longer be economically viable to go for extreme risks (as the consequences could not be passed on to others). The following three suggestions by the authors are meant to support a sustainable and resilient society, and are derived from the analysis above: (1) Cut down interdependencies by putting incentives to avoid business models which – create unnecessary global interdependencies, – do not create local jobs (or no jobs at all), – force people to move, – limit customer choices and flexibility without a need, – exploit the weakest parts of society. (2) Reduce complexity by putting incentives to avoid business models which – create unnecessarily complex procedures, – transfer risk into remote places, to the taxpayer, or to less knowledgeable parties – gamble on rights not being enforceable, – exploit taxation loopholes or taxation enforcement weaknesses. (3) Stop the acceleration of interconnectivity and complexity by putting strong economic incentives for simple business models creating local or community benefit. Research can make a major contribution to setting the right incentives, as nowadays many traditional concepts are not fit for purpose, and new ways of measuring resilience, fairness and sustainability need to be established. We therefore suggest developing a scientifically solid measure for fair GDP (FGDP) as an internationally acknowledged benchmark for growth to avoid extreme inequality and tension in societies. In addition, initiatives to measure resilience of societies in their multidimensional facets, trying to identify drivers of fragility as well as tipping points for slowly increasing instability, are recommended. 6. Conclusion The world has come to an unprecedented status of interconnectedness and complexity, both growing at an enormous speed, and it urgently requires a transition from short-term thinking to sustainable resilience. Such a change needs to be triggered by the right political, economic and societal incentives. There are clear ways ahead, but they need to be accompanied by organized support from the stakeholder groups involved. It will require a joint effort of public authorities, civil society, industry, and academia to lead the global transition towards a resilient society, offering fair long-term growth in a healthy and sustainable societal equilibrium.

#### Holistic modelling

Hickel and Kallis 19 (Jason Hickel - Professor @ Goldsmiths University of London specializes in development, finance, democracy, violence, and global political economy, PhD in Anthropology at the University of Virginia. & Giorgos Kallis- ICREA Professor in Environmental Sciences, PhD in Environmental Policy and Planning from the University of the Aegean in Greece , 4-17-2019, Taylor and Francis, “Is Green Growth Possible?” <https://doi.org/10.1080/13563467.2019.1598964> accessed: 7-14-2019 \*\*graphs are in the middle of text due to their placement in article, but I completed separated words and removed fragments) //bp

Carbon Emissions – Is Growth Compatible with the Paris Agreement? Unlike with resource use, there is a steady long-term trend toward relative decoupling of GDP from carbon emissions, and we know that absolute reductions in carbon emissions are possible to achieve. When it comes to climate change, however, the objective is not simply to reduce emissions (a matter of flows), but to keep total emissions from exceeding specific carbon budgets (a matter of stocks). For green growth theory, then, the question is not only whether we can achieve absolute decoupling and reduce emissions, but whether we can reduce emissions fast enough to stay within the carbon budgets for 1.5°C or 2°C, as per the Paris Agreement, while still continuing economic growth. A number of high-income countries have seen declining emissions in the twenty-first century, despite continued economic growth. Figure 4(a) shows declining emissions in the US and EU28, in both territorial and consumption-based terms, from 2006 to 2016 (i.e. absolute decoupling). However, emissions from the global South have continued upward, albeit at a slower rate than GDP (i.e. relative decoupling). China’s emissions declined slightly between 2014 and 2016 (a brief period of absolute decoupling), before growing again in 2017. On a global level, CO2 emissions have increased steadily, falling only during periods of economic recession (Figure 4(b)). Global emissions did level off in 2015 and 2016 while GDP continued to rise, prompting the International Energy Agency, a research arm of the OECD, to announce ‘Decoupling of global emissions and economic growth confirmed’ (IEA 2016), while media outlets celebrated ‘peak emissions’ (Meyer 2016). This news briefly came to constitute a key element of optimistic green growth narratives, until global emissions began to rise again in 2017 (1.6 per cent) and 2018 (2.7 per cent). Analysts attribute the temporary plateau to a shift in China away from coal and (mostly) toward oil and gas, and a shift in the US to natural gas.5 Once these shifts were complete, continued economic growth drove emissions up again. Overall, global carbon productivity has been slowing. World Bank data shows that carbon productivity (CO2 per 2010 $US GDP) improved steadily from 1960 to 2000, with decarbonisation happening at an average rate of 1.28 per cent per year (relative decoupling). However, from 2000 to

Chart

Description automatically generated

2014 there was no improvement in carbon productivity – in other words, not even relative decoupling has been achieved in the twenty-first century.6 High-income nations have done better, at least in terms of territorial emissions (the World Bank does not track consumption-based emissions), but even so progress has slowed, from an average rate of 1.91 per cent per year from 1970 to 2000, down to 1.61 per cent per year from 2000 to 2014. Existing trends are incompatible with the Paris Agreement targets. Business-as-usual is set to lead to 4.2°C of warming (2.5°C to 5.5°C) by 2100. Even with the Nationally Determined Contributions and Intended Nationally Determined Contributions under the Paris Agreement, global warming is still projected to reach 3.3°C (1.9°C to 4.4°C) – an improvement over the BAU scenario but still far exceeding the 1.5°C and 2°C thresholds.7 In order to keep warming below these thresholds, the world will have to make much more aggressive emissions reductions. The IPCC’s Fifth Assessment Report (AR5) includes 116 mitigation scenarios that are consistent with Representative Concentration Pathway 2.6 (RCP2.6), which offers the best chances of staying below 2°C. All of these scenarios are green growth scenarios in that they stabilise global temperatures while global GDP continues to rise. Rising GDP is a built-in feature of the Shared Socio-Economic Pathways (SSPs), which form the basis for the IPCC mitigation scenarios (Kuhnhenn 2018). AR5 warns, however, that these scenarios ‘typically involve temporary overshoot of atmospheric concentrations’ and ‘typically rely on the availability and widespread deployment of bioenergy with carbon capture and storage (BECCS)’ (2014, p. 23). Indeed, the vast majority scenarios for 2°C (101 of the 116) rely on BECCS to the point of achieving negative emissions.8 BECCS entails growing large tree plantations to sequester CO2 from the atmosphere, harvesting the biomass, burning it for energy, capturing the CO2 emissions at source and storing it underground. Relying on these ‘negative emissions technologies’ allows for a much larger carbon budget (about double the actual size) by assuming that we can successfully reduce global atmospheric carbon in the second half of the century. BECCS is highly controversial among climate scientists. It was first proposed by Obersteiner et al. (2001) and Keith (2001) at the turn of the century. IPCC modelling teams began including it in their scenarios from 2005, despite having no firm evidence of its feasibility. With the publication of AR5, BECCS was enshrined as a dominant assumption. Obersteiner has expressed alarm at the rapid uptake of his idea; he considers BECCS to be what he calls a ‘risk-management strategy’, or a ‘backstop technology’ in case climate feedback loops turn out to be worse than expected, and says the IPCC has ‘misused’ it by including it in regular scenarios to take pressure off of conventional mitigation pathways (i.e. emissions reductions) (Hickman 2016). In Keith’s (2001) initial formulation of the idea, he noted that while ‘measured use’ of biomass could help mitigate environmental problems, ‘large scale use of cropped biomass will not.’ Anderson and Peters (2016) point out that the ‘allure’ of BECCS is due to the fact that it allows politicians to postpone the need for rapid emissions reductions: ‘BECCS licenses the ongoing combustion of fossil fuels while ostensibly fulfilling the Paris Commitments.’ There are a number of concerns. First, the viability of power generation with CCS has never been proven to be economically viable or scalable; it would require the construction of 15,000 facilities (Peters 2017). Second, the scale of biomass assumed in the AR5 scenarios would require plantations covering land two to three times the size of India, which raises questions about land availability, competition with food production, carbon neutrality, and biodiversity loss (Smith et al. 2016; Heck et al. 2018). Third, the necessary storage capacity may not exist (De Coninck and Benson 2014, Global CCS Institute 2015). Anderson and Peters conclude that ‘BECCS thus remains a highly speculative technology’ and that relying on it is therefore ‘an unjust and high stakes gamble’: if it is unsuccessful, ‘society will be locked into a high-temperature pathway.’ This conclusion is shared by a growing number of scientists (e.g. Fuss et al. 2014, Vaughan and Gough, 2016, Larkin et al. 2017, Van Vuuren et al. 2017), and by the European Academies’ Science Advisory Council (2018). It is not clear that we can justifiably rely on BECCS, an unproven technology, to underwrite green growth theory. If we accept this point, then we must return to asking whether it is possible to maintain growth without relying on BECCS to stay within the carbon budgets consistent with the Paris Agreement. Without BECCS, global emissions need to fall to net zero by 2050 for 1.5°C, or by 2075 for 2°C.9 This entails reductions of 6.8 per cent per year and 4 per cent per year, respectively (Figure 5). Theoretically, this can be accomplished with (a) a rapid shift to 100 per cent renewable energy to eliminate emissions from fossil fuel combustion (Jacobson and Delucchi 2011); plus (b) afforestation and soil regeneration to eliminate emissions from land use change; plus (c) a shift to alternative industrial processes to eliminate emissions from the production of cement, steel, and plastic. The question is, can all of this be accomplished quickly enough? Only 6 of the 116 scenarios for 2°C in AR5 exclude BECCS. These work by assuming ‘optimal full technology’ in all other areas, plus mass afforestation, and with high mitigation costs. These represent theoretically possible pathways, but without any empirical evidence as to their feasibility. Results of empirical studies are not promising. Schandl et al. (2016) model what might be achieved with aggressive mitigation policies, without relying on BECCS. Their high-efficiency scenario has a carbon price starting at $50 per ton (rising by 4 per cent per year to $236 by 2050) plus a doubling in the material efficiency of the economy due to technological innovations (improving from a historical average rate of 1.5 per cent per year up to 4.5 per cent). Schandl et al provide no evidence for the feasibility of the efficiency improvements that they assume. Even so, the result shows that with global growth of 3 per cent per year, annual emissions plateau to 2050 but do not decline. In this scenario,

Chart, radar chart

Description automatically generated

growth in energy demand outstrips the rate of decarbonisation, violating the carbon budgets for 1.5°C and 2°C. The International Renewable Energy Association (IRENA 2018) have modelled a scenario for continued GDP growth compatible with 2°C by relying on a rapid shift to renewable energy (consistent with Jacobson and Delucchi 2011). The scenario requires adding 12,200 GW of solar and wind capacity by 2050, with a dramatic increase in installation rates (2.3 to 4.6 times faster than the present).10 The scenario also requires that the energy intensity of the global economy falls by twothirds (by 2.8 per cent per year, double the historical rate), lowering energy demand in 2050 to slightly less than 2015 levels.11 This is feasible inasmuch as the transition to wind and solar itself improves energy efficiency (Jacobson and Delucchi 2011).12 Still, even this optimistic scenario accomplishes only 90 per cent of the necessary emissions reductions for 2°C (likely because it pays no attention to emissions from land use change and cement production). The model relies on negative emissions technology to cover most of the remainder. Van Vuuren et al. (2018) consider ‘alternative pathways’ for meeting the Paris Agreement targets without relying on widespread use of negative emissions technologies. They model rising GDP in accordance with SSP2. In addition to a carbon tax and other aggressive mitigation strategies, their optimistic scenario includes the following settings: global population peaks at 8.4 billion in 2050 and declines to 6.9 billion by 2100; meat consumption declines 80 per cent by 2050; all new cars and airplanes are efficient from 2025; the world shifts to the most efficient technologies for steel and cement production, etc. Even with these highly optimistic assumptions in place, they find that the pressures of continued growth drive emissions to exceed the carbon budgets for 1.5°C and 2°C, without negative emissions technologies. Another way to approach this question is by looking at projected rates of decoupling. If we assume global GDP continues to grow at 3 percent per year (the average from 2010 to 2014), then decoupling must occur at a rate of 10.5 per cent per year for 1.5°C, or 7.3 per cent per year for 2°C. If global GDP grows at 2.1 per cent per year (as PWC predicts), then decoupling must occur at 9.6 per cent per year for 1.5°C, or 6.4 per cent per year for 2°C. All of these targets are beyond what existing empirical models indicate is feasible. The Schandl et al model indicates that decoupling can happen by at most 3 per cent per year under optimistic conditions. Other models arrive at similar conclusions. Before adopting BECCS assumptions, the IPCC (2000) projected decoupling of 3.3 per cent per year in a global best-case scenario. The C-ROADS tool (developed by Climate Interactive and MIT Sloan) projects decoupling of at most 4 per cent per year under the most aggressive possible abatement policies: high subsidies for renewables and nuclear power, plus high taxes on oil, gas and coal. All of these results fall short of the decoupling rate that must be achieved if the global economy continues to grow at expected rates. Holz et al. (2018) find that if we rule out widespread use of negative emissions technologies, the required rate of decarbonisation for meeting the Paris Agreement is ‘well outside what is currently deemed achievable, based on historical evidence and standard modelling.’ The challenge is even more difficult for rich nations. Anderson and Bows (2011) have modelled the emissions reductions necessary for achieving a 50 per cent chance of staying under 2°C (more relaxed than the two-thirds chance that the UNFCC calls for), without BECCS. They proceed from the principle of ‘common but differentiated responsibility’, whereby rich nations (Annex-1 nations) make more aggressive emissions reductions than poor nations, owing to their greater historical responsibility for emissions and their greater capacity for managing the costs of transition. They assume that Non-Annex 1 nations defer peak emissions until 2025, and thereafter reduce emissions by 7 per cent per year. They acknowledge that these are extremely ambitious assumptions but consider them to be the most feasible compromise between practicality and equity. To stay within the remaining carbon budget, Annex 1 nations need to reduce emissions by 8–10 per cent per year, beginning in 2015. This model was developed with data up to 2010; as the remaining carbon budget is now smaller, Anderson estimates that Annex 1 nations need to reduce emissions by 12 per cent per year.13 If we accept that Annex 1 nations need to achieve emissions reductions of 12 per cent per year, and if we assume that GDP growth in Annex 1 nations continues at 1.86 per cent per year (the average from 2010 to 2014), then decoupling must occur at a rate of 15.8 per cent per year.14 For perspective, this is eight times faster than the historic rate of decoupling in Annex 1 nations (viz., 1.9 per cent per year from 1970 to 2013), and it is important to bear in mind that the rate of decoupling has generally slowed over this period.15 It also exceeds the decoupling rate implied by the average G20 Nationally Determined Contributions under the Paris Agreement (viz., 3 per cent per year) by a factor of five. There is one empirical model that feasibly accomplishes emissions reductions consistent with the Paris Agreement, without relying on negative emissions technologies. Published by Grubler et al. (2018), it was included in the IPCC Special Report on 1.5°C (2018) in response to growing critiques of the IPCC’s reliance on BECCS. The scenario, known as ‘Low Energy Demand’ (LED), accomplishes emissions reductions compatible with 1.5°C by reducing global energy demand by 40 per cent by 2050. In addition to decarbonisation and afforestation, the key feature of this scenario is that global material production and consumption declines significantly: ‘The aggregate total material output decreases by close to 20 per cent from today, one-third due to dematerialization, and twothirds due to improvements in material efficiency.’ Dematerialisation is accomplished by shifting away from private ownership of key commodities (like cars) towards sharing-based models. LED differentiates between the global North and South. Industrial activity declines by 42 per cent in the North and 12 per cent in the South. With efficiency improvements, this translates into industrial energy demand declining by 57 per cent in the North and 23 per cent in the South. The LED scenario projects continued GDP growth at just over 2 per cent per year, which would make it consistent with green growth theory. However, the empirical basis for this GDP trend is not robust. It is derived from the MESSAGE-Globium model, which calculates GDP from only two inputs: labour supply (population size and productivity) and energy. The low energy demand in the LED scenario does not affect growth because it is offset by efficiency improvements. As the model is insensitive to changes in material throughput, reductions in production and consumption do not affect output. The paper offers no evidence that GDP will continue to grow despite such reductions. Charlie Wilson, one of the paper’s authors, acknowledged that ‘we did not consider broader questions of GDP growth or degrowth, and we did not explicitly report relationships between our scenario and GDP outcomes for this reason.’ 16 Conclusions and discussion The empirical data demonstrate that while absolute decoupling of GDP from emissions is possible and is already happening in some regions, it is unlikely to happen fast enough to respect the carbon budgets for 1.5°C and 2°C against a background of continued economic growth. Growth increases energy demand, making the transition to renewable energy more difficult, and increases emissions from land use change and industrial processes. Models that do project green growth within the constraints of the Paris Agreement rely heavily on negative emissions technologies that are either unproven or dangerous at scale. Without these technologies, the rates of decarbonisation required for 1.5°C or 2°C are significantly steeper than extant models suggest is feasible even with aggressive mitigation policies.

### AT: Tech Solves

#### Tech can’t solve---CCS and renewables fail, empirics, rebound, outsourcing, and politics

John Wiseman 17, Professorial Research Fellow at the Melbourne Sustainable Society Institute and with the Climate and Energy College, University of Melbourne, Adjunct Professor at the Melbourne School of Population and Global Health, Research Fellow at the Centre for Policy Development and Climate Change Policy Adviser, Sustainability Victoria, Ph.D. from Latrobe University, Samuel Alexander, lecturer with the Office for Environmental Programs, University of Melbourne, and research fellow, Melbourne Sustainable Society Institute, 2017, “The Degrowth Imperative: Reducing Energy and Resource Consumption as an Essential Component in Achieving Carbon Budget Targets,” in Transitioning to a Post-Carbon Society, p. 95-97

The first heroic assumption underpinning techno-optimist solutions is the ongoing reliance in many of the most influential large scale decarbonization strategies on CCS (carbon capture and storage). While CCS may play a valuable, albeit modest, long term role, the current state of knowledge suggests that we are still a very long way from affordable and scalable CCS deployment. Even the Global CCS Institute (2013: 5) has recently reported that, “while CCS projects are progressing, the pace is well below the level required for CCS to make substantial contribution to climate change mitigation”. The growing “emissions gap” is also providing increasing impetus for speculation about the “necessity” of geoengineering “solutions” with all their attendant concerns about ethical implications and unintended consequences (see Hamilton 2013).

The second debatable assumption is that technological innovation will necessarily and rapidly translate into global reductions in energy consumption. Important questions remain about the speed with which 100% renewable energy can realistically be achieved (see e.g. Smil 2010, 2014); the extent of fossil fuel energy consumption required to drive the initial massive expansion in renewable energy infrastructure; and the full life cycle energy return on investment (EROI) outcomes of solar and wind energy—particularly if these calculations factor in the full costs of energy storage (see e.g. Palmer 2013; Prieto and Hall 2013). Noting that emissions reductions of 4% p.a. in an economy growing at 2% p.a. are likely to require carbon intensity improvements of around 6% p.a., Anderson (2013) notes that he has yet to find any credible mainstream economist prepared to argue that prolonged emissions reductions of 3% or 4% or more are compatible with economic growth.

Indeed, as Lord Stern (2006: 231) himself has noted: There is likely to be a maximum practical rate at which global emissions can be reduced. At the national level, there are examples of sustained emissions cuts of up to 1% per year associated with structural change in energy systems... whilst maintaining strong economic growth. However, cuts in emissions greater than this have historically been associated only with economic recession or upheaval, for example, the emissions reduction of 5.2% per year for a decade associated with the economic transition and strong reduction in output in the former Soviet Union. These magnitudes of cuts suggest it is likely to be very challenging to reduce emissions by more than a few percent per year while maintaining strong economic growth.

The third reason for caution in assuming overly optimistic relationships between technological innovation, carbon intensity and emissions reductions is the impact of the “rebound effect” (see Jevons 1865; Herring and Sorrell 2009; Holm and Englund 2009; Jackson 2009). This phenomenon refers to the tendency for innovation and efficiency gains to be rapidly overwhelmed as cheaper unit costs combined with the formidable reach and power of the global advertising industry enable and encourage individuals to consume more of the same or alternative services and products. The harsh reality remains that global emissions continue to grow (IPCC 2013)—along with the global trends in the consumption of energy and resources—with apparent improvements in developed economy energy efficiency often masking the reality of energy intensive production being offshored to developing economies.

The likelihood of full and fast deployment of new technologies is the fourth problematic assumption that needs to be addressed given the formidable political and social obstacles standing in the way of rapid implementation. As noted in the recent Post Carbon Pathways review of learning from the implementation of large-scale decarbonization strategies (see Wiseman et al. 2013), experienced climate scientists and policymakers consistently come to the conclusion that the key obstacles standing in the way of rapid decarbonization are political and social rather than technological. Key roadblocks include the following.

#### Innovation faces diminishing marginal returns

Christopher Ketcham 17, writer for the Pacific Standard, among other publications, citing Joseph Tainter, a professor of sustainability at Utah State University, “The Fallacy of Endless Economic Growth,” 5/16/17, https://psmag.com/magazine/fallacy-of-endless-growth

Now, at the very moment that we need innovation to accelerate—to mount a viable response to climate change, to locate new resources and replace dwindling or despoiled ones—evidence suggests that the opposite is happening. Joseph Tainter, a professor of sustainability at Utah State University, examined innovation trends using 30 years of data from the U.S. Patent and Trademark Office. What he found was troubling. Slightly more than half of all patents issued in this country are to foreign entities, so Tainter considered changes to the number of patents per applicant to be an accurate indicator of global productivity as expressed through invention. In the major technical fields he studied—drugs and chemicals, metallurgy, energy, biotechnology, information technology, and so on—he found that the number of researchers on each patent steadily increased between 1974 and 2005. This means more time and man-hours—and presumably more money invested—for a declining return. In his 1988 book The Collapse of Complex Societies—a kind of companion volume to Limits—Tainter makes the case that as civilizations grow they produce increasingly complex problems that demand increasingly complex solutions. Complexity demands more energy, requiring new technologies for energy extraction. But, as Tainter's study suggests, innovation may have its own limits.

The concept of energy-return-on-investment, known as EROI, was originally coined in reference to fossil-fuel exploration, and is commonly used to compare the amount of energy required to extract, transport, and refine a particular resource with the amount of energy it ultimately provides. EROI for our master energy source happens to be plummeting, as discovery and extraction of fossil fuels becomes more difficult and costly. (The rising cost—which is to say complexity—of resource extraction and retrieval was one of Limits' broad projections that also turned out to be accurate.) EROI for global oil and gas production went from 30-to-1 in 1995 to 18-to-1 in 2006. In the U.S., the EROI for oil discovery in 1919 was an astonishing 1,000-to-1. By the 2010s, it was 5-to-1.

In mining, multifactor productivity—which reflects the efficiency with which the inputs of capital, labor, materials, services, and energy generate a unit of mineral product—has been on a downward slope since 2002. According to the Australian Bureau of Statistics, it now takes 40 percent more inputs to dig up minerals in general, while the grain sizes and ore grades of what's being retrieved are declining. The Journal of Environmental Science and Engineering reported in 2013 that, "under the present paradigm of use," the world, within decades, will begin seeing "scarcity" of "most of the strategically important metals and materials that are fundamental to [the] running of our societies." According to the study's lead authors, a chemical engineering professor at Lund University in Sweden and an applied systems analyst at Stockholm University, "scarcity may lead [to] 'peak civilization,' unless urgent countermeasures are systematically undertaken."

Even in the midst of substantial innovation, today's global economy has become more profligate and more wasteful, using more materials per unit of GDP than it did 20 years ago. According to a 2016 report from the International Resource Panel at the United Nations Environment Programme, the amount of virgin natural resource needed for a given amount of product has gone up 17 percent over a single decade. In 2000, it took an average 1.2 kilograms of materials to generate one dollar of global GDP. By 2010, it took 1.4 kilograms. The amount of primary materials extracted from the Earth globally rose from 22 billion tonnes in 1970 to 70 billion tonnes in 2010, with per capita global material use going from seven tonnes in 1970 to 10 tonnes over the same 40-year period. According to the report, there is "growing environmental pressure per unit of economic activity," not less.

Optimists will undoubtedly look to renewable energy as a stay against declining EROI and rising seas. But they may be blindsided by the stark limits of wind, solar, and hydro. Researchers at Monash University, marshaling considerable data, concluded that the cheerful scenarios projecting renewables will supply most of the world's energy by mid-century "assume unrealistic technical potentials and implementation times." Which means we'll be stuck mostly with fossil fuels to keep the expansion machine running. Tim Jackson of the University of Surrey has calculated that, at current rates of carbon density—the amount of carbon released per unit of energy consumed—our greenhouse gas emissions will increase by more than 2 percent per year. At that rate, by 2050 carbon dioxide emissions would be more than double what they were in 2015. To achieve a tenfold reduction in global emissions by 2050, carbon density would have to decline on average 8.6 percent annually—almost 10 times the rate at which it has declined over the last 50 years and 50 times faster than in the past decade. In other words, we would have to innovate carbon-reduction strategies at rates never before seen, with technologies of immense effectiveness whose global-scale implementation would be entirely unprecedented.

### AT: Tech Good

#### Dedev still has tech

**Trainer 2** (Ted, Senior Lecturer, School of Social Work, University of New South Wales, “If you want affluence, prepare for War,” The International Journal of Inclusive Democracy, July 2002, Volume 8, Issue 2, pg. 281-299)

The logically inescapable implications from the foregoing discussion is that global peace cannot be achieved before there has been a vast and historically unprecedented transition to "The Simpler Way'. The accelerating global predicament cannot be remedied until social, economic, political and cultural systems based on competitive individualism, acquisitiveness, affluence and growth are abandoned and replaced by ways of life based on production to meet needs rather than profits, high levels of individual and local self-sufficiency, co-operation, participation, mutual assistance and sharing, and above all on willing acceptance of materially simple lifestyles within zero-growth national economies.76 This does not mean hardship and deprivation; indeed it can be argued that high levels of simplicity, self-sufficiency and co-operation are the necessary conditions for a high quality of life, as well as for global justice and ecological sustainability. **Nor does it mean absence of** sophisticated **tech**nology **and research**. It does mean a landscape made up mostly of small towns and villages within comfortable distance of small cities by public transport, with relatively little heavy industry, travel and transport, international trade or big firms. Most ‘government’ would have to be carried out through small local participatory assemblies. Because large sectors of the present economy would no longer be necessary, the overall amount of work for monetary income would probably be reduced by two-thirds, enabling a much more relaxed pace of life. There would be no need to reduce the sophistication and quality of research and technology within socially desirable fields.

### AT: Space Col---2NC

#### Independent colony is impossible.

**Levchenko et al. 19**. Professors in the Plasma Sources and Applications Centre/Space Propulsion Centre, NIE, Nanyang Technological University. 2019. “Mars Colonization: Beyond Getting There.” Global Challenges, vol. 3, no. 1.

Settlement of Mars—is it a dream or a necessity? From scientific publications to public forms, there is certainly little consensus on whether colonization of Mars is necessary or even possible, with a rich diversity of opinions that range from categorical It is a necessity!20 to equally categorical Should Humans Colonize Other Planets? No.21 A strong proponent of the idea, Orwig puts forward five reasons for Mars colonization, implicitly stating that establishing a permanent colony of humans on Mars is no longer an option but a real necessity.20 Specifically, these arguments are: Survival of humans as a species; Exploring the potential of life on Mars to sustain humans; Using space technology to positively contribute to our quality of life, from health to minimizing and reversing negative aspects of anthropogenic activity of humans on Earth; Developing as a species; Gaining political and economic leadership. The first argument captures the essence of what most space colonization proponents feel—our ever growing environmental footprint threatens the survival of human race on Earth. Indeed, a large body of evidence points to human activity as the main cause of extinction of many species, with shrinking biodiversity and depleting resources threatening the very survival of humans on this planet. Colonization of other planets could potentially increase the probability of our survival. While being at the core of such ambitious projects as Mars One, a self‐sustained colony of any size on Mars is hardly feasible in the foreseeable future. Indeed, sustaining even a small number of colonists would require a continuous supply of food, oxygen, water and basic materials. At this stage, it is not clear whether it would be possible to establish a system that would generate these resources locally, or whether it would at least in part rely on the delivery of these resources (or essential components necessary for their local production) from Earth. Beyond the supply of these very basic resources, it would be quite challenging if not impossible for the colonists to independently produce hi‐tech but vitally important assets such as medicines, electronics and robotics systems, or advanced materials that provide us with a decent quality of life. In this case, would their existence become little more than the jogtrot of life, as compared with the standards expected at the Earth?22

#### Deep space travel is impossible

Robinson 16 [Kim Robinson, Scientific American.] “What Will It Take for Humans to Colonize the Milky Way?” 13 January 2016 (<https://www.scientificamerican.com/article/what-will-it-take-for-humans-to-colonize-the-milky-way1/>) – MZhu

The idea that humans will eventually travel to and inhabit other parts of our galaxy was well expressed by the early Russian rocket scientist Konstantin Tsiolkovsky, who wrote, “Earth is humanity’s cradle, but you’re not meant to stay in your cradle forever.” Since then the idea has been a staple of science fiction, and thus become part of a consensus image of humanity’s future. Going to the stars is often regarded as humanity’s destiny, even a measure of its success as a species. But in the century since this vision was proposed, things we have learned about the universe and ourselves combine to suggest that moving out into the galaxy may not be humanity’s destiny after all. The problem that tends to underlie all the other problems with the idea is the sheer size of the universe, which was not known when people first imagined we would go to the stars. Tau Ceti, one of the closest stars to us at around 12 light-years away, is 100 billion times farther from Earth than our moon. A quantitative difference that large turns into a qualitative difference; we can’t simply send people over such immense distances in a spaceship, because a spaceship is too impoverished an environment to support humans for the time it would take, which is on the order of centuries. Instead of a spaceship, we would have to create some kind of space-traveling ark, big enough to support a community of humans and other plants and animals in a fully recycling ecological system. On the other hand it would have to be small enough to accelerate to a fairly high speed, to shorten the voyagers’ time of exposure to cosmic radiation, and to breakdowns in the ark. Regarded from som e angles bigger is better, but the bigger the ark is, the proportionally more fuel it would have to carry along to slow itself down on reaching its destination; this is a vicious circle that can’t be squared. For that reason and others, smaller is better, but smallness creates problems for resource metabolic flow and ecologic balance. Island biogeography suggests the kinds of problems that would result from this miniaturization, but a space ark’s isolation would be far more complete than that of any island on Earth. The design imperatives for bigness and smallness may cross each other, leaving any viable craft in a non-existent middle. The biological problems that could result from the radical miniaturization, simplification and isolation of an ark, no matter what size it is, now must include possible impacts on our microbiomes. We are not autonomous units; about eighty percent of the DNA in our bodies is not human DNA, but the DNA of a vast array of smaller creatures. That array of living beings has to function in a dynamic balance for us to be healthy, and the entire complex system co-evolved on this planet’s surface in a particular set of physical influences, including Earth’s gravity, magnetic field, chemical make-up, atmosphere, insolation, and bacterial load. Traveling to the stars means leaving all these influences, and trying to replace them artificially. What the viable parameters are on the replacements would be impossible to be sure of in advance, as the situation is too complex to model. Any starfaring ark would therefore be an experiment, its inhabitants lab animals. The first generation of the humans aboard might have volunteered to be experimental subjects, but their descendants would not have. These generations of descendants would be born into a set of rooms a trillion times smaller than Earth, with no chance of escape. In this radically diminished enviroment, rules would have to be enforced to keep all aspects of the experiment functioning. Reproduction would not be a matter of free choice, as the population in the ark would have to maintain minimum and maximum numbers. Many jobs would be mandatory to keep the ark functioning, so work too would not be a matter of choices freely made. In the end, sharp constraints would force the social structure in the ark to enforce various norms and behaviors. The situation itself would require the establishment of something like a totalitarian state. Of course sociology and psychology are harder fields to make predictions in, as humans are highly adaptable. But history has shown that people tend to react poorly in rigid states and social systems. Add to these social constraints permanent enclosure, exile from the planetary surface we evolved on, and the probability of health problems, and the possibility for psychological difficulties and mental illnesses seems quite high. Over several generations, it’s hard to imagine any such society staying stable.

#### Space col brings with it WTDs and inter-species wars---universal extinction

Phil **Torres 18**. Project for Future Human Flourishing. 06/2018. “Space Colonization and Suffering Risks: Reassessing the ‘Maxipok Rule.’” Futures, vol. 100, pp. 74–85.

5. Space-Age Weaponry and the Balance of Terror Yet there is another strategy for neutralizing the Hobbesian trap, namely, a policy of deterrence, also known as a “balance of terror” or, during the Cold War, “mutually-assured destruction” (MAD). This asserts that “if you strike me, I will most assuredly strike back with equal or greater force, and if I strike you it will only be because you struck me first.”xvii Deterrence is only effective when one’s adversaries genuinely believe the statement, “I will most assuredly strike back.” This returns us to Hobbes’s third cause of conflict from section 3: glory, honor, or credibility. To establish credibility and, therefore, dissuade potential attackers, one has reason to engage in confrontations with others and, in doing so, to demonstrate one’s capacity for violence. The question is whether policies of deterrence implemented by civilizations throughout the cosmos would be sufficient to obviate war. To answer this question, let’s begin by considering the unsettling range of weapons that will likely be available to our spacefaring progeny; we will then explore how these weapons could enhance or mitigate the effectiveness of deterrence. 5.1 Weapons of Total Destruction (WTDs) There are a variety of “kill mechanisms” that one civilization could use to obliterate another. In relatively close propinquity, chemical and biological weapons could offer a means of targeted violence, since the deleterious effects of such weapons might be limited to a particular species (Deudney forthcoming). For example, the toxicity of a chemical X might be low for a species A but lethal to a species B. This could enable A to use X on B without fear of X harming A—a concern that has dissuaded some terrorists from employing chemical weapons. The same goes for a pathogenic germ Y: since pathogens often only harm single species, biological weapons could be used without the perpetrators worrying about becoming sick. With respect to artificial intelligences, there could be viral malware that affects only certain types of software; in this case, such viruses could be transferred not at the velocity of a sneeze but at the speed of light, traversing astronomically large stretches of space to devastate colonies of artificial-substrate beings. Another possibility involves weaponizing “minor planets” like asteroids. This hints at the deflection dilemma discussed by Sagan (1994), among others, whereby the very same technology that could deflect an asteroid away from Earth could also be used to redirect one toward it. The resultant “planetoid bombs” could be launched in the direction of target civilizations at extremely high velocities and inflict far greater destruction than all the nuclear arsenals on Earth combined (see Cole and Cox 1965; Deudney forthcoming). Even more, asteroids are extremely numerous in the solar system and have a wide range of sizes, with estimates of 1.1 to 1.9 million that have greater-than-1-kilometer diameters in the asteroid belt between Mars and Jupiter. (A 1- kilometer impactor striking Earth would likely annihilate humanity by causing an impact winter.) Thus, asteroids constitute an abundant source of easily obtainable, civilization-ending weaponry— a particularly worrisome fact given that the technological capabilities to redirect asteroids will likely emerge at an early stage in our diaspora “out of Earth,” as it were (see Deudney forthcoming). Other futuristic space weapons include military drones that either initiate attacks or engage in clandestine surveillance of other civilizations. Such drones could hide themselves from counter-surveillance detectors by employing metamaterial invisibility cloaks and propagate themselves through the von Neumann process of self-replication, that is, by converting raw materials into clones of themselves. There is also the possibility of using “heliobeams,” or “sun guns,” to destroy targets by concentrating large amounts of solar radiation via a concave mirror on a satellite. Even more catastrophic are direct-energy weapons (DEWs) like lasers and particlebeams that use highly focused energy to superheat their targets. In fact, the US government has already developed weapons of this sort—they are science fact rather than fiction—although future breakthroughs could enable them to become immensely more destructive. If this is the case, they will offer yet another mechanism for wreaking unprecedented harm (see Deudney forthcoming). Along these lines, Anders Sandberg (forthcoming) suggests that technologically advanced civilizations could potentially use gravitational waves to create black holes. Generating waves of sufficient intensity would be energetically inefficient, according to current physics, but they have the advantage that they can interact with dark matter objects, unlike electromagnetic-energy weapons. Even more, the universe appears to be in a “metastable” energy state. This suggests that one could tip it into a more stable, lower-energy state, perhaps by concentrating huge quantities of energy in tiny regions of spacetime, as occurs in some high-powered physics experiments. In other words, a particle collider could be weaponized to intentionally nucleate a “vacuum bubble,” or sphere of “true vacuum” spreading in all directions at the speed of light and destroying everything with which it comes into contact. Who might weaponize a particle collider? First, there could be actors who use the threat of a vacuum bubble for blackmail purposes. Second, there could be madmen (like Hitler) who create a vacuum bubble to avoid defeat. That is to say, a predatory actor could hold the following preference ordering: (i) triumphant victory over, say, its Local Group, (ii) total annihilation of the universe, and (iii) defeat. Third, particle colliders would also be the ideal WTD for RNUs, since it would enable them to obliterate not only all extant life in the universe but the very potential for life to arise—and it would do this without inflicting any suffering whatsoever.xviii Another possibility is that Tuckerian actors create a vacuum bubble for the purely defensive reason of eliminating all potential attackers in the universe. As Sandberg (2017) speculates, it might be possible for “certain configurations of matter, energy, black holes, etc. [to] induce a post-transition structure that can act as an assembler.” This “assembler” would enable “some information [to] be transmitted into the new state,” thus making it possible for a civilization to “survive,” in some sense, the universe settling into a lower-energy configuration. On the other side of this transition, the “structure” can recrudesce into a daughter new civilization with the certitude that it is completely alone and, therefore, safe. Finally, it is crucial to note that future beings—some of whom may have hugely augmented cognitive capacities—will almost certainly invent new weapons that are more powerful and effective than anything we could imagine. Such weapons could enable civilizations—or perhaps lone wolves, of which there could be, once again, trillions and trillions and trillions—to cause unprecedented injury to other civilizations. Consider the following passage from Bostrom (2013): One can readily imagine a class of existential-catastrophe scenarios in which some technology is discovered that puts immense destructive power into the hands of a large number of individuals. If there is no effective defense against this destructive power, and no way to prevent individuals from having access to it, then civilization cannot last, since in a sufficiently large population there are bound to be some individuals who will use any destructive power available to them. Scale this up from the individual level to the cosmopolitical level and the same conclusion follows: Life in the universe cannot last.

### AT: Asteroids

#### No impact and we got time

**Bennett 2010** (James, Prof of Economics at George Mason, *The Doomsday Lobby: Hype and Panic from Sputniks, Martians, and Marauding Meteors*, p. 144-145)

It should be noted that the Alvarez et al. hypothesis was not universally accepted. As Peter M. Sheehan and Dale A. Russell wrote in their paper “Faunal Change Following the Cretaceous–Tertiary Impact: Using Paleontological Data to Assess the Hazards of Impacts,” published in Hazards Due to Comets & Asteroids (1994), edited by Tom Gehrels, “many paleontologists resist accepting a cause and effect relationship” between the iridum evidence, the Chicxulub crater, and the mass extinction of 65 million years ago.15 For instance, Dennis V. Kent of the Lamont–Doherty Geological Observatory of Columbia University, writing in Science, disputed that a high concentration of iridium is necessarily “associated with an extraordinary extraterrestrial event” and that, moreover, “a large asteroid… is not likely to have had the dire consequences to life on the earth that they propose.”16 Briefly, Kent argues that the Alvarez team mistakenly chose the 1883 Krakatoa eruption as the standard from it extrapolated the effects of stratospheric material upon sunlight. Yet Krakatoa was too small a volcanic eruption from which to draw any such conclusions; better, says Kent, is the Toba caldera in Sumatra, remnant of an enormous eruption 75,000 years ago. (A caldera is the imprint left upon the earth from a volcanic eruption.) The volume of the Toba caldera is 400 times as great as that of Krakatoa – considerably closer to the effect that an asteroid impact might have. Yet the sunlight “attenuation factor [for Toba] is not nearly as large as the one postulated by Alvarez et al. for the asteroid impact.” Indeed, the Toba eruption is not associated with any mass extinctions, leading Kent to believe that “the cause of the massive extinctions is not closely related to a drastic reduction in sunlight alone.”17 Reporting in Science, Richard A. Kerr wrote that “Many geologists, paleontologists, astronomers, and statisticians… find the geological evidence merely suggestive or even nonexistent and the supposed underlying mechanisms improbable at best.” Even the iridium anomalies have been challenged: Bruce Corliss of the Woods Hole Oceanographic Institute argues that the major extinctions associated with the K–T event were not immediate and catastrophic but “gradual and apparently linked to progressive climate change.”18 Others argue that a massive volcanic event predating the Alvarezian killer asteroid created an overwhelming greenhouse effect and set the dinosaurs up for the knockout punch. A considerable number of scientists believe that gradually changing sea levels were the primary cause of the K–T Extinction. If either of these hypotheses is true – and a substantial number of geologists hold these positions — then the “killer asteroid” is getting credit that it does not deserve. Even if the K–T Extinction was the work of a rock from space, the Alvarez team credits a “probable interval of 100 million years between collisions with 10-km-diameter objects.”19 The next rendezvous with annihilation won’t be overdue for about 40 million years. We have time.

#### Nukes solve

Syal et. al 13 – Megan, M.S in Geological Science from Brown University, David Dearborn, PhD, Physicist @ Livermore National Labs, 1998 Shelby Fellow of the Australian Academy of Science, and has received two Pollock awards for work in astronomy, has held positions at the Copernicus Institute in Warsaw, the Institute of Astronomy in Cambridge, The California Institute of Technology, and Steward Observatory in Tucson, and Peter Schultz, PhD, Professor of Planetary Geoscience @ Brown, “Limits on the use of nuclear explosives for asteroid deflection”, https://pdfs.semanticscholar.org/dffd/703e8a4a3ba6acec5c299a504efd22df7d4e.pdf

Conclusions Nuclear explosives comprise the only present technology capable of deflecting the most catastrophic threats (4500 m) with a sufficient change in velocity to avert disaster. In the case of smaller bodies, if alternate methods fail or the warning time is too short, the nuclear option provides considerable mitigation when used only a few years prior to impact. Even for larger bodies, the payload mass necessary for a successful nuclear burst-driven deflection is well within current launch vehicle capabilities. We have now extended earlier simulations of nuclear deflection to examine the challenges of a smaller body and potentially shorter warning times (years). We have also included microporosity to begin to determine when this material property is a sensitive uncertainty. We find that a modest yield standoff burst can fragment a nonporous rubble structure, but that 16% porosity resulted in a substantially bound body. This result demonstrates that the non-porous case presents the highest risk of fragmentation, but it also suggests that robustly fragmenting smaller bodies can be accomplished by high yield standoff bursts, a strategy which reduces the extra mass requirements associated with rendezvous missions. This is an approach that we will study in more detail in the future. Interestingly, even when copious material is ejected, as long as the remaining bound material is imparted with a reasonable speed change, the mitigation against an Apophis-sized object can be substantial (when done a year before impact). Alternatively, very low yields or large heights of burst can deflect bodies of this size when there are decades to impact. Despite NEO structural and compositional uncertainties, detailed simulations show that nuclear explosives will provide considerable protection. While their use to perturb a body some decades out remains the more desirable option, fragmenting the body remains a viable back-up option with only a few years of lead-time.

### Transition---2NC

#### Collapse causes a transition---aligns social and economic forces that capitalize on existing momentum for political upheaval---that’s Kirk

#### Crisis now solves---waiting risks lock-in

Loorbach, et al, 16—DRIFT, Erasmus University, Rotterdam (Derk, with Flor Avelino, DRIFT, Erasmus University, Rotterdam, Alex Haxeltine, School of Environmental Sciences, University of East Anglia, Julia M. Wittmayer, DRIFT, Erasmus University, Rotterdam, Tim O'Riordan, School of Environmental Sciences, University of East Anglia, Paul Weaver, LUCSUS, Lund University, and René Kemp, ICIS, Maastricht University, “The economic crisis as a game changer? Exploring the role of social construction in sustainability transitions,” Ecology and Society 21(4):15)

Meanwhile, many political and public debates seem to be primarily concerned with standard, relatively short-term, economic issues, such as monetary losses, stop-and-start economic growth, increasing unemployment, falling real estate prices, failing banks, virtually bankrupt nations, and how to get back on course to economic growth. The standard responses when national governments are struggling to get their economies healthy again are mostly about inducing more money, austerity measures, and introducing financial regulations, all often part of a broader financial–economic logic (Stiglitz 2010). The dominant focus on fighting economic deficits and problems at the expense of investing in social and ecological deficits—thereby failing to address persistent problems in these areas—can be argued to be a short-term strategy to prop up an inherently unmanageable system. Examples are the support of system banks with public money and the green growth strategy (OECD 2009, 2013a). Transition theory (Grin et al. 2010, Markard et al. 2012) suggests that such short-term fixes are typical regime-based strategies to sustain existing structures, cultures, and practices, and to fend off the threats of more radical systemic change.

The transition perspective suggests that most regular policy and governance strategies essentially reproduce existing systems and, by definition, do not address the root causes of problems that are embedded in the same structures and cultures that determine how solutions are framed and implemented. Such path-dependent development optimizing existing institutional structures will inevitably lead to recurring crises and ultimately a more disruptive, shock-wise structural change of an incumbent regime. Transition studies thus argue that solutions that address symptoms rather than the underlying structural causes tend to reinforce a lock-in and result in further emergent problems (Rotmans and Loorbach 2010, Schuitmaker 2012). We argue that the underlying causes and mechanisms of the economic crises have not been thoroughly analyzed, let alone addressed through effective policies. In a globalized economy, fundamental changes will not likely come from actions by (national) governments or incumbent businesses, as these are inherently intertwined with and dependent upon the currently still dominant financial– economic systems and their governance. The need for alternative economic approaches, discourses, and systems is increasingly emphasized (Schor 2010, Simms 2013, Jackson 2013, van den Bergh 2013, Schor and Thompson, 2014). Even though the benefits of liberalization are still significant, it seems that the transfer of control from government to markets has substantially diminished possibilities for top-down policy making, adding to brittleness, complexity, and lock-in (Loorbach and LijnisHuffenreuter 2013).

In this paper, we take a transition perspective on transformative social innovation to conceptualize and map the systemic dynamics that have caused the economic crisis, as well as how it influences the dynamics of social transformation. We explore how the economic crisis might be considered as a phase in a broader economic transition and which types of changes coincide to develop into this direction. We thus view the economic crisis not as a phenomenon in isolation within a relatively short time frame, but as an intrinsic part, or perhaps a symptom, of deeper underlying structural societal changes over the longer term. The question we seek to address is how the economic crisis interacts with broader societal changes as well as which dynamics might accelerate or hamper more structural (sustainability) transitions. To this end, we ask when and how a macrolevel or landscape development like the economic crisis fundamentally changes the dominant logic, rules, and conditions of incumbent regimes. In other words, when does a macrodevelopment become a game changer (cf. Avelino et al. 2014)?

The paper builds upon theoretical work from the European FP7 project TRANSIT, which draws on transition theory to develop an empirically grounded theory on transformative social innovation. In this paper, we introduce the analytical perspective that we developed on transformative social innovation and two empirical examples. Although our analytical perspective suggests that alternatives and breakthroughs can come from any sector or actor, in this paper, we focus on the agency of social innovation and civil-society-led initiatives in providing and producing alternatives. The paper was developed through a number of iterations, workshops, and theoretical synthesizing. To develop our arguments, we build upon insights from sustainability transitions literature (Grin et al. 2010, Markard et al. 2012), social innovation research (Mulgan 2006, Murray et al. 2010, Franz et al. 2012, Westley 2013, Moulaert et al. 2013) and other fields aiming to understand the economic crisis. In addition, we include two empirical cases, transnational networks of social innovation, time banks, and the transition movement. For both cases, we draw upon a general literature review.

The paper is structured as follows. In the next section, “Economic change or transition?,” we introduce the economic crisis as a multifarious phenomenon, how we understand it from a transition perspective, and how it is understood from an economist’s point of view. We illustrate that it is an ambiguous phenomenon that is simultaneously seen as part of regular changes in that it is part of disruptive or transformative change. In the section “Making sense of the economic crisis?,” we present a number of alternative perspectives on the economic crisis that put forward particular fundamental and systemic causes of the economic crisis and how these are translated in so called “narratives of change.” In “Transformative social innovations,” we highlight two specific social innovation initiatives, time banks and transition towns, which have an evident transformative claim and potential, and reflect upon how such transformative social innovations relate (themselves) to the economic crisis. In “Reconceptualizing societal transformations and the role of the economic crisis,” we synthesize our findings and argue that the concepts of game changers and narratives could help to unpack the landscape and better understand how macro- and microlevels interact to trigger transformative changes at the mesolevel. In conclusion, we address the need for a better understanding of the transformative impacts of the different shades of change (in coevolution) vis-é-vis the restorative dynamics associated with incumbent regimes.

#### The support is there

Alperovitz, et al, 16—Lionel R. Bauman Professor of Political Economy at the University of Maryland, College Park Department of Government and Politics, former fellow of King's College, Cambridge, founding Fellow of the Harvard Institute of Politics, former Fellow at the Institute for Policy Studies, former Guest Scholar at the Brookings Institution, served as a Legislative Director in the US House of Representatives and the US Senate and as a Special Assistant in the US Department of State (Gar, with James Gustave Speth, Senior Fellow at The Democracy Collaborative, and is Co-Chair of The Next System Project, Ted Howard, President and Co-Founder of The Democracy Collaborative, and Joe Guinan, Executive Director of The Next System Project, Senior Fellow at The Democracy Collaborative, “Systemic Crisis and Systemic Change in the United States in the 21st Century,” <http://thenextsystem.org/wp-content/uploads/2016/09/NSPOberlin-final.pdf>)

The good news is that the inability of traditional politics and policies to address fundamental challenges has fueled an extraordinary amount of experimentation in communities across the United States and around the world. It has also generated increasing numbers of sophisticated and thoughtful proposals that build from the bottom and begin to suggest new systemic possibilities beyond the failed systems of the past and present. It is becoming possible to bring together and extend elements of innovative thinking and realworld practice in key areas to define the underlying structural building blocks of a range of alternatives capable of rebuilding the basis for democracy, liberty, equality, sustainability, and community in the United States in the twenty-first century. Unbeknownst to many, literally thousands of onthe-ground efforts have been developing. These include cooperatives, worker-owned companies, neighborhood corporations, and many little known municipal, state, and regional efforts. These emerging economic alternatives suggest different ways in which capital can be held in common by small and large publics. They include nonprofit community corporations and land trusts that develop lowincome housing, as well as community development financial institutions (CDFIs) that have over $108 billion in assets under their management.56 Employee ownership is also on the rise, involving three million more workers than are members of private sector unions. 57 A third of Americans belong to cooperatives, including credit unions that serve 107 million people and manage $1.3 trillion in assets, almost as much as is managed by Citi. 58 In the public sector, local government economic development programs invest in local businesses, while municipal enterprises build infrastructure and provide services, raising revenue and creating employment, diversifying the base of locally controlled capital. Public utilities, together with co-ops, make up nearly 90 percent of all electricity providers and generate over 20 percent of America’s electricity.59 From California to Alabama, public pension assets are being channeled into job creation and community development.60 Cities and states are looking to the creation of public banking systems like that of North Dakota. Trusts that allow for public ownership and management of natural resources provide revenue streams from capital, recalling the unjustly neglected ideas of James Meade.61 From parks and blood banks to libraries and the internet, commons management systems can provide an expanding zone of decommodification to buffer against the market. Public trusts can be extended into additional domains, from dry land to the electromagnetic spectrum, underwriting public services or issuing a citizen dividend. Community land trusts can ensure affordable housing and prevent disruptive gentrification and speculative real estate bubbles. New public strategies encompass both democratic public ownership and new planning capacities and functions. Even experts working on such matters rarely appreciate the sheer range of activity. Practical and policy foundations have been established that offer a solid basis for future expansion. A body of hardwon expertise is now available in each area, along with support organizations, and technical and other experts who have accumulated a great deal of direct problem-solving knowledge. The idea that we need a “new economy”—that the entire economic system must be radically restructured if critical social and environmental goals are to be met—runs directly counter to the American creed that capitalism as we know it is the best, and only possible, option. Most of the new projects, ideas, and research efforts have thus gained traction slowly and with little national attention. But in the wake of the financial crisis, they have proliferated and earned a surprising amount of support—and not only among advocates on the left. New terms have begun to gain currency in diverse areas with activist groups and constituencies, an indication that the domination of traditional thinking may be starting to weaken. Thus we encounter the sharing economy, the caring economy, the provisioning economy, the restorative economy, the regenerative economy, the sustaining economy, the collaborative economy, the solidarity economy, the gift economy, the resilient economy, the steady state economy, the new economy, and many, many more. There are calls for a Great Transition, or for a reclamation of the Commons. Creative thinking by researchers and engaged scholars is also contributing to the ferment, and policies at the state and local level can help move projects to much more powerful scale and community-wide impact. Larger scale strategic options that build on what is being learned locally are beginning to be sketched as the basis for longer-term national strategies. The press covers very little of this, but the various institutional efforts have begun to develop new strategies that suggest broader possibilities for change. One promising model builds on work in Cleveland, Ohio, where a linked group of workerowned companies has developed, supported in part by the massive purchasing power of local hospitals and universities. These cooperative firms include a solar installation and weatherization company, an industrial scale ecologically advanced laundry, and a greenhouse capable of producing over three million heads of lettuce and 300,000 pounds of herbs a year.62 This effort, modeled in part on the 74,000-person Mondragón cooperative network in the Basque region of Spain, will create new businesses, as time goes on.63 However, its goal is not simply worker ownership, but the democratization of wealth and sustainable community building in general in an extremely poor neighborhood of what was once a thriving industrial city. Linked by a community-serving non-profit corporation and a revolving fund, the companies cannot be sold outside the network; they also return ten percent of their profits to help develop additional worker-owned firms and grow the network. Cities across the United States—and overseas as well—are looking to the Cleveland Model as an inspiration for their own community wealth building efforts. A critical element of the overall sustainability strategy points to what is essentially a quasi-public community stabilizing planning model. Hospitals and universities in the area currently spend $3 billion a year on goods and services—none, until recently, purchased from the immediately surrounding neighborhood. The Cleveland Model is supported in part by decisions of these substantially publicly financed institutions to allocate part of their procurement to the worker-coops in support of a larger community-building agenda. The taxpayer funds that support institutions of this kind thereby do double duty by helping to support the broader community through the new localized purchasing arrangements. The same is true for a range of municipal, state, and other federal policies available to local businesses, including employee-owned firms. Note carefully that such stabilization also undercuts the growth imperative—and suggests principles that can also be applied at higher levels. Such approaches cannot claim to provide all the answers. But a number of exploratory efforts emphasize fundamental changes in underlying political-economic institutions. Developing detailed and sophisticated alternatives that can be refined over time is a prerequisite if we are to stimulate a serious and wide-ranging debate around a broader menu of institutional possibilities for future development than the narrow range of choices commonly discussed. The need for a major change of direction is increasingly obvious. Efforts to cobble together “solutions” to today’s challenges commonly draw upon the very same institutional arrangements and practices that gave rise to the problems in the first place. What is required is a self-conscious effort to face the fact that the system itself has to be changed and a different kind of political economy created. Although precisely what “changing the system” means is obviously a matter of debate, certain key points are clear. The new movements seek a cooperative, caring and community-nurturing economy that is ecologically sustainable, equitable, and socially responsible—one that is based on rethinking and democratizing the nature of ownership at every level and, along with this, challenging the growth paradigm that is the underlying assumption of all conventional policies. In short, these movements seek an economy that gives true priority to people, place, and planet. Such an economy, so different from our own, requires a new vocabulary, beyond the narrow choice between “capitalism” and “socialism.” It’s easy to overestimate the possibilities. Emerging ideas and institutional explorations are limited compared with the power of Wall Street banks and the other corporate giants of the American economy. On the other hand, precisely because the existing structures of power have created enormous economic problems and fueled public anger, the opportunity for a more profound shift exists. Unexpectedly rapid change is not out of the question. We have already seen how, in moments of crisis, the nationalization of auto giants like General Motors and Chrysler can suddenly become a reality. Such crises are likely to be repeated in the future, possibly with more far reaching outcomes over time. When the next financial breakdown occurs, huge injections of public money may well lead to the breakup or de facto takeover of major financial institutions. At the same time, various forms of larger institutional experimentation—and pressure for further experimentation—are also clearly in the cards.

#### Even if there’s resistance, the transition is forced

David Holmgren 13, founder of Holmgren Design Services, an environmental design and consulting firm, inventor of the Permaculture system for regenerative agriculture, 2013, “Crash on Demand: Welcome to the Brown Tech Future,” Simplicity Institute report, <http://simplicityinstitute.org/wp-content/uploads/2011/04/CrashOnDemandSimplicityInstitute.pdf>

The evidence that the global financial system is a not-so-slow moving train crash is getting stronger. That investors and the billion or so middle class people who have any savings and discretionary expenditure are losing faith, might be an understatement. It may be that paralysis and inertia is all that is holding the system together. A collapse in credit could make it very difficult to raise the finance necessary for the ongoing extraction of tar sands, shale gas and other mad resource extraction projects that are accelerating the production of GGE[Greenhouse Gas Emissions]. A deflationary spiral that follows from a credit crisis and collapsing asset (housing, etc.) values could change behaviour to the extent that people stop spending on anything but essentials because of job insecurity and the fact that everything will be cheaper next month. I believe the chances of global economic collapse (in the next five years) being severe enough to achieve this have to be rated at least 50%. Further I believe many climate activists and policy professionals are shifting to at least privately hoping this might be the case because the chances of a planned powerdown seems to be fading. If we accept a global financial crash could make it very difficult, if not impossible, to restart the global economy with anything other than drastically reduced emissions, then an argument can be mounted for putting effort into precipitating that crash, the crash of the financial system. Any such plan would of course invite being blamed for causing it when it happens. No one wants to be strung up along with the bankers for causing a global version of Greece, Egypt or many other countries, let alone the horrors of Syria. On the other hand, we have no precedent to indicate how bad conditions might be in currently affluent countries. The picture I am building is that it is almost inevitable that those who warn of the crisis will get the blame for causing it. So if we are going to be blamed anyway, we could be proactive about it and at least get the advantage for humanity of crisis now, rather than later. For the people of Syria caught in the grip of climate, energy and geopolitical struggle, all this hardly matters because it couldn't get worse for them. In fact conditions in such stricken places could actually improve if global superpower competition is disabled by the collapse of the global finance. Even the average citizen in Greece or Egypt might be hoping to see the remaining affluent countries get a 'taste of their own medicine'. The complexity of global human overshoot, so long predicted, and now unfolding, is far too multifaceted to be captured by any simple story about good, innocence, evil and blame. Before considering whether this is a good idea or not, I want to consider whether concerted action by limited numbers of activists could bring it about? Given the current fragilities of global finance, I believe a radical change in the behaviour of a relatively small proportion of the global middle class could precipitate such a crash. For example a 50% reduction of consumption and 50% conversion of assets into building household and local community resilience by say 10% of the population in affluent countries would show up as 5% reduction in demand in a system built on perpetual growth and a 5% reduction in savings capital available for banks to lend. Small fluctuations in the supply-demand balance can have a massive effect on prices. Further, when the system has been growing due to rising debt, arguably for decades, then the vulnerability to drops in demand can be massive. For example, small drops in demand for new houses and the high fuel costs of commuting for those servicing mortgages, triggered the collapse of the housing bubble in the USA and other countries. It seems obvious to me that it is easier to convince a minority that they will be better off by disengaging from the system than any efforts to build mass movements demanding impossible outcomes or convincing elites to turn off the system that is currently keeping them in power. I accept that many people find the idea of assisting economic collapse abhorrent, even if that collapse is becoming more and more likely as a collective outcome of human actions. Daryl Taylor uses the caring metaphor "hospicing and euthanasing" the old/dying system along with "doula-ing and midwifing the new/emerging system. Whatever the metaphors, climate activists who believe we are on the verge of runaway catastrophic climate change that will be far worse than simply stalling the economy, do have options other than shouting louder for mitigation or shifting to adaptation and defence. Rather than simply planning for bad and rocky energy descent delivered initially by economic depression, they could choose to focus their energy on actively trying to destroy faith in the financial system.

### AT: Developing Countries---2NC

#### Degrowth is especially effective with developing countries

Mikel F. **Qafa 17**. Candidate for a Master’s Degree in philosophy, politics and economics at Witten/Herdecke University, in Germany. 06/2017. “Can Degrowth Rescue Sub-Saharan Africa?” International Journal of Technology Management & Sustainable Development, vol. 16, no. 2, pp. 191–200.

The idea of ‘lesser consumption’ that the Degrowth movement supports is not compatible with the politics of poverty that the Global North (Kegley 2008) has tried to implement in eradicating poverty and inequality in the poorest region of the world. The concept of lesser consumption cannot possibly be referring to this region (as mentioned earlier in the article, a large share of the population still lives under $1.25 a day) as it is, but to the more developed countries of the Global North. One of the schemes that support the Degrowth claims that the North should start reducing economic growth in order to allow for space in the biosphere as the South starts its economic growth stage (Demaria et al. 2014). What we have witnessed in the past decade is that politics in the international system have delayed solutions to climate change and have exacerbated the damage caused to the environment while the world’s ’sweatshops’ – referring to India and China – arduously delay participation in a global climate change agreement (Oatley, 2013). The argument is that this would cause a reduction in economic growth for China and India and drive foreign capital out of the country. They claim that they have the right to continue growing because the United States and Western Europe grew without having any limits on their growth levels. If it took such a long time to get a potential agreement between these global powers,11 we can only estimate the incredibly long time it would take to educate the developing Global South to follow a path towards an imaginary ‘sustainable growth’ (Demaria et al. 2014). Regardless of the efficiency we achieve by each new development (without bringing Jevon’s paradox to light), the amount of biosphere saved by a Degrowth of the Global North would never match the amount of waste a growing Global South would generate. And this is simply taking into account the lack of energy efficiency and the sheer size of the population that will be ready to consume. It is startling to find that the fastest growing economies are not those in developing countries but in the already developed economies, which makes the idea of a North slowdown even harder to believe. A strategy we came across as part of the suggested principles of Degrowth was the use of basic and/or ceiling income for citizens (Demaria et al. 2014). It would be very hard to imagine both of these policies featured in the property and taxation systems of developed countries. Unless we manage to decolonize the imagination of society members into not needing to accumulate wealth and not needing to consume so much, it would be impossible to vote these policies into law. People would not find the basic income policy troubling because that would be in direct confrontation with poverty, but if we are to embrace the maximum income policy it would require quite a restructuring of the existing system. For a moment let us assume that we overrun the institutional complications and manage to establish the maximum income policy into law and the earnings from this policy would go to fund the basic income for the rest of the population. The fundamentals of economics teach us that people will not work as hard if they have a guaranteed basic income, which poses a serious threat to Degrowth. Citizens could be spending this money on importing products or travel, and thus the money will leave the country. The only way for the government to continue this programme would be to either produce new money (inflation and hyperinflation as was the case in Zimbabwe (The Economist 2013)) or promote economic growth. Assuming for argument’s sake that it would not place a problem on the financial feasibility of the programme, this formulation would collapse the innovation and research structures because much of the research conducted nowadays is to provide affordable products to the much larger lower income class and provide high-income citizens with exclusive products and services. The reduction in consumption of the ‘high-income’ class will not be enough to account for the increase in consumption of the lower-income class. When the latter class does not exist anymore, incentives to invest into such research would diminish. But this presents an even greater problem because we end up with more people who can afford products they could not before.12 A surge in consumption and production would follow. This means that we would see Jevon’s13 paradox in reverse as new inventions are created more slowly and consumption for such products diminishes when more expensive products can be afforded. Basic income would be very beneficial to Africa at first because poverty and inequality would be addressed immediately, but with its current economy it would be difficult to imagine this sudden growth in income without an increase in consumption that would exacerbate their ecosystem. A system that runs on these two principles will only see higher consumption levels. Many African communities are still founded on the basis of and structured via communal work and shared activities, and therefore in many parts of the continent [Africa] the Degrowth movement will find more momentum than in the Global North. What needs to change is not only the semantics but the creation of a fair redistributive economics that would not seek to increase the economic pie overall with growth, but would instead slice it differently. Future of Degrowth in Sub-Sharan Africa Among continents, Africa will suffer the greatest harm from climate change because it has a very low adaptive capacity to the effects induced by it. African governments are unable to find means to increase crop yields or potable water sources at the same levels of consumption (Frieden et al. 2009). Global warming will cause severe and long droughts in some regions, along with floods in others, further increasing the continent’s vulnerability. Water sources in Sub-Saharan Africa have already started disappearing at a rate much faster than anticipated. Many plants and species will go extinct as the changes in the ecosystem become harsher. Southern Africa is an area that due to its climate is unable to fight several diseases that otherwise would not thrive in the Global North due to the cold weather. Winter could be considered the world’s most effective public health intervention (Chari and Corbridge 2008). The two most influential international agencies in advising developing countries, IMF and the World Bank, currently place more emphasis on institutional reforms such as overhauling a nation’s civil service or its tax administration than on technologies needed to fight tropical diseases and low agricultural productivity (Frieden et al. 2009). Growing economies of the North demand resources increasingly. As western Corporations seek to expand commodity frontiers by using supplies and resources of the African continent, it further harms the African environment and reduces deposits of resources for the local inhabitants to use in the future. The biggest challenge that modern societies face is in finding sources for its energy needs. Africa has 8 per cent of the world’s fossil fuel reserves and leads in underground resources for only ten of the 100 most used and rare minerals, thus it needs to rethink how it allows the northern corporations extract these resources (Simons 2013). African countries in Sub-Saharan Africa have difficult challenges ahead of them, the most important ones being the reduction of inequality and poverty, eradication of diseases and finding/exploiting renewable energy sources to support their development. According to several research studies, Sub-Saharan Africa can power their entire region on renewable energy (IRENA 2014). Just a fraction of the sunlight that falls on the Sahara desert can satisfy all of the continent’s energy needs now and in the near future, and this is a resource that cannot be exploited by foreign multinationals because energy transportation to other continents is not feasible due to high costs (Taplin 2013). Tapping these resources has the benefit of not allowing African governments to turn into rentier states14 because they cannot export this resource too far from the region. Thus it will boost both economic growth and directly confront the challenges faced by the poorer populations without needing to become the world’s next ’sweatshop’. The geographical advantage of the region with respect to renewable energy production can only be amplified through innovation. Thus, investment in regionwide education is highly recommended. Africa does not need to look at the northern economies as models after which to design their countries, but instead they need to employ strategies that are best suited to their tropical and subtropical environment. Almost none of the programmes that have been established in the West will be effective in this region, including water supply and sanitation. Africa does not need to reinvent western programmes to improve outcomes of health, education, or family planning, but it needs to use design-thinking strategies to create programmes that would be specific to every region and would accommodate for changes that climate change will bring (Brown, 2008) As the world runs after energy, Africa needs to seize the opportunity and create energy from the renewable resources it has been bestowed with. These sources have the highest Energy Return on Energy Invested (EROI) among all renewables. But the path will not be so easy for the countries in Sub-Saharan Africa. Climate change will be harsh on the region and it has the potential to undo the progress that has been achieved until now with respect to the reduction of poverty and disease prevention. Degrowth offers a framework that is difficult to be accepted and implemented in the Global North due to the perception of consumption that is unlikely to change, but it can surely find space for certain principles of it in Africa. After examining the use of GDP as a measure of economic growth and development for a country, we came to the conclusion that it is deeply misleading since it does not portray any sort of development or real growth. Use of other biophysical and social indicators (Demaria et al. 2014) to denote growth and development would help agencies address problems easier as they become more evident and better studied. The other two principles that we assessed in this article were ’basic’ and ’ceiling’ income. Although a largely difficult system to implement because of the necessary changes and uncertainties in the new redistribution system, it would be the most direct way to confront poverty in Africa. The main issue we found with these two principles was a reversal of Jevon’s paradox as invention occurs at a slower rate and that eventually only economic growth and constant consumption would maintain such a system. Time has come for the Global North and Africa to embrace the principles of Degrowth and adapt before they are forced to do so by natural disasters caused by human activity. Further studies in the field will reveal why and how Degrowth will be the framework that will save the planet and humanity. For now we need to acknowledge the damages we have caused15 and focus not only on efficiency improvement but on consuming what is necessary for our subsistence.

### AT: Nuclear War Causes Extinction---1NC

#### Nuclear war can’t cause extinction---first, models

**Reisner et al. 18** [Jon Reisner – Climate and atmospheric scientist at the Los Alamos National Laboratory. Gennaro D’Angelo – Climate scientist at the Los Alamos National Laboratory, Research scientist at the SETI institute, Associate specialist at the University of California, Santa Cruz, NASA Postdoctoral Fellow at the NASA Ames Research Center, UKAFF Fellow at the University of Exeter. Eunmo Koo - Scientist at Applied Terrestrial, Energy, and Atmospheric Modeling (ATEAM) Team, in Computational Earth Science Group (EES-16) in Earth and Environmental Sciences Division and Co-Lead of Parallel Computing Summer Research Internship (PCSRI) program at the Los Alamos National Laboratory, former Staff research associate at UC Berkeley. Wesley Even - Computational scientist in the Computational Physics and Methods Group at Los Alamos National Laboratory. Matthew Hecht – Atmospheric scientist at the Los Alamos National Laboratory. Elizabeth Hunke - Lead developer for the Los Alamos Sea Ice Model (CICE) at the Los Alamos National Laboratory responsible for development and incorporation of new parameterizations, model testing and validation, computational performance, documentation, and consultation with external model users on all aspects of sea ice modeling, including interfacing with global climate and earth system models. Darin Comeau – Climate scientist at the Los Alamos National Laboratory, Randy Bos - Project leader at the Los Alamos National Laboratory, former Weapons Effects program manager at Tech-Source, James Cooley – Computational scientist at the Los Alamos National Laboratory specializing in weapons physics, emergency response, and computational physics, “Climate impact of a regional nuclear weapons exchange:An improved assessment based on detailed source calculations,” March 16, 2018, <https://agupubs.onlinelibrary.wiley.com/doi/full/10.1002/2017JD027331>]

The no-rubble simulation produces a significantly more intense fire, with more fire spread, and consequently a significantly stronger plume with larger amounts of BC reaching into the upper atmosphere than the simulation with rubble, illustrated in Figure 5. While the no-rubble simulation represents the worst-case scenario involving vigorous fire activity, only a relatively small amount of carbon makes its way into the stratosphere during the course of the simulation. But while small compared to the surface BC mass, stratospheric BC amounts from the current simulations are significantly higher than what would be expected from burning vegetation such as trees (Heilman et al., 2014), e.g., the higher energy density of the building fuels and the initial fluence from the weapon produce an intense response within HIGRAD with initial updrafts of order 100 m/s in the lower troposphere. Or, in comparison to a mass fire, wildfires will burn only a small amount of fuel in the corresponding time period (roughly 10 minutes) that a nuclear weapon fluence can effectively ignite a large area of fuel producing an impressive atmospheric response. Figure 6 shows vertical profiles of BC multiplied by 100 (number of cities involved in the exchange) from the two simulations. The total amount of BC produced is in line with previous estimates (about 3.69 Tg from no-rubble simulation); however, the majority of BC resides below the stratosphere (3.46 Tg below 12 km) and can be readily impacted by scavenging from precipitation either via pyro-cumulonimbus produced by the fire itself (not modeled) or other synoptic weather systems. While the impact on climate of these more realistic profiles will be explored in the next section, it should be mentioned that these estimates are still at the high end, considering the inherent simplifications in the combustion model that lead to overestimating BC production. 3.3 Climate Results Long-term climatic effects critically depend on the initial injection height of the soot, with larger quantities reaching the upper troposphere/lower stratosphere inducing a greater cooling impact because of longer residence times (Robock et al., 2007a). Absorption of solar radiation by the BC aerosol and its subsequent radiative cooling tends to heat the surrounding air, driving an initial upward diffusion of the soot plumes, an effect that depends on the initial aerosol concentrations. Mixing and sedimentation tend to reduce this process, and low altitude emissions are also significantly impacted by precipitation if aging of the BC aerosol occurs on sufficiently rapid timescales. But once at stratospheric altitudes, aerosol dilution via coagulation is hindered by low particulate concentrations (e.g., Robock et al., 2007a) and lofting to much higher altitudes is inhibited by gravitational settling in the low-density air (Stenke et al., 2013), resulting in more stable BC concentrations over long times. Of the initial BC mass released in the atmosphere, most of which is emitted below 9 km, 70% rains out within the first month and 78%, or about 2.9 Tg, is removed within the first two months (Figure 7, solid line), with the remainder (about 0.8 Tg, dashed line) being transported above about 12 km (200 hPa) within the first week. This outcome differs from the findings of, e.g., Stenke et al. (2013, their high BC-load cases) and Mills et al. (2014), who found that most of the BC mass (between 60 and 70%) is lifted in the stratosphere within the first couple of weeks. This can also be seen in Figure 8 (red lines) and in Figure 9, which include results from our calculation with the initial BC distribution from Mills et al. (2014). In that case, only 30% of the initial BC mass rains out in the troposphere during the first two weeks after the exchange, with the remainder rising to the stratosphere. In the study of Mills et al. (2008) this percentage is somewhat smaller, about 20%, and smaller still in the experiments of Robock et al. (2007a) in which the soot is initially emitted in the upper troposphere or higher. In Figure 7, the e-folding timescale for the removal of tropospheric soot, here interpreted as the time required for an initial drop of a factor e, is about one week. This result compares favorably with the “LT” experiment of Robock et al. (2007a), considering 5 Tg of BC released in the lower troposphere, in which 50% of the aerosols are removed within two weeks. By contrast, the initial e-folding timescale for the removal of stratospheric soot in Figure 8 is about 4.2 years (blue solid line), compared to about 8.4 years for the calculation using Mills et al. (2014) initial BC emission (red solid line). The removal timescale from our forced ensemble simulations is close to those obtained by Mills et al. (2008) in their 1 Tg experiment, by Robock et al. (2007a) in their experiment “UT 1 Tg”, and © 2018 American Geophysical Union. All rights reserved. by Stenke et al. (2013) in their experiment “Exp1”, in all of which 1 Tg of soot was emitted in the atmosphere in the aftermath of the exchange. Notably, the e-folding timescale for the decline of the BC mass in Figure 8 (blue solid line) is also close to the value of about 4 years quoted by Pausata et al. (2016) for their long-term “intermediate” scenario. In that scenario, which is also based on 5 Tg of soot initially distributed as in Mills et al. (2014), the factor-of2 shorter residence time of the aerosols is caused by particle growth via coagulation of BC with organic carbon. Figure 9 shows the BC mass-mixing ratio, horizontally averaged over the globe, as a function of atmospheric pressure (height) and time. The BC distributions used in our simulations imply that the upward transport of particles is substantially less efficient compared to the case in which 5 Tg of BC is directly injected into the upper troposphere. The semiannual cycle of lofting and sinking of the aerosols is associated with atmospheric heating and cooling during the solstice in each hemisphere (Robock et al., 2007a). During the first year, the oscillation amplitude in our forced ensemble simulations is particularly large during the summer solstice, compared to that during the winter solstice (see bottom panel of Figure 9), because of the higher soot concentrations in the Northern Hemisphere, as can be seen in Figure 11 (see also left panel of Figure 12). Comparing the top and bottom panels of Figure 9, the BC reaches the highest altitudes during the first year in both cases, but the concentrations at 0.1 hPa in the top panel can be 200 times as large. Qualitatively, the difference can be understood in terms of the air temperature increase caused by BC radiation emission, which is several tens of kelvin degrees in the simulations of Robock et al. (2007a, see their Figure 4), Mills et al. (2008, see their Figure 5), Stenke et al. (2013, see high-load cases in their Figure 4), Mills et al. (2014, see their Figure 7), and Pausata et al. (2016, see one-day emission cases in their Figure 1), due to high BC concentrations, but it amounts to only about 10 K in our forced ensemble simulations, as illustrated in Figure 10. Results similar to those presented in Figure 10 were obtained from the experiment “Exp1” performed by Stenke et al. (2013, see their Figure 4). In that scenario as well, somewhat less that 1 Tg of BC remained in the atmosphere after the initial rainout. As mentioned before, the BC aerosol that remains in the atmosphere, lifted to stratospheric heights by the rising soot plumes, undergoes sedimentation over a timescale of several years (Figures 8 and 9). This mass represents the effective amount of BC that can force climatic changes over multi-year timescales. In the forced ensemble simulations, it is about 0.8 Tg after the initial rainout, whereas it is about 3.4 Tg in the simulation with an initial soot distribution as in Mills et al. (2014). Our more realistic source simulation involves the worstcase assumption of no-rubble (along with other assumptions) and hence serves as an upper bound for the impact on climate. As mentioned above and further discussed below, our scenario induces perturbations on the climate system similar to those found in previous studies in which the climatic response was driven by roughly 1 Tg of soot rising to stratospheric heights following the exchange. Figure 11 illustrates the vertically integrated mass-mixing ratio of BC over the globe, at various times after the exchange for the simulation using the initial BC distribution of Mills et al. (2014, upper panels) and as an average from the forced ensemble members (lower panels). All simulations predict enhanced concentrations at high latitudes during the first year after the exchange. In the cases shown in the top panels, however, these high concentrations persist for several years (see also Figure 1 of Mills et al., 2014), whereas the forced ensemble simulations indicate that the BC concentration starts to decline after the first year. In fact, in the simulation represented in the top panels, mass-mixing ratios larger than about 1 kg of BC © 2018 American Geophysical Union. All rights reserved. per Tg of air persist for well over 10 years after the exchange, whereas they only last for 3 years in our forced simulations (compare top and middle panels of Figure 9). After the first year, values drop below 3 kg BC/Tg air, whereas it takes about 8 years to reach these values in the simulation in the top panels (see also Robock et al., 2007a). Over crop-producing, midlatitude regions in the Northern Hemisphere, the BC loading is reduced from more than 0.8 kg BC/Tg air in the simulation in the top panels to 0.2-0.4 kg BC/Tg air in our forced simulations (see middle and right panels). The more rapid clearing of the atmosphere in the forced ensemble is also signaled by the soot optical depth in the visible radiation spectrum, which drops below values of 0.03 toward the second half of the first year at mid latitudes in the Northern Hemisphere, and everywhere on the globe after about 2.5 years (without never attaining this value in the Southern Hemisphere). In contrast, the soot optical depth in the calculation shown in the top panels of Figure 11 becomes smaller than 0.03 everywhere only after about 10 years. The two cases show a similar tendency, in that the BC optical depth is typically lower between latitudes 30º S-30º N than it is at other latitudes. This behavior is associated to the persistence of stratospheric soot toward high-latitudes and the Arctic/Antarctic regions, as illustrated by the zonally-averaged, column-integrated mass-mixing ratio of the BC in Figure 12 for both the forced ensemble simulations (left panel) and the simulation with an initial 5 Tg BC emission in the upper troposphere (right panel). The spread in the globally averaged (near) surface temperature of the atmosphere, from the control (left panel) and forced (right panel) ensembles, is displayed in Figure 13. For each month, the plots show the largest variations (i.e., maximum and minimum values), within each ensemble of values obtained for that month, relative to the mean value of that month. The plot also shows yearly-averaged data (thinner lines). The spread is comparable in the control and forced ensembles, with average values calculated over the 33-years run length of 0.4-0.5 K. This spread is also similar to the internal variability of the globally averaged surface temperature quoted for the NCAR Large Ensemble Community Project (Kay et al., 2015). These results imply that surface air temperature differences, between forced and control simulations, which lie within the spread may not be distinguished from effects due to internal variability of the two simulation ensembles. Figure 14 shows the difference in the globally averaged surface temperature of the atmosphere (top panel), net solar radiation flux at surface (middle panel), and precipitation rate (bottom panel), computed as the (forced minus control) difference in ensemble mean values. The sum of standard deviations from each ensemble is shaded. Differences are qualitatively significant over the first few years, when the anomalies lie near or outside the total standard deviation. Inside the shaded region, differences may not be distinguished from those arising from the internal variability of one or both ensembles. The surface solar flux (middle panel) is the quantity that appears most affected by the BC emission, with qualitatively significant differences persisting for about 5 years. The precipitation rate (bottom panel) is instead affected only at the very beginning of the simulations. The red lines in all panels show the results from the simulation applying the initial BC distribution of Mills et al. (2014), where the period of significant impact is much longer owing to the higher altitude of the initial soot distribution that results in longer residence times of the BC aerosol in the atmosphere. When yearly averages of the same quantities are performed over the IndiaPakistan region, the differences in ensemble mean values lie within the total standard deviations of the two ensembles. The results in Figure 14 can also be compared to the outcomes of other previous studies. In their experiment “UT 1 Tg”, Robock et al. (2007a) found that, when only 1 Tg of soot © 2018 American Geophysical Union. All rights reserved. remains in the atmosphere after the initial rainout, temperature and precipitation anomalies are about 20% of those obtained from their standard 5 Tg BC emission case. Therefore, the largest differences they observed, during the first few years after the exchange, were about - 0.3 K and -0.06 mm/day, respectively, comparable to the anomalies in the top and bottom panels of Figure 14. Their standard 5 Tg emission case resulted in a solar radiation flux anomaly at surface of -12 W/m2 after the second year (see their Figure 3), between 5 and 6 time as large as the corresponding anomalies from our ensembles shown in the middle panel. In their experiment “Exp1”, Stenke et al. (2013) reported global mean surface temperature anomalies not exceeding about 0.3 K in magnitude and precipitation anomalies hovering around -0.07 mm/day during the first few years, again consistent with the results of Figure 14. In a recent study, Pausata et al. (2016) considered the effects of an admixture of BC and organic carbon aerosols, both of which would be emitted in the atmosphere in the aftermath of a nuclear exchange. In particular, they concentrated on the effects of coagulation of these aerosol species and examined their climatic impacts. The initial BC distribution was as in Mills et al. (2014), although the soot burden was released in the atmosphere over time periods of various lengths. Most relevant to our and other previous work are their one-day emission scenarios. They found that, during the first year, the largest values of the atmospheric surface temperature anomalies ranged between about -0.5 and -1.3 K, those of the sea surface temperature anomalies ranged between -0.2 and -0.55 K, and those of the precipitation anomalies varied between -0.15 and -0.2 mm/day. All these ranges are compatible with our results shown in Figure 14 as red lines and with those of Mills et al. (2014, see their Figures 3 and 6). As already mentioned in Section 2.3, the net solar flux anomalies at surface are also consistent. This overall agreement suggests that the inclusion of organic carbon aerosols, and ensuing coagulation with BC, should not dramatically alter the climatic effects resulting from our forced ensemble simulations. Moreover, aerosol growth would likely shorten the residence time of the BC particulate in the atmosphere (Pausata et al., 2016), possibly reducing the duration of these effects.

#### Second, islands

Turchin and Green 18 [Alexey Turchin, Scientist for the Foundation Science for Life Extension in Moscow, Russia, Founder of Digital Immortality Now, author of several books and articles on the topics of existential risks and life extension, and Brian Patrick Green – Director of technology ethics at the Markkula Center for Applied Ethics, teaches AI ethics in the Graduate School of Engineering at Santa Clara University, “Islands as refuges for surviving global catastrophes,” September 2018, July 20, 2019, <https://www.emerald.com/insight/content/doi/10.1108/FS-04-2018-0031/full/html?fullSc=1&mbSc=1&fullSc=1>]

Different types of possible catastrophes suggest different scenarios for how survival could happen on an island. What is important is that the island should have properties which protect against the specific dangers of particular global catastrophic risks. Specifically, different islands will provide protection against different risks, and their natural diversity will contribute to a higher total level of protection: Quarantined island survives pandemic. An island could impose effective quarantine if it is sufficiently remote and simultaneously able to protect itself, possibly using military ships and air defense. Far northern aboriginal people survive an ice age. Many far northern people have adapted to survive in extremely cold and dangerous environments, and under the right circumstances could potentially survive the return of an ice age. However, their cultures are endangered by globalization. If these people become dependent on the products of modern civilization, such as rifles and motor boats, and lose their native survival skills, then their likelihood of surviving the collapse of the outside world would decrease. Therefore, preservation of their survival skills may be important as a defense against the risks connected with extreme cooling. Remote polar island with high mountains survives brief global warming of median surface temperatures, up to 50˚C. There is a theory that the climates of planets similar to the Earth could have several semi-stable temperature levels (Popp et al., 2016). If so, because of climate change, the Earth could transition to a second semi-stable state with a median global temperature of around 330 K, about 60˚C, or about 45˚C above current global mean temperatures. But even in this climate, some regions of Earth could still be survivable for humans, such as the Himalayan plateau at elevations above 4,000 m, but below 6,000 (where oxygen deficiency becomes a problem), or on polar islands with mountains (however, global warming affects polar regions more than equatorial regions, and northern island will experience more effects of climate change, including thawing permafrost and possible landslides because of wetter weather). In the tropics, the combination of increased humidity and temperature may increase the wet bulb temperature above 36˚C, especially on islands, where sea moisture is readily available. In such conditions, proper human perspiration becomes impossible (Sherwood and Huber, 2010), and there will likely be increased mortality and morbidity because of tropical diseases. If temperatures later returned to normal – either naturally or through climate engineering – the rest of the Earth could be repopulated. ‘‘Swiss Family Robinsons’’ survive on a tropical island, unnoticed by a military robot ‘‘mutiny’’. Most AI researchers ignore medium-term AI risks, which are neither near-term risks, like unemployment, nor remote risks, like AI superintelligence. But a large drone army – if one were produced – could receive a wrong command or be infected by a computer virus, leading it to attack people indiscriminately. Remote islands without robots could provide protection in this case, allowing survival until such a drone army ran out of batteries, fuel, ammunition or other supplies: Primitive tribe survives civilizational collapse. The inhabitants of North Sentinel Island, near the Andaman Islands in the Indian Ocean, are hostile and uncontacted. The Sentinelese survived the 2004 Indian Ocean tsunami apparently unaffected(Voanews, 2009), and if the rest of humanity disappear, they might well continue their existence without change**.** Tropical Island survives extreme global nuclear winter and glaciation event. Were a nuclear, bolide impactor or volcanic “winter” scenario to unfold, these islands would remain surrounded by Warm Ocean, and local volcanism or other energy sources might provide heat, energy and food. Such island refuges may have helped life on Earth survive during the **“**Snowball Earth” event in Earth’s distant past (Hoffman et al., 1998). Remote island base for project “Yellow submarine”. Some catastrophic risks such as a gamma ray burst, a global nuclear war with high radiological contamination or multiple pandemics might be best survived underwater in nuclear submarines (Turchin and Green, 2017). However, after a catastrophe, the submarine with survivors would eventually need a place to dock, and an island with some prepared amenities would be a reasonable starting point for rebuilding civilization. Bunker on remote island. For risks which include multiple or complex catastrophes, such as a bolide impact, extreme volcanism, tsunamis, multiple pandemics and nuclear war with radiological contamination, island refuges could be strengthened with bunkers. Richard Branson survived hurricane Irma on his own island in 2017 by seeking refuge in his concrete wine cellar (Clifford, 2017). Bunkers on islands would have higher survivability compared to those close to population centers, as they will be neither a military target nor as accessible to looters or unintentionally dangerous (e.g. infected) refugees. These bunkers could potentially be connected to water sources by underwater pipes, and passages could provide cooling, access and even oxygen and food sources.

### AT: Disease---2NC

#### Disease won’t cause extinction – even before we had our current level of health infrastructure and sanitation, even the most virulent strains of disease didn’t cause extinction

Halstead 19 John Halstead, doctorate in political philosophy. [Cause Area Report: Existential Risk, Founders Pledge, https://founderspledge.com/research/Cause%20Area%20Report%20-%20Existential%20Risk.pdf]//BPS

However, there are some reasons to think that naturally occurring pathogens are unlikely to cause human extinction. Firstly, Homo sapiens have been around for 200,000 years and the Homo genus for around six million years without being exterminated by an infectious disease, which is evidence that the base rate of extinction-risk natural pathogens is low.82 Indeed, past disease outbreaks have not come close to rendering humans extinct. Although bodies were piled high in the streets across Europe during the Black Death,83 human extinction was never a serious possibility, and some economists even argue that it was a boon for the European economy.84 Secondly, infectious disease has only contributed to the extinction of a small minority of animal species.85 The only confirmed case of a mammalian species extinction being caused by an infectious disease is a type of rat native only to Christmas Island.

#### Seriously never in 3.8 billion years of life

Easterbrook 18 Gregg Easterbrook, fellow in economics and government studies at the Brookings Institute and a fellow in international affairs at the Fulbright Foundation. [It’s better than it looks: the case for optimism in an age of fear, first edition, New York: PublicAffairs, Hachette Book Group]//BPS

DISEASES CAUSE SUFFERING BUT DO not run wild mainly because the biosphere is elaborately conditioned to defeat germs and viruses. So far as is known, there has never been an unstoppable contagion—“never” in this sense not meaning “recently” but never: not during the 3.8 billion years life has existed. Mammal bodies contain an amazing range of proteins and biological pathways that arose to counteract contagion. Animals, plants, and pathogens developed jointly: the living ecosystem has been resisting disease for eons. Had any disease ever “won,” the result would have been lights-out for the disease, which would have lost its hosts. That plants, mammals, and people are here is proof the diseases don’t win.

### AT: EMPs---2NC

#### No impact to EMPs

Hall 19 [Allen Hall, expert in Aerospace Management, Manufacturing, Engineering and IT, worked closely with the military, research labs, FFRDC’s, AFRL, NAVSEA / NAVAIR, all the major ALC’s and all the aerospace OEM’s,“Who would win in a war between Russia and the US?,” March 25, 2019, <https://www.quora.com/Who-would-win-in-a-war-between-Russia-and-the-US/answer/Allen-E-Hall-2>]

In the case of high altitude nuclear bursts, two main EMP types come into play, “fast pulse” and the “slow pulse.” The fast pulse EMP field is created by gamma ray interaction with stratospheric air molecules. It peaks at tens of kilovolts per meter in a few nanoseconds, and lasts for a few hundred nanoseconds. The broad-band frequency content of (0-1000 megahertz) enables it to couple to electrical and electronic systems in general, regardless of the length of their penetrating cables and antenna lines. Induced currents range into the 1,000s of amperes. The “slow pulse” EMP is caused by the distortion of the earth’s magnetic field lines due to the expanding nuclear fireball and rising of heated and ionized layers of the ionosphere. These effects are limited to Earth's Ionosphere, a range of altitude between 50 and 600 miles above the earth’s surface. The strength of EMP’s are limited bt the Gamma ray release of the nuclear explosion. A bomb not specifically designed to enhance this will not normally result in a high field strength value and the EMP will do little permanent as a result.

Diagram

Description automatically generated

As an example, the chart above shows the effect of prompt Gamma ray output and how it affects field strength. [67] The 1.4 MT Starfish Prime test produced a 1.4kt prompt Gamma Ray output which resulted in a peak field strength of about 50,000 v/m. This is about the minimum energy needed to do substantial damage to a country's electrical systems but even at that level many things would be left unharmed as the danger diminishes with distance. Starfish produced the largest fields of the high-altitude detonations; they caused outages of the series-connected street-lighting systems of Oahu (Hawaii), probable failure of a microwave repeating station on Kauai, failure of the input stages of ionospheric sounders and damage to rectifiers in communication receivers, Other than the failure of the microwave link, no problem was noted in the telephone system. No failure was noted in the telemetry systems used for data transmission on board the many instrumentation rockets. There was no apparent increase in radio or television repairs subsequent to any of the Johnson Island detonations. The failures observed were generally in the unprotected input stages of receivers or in rectifiers of electronic equipment; transients on the power line probably caused the rectifier failures. There was one failure in the unprotected part of an electronic system of the LASL Optical Station on top of Mount Haleakala on Maui Island.[68] DoD EMP SIMULATIONS TESTS We tested a sample of 37 cars in an EMP simulation laboratory, with automobile vintages ranging from 1986 through 2002. ... The most serious effect observed on running automobiles was that the motors in three cars stopped at field strengths of approximately 30 kV/m or above. In an actual EMP exposure, these vehicles would glide to a stop and require the driver to restart them. Electronics in the dashboard of one automobile were damaged and required repair. Based on these test results, we expect few automobile effects at EMP field levels below 25 kV/m. Approximately 10 percent or more of the automobiles exposed to higher field levels may experience serious EMP effects, including engine stall, that require driver intervention to correct. Five of the 18 trucks tested did not exhibit any anomalous response up to field strengths of approximately 50 kV/m. Based on these test results, we expect few truck effects at EMP field levels below approximately 12 kV/m. At higher field levels, 70 percent or more of the trucks on the road will manifest some anomalous response following EMP exposure. Approximately 15 percent or more of the trucks will experience engine stall, sometimes with permanent damage that the driver cannot correct. Results indicate that some computer failures can be expected at relatively low EMP field levels of 3 to 6 kilovolts per meter (kV/m). At higher field levels, additional failures are likely in computers, routers, network switches, and keyboards embedded in the computer-aided dispatch, public safety radio, and mobile data communications equipment. ... none of the radios showed any damage with EMP fields up to 50 kV/m. While many of the operating radios experienced latching upsets at 50 kV/m field levels, these were correctable by turning power off and then on.[69] Contrary to many sensational headlines, the US Military is well protected from most EMP’s. For decades now the military has defined systems around survivability. The details of such are contained here: E.6 Military Standards DTRA and its predecessor agencies have developed, and regularly update, military standards (MIL-STDs) designed to aid in the design, development, test, and evaluation of DoD systems subjected to nuclear and EMP environments. These MIL-STDs cover nuclear-generated EMP survivability of aircraft, maritime, and other systems in coordination with the Air Force and the Navy, as well as the broader community of stakeholders. The following are some of the relevant MIL-STDs: MIL-STD-1766, Nuclear Hardness and Survivability Program Requirements for ICBM Weapon Systems defines nuclear hardness and survivability requirements and practices for use during the concept exploration, demonstration and validation, full-scale development, production, and deployment phases of the acquisition life-cycle of ICBM weapon systems. MIL-STD-2169C, HEMP Environment Standard (Classified) defines high-altitude EMP environments for system hardness design and testing. MIL-STD-3023, HEMP Protection for Military Aircraft establishes design margin, performance metrics, and test protocols for HEMP protection of military aircraft with nuclear EMP survivability at three hardness levels. This MIL-STD may also be used for aircraft that support multiple missions. Subsystems of the aircraft required to fully comply with the provisions of the standard are designated as Mission-Critical Subsystems having a HEMP survivability requirement. This approach also allows for consideration of platforms not yet addressed in this standard, such as Unmanned Aerial Vehicles. MIL-STD-188-125, HEMP Protection for Ground-Based C4I Facilities Performing Critical, Time Urgent Missions is in the process of being updated. DTRA is investigating present capabilities and shortfalls of power filters as well as utilizing test results from EMP simulators. MIL-STD-4023, Maritime EMP Standard establishes performance metrics, test protocols, and hardness margin levels for HEMP protection of military surface ships that must function when subjected to a HEMP environment. Satellite System Nuclear Survivability (SSNS) Environment Standard defines nuclear weapon environment levels for evaluating satellite system performance in nuclear scenarios. Comprehensive Atmospheric Nuclear Environments Standard (CANES) provides detailed nuclear environments and effects for a number of different nuclear weapon-types as a function of height of burst. A supplement to this MIL-STD covers nuclear-disturbed communication environments and nuclear ground burst environments.[70] DoD has adopted protective priorities using commercial protective equipment. The Department of Defense (DoD) has experience in prioritizing and protecting systems since the 1960s. The DoD has prioritized and has protected selected systems against EMP (and, by similitude to E3, GMD effects). DoD places emphasis on protecting its strategic triad and associated command, control, communications, computer, and intelligence (C4I) systems. Nuclear EMP will burn out every exposed electronic system is FALSE. The DoD and Congressional EMP Commission’s EMP test data demonstrates that smaller, self-contained systems that are not connected to long-lines tend not to be affected by EMP fields**.** Examples of such systems include vehicles, hand-held radios, and disconnected portable generators. If there is an effect on these systems, it is more often temporary upset rather than component burnout. [71] The NRC on Nuclear Power Facilities Vulnerabilities “The most probable effect of EMP on a modern nuclear power plant is an unscheduled shutdown. EMP may also cause an extended shutdown by the unnecessary activation of some safety-related systems. In general, EMP would be a nuisance to nuclear plants, but it is not considered a serious threat to plant safety. Counter-measures to minimize the effects of EMP have been recommended. Implementation of these recommendations would also increase the protection of the plant against damage by lightning, switching, and electromagnetic interference transients as well as general failures in electrical, control, and instrument power. “[72] As part of a larger EMP study in the 1980’s Sandia Laboratories analyzed the “worst case” scenario and concluded that EMP poses no substantial threat to such (nuclear**)** plants based upon both analysis and simulated EMP tests.[73] The NRC’s current statement The NRC requires U.S. nuclear power plants to be able to shut down safely in the face of many extreme events – tornados, hurricanes and earthquakes. But the NRC also takes into account far more unusual events, like solar flares and man-made electromagnetic pulse (EMP). Both can affect generators, transformers and other parts of the electric grid – which in turn could affect nuclear power plants. The NRC has been examining these issues for more than 30 years, starting in the late 1970s when the agency studied how EMP could affect nuclear power plant safe-shutdown systems. In February 1983 the NRC issued the study’s conclusion: nuclear power plants’ safety systems can do their jobs after an EMP event. The agency revisited the issue in 2007 to account for the increasing use of digital computer systems in nuclear plants, which potentially could be more susceptible to EMP. The agency continued to conclude as recently as two years ago that nuclear power plants can safely shut down following an EMP event. Additional research in 2010 analyzed and compared solar or geomagnetically-induced current events to those of the EMP events previously analyzed. This work led to the same conclusion as the EMP studies – U.S. nuclear power plants can safely shut down if a solar storm disrupts the grid. The edge of the NRC’s authority lies in a nuclear power plant’s electric switchyard, where our rules mesh with those of the Federal Energy Regulatory Commission, which oversees the nation’s electric grids. Another body, the North American Electric Reliability Corporation develops and enforces grid reliability standards. The NRC works closely with FERC and NERC on grid reliability issues, including the effects of solar or geomagnetic storms and EMP. In 2015 FERC began the process of creating reliability standards to protect the grid against these events.[74] This new standard was made into law on November, 17, 2016.[75][76] The NRC continues to update operator guidelines and requirements with changes in technology or new understandings on issues previously not covered such as the events at Fukushima in 2011. Safety enhancements on topics like spent fuel cooling pools are covered in regular NRC updates, the latest being 2015 titled Mitigation of Beyond-Design-Basis Events[77] . EMP Comparisons with lightning Lightning shares many of characteristics of E2, but contrary to what is often quoted, its magnitude can exceed even the peak E1 fields in the discharge region. Research on lightning indicates that a stroke may contain significant components with rise-time of less than 10−7 sec and electric fields greater than 106V/m—more than a order of magnitude greater than even the highest peak E1 fields, from the biggest nuclear devices. The implications of lightning research for EMP vulnerability is a critical topic to include in any future peer-reviewed study of the EMP threat.[78]

### AT: Famine---2NC

#### No famine impact

Denkenberger et al. 17 [David, International Journal of Disaster Risk Reduction, Global Catastrophic Risk Institute, Jan 5, 2017, “Feeding Everyone if the Sun is Obscured and Industry is Disabled,” <https://www-sciencedirect-com.proxy.lib.umich.edu/science/article/pii/S2212420916305453>]

For combined sun blocking and industrial failure scenarios, the reduced output of conventional agriculture would present a threat of causing mass starvation. This study showed that one solution in the short term is extracting edible calories from killed leaves using distributed mechanical processes. Then a constrained food web could be formed where part of the remainder from this could be fed to chickens, and the rest coupled with leaf litter could have mushrooms grown on it. A second group of solutions is growing mushrooms on dead trees and the residue going to cellulose digesting animals such as cattle and rabbits. Typically, in these catastrophes the sun is not blocked completely, so some agriculture would be possible based off of existing farming in extreme environments (e.g. growing UV and cold tolerant crops in the tropics). Furthermore, the cooling climate would cool the upper layer of the ocean, causing upwelling of nutrient-rich deep ocean water. This would facilitate algae growth in the ocean, feeding fish; retrofitting of ships to be sail powered could enable significant fishing. The results of this study show these solutions could enable the feeding of everyone given minimal preparation, and this preparation should be a high priority now.

### AT: Food/Starvation---2NC

#### And the ag system is unsustainable now – nutrient cycles, soil erosion, social dislocation, energy, climate change – try or die for a shift

McMichael 16 (Philip McMichael, professor of development sociology at Cornell University, “Food Security, Land, and Development”, 11 June 2016, The Palgrave Handbook of International Development. Palgrave Macmillan, London, https://doi.org/10.1057/978-1-137-42724-3\_37)

Monopolising land for agro-industry and emission offsets is unsustainable over the longer run. Industrial agriculture has experienced a declining biophysical productivity, with soil depletion and a drop in efficiency of nitrogen use from 60% to 20% from the 1950s to the 1990s (Ploeg 2010, 100), and the expense of ‘biophysical override’ rising with the price of commodity inputs, including energy (Weis 2007 ). These trends are expressed in falling agro-industrial grain yields—from increases between 5 % and 10 % at the height of the green revolution (1960s) to 1 % or less in the new millennium (Cribb 2010 : 8). Further, soil erosion occurs at a rate likely to destroy two-thirds of the world’s productive land by 2050, the global nutrient cycle is declining with the exhaustion of world phosphate reserves, there is rising competition for freshwater for agriculture, which already uses 70 %, and the ocean fish catch is predicted to collapse by 2040 (Cribb 2010 : 10–11, 54, 76). Meanwhile, the industrial food system ‘expends 10–15 energy calories to produce 1 calorie of food, constituting a reversal of the original purpose of agriculture’ (Taylor 2014 : 92). Related to this resource intensiveness is the substantial responsibility of modern agriculture for approximately 30 % of greenhouse gas emissions (McMichael et al. 2007 ; Sage 2012 : 113). 16 In other words, the industrial food system is a source of the problem for which it is considered the solution.

As above, recycling the problem as solution is embedded in an ontology that assumes small scale, localised production systems are inadequate to modern needs. But modern needs are filtered through the market lens, in turn, jeopardising social sustainability. As the IAASTD report noted, markets fail to adequately value environmental and social harm (2008). That is, application of a standardising metric deepens market rule, and interprets social needs and ‘ecosystem services’ in interchangeable and abstract terms—much like the abstraction of nature in value theory. The IAASTD continues: ‘the path of global agricultural development has been narrowly focused on increased productivity rather than on a more holistic integration of natural resource management with food and nutritional security’ (Ibid: 17–18)—underlining agriculture’s multifunctional contribution to complex social reproduction issues, including restoring soil fertility and maintaining ecological resilience. The IAASTD report coincided with and contributed to an emerging scientific consensus that the relative yields of organic/agro-ecological versus non-organic farming are sufficient to provision the current daily average consumption of calories across the world (Pretty and Hine 2001 ; Pretty et al. 2003 ; Badgley et al. 2007 ; CFS 2013 ). Further: ‘research shows that small farms are more productive than large farms if total output is considered rather than yield from a single crop….Yield advantages can range from 20 to 60 per cent, because polycultures reduce losses due to weeds, insects and diseases and make a more efficient use of the available resources of water, light and nutrients’ (Altieri and Nicholls 2008 : 474).

#### But the transition solves – small farms produce enough foods sustainably

Altieri 09 (Miguel A. Altieri, professor of agroecology at the University of California at Berkeley, “Agroecology, Small Farms, and Food Sovereignty”, Jul 01, 2009, https://monthlyreview.org/2009/07/01/agroecology-small-farms-and-food-sovereignty/)

Small Farmers as Key Actors for Regional Food Security

In Latin America, there were about 16 million peasant production units in the late 1980s, occupying close to 60.5 million hectares—34.5 percent of the total cultivated land. The peasant population includes 75 million people representing almost two-thirds of Latin America’s total rural population. The average farm size of these units is about 1.8 hectares, although the contribution of peasant agriculture to the general food supply in the region is significant. These small units of production were responsible for 41 percent of the agricultural output for domestic consumption and for producing at the regional level, 51 percent of the maize, 77 percent of the beans, and 61 percent of the potatoes.7 The contribution to food security of this small-farm sector is today as crucial as twenty-five years ago.

Africa has approximately 33 million small farms, representing 80 percent of all farms in the region. The majority of African farmers (many of them are women) are smallholders, with two-thirds of all farms below 2 hectares and 90 percent of farms below 10 hectares. Most small farmers practice “low-resource” agriculture which is based primarily on the use of local resources, but which may make modest use of external inputs. Low-resource agriculture produces the majority of grains, almost all root, tuber, and plantain crops, and the majority of legumes. Most basic food crops are grown by small farmers with virtually no or little use of fertilizers and improved seed.8 This situation, however, has changed in the last two decades as food production per capita has declined in Africa. Once self-sufficient in cereals, Africa now has to import millions of tons to fill the gap. Despite this increase in imports, smallholders still produce most of Africa’s food.

In Asia, China alone accounts for almost half the world’s small farms (on 193 million hectares), followed by India with 23 percent, and Indonesia, Bangladesh, and Vietnam. Of the majority of more than 200 million rice farmers who live in Asia, few cultivate more than 2 hectares of rice. China has probably 75 million rice farmers who still practice methods similar to those used more than 1,000 years ago. Local cultivars, grown mostly on upland ecosystems and/or under rain-fed conditions, make up the bulk of the rice produced by Asian small farmers.9

#### Tipping point is now – crisis now is *better* than environmental collapse

Tilzey 18 (Mark, Senior Research Fellow in Governance of Food and Farming Systems, Centre for Agroecology, Water and Resilience at Coventry University, *Political Ecology, Food regimes, and Food Sovereignty*: *Crisis, Resistance, and Resilience*, 2018)

Cumulative resistance to both super-exploitation and to accumulation by dispossession, by proletarian, semi-proletarian, peasant and indigenous social movements, entailing calls, variously, for renewed national, post-national, and food, sovereignty, is therefore the response to this conjuncture, constituting a rising political, or first, contradiction for neoliberalism. The financial and food shocks of 2007/8 propelled a Polanyian, ‘systemic’ double movement towards greater state intervention in the market, or deployment of ‘extra-economic’ mechanisms, involving direct land appropriation overseas, and/or neo-productivism at home. Overall, since those shocks, there has been a trend towards greater, albeit piecemeal, regulation of monopoly finance capital to mitigate price volatility and speculation, without, as yet, sundering the regime of accumulation that underpins neoliberalism. Nonetheless, accelerating contradictions for this regime, both through political unrest and through constraints on the supply of ‘cheaps’ in the conditions of production (‘second’ contradiction), suggest strongly that it is increasingly crisis prone and subject to challenge from a variety of political sources, both ‘sub-hegemonic’ (reformist), ‘alter-hegemonic’ (‘progressive’), and ‘counter-hegemonic’ (‘radical’). Although still dominant globally, neoliberalism appears, nonetheless, to be undergoing a developmental crisis as a result of the conjoined operation of the ‘first’ and ‘second’ contradictions of capital. I examine the dynamics of challenge from reformist, ‘progressive’, and ‘radical’ movements in the next chapter.

### AT: Ozone---2NC

#### Not extinction---bounces back, in the meantime wear glasses and sunscreen!

Brian **Martin 82** [Brian Martin (Professor of Social Sciences @ the University of Wollongong) December 1982 “The global health effects of nuclear war” Current Affairs Bulletin, Vol. 59, No. 7, pp. 14-26, online @ http://www.uow.edu.au/arts/sts/bmartin/pubs/82cab/index.html]

Another major threat to ozone comes from nuclear explosions. Nitric oxide is produced essentially by the 'burning' of nitrogen in the atmosphere, and this occurs whenever air temperatures are sufficiently hot: in automobile engines, in aircraft engines and in nuclear explosions. Studies of the creation of oxides of nitrogen by nuclear explosions were first undertaken as part of the SST debate, to determine whether the nuclear weapons tests in the 1950s and 1960s had reduced observed ozone levels.[28] It was only in 1974 that John Hampson made a point which had been overlooked, namely that large-scale nuclear war could cause a major and disastrous reduction in ozone levels.[29] Calculations made in the mid-1970s assuming large nuclear arsenals with many high-yield explosions concluded that reductions of ozone could reach 50 per cent or more in the northern hemisphere, with smaller reductions in the southern hemisphere.[30] But since the number of high-yield weapons in present nuclear arsenals is now smaller, much less oxides of nitrogen would be deposited in the stratosphere by nuclear war than assumed in earlier calculations, and so significant ozone reductions are unlikely.[31] This conclusion remains tentative. The actual behaviour of stratospheric ozone is quite complicated, involving many chemical compounds and numerous chemical reactions, the changing effects of temperature, the angle and intensity of sunlight, and the effect of air motions. Computer models of the effects of nuclear war on ozone are able to take into account only a part of this complexity, and new information about chemical reaction rates in particular have led in the past to periodic revisions in the calculated effects of added oxides of nitrogen. If significant ozone reduction did occur, the most important direct effect on humans would be an increase in skin cancer. However, this is seldom lethal, and could be avoided by reducing exposure to sunlight. Potentially more serious would be effects on crops.[32] Some of the important grains, for example, are sensitive to uv. Whether the net effects on crop yields would be significant is hard to estimate. But whatever the reduction in ozone, ozone levels would return pretty much to normal after a few years.[9] It seems unlikely that in the context of a major nuclear war the changes in uv alone would be of serious concern. In particular, the threat of human extinction raised by Jonathan Schell in The Fate of the Earth,[33] based mostly on effects of increased uv from ozone reduction, seems very small indeed. It is sometimes claimed that nuclear war could destroy ozone to such an extent that humans and animals would be blinded by excess uv. Even if large numbers of high-yield weapons were exploded, this possibility seems very unlikely except for a contribution to snow blindness in the far north. Stratospheric ozone can never be completely removed, but at most reduced greatly. Even if a 50 per cent or more reduction in ozone occurred - and as noted this seems improbable with present nuclear arsenals - protection from uv for humans could be obtained from sunglasses or just ordinary glasses, which absorb uv. For animals, the following considerations are relevant. Ozone levels vary considerably from place to place and from time to time, both seasonally and daily (sometimes by up to 50 per cent). Sunlight at the equator typically passes through only half as much ozone as at the mid-latitudes, yet animals at the equator are not known to go blind more often than elsewhere. Furthermore, most ozone reductions from a nuclear war would be in the mid and high latitudes, where ozone levels are higher to start with and where the 'path length' of sunlight through ozone is increased due to its oblique angle of incidence. But this does not mean complacency is warranted, as the concerns of John Hampson illustrate.

#### The ozone layer doesn’t matter

Matt **Ridley 14**. DPhil from Oxford, Fellow of the Academy of Medical Sciences, The Times. September 15, 2014. “The ozone hole isn’t fixed. But that’s no worry”, http://www.thetimes.co.uk/tto/opinion/columnists/article4206440.ece

How much damage did the ozone hole ever threaten to do anyway? It is fascinating to go back and read what the usual hyperventilating eco-exaggerators said about ozone thinning in the 1980s. As a result of the extra ultraviolet light coming through the Antarctic ozone hole, southernmost parts of Patagonia and New Zealand see about 12 per cent more UV light than expected. This means that the weak September sunshine, though it feels much the same, has the power to cause sunburn more like that of latitudes a few hundred miles north. Hardly Armageddon. The New York Times reported “an increase in Twilight Zone-type reports of sheep and rabbits with cataracts” in southern Chile. Not to be outdone, Al Gore wrote that “hunters now report finding blind rabbits; fisherman catch blind salmon”. Zoologists briefly blamed the near extinction of many amphibian species on thin ozone. Melanoma in people was also said to be on the rise as a result. This was nonsense. Frogs were dying out because of a fungal disease spread from Africa — nothing to do with ozone. Rabbits and fish blinded by a little extra sunlight proved to be as mythical as unicorns. An eye disease in Chilean sheep was happening outside the ozone-depleted zone and was caused by an infection called pinkeye — nothing to do with UV light. And melanoma incidence in people actually levelled out during the period when the ozone got thinner. Then remember that the ozone hole appears when the sky is dark all day, and over an uninhabited continent. Even if it persists into the Antarctic spring and spills north briefly, the hole allows 50 times less ultraviolet light through than would hit your skin at the equator at sea level (let alone at a high altitude) in the tropics. So it would be bonkers to worry about UV as you sailed round Cape Horn in spring, say, but not when you stopped at the Galapagos: the skin cancer risk is 50 times higher in the latter place.

### Grid Link---1NC

#### The aff prevents grid collapse – collapses the economy.

**Guterl 12** [Fred Gutter, executive editor, Scientific American, Nov 28, 2012, “Armageddon 2.0,” Bulletin of the Atomic Scientists]

The consequences of going without power for months, across a large swath of the United States, would be devastating. Backup electrical generators in hospitals and other vulnerable facilities would have to rely on fuel that would be in high demand. Diabetics would go without their insulin; heart attack victims would not have their defibrillators; and sick people would have no place to go. Businesses would run out of inventory and extra capacity. Grocery stores would run out of food, and deliveries of all sorts would virtually cease (no gasoline for trucks and airplanes, trains would be down). As we saw with the blackouts caused by Hurricane Sandy, gas stations couldn't pump gas from their tanks, and fuel-carrying trucks wouldn't be able to fill up at refueling stations. Without power, the economy would virtually cease, and if power failed over a large enough portion of the country, simply trucking in supplies from elsewhere would not be adequate to cover the needs of hundreds of millions of people.

#### Only depression-level collapse is necessary and sufficient to spark movements towards localized sustainability

Trainer ’19 [Ted; Conjoint Lecturer in the School of Social Sciences, University of New South Wales, “Entering the era of limits and scarcity: the radical implications for social theory,” Journal of Political Ecology Vol. 26, 2019]

Yet it is very unlikely that the kind of transition envisaged could begin unless there is major breakdown in the existing consumer-capitalist system. As long as it keeps the supermarket shelves stocked, discontent is likely to be muted, and focused on demands for more jobs and higher incomes rather than system replacement. The Goldilocks outcome would seem to be an economic depression that falls short of catastrophic breakdown, but is serious enough to convince large numbers that the system is not going to provide for them.

The challenge to the Left

This analysis has especially important implications for those who are radically critical of consumercapitalist society. Firstly it is evident that the revolution required to solve the problem is far bigger than that which Marx envisaged. Merely getting rid of capitalism will not suffice. Secondly, the most promising frontier now for such critics is the challenge to current society being set by unsustainable resource and ecological impacts. Latouche said the limits to growth are giving critical theory its last chance (2012: 75). Yet the foregoing argument has been that this opportunity has hardly been recognized, let alone taken up. Bookchin saw this some time ago. "The New Left, like the old left, has never grasped the revolutionary potential of the ecological issues, nor has it used ecology as a basis for understanding the problems of communist reconstruction and utopia" (1973: 242). Significant and increasing numbers of ordinary people are seriously concerned about these issues and are thinking more or less in the general direction of replacing consumer-capitalism with localism and simpler ways. These themes are likely to be the most effective foundations for critical social theory and practice now.

But unfortunately the Left has a deeply entrenched reluctance to embrace these ideas. The traditional assumption has been that when power has been taken from the capitalist class, the contradictions preventing full application of the productive forces will be removed and technical advance will lift all to material wealth. Socialism is distinctly not conceived today in terms of frugality or localism. Indeed some socialists embrace 'ecomodernist' ideas, notably Phillips (2014) and Sharzer (2012), who explicitly spurn the suggestion that local or simpler ways are necessary or desirable.

David Harvey represents the many Marxists who reject localism both as a goal and as a revolutionary strategy in favor of the typical socialist focus on action at the state level (Harvey 2017). For a critique, see Springer (2017). The Marxist position fails to address current circumstances, where the goal must be to contradict individualistic competitive affluence and must focus on citizen involvement in local economies. Major change at the central or state level cannot be achieved before a profound cultural revolution has been achieved, and this is most likely to occur via developments at the local level.

Delusion and denial: the inability to respond

There are difficult and puzzling issues for social theorists that will not be taken up in this article. They are the psychological and institutional reasons for the failure to deal adequately with the limits to growth predicament, or with its major sub-problems such as the looming petroleum supply, debt, and climate change crises. The core phenomenon to be explained here would seem to be failure to even recognize the existence and/or seriousness of the problems, rather than lack of appropriate remedial action.

The essential causal factor is surely that if the limits to growth analysis is accepted then perhaps the most deeply entrenched post-Enlightenment assumption has to be jettisoned, i.e., the taken-for-granted conviction that progress and the good life are defined by capacity to produce and consume more and more material wealth. The suggestion that the supreme social goal should be materially simple lifestyles and systems, with no prospect of rising to greater affluence over time, would seem to be about as distasteful and unthinkable to workers and the lumpenproletariat as to the super-affluent 1%.

6. Conclusions: a reorientation of social theory

The argument is that the advent of the limits to growth issue should be seen as requiring a major shift in the focal concerns of social theorists, especially those interested in critical perspectives on contemporary society and in sustainability and utopian themes. To begin with, a limits perspective involves a commitment to an inescapable logic that leads to quite specific conclusions regarding desirable social forms and how they might be achieved. If the limits are as severe as has been argued, then the goal must be transition from consumer-capitalist society to a general form that involves far lower resource use, and this has to mean mostly small-scale local economies that are self-governing, basically cooperative and committed to materially frugal lifestyles. If this is so, then the transition is essentially a cultural problem, and it is difficult to imagine how these ways could be established other than through a slow grass-roots process whereby ordinary people increasingly coerced by scarcity and economic deterioration take on the restructuring of their own suburbs, towns and regions (Alexander and Gleeson 2019).

### AT: US Not Key---2NC

#### US collapse goes global

George Friedman 17, Geopolitical Forecaster and Strategist, “An American Recession And The World” https://www.huffingtonpost.com/entry/an-american-recession-and-the-world\_us\_5900b1f6e4b06feec8ac9251

Recessions are unpleasant and hurt some people disproportionately. However, the U.S. recession will likely hurt other countries more than the United States. When combined with other global economic problems, the recession will likely weaken Europe’s anemic recovery and strike another blow at the Chinese. It will also put further downward pressure on commodity prices, considering that the United States is the world’s largest importer and has been, to some extent, the engine stabilizing the international system.

The 2007-09 recession hurt the Chinese tremendously because their biggest export customers were the United States and Europe. In due course, the Chinese slowdown cut China’s consumption of industrial commodities, including oil, hitting countries like Russia and Saudi Arabia. This is part of the global exporters’ crisis I have written about previously. The United States avoided the worst of this because, while it is the second-largest exporter in the world, exports account for only about 12.6 percent of its GDP (the U.S. ranks only 161st in the world in terms of exports as a percent of GDP, according to the World Bank). In part, this lack of dependence on exports helped U.S. GDP grow on its internal engine. More important is that the U.S. is less vulnerable to global downturns than other countries.

The decline in the U.S. economy will inevitably involve a drop in U.S. imports. Under normal circumstances, this slump would not destabilize the system. But we have not been living under normal circumstances since 2008. More precisely, we are now living in a new normal. In the new normal, countries that were driven by exports are now using diminished export demand to simply maintain their economies in the hopes of generating enough domestic demand to replace lost markets. In most cases, they have achieved a fairly precarious balance at this point that is much more subject to destabilization than in previous cycles. A relatively small drop in global demand can have a substantial impact. Thus, a routine U.S. recession will lead to a small global decline, reversing gains in stabilization made in recent years.

The downturn in export demand will have a ripple effect because exporting countries are also importing countries. As American demand contracts, exporters’ economies will be affected and their need for imports will contract as well. This domino effect is normal. The problem is that the international system’s vulnerability has grown dramatically because many countries have become excessively reliant on exports, and this has been accompanied by a general weakness in their domestic economies. Therefore, the ripple effect, while not a tidal wave, will be more substantial than would have been the case before 2008.

#### US shock spills over globally

Desomnd Lachman 16, resident fellow at the American Enterprise Institute, was formerly a deputy director in the International Monetary Fund, 8-16-16, “A time for US world economic leadership,” https://www.aei.org/publication/a-time-for-u-s-world-economic-leadership/

A striking feature of today’s global economic landscape is the many weaknesses in the world’s major economies. In Europe, following the Brexit vote, the United Kingdom’s economy is likely to be beset by many years of investor uncertainty as it renegotiates its complex relationship with Europe. Meanwhile Italy, the Eurozone’s third-largest economy, is having to cope with major difficulties in its banking system, the over-indebtedness of its government, and growing public antipathy to the Euro. This is all the more serious considering that Italy will hold a constitutional referendum later this year, which could see a fall in the Italian government. It also must be of concern that, unlike Greece, Italy is simply too big for Europe to save should it face an economic and political meltdown. In Asia, Japan’s over-indebted economy is again flirting with both deflation and economic recession, while the Chinese economy is struggling to make the transition away from an investment- and export-led economy to one led by consumption and the service sector. At the same time, major emerging market economies like Brazil, Russia and South Africa are all having to cope with depressed international commodity prices and with excessive corporate U.S. dollar indebtedness. Further clouding the global economic outlook is the fact that the world is now drowning in debt. Indeed, a recent McKinsey Global Institute study found that private and public sector debt levels around the world today are very much higher than they were in 2008 on the eve of the Great Economic Recession. This makes it all the more important that the world economy is not hit by a renewed shock that might cause the world economy to falter and that would make the repayment of that debt all the more difficult. It is against this troubled background that one would think that the last thing that the world economy needs right now is a period of investor uncertainty in the United States, the world’s largest economy. Yet that is very well what could happen if the presidential candidates continue to outbid themselves on tax giveaways and lavish public spending promises that might compromise the country’s public finances.

#### The US is key to the global economy

Kose ‘17

(et al - “Understanding the global role of the US economy”, M. Ayhan Kose Director of the Development Prospects Group, World Bank Group, Csilla Lakatos Economist in the Development Prospects Group (DECPG) of the World Bank, Franziska Ohnsorge Lead Economist in the Development Economics (DEC) Vice Presidency, World Bank, Marc Stocker Senior Economist, Development Prospects Group, World Bank, 27 February 2017, https://voxeu.org/article/understanding-global-role-us-economy

**Because of its size and interconnectedness, developments in the US economy are bound to have important effects around the world**. The US has the world’s single largest economy, accounting for almost a quarter of global GDP (at market exchange rates), one-fifth of global FDI, and more than a third of stock market capitalisation. It is the **most important** export destination for one-fifth of countries around the world. The US dollar is the most widely used currency in global trade and financial transactions, and changes in US monetary policy and investor sentiment play a major role in driving global financing conditions (World Bank 2016). At the same time, the global economy is important for the US as well. Affiliates of US multinationals operating abroad, and affiliates of foreign companies located in the US account for a large share of US output, employment, cross-border trade and financial flows, and stock market capitalisation. Recent studies have examined the importance of global growth for the US economy (Shambaugh 2016), the global impact of changes in US monetary policy (Rey 2013), or the global effect of changing US trade policies (Furman et al. 2017, Crowley et al. 2017). It is likely that there will be shifts in US growth, monetary and fiscal policies, as well as uncertainty in US financial markets. What will be the global spillovers? Our recent work (Kose et al. 2017) attempts to answer these questions: How synchronised are US and global business cycles? How large are global spillovers from US growth and policy shocks? How important is the global economy for the US? How synchronised are US and global business cycles? Business cycles in the US, other advanced economies (AEs), and emerging market and developing economies (EMDEs) have been highly synchronous (Figure 1.A). This partly reflects the strength of global trade and financial linkages of the US economy with the rest of the world, but also that global shocks drive common cyclical fluctuations. This was particularly the case at the time of the 2008-09 Global Crisis. It is not a new phenomenon, however. Although the four recessions the global economy experienced since 1960 (1975, 1982, 1991, and 2009) were driven by many problems in many places, they all overlapped with severe recessions in the US (Kose and Terrones 2015). Other countries tend to be in the same business cycle phase as the US roughly 80% of the time (Figure 1.B). The degree of synchronisation with US financial cycles is slightly lower, but still significant – credit, housing, and equity price cycles are in the same phase about 60% of the time. Although it is difficult to establish empirically whether the US economy leads business and financial cycle turning points in other economies, recent research indicates that the US appears to influence the timing and duration of recessions in many major economies (Francis et al. 2015). Figure 1 Synchronisation of business cycles Sources: Haver Analytics; World Bank; Kose and Terrones (2015); IMF. Notes: Average share of years in which business cycles in the US and all economies were in the same phase. A higher share suggests more synchronization between two countries. How large are global spillovers from US growth and policy shocks? A surge in US growth – whether due to expansionary fiscal policies or other reasons – could provide a **significant bo**ost to the global economy. **Shocks to the US economy transmit to the rest of the world through three main channels**. An acceleration in US activity can lift growth in trading partners directly through an **increase in import demand**, and **indirectly by strengthening productivity spillovers embedded in trade.** Financial market developments in the US may **have even wider global implications**. US bond and equity markets are the largest and most liquid in the world and the US dollar is the currency mostly widely used in trade and financial transactions. This makes US monetary policy and investor confidence important drivers of global financial conditions (Arteta et al. 2015, IMF2015). Given its role in global commodity markets (the US is both the world’s largest gas and oil consumer and producer), changes in US growth prospects can affect global commodity prices. This affects activity, fiscal and balance of payment developments in commodity exporters. Estimates indicate that a percentage-point increase in US growth could boost growth in advanced economies by 0.8 of a percentage point, and in emerging market and developing economies by 0.6 of a percentage point after one year (Figure 2.A). Investment could respond even more strongly. A boost to investment could come for instance from fiscal stimulus measures – but the effect would largely depend on the circumstances of the implementation of these measures, including the amount of remaining economic slack, the response of monetary policy, and the adjustment of household and business expectations to the prospect of higher deficit and debt levels. A faster tightening of US monetary policy than previously expected could, for instance, lead to sudden increases in borrowing costs, currency pressures, financial market volatility, and capital outflows for more vulnerable emerging market and developing economies. Even in the absence of actual policy changes, heightened uncertainty driven by financial market volatility or ambiguity about the direction and scope of US policies could discourage investment both in the US and in the rest of the world. Empirical estimates suggest that a sustained 10% increase in US stock market volatility (specifically, the VIX) could, after one year, reduce investment growth in the US by about 0.6 of a percentage point, in other advanced economies by around 0.5 of a percentage point, and in emerging market and developing economies by 0.6 of a percentage point (Figure 2.B). Figure 2 US growth and uncertainty spillovers A. Growth spillovers Notes: Cumulative impulse responses of GDP growth in other advanced economies (AEs) and EMDEs to a percentage-point increase in growth in real GDP in the US. Growth spillovers are based on a Bayesian vector autoregression model. The sample for other AEs includes Eurozone (19 countries), Canada, Japan, and the UK and 19 EMDEs for 1998Q1-2016Q2. B. Uncertainty spillovers on investment growth Sources: Haver, Bloomberg, World Bank estimates. Notes: Cumulative impulse responses after one year of investment growth in the US, 23 other AEs, and 18 EMDEs to a 10% increase in the US VIX. Vector autoregressions were estimated for 1998Q1-2016Q2 with two lags. How important is the global economy for the US? Important as the US is to the global economy, the US economy is also affected by its trade and financial linkages with the rest of the world. Global economic developments play an important role in driving activity and financial markets in the US. US multinationals account for a large share of US output and labour productivity growth, and their presence in financial markets is large. In turn, foreign multinationals operating in the US provide a large share of US employment and exports (Figure 3.A). Much of the global value chain activity is conducted through US multinational corporations and their affiliates abroad. Overall, one-quarter of US exports represents US value added embedded in other countries' exports. This ‘forward participation’ is particularly high in chemicals, business services, and electronics, and with China, Canada, and Mexico. ‘Backward participation’ is more limited: the average import content of US exports was 13% in 2014, well below the average for other advanced economies (27%). This interconnectedness is an important source of spillovers between the US and the global economy. As a result, growth setbacks originating in other economies, or policy changes affecting market access of US companies, can have detrimental effects on the US. These effects are particularly noticeable in the more globally integrated manufacturing sector (Figure 3.B). Figure 3. Importance of the global economy for the US economy Role of foreign multinational corporations in the US Sources: Bureau of Economic Analysis, World Bank estimates. Notes: Share of multinational corporations in US sales, exports and imports of goods and employment. "Sales" indicates sales of multinational corporations in gross output of US private sector industries. Data covers 2010-2013. Spillover to US from 1 percentage point increase in global, advanced economy, and emerging market and developing economy growth Sources: Bureau of Economic Analysis, World Bank estimates. Notes: Cumulative impulse responses after one year of GDP or industrial production (IP) growth in the US following a 1 percentage point increase in GDP or industrial production growth in 22 other AEs and 19 EMDEs (13 EMDEs for industrial production). ‘Global’ indicates the weighted average impact of AEs and EMDEs. Vertical lines indicate 16th-84th percentile confidence bands. Vector autoregression models are estimated for 1998Q1-2016Q2 with four lags. Acceleration or uncertainty? **Given its size and the strength of its ties with the global economy, shocks to the US economy are transmitted globally through many channels.** On the one hand, an acceleration in US growth could be expected to have positive effects for the rest of the world, if not counterbalanced by increased trade barriers or an unexpected tightening of global financing conditions. On the other hand, persistent policy uncertainty could hamper growth throughout the global economy, and could have particularly adverse effects on investment growth in emerging market and developing economies, which have already showed weakness in recent years (World Bank 2017).