# \*\*\*\*Resilience Neg: GDI22 Starter\*\*\*\*

# Case Ans: Cyber / Alliance

### Cyber Ans: 1NC

#### Cyber threat is overblown—Russian efforts against Ukraine prove

Marschmeyer, CSS Senior Researcher and Kostyuk, Georgia Tech Assistant Professor, ‘22

[Lennart Maschmeyer, Senoir Researcher, Center for Security Studies, ETH Zurich and PhD, University of Toronto and Nadiya Kostyuk, Assistant Professor, School of Public Policy, Georgia Institute of Technology, “There Is No Cyber ‘Showck and Awe’: Plausible Threats in the Ukrainian Conflict,” WAR ON THE ROCKS, 2—8—22, <https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/>, accessed 5-11-22]

These predictions suggest that cyber operations will provide significant strategic advantages to Russia either as complements to military force, or as standalone instruments — or at least that policymakers and commentators think that they will. Current warnings of escalating cyber warfare conjure deep-seated fears of cyber doom and the recurring specter of a “cyber Pearl Harbor” strategic surprise attack. In practice, however, cyber warfare has been a failure. Our research shows that cyber operations have remained irrelevant on the battlefield, while standalone operations to weaken Ukraine through election interference, critical infrastructure sabotage, and economic disruption largely failed to contribute to Russia’s strategic goals of making Ukraine abandon its pro-European Union and pro-NATO foreign policy. Consequently, current fears of cyber warfare defy not only Russia’s track record in Ukraine, but also strategic logic. Given that Russia’s cyber operations have failed to produce significant strategic value to date, why would we expect this to suddenly change now? Or, to put it more pointedly: If cyber operations offer such effective and potent instruments, why did Russia go through the trouble (and costs) to mobilize its troops? Current predictions of cyber onslaught do not offer a persuasive answer.

Giving in to these fears risks fighting phantom threats, playing into Russia’s hands by distracting from the need to counter its military threat and sowing fear and confusion — at least among Western audiences. A level-headed analysis of the threat that distinguishes what is theoretically possible from what is practically feasible is urgently needed. Our research suggests that, contrary to hysteria, cyber operations will remain of secondary importance and at best provide marginal gains to Russia.

Expectations Versus Evidence: Cyber Operations and Their Limits

There are three distinct perspectives on the strategic role and value of cyber operations in conflict. Early scholarship on cyber conflict expected cyber operations to be primarily important in conventional military conflict, enabling crippling strategic strikes analogous to the surprise attack on Pearl Harbor during World War II. If successful, cyber operations could thus be substituted for the use of force. Yet research throughout the 2010s made the limitations of cyber operations as a means of force projection increasingly clear.

Subsequent scholarship thus sees cyber operations primarily as complements to force. Possible effects include disrupting command and control and communications systems, sabotaging equipment and infrastructure, spreading disinformation, and conducting psychological warfare to undermine morale among enemy troops.

The third and increasingly influential perspective instead suggests cyber operations are primarily relevant in “gray zone” conflict short of war. In this view, cyber operations offer standalone instruments of power that can influence and weaken an adversary through critical infrastructure sabotage, economic disruption, and influence operations. Hence, as in cyber Pearl Harbor scenarios, it also suggests that cyber operations could substitute for the use of force — achieving similar goals without going to war. However, rather than through a massive surprise strike, this third school of thought expects the effects to be gradual and cumulative, eroding adversary strength over multiple operations.

The empirical record of cyber conflict, however, suggests that what is feasible in practice is far more limited. Ukraine has been a “giant test lab” where Russia, one of the world’s foremost cyber powers, has experimented with cyber operations for eight years. Yet these operations have failed to produce significant strategic value either as force complements or standalone tools.

The substitutability argument — that states can or do substitute cyber operations for the use of force — has little empirical support since Russia levied no major cyber operations against Ukraine in the runup to the military escalation of the conflict in 2014. While it is possible that we do not know about such operations given their veil of secrecy, it is clear that any attempted but undetected cyber surprise strike failed to produce any measurable effects.

Evidence supporting the complementarity perspective is similarly sobering. One of us has examined the role of low-level disruptive cyber operations in the military conflict and their relevance for battlefield events (and outcomes). Disruptive attacks can directly affect military operations as they seek to sabotage an opponent’s ability to fight. For example, the Russia-backed separatists in the Donbas and Luhansk regions used malware to retrieve data from mobile devices on the locations of Ukrainian artillery troops, facilitating better reconnaissance against these troops. Pro-Ukrainian hackers hijacked CCTV cameras behind enemy lines to obtain intelligence on the movement of Russian artillery in the separatist-controlled territories.

Focusing on the period of the most intense fighting, between 2014 and 2016 — the time when, if cyber tools are an effective complement to armed force, Russia would have been most likely to use them — we applied a series of statistical tests to thousands of cyber and military operations. The findings showed a strong, escalatory dynamic between military operations by both sides but no significant correlation in either direction between military and cyber operations, and no reciprocity between cyber operations. This evidence demonstrates that in one of the first armed conflicts where both sides used low-level cyber operations extensively, digital operations unfolded independently from the events on the ground and had no discernible effect on them. Hence, in stark contrast to expectations about the force-multiplying advantages of cyber operations, these findings suggest hacking groups faced considerable difficulties in responding to battlefield events, much less shaping them.

Finally, the track record of cyber operations as standalone instruments in gray zone conflict in Ukraine also falls far short of expectations. One of us has examined the operational mechanisms, effects, and strategic value of five major Russia-sponsored cyber operations, including election interference, critical infrastructure sabotage, and economic disruption. Contrary to prevailing expectations, the majority made no measurable contribution towards Russia’s strategic goals. The NotPetya operation, whose large-scale disruption of businesses wiped off half a percentage point of Ukraine’s gross domestic product in 2017, is the exception. Yet this operation underlined a key shortcoming of cyber operations: the risk of losing control over the spread of effects, producing unintended consequences, added costs, and correspondingly lowering strategic value. Forensic analysis by internet security company ESET revealed that the Sandworm hacking group underestimated how far NotPetya’s data-destroying malware would spread. It “went out of control” and spread far beyond Ukraine, even disrupting targets in Russia — including the state-controlled oil giant Rosneft. These disruptions within Russia will have caused additional costs, as did the sanctions that Western countries imposed on Russia in response to NotPetya’s international disruption.

Evidence from Ukraine thus supports neither the force substitute nor the force complement argument. Instead, cyber operations have been most relevant as standalone, lower-intensity alternatives to the use of force — more in line with the third school of thought. Yet by and large they fell short of providing measurable strategic value. Indeed, all available evidence indicates that Russia’s cyber warfare efforts against Ukraine — combined with its larger gray zone campaign — have failed to make Ukraine abandon its rapprochement with the West. That is why Russia has mobilized its army, attempting to prevent Ukraine from joining the Western alliance through threat of invasion.

Plausible Threats in the Conflict Ahead

Considering the underwhelming track record of cyber warfare in Ukraine to date, there is little reason to expect cyber doom of the kind that some now predict. For these warnings of a Russian cyber onslaught to become reality, cyber operations would need to produce effects at a scope and scale that they have previously failed to attain. Importantly, current warnings fail to make a persuasive case on why we should expect such a transformation.

Rather, they rest on the implicit assumption that with the change in strategic context, the role of cyber operations will change as well. This comes out clearest in Maggie Miller’s recent commentary suggesting that military escalation in Ukraine would finally herald “a true cyberwar” where Russia could “take down the power grid” or launch a disinformation campaign to undermine the government in Kyiv. Dmitri Alperovitch offers a more level-headed analysis, underlining that cyber operations alone will fall short of achieving Russia’s goals. However, he also suggests that they can complement force as an “extension of warfare itself,” disrupting command and control to provide battlefield advantages, sabotaging critical infrastructure, and undermining public trust in the government to “send a powerful signal that resistance is futile.” Yet, as we have seen, Russia has attempted most of these objectives in the past and has failed. Even in a full-scale invasion, we have the same aggressor, with the same hacking groups, with the same skill level going after the same sets of possible targets. Why would we expect different results?

Changing the strategic context of deployment does not change the mechanism of action that cyber operations rely upon to produce outcomes — and its intrinsic constraints. Cyber operations rely on a mechanism of subversion that exploits vulnerabilities in adversary systems to use them against the adversary. This mechanism holds great strategic promise but poses significant operational challenges. It requires creativity and cunning to remotely manipulating complex systems that others designed and operate without alerting the victim to one’s presence. These challenges produce an operational trilemma between the speed, intensity of effects, and level of control that actors have over these effects. This trilemma limits strategic value, since in most circumstances cyber operations will be too slow, too weak, and too volatile to contribute measurably to strategic goals. The constraining role of this trilemma is evident across all five of Russia’s disruptive cyber operations against Ukraine thus far, underlining their relevance. Importantly, all available evidence indicates that these intrinsic constraints limit the strategic value of cyber operations regardless of strategic contexts.

### Cyber Ans: 2NC

#### No deadly cyber attacks—empirics prove

Lewis 20

(senior vice president and director of the Technology Policy Program at the Center for Strategic and International Studies). Lewis, James. 2020. “Dismissing Cyber Catastrophe.” Center for Strategic & International Studies. August 17, 2020. 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. 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. 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 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.

#### Cyber wars don’t escalate—empirics

Jensen, Atlantic Council senior fellow, ‘19

[Benjamin Jensen, Senior Fellow, Atlantic Council and dual academic appointment, Marine Corps University and School of Intenrational Service, American University, “What a U.S. Operation in Russia Shows About the Limits of Coercion in Cyber Space,” WAR ON THE ROCKS, 6—20—19, https://warontherocks.com/2019/06/what-a-u-s-operation-in-russia-shows-about-the-limits-of-coercion-in-cyber-space/]

As social scientists start using larger data sets and experiments to analyze cyber operations, they are casting doubt on whether coercion in this new domain works at all.  Wargame experiments analyzing [cyber attacks against critical infrastructure](https://warontherocks.com/2017/07/cyber-attacks-on-critical-infrastructure-insights-from-war-gaming/) reveal difficulties coordinating responses between private industry and the national security establishment, as well as a reluctance to escalate when a cyber incident might cause significant economic damage. Other [experiments](https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint) and [simulations](https://cltc.berkeley.edu/2018/04/16/cyber-operations-conflict-lessons-analytic-wargames-2/) similarly demonstrate that players, including national security experts, are unlikely to escalate in response to cyber acts alone. Players seem reluctant to risk World War III over hacking. This hesitation likely is due to the covert character of cyber campaigns and the fact that any predicted coercive effects, to include deterrence, are [expectations about the future](https://twitter.com/RidT/status/1140101505074311169). Because cyber operations occur in the shadows, politicians can hide the fallout in the short term and avoid public pressure to respond.

There are real concerns about whether cyber operations are a sufficiently costly signal or even the right instrument of power to coerce rivals. [Previous studies](https://global.oup.com/academic/product/cyber-strategy-9780190618094?cc=us&lang=en&) have found cyber operations can compel rivals, but only when used in conjunction with other instruments of power. It is also unclear whether cyber operations achieve demonstrable battlefield effects. A recent study by [Nadiya Kostyuk and Yuri Zhukov](https://journals.sagepub.com/doi/abs/10.1177/0022002717737138) finds cyber attacks in Syria and Ukraine did not change combatant behavior. These findings echo earlier studies questioning [the efficacy](https://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00136) and [very concept of cyber war](https://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939?journalCode=fjss20).

### Cyber Ans: NC3 Attacks—1NC

#### No C3 vulnerability—proprietary design, redundancy, airgapping, human safeguards

Caylor ’16 [Matt Caylor, Lt. Commander, U.S. Air Force, “The Cyber Threat to Deterrence,” WAR ON THE ROCKS, 2—1—16, <https://warontherocks.com/2016/02/the-cyber-threat-to-nuclear-deterrence/>, accessed 1-19-22]

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.

### Cyber Ans: NC3 Attacks—2NC

#### Cyber attacks against nukes cannot be prevented

Spector, James Martin Center senior fellow, ‘22

[Leonard Spector, former senior official, US National Nuclear Security Administration and Distinguished Senior Fellow, James Martin Center for Nonproliferation Studies, “Cyber Offense and a Changing Strategic Paradigm,” WASHINGTON QUARTERLY v. 45 n. 1, Spring 2022, p. 41]

It is also widely accepted that airtight defenses against such offensive cyber efforts are not possible.11 Moreover, it is generally believed that the increasing complexity of newer nuclear weapon systems and their associated software makes them more vulnerable to cyber disruption than older ones. The same holds true for critical infrastructure, as management of those systems relies increasingly on advanced digital controls. This means that each of the states at issue here must recognize that its nuclear weapon systems and critical infrastructure are currently vulnerable to cyber sabotage and will remain so going forward. Because the opponent’s cyber intrusions are intended to be undetectable, however, none of these states can know with confidence how badly or in what respect its nuclear assets and critical infrastructure may be at risk of disruption in a future confrontation.

### Cyber Ans: Norms Fail—1NC

#### Can’t establish cyber norms

Maurer ’19 [Tim Maurer, Co-Director, Cyber Policy Initiative, Carnegie Endowment for International Peace, “A Dose of Realism: The Contestation and Politics of Cyber Norms,” HAGUE JOURNAL ON THE RULE OF LAW, 2019, SpringerLink]

3.5 Part 5: Metacontestation Over the UNGGE Process

While some UN member states have criticized the UNGGE process as lacking legitimacy because of its limited membership, there are other forces tearing at the fabric of the regime that has been built around the UNGGEs. These criticisms can be considered a standalone metacontestation over the existing UN process writ large. Its critics question whether the UN process has been sufciently impactful, whether it is worth pursuing further, and whether it ought to be replaced with a diferent process. These arguments focus on (1) the broad scope and vague nature of agreements, (2) the inadequacy of addressing the deteriorating security environment, (3) the hidden agendas, including hypocrisy, of some stakeholders, and (4) the disconnect between those negotiating and those carrying out ofensive operations.

1. Broad scope and vague nature of agreements A common critique from ofcials in national security agencies is that the framework developed by the UNGGE is too broad and too vague to be truly effective at establishing rules of the road adhered to by those carrying out offensive cyber operations (Burgess 2018; Baker 2017; Fischerkeller and Harknett 2018). Their skepticism refects the still nascent and continuously maturing understanding of the technology’s impact on the balance of power, its use as an instrument of statecraft, and the security dilemma that is as present online as it is ofine. As an alternative approach, this group of stakeholders proposes to focus on agreements based on emerging state practice and more narrowly defined areas of common interest as the basis for cyber norms that could then be expanded over time (Fischerkeller and Harknett 2018; Fischerkeller 2018).

2. Inadequacy of addressing deteriorating security environment A separate point of critique of the UNGGE process makes the opposite argument. Instead of viewing the UNGGE’s framework as too broad and ambitious, this separate camp of critics argues that the UNGGE process has not been ambitious enough. They see a functional need for international cooperation among governments and transnational cooperation among nongovernmental actors to address the deteriorating cybersecurity environment. A leading voice of this group is the multinational company Microsoft. After years of being involved in international cyber norms discussions, Microsoft CEO Brad Smith elevated the company’s engagement to an unprecedented level by calling for a Digital Geneva Convention (Smith 2017; Meredith 2018). In the wake of the economic costs caused by the 2017 WannaCry and NotPetya, these voices have become louder with a growing number of CEOs joining the chorus (Greenberg 2018; Cybersecurity Tech Accord 2018; Siemens 2018). In addition, the UN Secretary General made the topic a priority in 2018 supporting a more ambitious agenda (Khalip 2018; Fidler 2018).

This group of norm entrepreneurs remains very active trying to further advance the cyber norms discussion by keeping the pressure on governments.26 For example, Microsoft broadened its eforts beyond its engagement as a single company by creating the ‘Tech Accord’ consortium counting more than 70 global companies at the beginning of 2019 (Cybersecurity Tech Accord 2018). In late 2017, Siemens established a nonrival network of a dozen companies creating a ‘Charter of Trust’ focusing specifcally on supply chain integrity (Siemens 2018). Meanwhile, the Dutch government led the charge to add a norm protecting the core of the Internet to the list of norms agreed to through the 2015 UNGGE (Broeders 2016). The French government’s desire to maximize the impact of the Paris Peace Forum launched in 2018 at the 100th anniversary of the end of World War I led to the adoption of the Paris Call for Trust and Security in Cyberspace in November 2018 that explicitly references the norm to protect the core of the Internet (France Diplomatie 2018). The Paris Call has also been described as an umbrella framework for the activities of various norm entrepreneurs.27

3. Hidden agendas Those promoting a more ambitious agenda have encountered a number of challenges due to the dynamics among and within governments. First, among governments, calls for a treaty have been met with resistance by Western governments. Concerned about Moscow’s true intentions, these governments worry that any push for a treaty will empower Moscow’s longstanding proposal. Their concerns explain continued resistance by Washington and Western capitals with respect to the draft International Code of Conduct that Moscow and Beijing developed in 2011, updated in 2015, and have been promoting since (see McKune 2015.) They also help explain why Microsoft’s call for a Digital Geneva Convention has met similar resistance and illustrate that overcoming this path dependence would require exceptional circumstances. Second, within governments, national security agencies are reluctant to internalize and adhere to the norms refected in the UNGGE agreements due to the still nascent understanding of the domain, a related desire to preserve options until a mature strategic framework has emerged, and the dynamics of the security dilemma (Burgess 2018, Efrony and Shany 2018). A good illustration of this still maturing understanding of the technology is the argument promoted by some that there is moral obligation to use hacking instead of conventional weaponry if the efects of the former are less harmful than the latter (Hollis 2014).

4. Disconnect between those negotiating and those conducting ofensive cyber operations A fnal obstacle worth mentioning—rather in form of a hypothesis than conclusive analysis—is that a particular challenge for negotiating cyber norms may be that the conduct of ofensive cyber operations originated in and continues to be closely tied to intelligence agencies, the most secretive parts of any government (Smeets 2018). Until recently, their public engagement was minimal. For example, the acronym of the U.S. National Security Agency (NSA) has been commonly referred to as ‘No Such Agency.’ The bureaucratic culture of these agencies is therefore not infused with a history of interactions with their respective counterparts internationally (apart from the norms governing spy swaps that emerged during the Cold War.) Unlike the militaries of the world that—despite fghting each other—have developed norms for the exchange of prisoners, the treatment of the wounded, and other activity, this sort of interaction is not part of intelligence agencies’ DNA.28 With that said, the pace of change afecting intelligence agencies in the past 5 years alone is breathtaking with potential changing attitudes toward such interactions. For example, from the NSA to the Australian signals directorate, agencies now even have active Twitter accounts and terms such as Five Eyes have become household names (Australian Signals Directorate 2018).

### Cyber Ans: Norms Fail—2NC

#### Existing norms prove – even if we make them nobody will agree on interpretation

Maurer ’19 [Tim Maurer, Co-Director, Cyber Policy Initiative, Carnegie Endowment for International Peace, “A Dose of Realism: The Contestation and Politics of Cyber Norms,” HAGUE JOURNAL ON THE RULE OF LAW, 2019, SpringerLink]

There is severe confusion about cyber norms. It is not uncommon to encounter statements from diplomats implying that norms, per defnition, are voluntary in nature and never legally binding—in contradiction to the decades-old academic literature of sociology and international relations theory.3 What is to blame for the confusion? Politics and the gap between academics and practitioners. Yet, this confusion also refects an undercurrent of competing political systems that afects the terminology used in this area. It is therefore worth briefy unpacking what (cyber) norms are and how to defne them given the implications for contestation. One of the key points of confusion centers on the relationship between norms and laws. In academia, scholars debate whether legal norms enjoy a special status compared to norms generally.4 Finnemore argues they do not because “There are, after all, many kinds of norms in the world—social, cultural, professional, moral, religious, and familial” (Finnemore 1999: 701).5 Others argue that norms tied to law stand out because of the level of compliance given rise to concepts such as ‘soft law’ and ‘hard law’ (Abbott and Snidal 2000; see Jose (2018): 25). More recently, Finnemore and Holllis concluded that “Simply put, laws can serve as a basis for formulating norms, just as norms can be codifed in law” (Finnemore and Hollis 2016: 442)”.6 In international politics, the concept of ‘voluntary norms’ emerged as a political strategy developed by the U.S. Department of State in juxtaposition to Russia’s proposal for a legally binding arms control treaty on information security. Moscow approached Washington with this idea in the late 1990s which the U.S. government opposed for several reasons. One of the key decision-makers involved, Richard Clarke, “viewed the Russian proposal as largely a propaganda tool” in addition to considering verifcation of a cyber agreement “impossible” and that “the U.S. had not yet explored what it wanted to do in the area of cyber war. It was not obvious then whether or not cyber war added to or subtracted from U.S. national security (Clarke and Knake 2011: 219)”. Other factors that have come up since are the quickly evolving nature of the technology challenging the longevity of a potential international treaty and growing concerns that the broad defnition of ‘information security’ advanced by Moscow and Beijing is a Trojan horse for content control and a human rights issue at heart. Another is the difculty of attributing malicious cyber activity and the related ability to hold actors responsible (Rid and Buchanan 2015; Lindsay 2015; Brantly et al. 2016; Eglof and Wenger 2019). After the U.S. decided to reject the Russian proposal, it was in search for a strategy to advance its own agenda while still engaging with the Russians when the issue rose in prominence, namely after the 2007 DDoS attack against Estonia and the 2008 compromise of the classifed networks of the U.S. Department of Defense.7 Principally opposed to a legally binding agreement as a goal, the U.S. government came up with the idea for the international community to develop ‘voluntary norms’ in addition to arguing that existing international law applies to cyberspace. The 2015 UNGGE report therefore repeatedly highlights the “voluntary, non-binding” nature of the norms it outlines for cyberspace (UN Group of Governmental Experts 2015). The process that emerged out of these early days has since been scrutinized, including its dynamics and actors, by several scholars (Kavanagh and Staufacher 2014; Hurwitz 2014; Cornish 2015; Farrell 2015; Erskine and Carr 2016; Tikk-Ringas 2016; Macák 2017; Hurel and Lobato 2018). Ultimately, these factors explain the confusion and highlight the need to pay close attention what actors mean when they use the term ‘norm.’

#### No Cnorms—fragmentation of opinions and global power conflict means that there’s no consensus

Maurer ’19 [Tim Maurer, Co-Director, Cyber Policy Initiative, Carnegie Endowment for International Peace, “A Dose of Realism: The Contestation and Politics of Cyber Norms,” HAGUE JOURNAL ON THE RULE OF LAW, 2019, SpringerLink.

In 2017, the same year that the two biggest cyber attacks to date—WannaCry and NotPetya—occurred, international negotiations over norms for cyberspace collapsed. With each attack causing several billions of U.S. dollars in economic damage worldwide, the cyber attacks raise the question: why did the international community through the UN Group of Governmental Experts (UNGGE1 ) fail to reach a consensus on how to advance the emerging regime of norms for cyberspace? On the surface, states such as the US, Cuba and India argue that it was a disagreement over international law (Markof 2017; Rodriguez 2017; Sukumar 2017). Yet, the iceberg underneath is a mix of great power politics, competing and occasionally clashing political systems, and continued uncertainty with respect to a new technology.

Overall, states’ approach to norms for cyberspace remains highly contested internationally among governments and fragmented domestically within governments. Cyber norms are still in their “constituting phase” (Wiener 2014). Agreed upon, explicitly stated norms are considered voluntary, defned vaguely, and internalized weakly (Farrell and Glaser 2017: 16). Implicit state practice is slowly emerging, yet poorly understood, and cloaked in secrecy. Nevertheless, the diplomatic activities over the past two decades have shaped signifcantly how governments think about cyber norms and how they behave accordingly (Nye 2018).

To understand the dynamics of the international cyber norms contestation, various lenses can be applied. In addition to signs of the security dilemma impacting states’ behavior (Buchanan 2017), competing conceptual approaches and key terms explain this outcome. These include key concepts such as ‘norms’ (Finnemore and Hollis 2016), ‘deterrence’ (White House 2018a), even ‘information security’ and ‘cyber security’ (Maurer and Morgus 2014), with new concepts such as ‘persistent engagement’ (Fischerkeller and Harknett 2018) complementing the mix. Each of them is associated with a specifc bureaucratic agency advancing its own agenda. Even the behavior of individual actors is worth mentioning as the two key diplomats in the U.S. and Russia leading these negotiations have not changed in the last 20 years achieving unusual infuence setting the agenda, strategies, and pace of the discussions since the process began.2

#### Cyber norms fail—realism.

Mueller 18

(founder of IGP an internationally prominent scholar specializing in the political economy of information and communication). Milton Mueller. 9-4-2018. "A Farewell to Norms." Internet Governance Project; <https://www.internetgovernance.org/2018/09/04/a-farewell-to-norms/>.

Why norms fail The literature and conferences on norms have generated a kind of self-referential momentum based on this premise, and yet, cyber-conflict among states is as intense as ever. While it’s true that there are not a lot of alternative governance mechanisms available, the idea that norm development helps avoid conflict is something that needs to put to the test, empirically and logically. Let’s first make a brief general argument about the limitations of norms and then turn to specific evidentiary exhibits. To respond to Eichensehr’s bullet points: Of course norms are easier to develop and agree on than treaties. As general principles with no binding force, it is easy for states to formulate generalities that sound nice and agree to them without any credible commitment. Does this accomplish anything? The fact that norms can develop through unilateral declarations, bilateral agreements, or groups of states indicates that they still leave us in a state of anarchy, with multiple actors telling others what they think states should do and plenty of room for maneuvering around constraints states don’t like. But with dozens of different and possibly conflicting norms flying around, how can the discourse have any impact on what states actually do? True, cyber norms can – and should – evolve through state practice, but again that means that we don’t really have rules that shape behavior, we just have an open-ended normative discourse. That states will alter their normative positions as facts on the ground evolve, based on their own interests, is a realistic/positivistic description of what will in fact happen, it is not a normative prescription that channels behavior in a certain direction. The claim that conflicting norms “foster valuable clarity” about states’ actions is not always true. The parties engaged in a normative discourse – states – are known to be secretive, deceptive, frequently hypocritical, and likely to defect whenever it serves their interest. But even when states honestly formulate and promote their conflicting norms, we are still in a state of anarchy. And usually their actions are clearer than their words. Two recent incidents of cyber conflict provide support for these jaundiced conclusions: they show that norm development cannot overcome basic conflicts of interest among rival powers, and that states advancing specific norms repeatedly violate them.

#### The Talinn Manual proves—no one outside NATO signed on

Sangiovanni 18

(Reader in International Relations and a Fellow of Sidney Sussex College at Cambridge University, PhD in Political Science from the European University Institute). Mette Eilstrup-Sangiovanni. “Why the World Needs an International Cyberwar Convention”, Philosophy & Technology, Volume 31, Number 3

The Necessity of an International Cyberwar Convention This section presents the case for negotiating an international convention to govern cyber conflict between states. Despite growing threats from actors using ICT for aggressive and illicit purposes, few treaties address international cyber security issues. Presently, the main international agreements governing cyber conduct are the 2001 Convention on Cybercrime (and its Additional Protocol, 2006) and the Shanghai Cooperation Organization’s International Information Security Agreement (2009) (Vihul & Schmitt 2016, 39–40). Both agreements are severely limited, however, in terms of both their scope and membership.Footnote17 Calls for negotiating a comprehensive international treaty to govern cyber conflict—a so-called E-neva Convention—have so far met with disapproval, especially from Western states (ibid.)Footnote18 To date, the most elaborate discussions of cyber governance have thus focused on bringing existing international law to bear on cyber conflict. The *Tallinn Manual on the International Law Applicable to Cyber Warfare* (2013) is the most widely cited outcome of such discussions. This manual formulates a set of rules for how existing international law—chiefly *jus ad bellum*, international humanitarian law (IHL) and laws of state responsibility—apply in a cyber context (Talinn Manual 2013; Schmitt and Vihul 2014a, b, 2016; Lucas 2016). But while the Tallinn Manual (hereafter “the Manual”) provides a useful starting point for focusing attention on the need for stronger international cyber-governance, its practical value as an instrument to restrain cyber conflict is modest for (at least) three reasons. First, as Lucas points out (2017, 40), the Manual has generally failed to gain support outside the narrow group of NATO member-states that sponsored it. Second, the Manual does not propose or promulgate new international rules for the cyber domain but merely offers an interpretation of how existing laws may apply. So far, this interpretation has largely failed to persuade states to restrain their activities in the cyber domain (Lucas 2017, 17). What is more, the interpretation of many *jus ad bellum* and *jus in bello* treaty provisions as applied to cyber conflict remain unsettled (Schmitt and Vihul 2016, 43). Anticipating, as some of the leading legal scholars behind the Manual do, that “interpretative dilemmas concerning treaty law will be resolved through the recurrent practice of states in their application” (Ibid., 43–44) seems optimistic, especially when considering that the interpretation offered in the Manual has so far failed to influence state practice or opinio juris. Third, even if states were to agree on the general applicability of jus ad bellum and IHL in the cyber domain (which presently they do not), such agreement would hardly suffice. Each one of the international treaties and conventions currently governing the production, stockpiling, sale, transfer, and use of specific classes of armaments is testament to the states’ recognition that the general international prohibition on the use of force and IHL are by themselves insufficient to prevent or restrain international armed conflict.

#### No agreement—Russia and China ignore, security concerns trump

Shires ‘18

James Shires, 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, University of London, and BA from the University of Cambridge, “Between Multistakeholderism and Sovereignty: Cyber Norms in Egypt and the Gulf States”, War on the Rocks, 10/12/2018, <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.

### Cyber Ans: Nuclear Escalation

#### Air-gapping solves nuclear escalation.

Futter 16—(Associate Professor of International Politics and Director of Research for Politics and International Relations at the University of Leicester). Andrew Futter. 2016. “War Games Redux? Cyberthreats, US–Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control”, European Security, Volume 25, Issue 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).

#### No nuclear retaliation

Patrick Tucker 18, 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”, Defense One, 2/2/2018, <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 Ans: Status Quo Solves

#### NATO is acting now—cyber response teams, etc

Simpson and Atkinson, Western University scholars, ‘20

[Erika Simpson, Associate Professor, International Politics, Western University, and Ryan Atkinson, PhD Candidate, Western Univeristy, “Hybrid Warfare NATO’s Next Headache,” 2—28—20, https://lfpress.com/opinion/columnists/simpson-hybrid-warfare-natos-next-headache]

Our meetings with senior NATO policy-makers underlined that a new era of conflict has begun. We learned **NATO is making a strong effort to collect and evaluate information about hybrid attacks directed against its member states**. **It is also developing rapid-reaction cyber-defence teams that can be sent at an ally’s request in a crisis**. **The cyber teams work on civil emergency planning, critical infrastructure protection, counterterrorism and energy protection**. **This is an inexpensive way to respond to threats below the threshold of Article 5** — the collective defence obligation enshrined in the 1949 Washington Treaty at the founding of NATO. But **could a hybrid attack trigger Article 5**? Diplomats rather implausibly asserted **NATO’s response would be context-driven based on decisions rapidly arrived at by all the allies by consensus**. Hackers operating at the sub-state level could be difficult to name and shame. Attribution difficulties would also prevent discovering their motives. NATO wants to prevent conflicts from escalating and seeks to develop counter-strategies that would improve intelligence sharing. **Beyond NATO, more units are being dedicated to deal with hybrid threats**, such as the European Centre of Excellence established by Finland. But all this work requires the sharing of confidential information and classified documents, which means significant trust must be built. Yet much of **the burden will be on individual NATO member states to develop sufficient resilience to counter cyber attacks**. **All allies will need to improve their resilience**, **and NATO is producing benchmark guidelines to facilitate an alliance-wide common approach**. Some allies are expected to ask NATO to protect them against low-level hazards, but they will likely be told they should learn to cope with those on their own. NATO is working to defend allies trapped in protracted engagements in this grey zone of warfare. All of us will need to look at hybrid threats without rose-colored glasses

### NATO Ans: Cohesion Alt Causes—1NC

#### NATO cannot act cohesively—multiple reasons

Lucas, CEPA fellow, ‘22

[Edward Lucas, Nonresident Fellow, Center for European Policy Analysis, “NATO Is Out of Shape and Out of Date,” FOREIGN POLICY, 6—7—22, <https://foreignpolicy.com/2022/06/07/nato-ukraine-russia-war-alliance-reform-geopolitics-military/>, accessed 6-10-22]\

Yet look a little more closely, and the picture is far less rosy. Notwithstanding its apparent unity of purpose since the start of Russia’s war, NATO looks out of shape and out of date. In the run-up to their summit, the allies have been furiously haggling over the language in their new strategic concept, which will frame the alliance’s mission for the coming years and will be unveiled in Madrid. What will it say about Russia? About China? What sacrifices and risks are the member states really willing to accept? Are they willing to pool sovereignty in order to streamline decision-making?

Nothing in recent weeks suggests that these questions will get clear answers. For starters, the 30-strong alliance is unwieldy. In military terms, only a handful of members matter—above all, the United States—but in political terms, even little Luxembourg and Iceland get a voice. Worse, the political divides are huge. Turkey under President Recep Tayyip Erdogan is a semi-authoritarian state that flirts with Russia and fumes at what it considers European meddling over human rights. Hungary under Prime Minister Viktor Orban is taking a different but downward path, fusing wealth and power into a new system of control at home and undermining U.S. and European attempts to put pressure on Russia and China. Macron’s relentless posturing and German Chancellor Olaf Scholz’s foot-dragging create constant obstacles and distractions. The two leader’s weaknesses, on glorious display since the start of the war, have already enriched the language: Scholzen is a German neologism for “dither,” while makronic in Polish (and its equivalent in Ukrainian) can be roughly translated as “vacuous grandstanding while doing nothing.”

Macron and Scholz corrode decision-making with their foibles and thus place a big question mark over the alliance’s credibility and cohesion. Any threat or provocation from Russia is unlikely to be clear or conveniently timed. More likely it will be something deliberately ambiguous, such as a Russian drone that “accidentally” strays onto the territory of a front-line state and hits a target. Some countries would favor a tough response. Others would fear escalation and want dialogue. Still others would take the ambiguity as a convenient excuse to do nothing. Would the 30—soon to be 32—national representatives in the North Atlantic Council, the alliance’s deliberative body, really make a speedy and tough decision on how to react? More likely, some of them would plead for delay, diplomacy, and compromise. Those actually facing the possibility of attack would be far more hawkish, preferring a sharp military confrontation to even the smallest Russian victory. “Not one inch, not one soul,” a senior military figure from one of the Baltic states, speaking anonymously, told me. “We have seen what they did in Ukraine.”

### NATO Ans: Cohesion Alt Causes—2NC

#### COVID will make everything worse

Gvosdev 20

(Nikolas K. Gvosdev is the Editor of Orbis: FPRI's Journal of World Affairs and a Senior Fellow in FPRI's Eurasia Program. He is also a Professor of National Security Affairs, holding the Captain Jerome E. Levy Chair in Economic Geography and National Security at the U.S. Naval War College in Newport, Rhode Island, 3-23-2020, accessed on 9-13-2020, Foreign Policy Research Institute, "The Effect of COVID-19 on the NATO Alliance - Foreign Policy Research Institute", https://www.fpri.org/article/2020/03/the-effect-of-covid-19-on-the-nato-alliance/)

Effects on Alliance Cohesion Another trend that the coronavirus may accelerate is the loss of intra-alliance cohesion and solidarity. Just prior to the eruption of the COVID-19 pandemic in the West, the Pew Research Trust released its latest findings (February 2020) on how NATO is viewed by the publics of the alliance members. Their research concluded: There is widespread reluctance to fulfill the collective defense commitment outlined in Article 5 of NATO’s founding treaty. When asked if their country should defend a fellow NATO ally against a potential attack from Russia, a median of 50% across 16 NATO member states say their country should not defend an ally, compared with 38% who say their country should defend an ally against a Russian attack. Intra-alliance cohesion was further shaken by the Idlib crisis—when it appeared that Turkey’s NATO allies were not fully on board with giving Ankara the blank check it requested to confront Russia in Syria—and by Turkey’s subsequent decision to again permit migrants and refugees to transit Turkish territory in order to be able to reach the European Union. Turkey’s perspective, of course, is that since it is not an EU member, it should not have to necessarily carry water for European states. From a security perspective, one member of NATO was choosing not to prevent, but even to encourage, a trend that threatened the security of its ostensible allies. To be sure, the coronavirus did not create this situation, but it further erodes confidence in the proclamations of solidarity that ritually end every NATO summit. In the past month, as the virus spreads throughout the world, NATO (and EU) allies have seen their partners hoarding equipment and medical supplies. Moreover, intra-alliance borders have been closed down, not only between NATO and EU members within Europe, but also bans forbidding travel across the Atlantic have been enacted. The perception that the United States is prepared to go it alone and look out for its well-being without concern for its closest allies reinforces pre-existing trends; Europeans, in turn, believe that their side of the Atlantic must be prepared to de-couple from Washington for its own security—and the messages they are receiving from the United States over coronavirus adds further grist to that mill. Meanwhile, Beijing has reaped a public relations bonanza from its moves to send assistance to virus-ravaged Italy and Spain, which has highlighted the initial lack of concrete support from Rome’s and Madrid’s Western partners. While the European Union has taken the brunt of the criticism, the United States has not used NATO as a way to develop a coalition to combat the virus. NATO ally Turkey had used indecision over Syria to justify its willingness to buck NATO solidarity to forge a closer relationship with Russia; now, Italy feels justified in closer collaboration with Beijing, including on the Belt and Road Initiative, because of the perception that Western solidarity has failed Rome in its time of need. Beyond the political perception that NATO has failed the solidarity test, the practical realities of the pandemic call into question the operational basis of NATO’s deterrent mission: the ability to field forces in sufficient strength to deter or repel any possible incursion. If one result of the pandemic has been a push for countries to withdraw their national contingents from overseas missions to concentrate on the home front, then a second is a growing reluctance for countries to send—or receive—forces for fear that they will spread the disease. Norway canceled the regional “Cold Defender” exercise that should have been held in March 2020 over concerns for troops coming into Norway, and other countries, such as Finland, were reluctant to dispatch their forces. The major Europe-wide NATO exercise for 2020, “European Defender,” which was designed, in part, to demonstrate to outside adversaries (read: Russia) that the United States could quickly reinforce the continent, is being scaled back, amidst a new Department of Defense directive that has halted the movement of U.S. forces and equipment. The Russia Factor Signs of discord in NATO are always carefully monitored by Russia. The 2015 Russian national security strategy categorizes the alliance as a threat to Russian strategic interests, even if some of its member (like Germany, France, Italy, Turkey, and Hungary) are, at a bilateral level, important strategic partners. It is not surprising, therefore, that the Kremlin, even if it has not explicitly commissioned a disinformation campaign, sees value in having its news and information outlets push narratives that seek to accelerate discord and disunity among NATO members. Depending on the course of the pandemic, we could very easily see a new Russian information campaign. Such a campaign would target publics in southern and western Europe and would question the value of an alliance which was ineffective in its response to the virus but which demands that they be prepared to risk conflict with Russia—while also sowing more doubts in both NATO and non-NATO neighbors about how much faith they are willing to place in alliance guarantees. The Russian decision to dispatch military medical specialists and equipment to Italy is also being contrasted with the initially lackluster EU/NATO response. Better messaging, however, is not going to be a sufficient response. Nor should NATO assume that once this crisis has passed, it will be a return to business as usual. For one thing, there could be recurrent flare-ups of COVID-19, leading to the re-imposition of travel bans, border closures, and movement of personnel. The economic fallout from the pandemic is going to impact budgets and policies for years to come.

#### Military structural problems limit alliance effectiveness

Lucas, CEPA fellow, ‘22

[Edward Lucas, Nonresident Fellow, Center for European Policy Analysis, “NATO Is Out of Shape and Out of Date,” FOREIGN POLICY, 6—7—22, <https://foreignpolicy.com/2022/06/07/nato-ukraine-russia-war-alliance-reform-geopolitics-military/>, accessed 6-10-22]\

The political weaknesses are matched by military ones. By far the most important country in the alliance is the United States. The U.S. security guarantee to Europe—with its threat of devastating conventional and, if necessary, nuclear response to any attack—is the cornerstone of the alliance. “All for one and one for all” sounds fine, but nobody in the Kremlin will tremble at the thought of Spanish, Dutch, or Canadian displeasure. Yet the result of this is a colossal dependence on U.S. capabilities, ranging from ammunition and spare parts (of which European countries’ stockpiles are notoriously skinny) to military transports that move forces quickly and efficiently over long distances. Even if Europe’s new defense spending plans materialize, they will not change the fact that only U.S. armed forces can move with the scale and speed necessary to defend territory from a country like Russia.

Conversely, the countries that most need defending—Estonia, Latvia, and Lithuania—are the least able to bear the burden themselves. They need advanced weapons, particularly for air and missile defense, that they cannot afford themselves. The thin neck of land along the Polish-Lithuanian border, the so-called Suwalki Gap, is particularly vulnerable to attack from Russia’s militarized Kaliningrad exclave and Belarus, from which Russia attacked Ukraine. Poland and Lithuania both want a big U.S. military presence—either a permanent base or a persistent rotation of forces—to safeguard this strategic chokepoint.

Yet NATO command structures and planning do not fully reflect the imbalance of forces between the United States and Europe. They rely on the fiction that the European allies are more or less equal partners. Even military lightweights need to have important-sounding jobs and installations, making the North Atlantic Council the military version of a parliament dividing out the pork.

The resulting command structure is like a tangled pile of spaghetti. In the Baltic region alone, NATO has several multinational headquarters, one divisional headquarters split between Latvia and Denmark, another divisional headquarters in Poland, and a corps headquarters at a different location in Poland. Overall responsibility for the defense of Europe is divided between three Joint Forces Command headquarters in Naples, Italy; Brunssum, the Netherlands; and Norfolk, Virginia. But the top U.S. military commander in Europe, Air Force Gen. Tod Wolters, is based at Supreme Headquarters Allied Powers Europe in Mons, Belgium. A maritime strategy for the Baltic Sea region has yet to be decided—which is just as well, because NATO has yet to create a naval headquarters for the region. Nor has the alliance drawn up real military plans for the reinforcement and defense of its northeastern members, let alone decided who would actually provide the forces and equipment in order to make them credible. Military mobility is meant to be the responsibility of Joint Support and Enabling Command, headquartered in Ulm, Germany, and originally set up as part of the European Union’s own defense policy.

#### Expansion-induced problems weaken the alliance

Cancian 19

(defense expert at the Center for Strategic and International Studies). Cancian, Mark. 2019. “Stop The Madness of NATO Expansion.” Breaking Defense. December 13, 2019. https://breakingdefense.com/2019/12/stop-the-madness-of-nato-expansion/.

Expansion also inflames anti-NATO sentiment by feeding skepticism about its benefits. One of the strongest arguments for the alliance is that it is better to have lots of rich, powerful allies when facing threats. Adding weak nations undermines this argument. Thus, President Trump has regularly criticized NATO as a “bad deal” for the United States while French President Emmanuel Macron has called NATO “brain-dead.” Finally, expansion incorporates countries with short and shallow democratic traditions. North Macedonia, like the newly added NATO countries of Croatia, Montenegro, and Albania, has made great strides in improving governance, for which they all deserve credit, but they lack the robust institutions that justify military burdens to NATO publics. Someday this over-expansion will produce a crisis. Perhaps the crisis will arise from an intra-NATO dispute; perhaps from a local dispute that involves, for example, long-standing tensions between Serbia and its NATO neighbors Croatia or North Macedonia; or perhaps the treatment of an ethnic minority like Russians in the Baltic countries. If dragged into messy conflicts in which they have few interests, countries may come to openly question the entire NATO project and endanger a key element of European, indeed, global stability. NATO needs to draw the line now. Behind North Macedonia are nearly 20 other partners who might also want to join NATO. And who can blame them. By joining NATO they gain security and status at little cost.

### NATO Ans: Consensus Problems

#### Unrelated disputes undermine the ability to generate consensus

Lute & Burns, Harvard researchers, ‘19

[Ambassador Douglas Lute, Senior Fellow, Belfer Center and President, Cambridge Global Advisors and Ambassador Nicholas Burns, Professor, Diplomacy and International Politics, Harvard Kennedy School, “NATO at Seventy: An Alliance in Crisis,” Project on Europe and the Transatlantic Relationship, Belfer Center for Science and International Affairs, Harvard Kennedy School, 2—19, p. 23]

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.

### NATO Ans: Resilient

#### NATO is resilient—history proves

Slapakova 20

(policy researcher working on counter-terrorism, emerging security threats and defence capability development). Linda Slapakova. 1/15/20, “What International Relations Theory can tell us about NATO’s ‘Mort Cérébrale’,” <https://www.globalpolicyjournal.com/blog/15/01/2020/what-international-relations-theory-can-tell-us-about-natos-mort-cerebrale>

In the prelude to the NATO summit in London commemorating the 70th anniversary of the founding of the alliance, discussions were overshadowed by a now-infamous Economist interview with French President Emmanuel Macron. In the interview, the French President claimed that NATO is experiencing a “brain death” – a ‘mort cérébrale’ resulting from a lack of institutional capacity to prevent, mitigate, or effectively respond to unilateral action from individual allies which could be disruptive to the alliance’s agenda. President Macron’s remarks precipitated a debate concerning NATO’s relevance (or irrelevance) in the post-Cold War international system, its (potentially failing) adaptation to new security and strategic circumstances, and the constraints imposed by NATO’s seeming lack of institutionalisation and ability to prevent unilateral action taken by individual members. Although NATO does not feature frequently in International Relations (IR) theory, and IR debates are more often than not virtually absent from NATO scholarship, this article draws on existing literature to examine the extent to which IR can shed light on the debate over NATO’s alleged ‘mort cérébrale’. In doing so, the article argues that in spite of its self-induced crises of confidence, and despite important weaknesses and challenges, insights from IR scholarship suggest that news of NATO’s demise are greatly exaggerated. NATO’s adaptation in the post-cold war international system In the days and weeks following President Macron’s remarks, the question of NATO’s irrelevance and potential demise dominated debates, with less attention being paid to the issue which Macron’s comment was actually directed at, namely Turkey’s offensive into Syria and the US’ sanctioning of this move; both of which occurred without prior discussion or consent of other NATO allies. While the escalatory nature of the debate may seem surprising to some, it represents more of a rule than an exception. It is symptomatic of the overall state of debate about NATO in the post-Cold War era: NATO is, seemingly, constantly on the brink of collapse. As commentators have attempted to come to grips with any given crisis, a ‘NATO-in-crisis’ body of literature has developed. This literature claims that “disputes within the Alliance grow more debilitating over time, in the sense that each new crisis is promptly labelled the worst ever.” However, none of the predictions of NATO’s collapse have materialised thus far. According to IR theorists, several factors contribute to this endurance of the North Atlantic alliance. The first factor is the value of established institutions in promoting stability and enabling cooperation between states in the international system. Institutions are generally costly to maintain, and existing institutions may be less than optimally efficient, but such costs often pale in comparison to the costs of unilateral action or the upfront costs of creating of new institutions. While this is the general rule, a number of factors determine the weight of those relative costs, including the availability of institutional assets in the form of norms, rules, and procedures. In the case of NATO these assets have developed to be sufficiently hybrid to allow for post-Cold War adaptation to new security and strategic challenges after the Soviet threat – NATO’s raison d’être – disappeared. In this sense, although NATO may be perceived as originally tasked with an explicit mandate to provide territorial defence and deterrence against the Soviet threat, the nature of its institutional assets create incentives for member states to adapt the institution to a new security and strategic environment rather than facing emerging threats unilaterally, or with the help of new organisations. Secondly, members may be perceived as developing a “vested interest in maintaining existing institutional arrangements” through what John Ikenberry describes as ‘institutional stickiness’. As an institution with distinct Western and liberal character, the normative and ideational aspects of NATO’s mandate may be seen as contributing to such stickiness. This includes NATO’s perceived success as a security community, as well as its “ability to re-produce ‘the West’ as a geo-cultural space that serves as its security referent object” in a more discursive sense. In spite of the many criticisms directed at NATO for its insufficiencies in the face of existing and emerging threats, NATO continues to be seen as a crucial beacon for the Western liberal international order. In times when emerging powers are perceived to pose a threat to such an order, it may be argued that NATO’s institutional stickiness will strengthen, rather than weaken, on the basis of its normative character. Thirdly, scholars have stipulated the central role of institutional change and adaptation for explaining NATO’s resilience. With a significant evolution in NATO’s role and responsibilities in the post-Cold War era, a crucial factor in understanding NATO’s resilience has been the ability of NATO allies to negotiate a balance between the alliance’s roles and responsibilities, particularly those of collective defence and out-of-area engagements. As Johnston argues, NATO adaptation has taken place in the context of various historical events representing ‘critical junctures’ for the institution. Analysis of these critical junctures also reveals the agency of NATO’s institutional actors vis-a-vis member states with the help of instruments such as agenda-setting, moderating, and co-opting powers. Despite the appearance to the contrary, NATO is more institutionalised than traditional military alliances, which helps explain its post-Cold War adaptation. With or without brain death: NATO is here to stay No doubt, NATO’s decision-making will continue to be hampered by intra-alliance disputes over highly contentious issues such as Turkey’s recent intervention in Syria. As much as this issue can be perceived as a crisis for the alliance, NATO has faced and survived such situations before. In explaining this dynamic, IR scholarship has highlighted various mechanisms that explain NATO outliving its raison d’être and continuing to exist in the post-Cold War international system. NATO is more institutionalised and resilient than might appear from recent debates, which among other things ignore the agency of institutional actors and common interest of member states in mitigating conflict and crises. There is therefore good reason to believe that NATO is more likely than not to adapt to new security and strategic challenges rather than experience a self-annihilating “brain death.” However, this is not to say that the current situation is not detrimental to the alliance. The effectiveness of NATO’s deterrence function fundamentally hinges on the perception of unity and commitment towards collective defence. Should member states choose to act unilaterally and escalate every dispute to a debate over NATO’s very survival, the credibility of the alliance and its deterrent will undoubtedly suffer as a consequence.

# Case Ans: Hybrid / Russia

### Democracy Ans: 1NC

#### Democracy is resilient but fails

Doorenspleet, University of Warwick Politics professor, ’19

[Renske Doorenspleet, Politics Professor at the University of Warwick, “Conclusion: Rethinking the Value of Democracy,” Rethinking the Value of Democracy, Springer Berlin Heidelberg, 2019, pp. p. 239-243]

Key Findings: Rethinking the Value of Democracy

The value of democracy has been taken for granted until recently, but this assumption seems to be under threat now more than ever before. As was explained in Chapter 1, democracy’s claim to be valuable does not rest on just one particular merit, and scholars tend to distinguish three different types of values (Sen 1999). This book focused on the instrumental value of democracy (and hence not on the intrinsic and constructive value), and investigated the value of democracy for peace (Chapters 3 and 4), control of corruption (Chapter 5) and economic development (Chapter 6). This study was based on a search of an enormous academic database for certain keywords,6 then pruned the thousands of articles down to a few hundred articles (see Appendix) which statistically analysed the connection between the democracy and the four expected outcomes.

The frst fiding is that a reverse wave away from democracy has not happened (see Chapter 2). Not yet, at least. Democracy is not doing worse than before, at least not in comparative perspective. While it is true that there is a dramatic decline in democracy in some countries,7 a general trend downwards cannot yet be detected. It would be better to talk about ‘stagnation’, as not many dictatorships have democratized recently, while democracies have not yet collapsed.

Another fnding is that the instrumental value of democracy is very questionable. The feld has been deeply polarized between researchers who endorse a link between democracy and positive outcomes, and those who reject this optimistic idea and instead emphasize the negative effects of democracy. There has been ‘no consensus’ in the quantitative literature on whether democracy has instrumental value which leads some beneficial general outcomes. Some scholars claim there is a consensus, but they only do so by ignoring a huge amount of literature which rejects their own point of view. After undertaking a large-scale analysis of carefully selected articles published on the topic (see Appendix), this book can conclude that the connections between democracy and expected benefts are not as strong as they seem. Hence, we should not overstate the links between the phenomena.

The overall evidence is weak. Take the expected impact of democracy on peace for example. As Chapter 3 showed, the study of democracy and interstate war has been a fourishing theme in political science, particularly since the 1970s. However, there are four reasons why democracy does not cause peace between countries, and why the empirical support for the popular idea of democratic peace is quite weak. Most statistical studies have not found a strong correlation between democracy and interstate war at the dyadic level. They show that there are other—more powerful—explanations for war and peace, and even that the impact of democracy is a spurious one (caveat 1). Moreover, the theoretical foundation of the democratic peace hypothesis is weak, and the causal mechanisms are unclear (caveat 2). In addition, democracies are not necessarily more peaceful in general, and the evidence for the democratic peace hypothesis at the monadic level is inconclusive (caveat 3). Finally, the process of democratization is dangerous. Living in a democratizing country means living in a less peaceful country (caveat 4). With regard to peace between countries, we cannot defend the idea that democracy has instrumental value.

Can the (instrumental) value of democracy be found in the prevention of civil war? Or is the evidence for the opposite idea more convincing, and does democracy have a ‘dark side’ which makes civil war more likely? The findings are confusing, which is exacerbated by the fact that different aspects of civil war (prevalence, onset, duration and severity) are mixed up in some civil war studies. Moreover, defining civil war is a delicate, politically sensitive issue. Determining whether there is a civil war in a particular country is incredibly diffcult, while measurements suffer from many weaknesses (caveat 1). Moreover, there is no linear link: civil wars are just as unlikely in democracies as in dictatorships (caveat 2). Civil war is most likely in times of political change. Democratization is a very unpredictable, dangerous process, increasing the chance of civil war significantly. Hybrid systems are at risk as well: the chance of civil war is much higher compared to other political systems (caveat 3). More specifcally, both the strength and type of political institutions matter when explaining civil war. However, the type of political system (e.g. democracy or dictatorship) is not the decisive factor at all (caveat 4). Finally, democracy has only limited explanatory power (caveat 5). Economic factors are far more significant than political factors (such as having a democratic system) when explaining the onset, duration and severity of civil war. To prevent civil war, it would make more sense to make poorer countries richer, instead of promoting democracy. Helping countries to democratize would even be a very dangerous idea, as countries with changing levels of democracy are most vulnerable, making civil wars most likely. It is true that there is evidence that the chance of civil war decreases when the extent of democracy increases considerably. The problem however is that most countries do not go through big political changes but through small changes instead; those small steps—away or towards more democracy—are dangerous. Not only is the onset of civil war likely under such circumstances, but civil wars also tend to be longer, and the confict is more cruel leading to more victims, destruction and killings (see Chapter 4).

A more encouraging story can be told around the value for democracy to control corruption in a country (see Chapter 5). Fighting corruption has been high on the agenda of international organizations such as the World Bank and the IMF. Moreover, the theme of corruption has been studied thoroughly in many different academic disciplines—mainly in economics, but also in sociology, political science and law. Democracy has often been suggested as one of the remedies when fghting against high levels of continuous corruption. So far, the statistical evidence has strongly supported this idea. As Chapter 5 showed, dozens of studies with broad quantitative, cross-national and comparative research have found statistically signifcant associations between (less) democracy and (more) corruption. However, there are vast problems around conceptualization (caveat 1) and measurement (caveat 2) of ‘corruption’. Another caveat is that democratizing countries are the poorest performers with regard to controlling corruption (caveat 3). Moreover, it is not democracy in general, but particular political institutions which have an impact on the control of corruption; and a free press also helps a lot in order to limit corruptive practices in a country (caveat 4). In addition, democracies seem to be less affected by corruption than dictatorships, but at the same time, there is clear evidence that economic factors have more explanatory power (caveat 5). In conclusion, more democracy means less corruption, but we need to be modest (as other factors matter more) and cautious (as there are many caveats).

The perceived impact of democracy on development has been highly contested as well (see Chapter 6). Some scholars argue that democratic systems have a positive impact, while others argue that high levels of democracy actually reduce the levels of economic growth and development. Particularly since the 1990s, statistical studies have focused on this debate, and the empirical evidence is clear: there is no direct impact of democracy on development. Hence, both approaches cannot be supported (see caveat 1). The indirect impact via other factors is also questionable (caveat 2). Moreover, there is too much variation in levels of economic growth and development among the dictatorial systems, and there are huge regional differences (caveat 3). Adopting a one-size-ftsall approach would not be wise at all. In addition, in order to increase development, it would be better to focus on alternative factors such as improving institutional quality and good governance (caveat 4). There is not suffcient evidence to state that democracy has instrumental value, at least not with regard to economic growth. However, future research needs to include broader concepts and measurements of development in their models, as so far studies have mainly focused on explaining cross-national differences in growth of GDP (caveat 5).

Overall, the instrumental value of democracy is—at best—tentative, or—if being less mild—simply non-existent. Democracy is not necessarily better than any alternative form of government. With regard to many of the expected benefts—such as less war, less corruption and more economic development—democracy does deliver, but so do nondemocratic systems. High or low levels of democracy do not make a distinctive difference. Mid-range democracy levels do matter though. Hybrid systems can be associated with many negative outcomes, while this is also the case for democratizing countries. Moreover, other explanations—typically certain favourable economic factors in a country—are much more powerful to explain the expected benefts, at least compared to the single fact that a country is a democracy or not. The impact of democracy fades away in the powerful shadows of the economic factors.8

### Democracy Ans: 2NC

#### No democracy impact—too many other causes and does not prevent war

Bennett, journal editor, ‘18

[Jonah Bennett, editor-in-chief, “The Rise and Fall of Liberal Democratic Peace Theory.” PALLADIUM MAGAZINE, 10—15—18,

<https://palladiummag.com/2018/10/15/the-rise-and-fall-of-liberal-democratic-peace-theory/>.

But something happened in the early 2000s. The unfolding of history as liberalism had been disrupted. The attacks of September 11, the subsequent bungling of intelligence regarding WMDs, the United States’ decision to drag its NATO allies into a series of embarrassing and ultimately ineffectual wars in the Middle East, numerous botched attempts at regime change and nation-building, and aggressive ideological demands as pre-conditions for diplomacy, have devastated the credibility of the U.S.-driven, Western liberal order. In some areas, history is now forking from the liberal path with a surprising confidence. Axios declared 2018 the year of the strongman, but it can also be called the year of liberalism in crisis. Russia, Egypt, China, Poland, Hungary, the Philippines, and Turkey—among others—have gained a renewed sense of self and conviction in their opposition to liberalism, as opposed to merely carving out for themselves an unprincipled exception to liberalism and ceding it the moral high ground. Even in Europe, where liberal democracy claims some of its greatest accomplishments, liberalism is beginning to unravel on the periphery in countries like Poland, Hungary, and Italy. Jair Bolsonaro, who notably expressed sympathy for a military dictatorship, has done tremendously well so far in the Brazilian presidential election. Neither soft, nor hard evangelism of liberalism is working the way it used to. For liberal theorists, the prospect of a liberal democratic world peace is now questionable. The Economist has put out a call to arms to defend liberalism as the most successful idea of the last 400 years. Whether this call results in anything substantial remains to be seen. But there is a palpable sense that liberalism is facing a serious new opposition. Despite this trend, liberalism’s theorists have a hope encapsulated by Daniel Deudney and G. John Ikenberry’s 2009 pronouncement that “liberal states should not assume that history has ended, but they can still be certain that it is on their side.” And yet, in the nine years following this bold pronouncement, history has not been especially kind to liberalism. Texas A&M political science professor Christopher Layne, writing in early 2018, has summed up the current situation aptly, namely that China as an increasingly self-aware superpower is already reshaping the world order away from Pax Americana: The US foreign policy establishment does not grasp this, and, instead, has invested the idea of a ‘rules-based, institutionalized’ international order with a talismanic quality. It claims that rules and institutions are politically neutral, and, ipso facto, beneficial for all. However, in international politics, who rules makes the rules. Rules and institutions reflect the distribution of power in the international system. A power transition is taking place in the early twenty-first century: US power is in relative decline and China is rising quickly. No international order—not even the Pax Americana—lasts forever. The liberal world order cannot survive the erosion of US hegemonic power. It is this structural change, not Donald Trump, that threatens the post-Second World War international order’s survival. It requires a huge leap of faith to believe that a risen China will continue to subordinate itself to the Pax Americana. Which brings us to the question: given that the prospect of an expanded democratic peace is starting to hit some hard limits, how well does liberal democratic peace theory actually explain the peace that has existed among liberal democratic states? Although LDP theory is taken as an empirical law in international relations, it has picked up a number of qualifications, making the theory far less interesting than first presented. Here are various renditions of the theory since its modern inception in the 1960s: Claim 1: liberal democracies go to war less than non-liberal democracies. The most significant abandonment in the field has been of the monadic hypothesis: that liberal democratic states are less likely to go to war compared to non-liberal democratic states. Henry Farber and Joanne Gowa have convincingly shown that, statistically, democracies on average have the same probability of going to war as non-democracies. At this point, no one holds the monadic hypothesis. Claim 2: no liberal democracy has fought another liberal democracy since 1816 (notably after 1812) This claim from Michael Doyle has increasingly fallen out of favor. There weren’t many democracies prior to 1945, and so the number of dyadic pairs of liberal democratic countries that could have gone to war was extremely limited. For example, Doyle excludes Great Britain from counting as a liberal democracy until 1832 and denies that the Spanish-American War of 1898 should count, even though the Polity II data set lists Spain as a democracy in 1898. Others have argued that the Second Philippines War of 1899 shouldn’t count either, as at the time the Philippines hadn’t held an election yet. This strong claim has largely been dropped because of a) exception cases that require new qualifications to explain, and b) the fact that there weren’t enough existing liberal democracies to achieve significance. All totaled, there are around 50 exception cases suggested in the literature. Claim 3: mature liberal democracies tend not to go to war/don’t go to war with one another Although Peru and Ecuador fought while both were liberal democracies, some maintain that the war occurred before the “pacifying effects” of liberal democracy had enough time to work, meaning maturity was lacking. Yet another qualification. Interestingly, the U.S. intervened militarily to topple Salvador Allende after he was democratically elected in Chile. Israel invaded Lebanon in 1981, but at the time, Lebanon’s government was in disarray. R.J. Rummel states that the Israeli attack on the United States’ USS Liberty in 1967 counts as conflict below the level of war, but argued that Israel at the time was “only partially free.” That Finland joined up with the fascists from 1941 to 1944 apparently shouldn’t count, as no Finnish troops attacked troops from a liberal democratic country, though Great Britain bombed Finland in 1941. Claim 4: mature liberal democracies in the post-1945 era don’t go to war with one another The addition of the ‘post-1945 era’ qualification came later in the development of LDP theory, and while it may be a disappointing qualification, it may be necessary, given the small-N universe of liberal democracies before 1945. Bruce Russett admits that “the absence of murderous quarrels between democracies was not too surprising, and may need—at least for the pre-1945 era—little further explanation.” Claim 5: mature liberal democracies in the post-1945 era don’t go to war with one another, but for normative reasons, not structural reasons It’s claimed that the structural elements of liberal democratic states, namely separation of powers, checks and balances, elections, the free press, etc. should result in less war in general, but this is essentially equivalent to the monadic hypothesis, which has been largely abandoned. So, it might be possible to explain the absence of war through the normative mechanisms of liberal democratic states, as opposed to structural elements. Zeev Maoz and Bruce Russett argue that while there is some support for the structural model, the normative model has more support and better consistency. The above examples illustrate continuing iterations of the theory. This trajectory is by no means perfectly linear, nor is there consensus on how many qualifications are required, but the fact that these qualifications have continued to pile on is evidence that LDP theory is now much closer to triviality than when first introduced.

### Hybrid War Ans: 1NC

#### Hybrid war won’t escalate

Sari 19

(Senior Lecturer in Law, University of Exeter; Director, Exeter Centre for International Law; Fellow, Supreme Headquarters Allied Powers Europe; Fellow, Allied Rapid Reaction Corps). Aurel Sari. 6/6/19, "The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats", Harvard National Security Journal, Vol. 10, Issue 2, <https://harvardnsj.org/wp-content/uploads/sites/13/2019/06/Mutual-Assistance-Clauses-of-the-North-Atlantic-and-EU-Treaties.pdf>

Nevertheless, the threat of subversion should not be overrated, either. In particular, the widespread unease over the blurring of the line between war and peace must be put into perspective. Hybrid warfare in its original, narrow sense describes a style of operational art: the integrated use of conventional and unconventional methods of warfighting in the same battlespace. Armed conflict, whether actual or impending, is integral to the concept. By contrast, hybrid warfare in its broader sense describes the use of the full range of instruments by hostile actors in pursuit of their strategic goals. Here, hybrid warfare no longer refers to a method of waging war, but to the combination of diverse levers of influence for the purposes of geopolitical competition. Hard power and the threat of military confrontation remain essential components of the concept, but actual or imminent hostilities do not. Describing non-forcible measures carried out by hostile powers as hybrid warfare may be justified in circumstances where these activities constitute shaping operations in anticipation of armed conflict or where they form part of ongoing hostilities.283 However, in the absence of any realistic connection with actual or impeding war, labeling such measures as acts of warfare, whether hybrid or not, is a misnomer.284 It may convey the hostile nature of geopolitical confrontation,285 but it is still hyperbole. The dividing line between war and peace may look blurred when it is viewed from the perspective of a wide understanding of hybrid warfare, but this is so largely because the very use of the concept in such a loose manner creates a link between non-forcible acts falling below the threshold of war and the mere prospect of war.286 Russian theorists of contemporary conflict have avoided such conceptual freefall by insisting that violence is an integral element of warfare.287 Since hybrid warfare in a broad sense does not necessarily involve armed violence, the question arises whether mutual defense clauses should be considered as implicated in such circumstances at all. There are compelling reasons to answer in the negative. On their own, acts of hostile interference not entailing the use of force are unlikely to subvert Article 5 NAT or Article 42(7) TEU. As Russia’s interventions in Georgia and Ukraine demonstrate, there is little evidence that nonmilitary instruments have rendered the use of armed force redundant. Tweets do not seize ground—infantry battalions do. Since states are not capable of achieving traditional military objectives, such as seizing and holding ground, without employing armed force, they are not able to circumvent mutual defense guarantees by limiting themselves solely to non-forcible measures. At the same time, the fact that specific incidents are not caught by Article 5 or Article 42(7) does not necessarily point to a flaw in their design. Take, for example, the attempted murder of Sergei Skripal with a chemical nerve agent in Salisbury on March 4, 2018, an act which the British Government declared to be an unlawful use of force.288 While commentators are divided as to whether the incident did in fact amount to the use of force,289 they concur that it certainly did not reach the level of an armed attack.290 Indeed, the UK and its allies studiously refrained from describing it as an armed attack.291 The Salisbury incident thus escaped the reach of Article 5. Yet this is not the result of some drafting deficiency, but reflects the fact that not every security challenge gives rise to the right of self-defense under international law.292 Similarly, the fact that Chinese warships support the frontline operations of Chinese civilian and coast guard vessels in the South China Seas by providing a deterrent effect does not mean that their mere presence constitutes an armed attack. Nor should we assume that military force is an appropriate and effective response to every type of threat.293 There are plenty of hostile actions in response to which it would be unreasonable to use force—either because doing so would be disproportionate to the threat, and thus morally and politically unpalatable, or because it would carry a real risk of escalation with limited prospects of compelling the adversary to submit to our will, or both.

### Hybrid War Ans: 2NC

#### Many barriers stop escalation—strategic links

Baezner & Robin, CSS & CDP scholars, ‘17

[Marie Baezner and Patrice Robin, “Cyber-Conflict Between the United States of America and Russia,” CSS Cyberdefense Hopspot Analyses, Cyber Defense Project and Center for Security Studies, ETH Zurich, 6—17, p. 13]

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.

#### Russian hybrid efforts fail—Baltics experience proves

Lanoszka, University of Waterloo scholar, ‘20

[Alexander Laoszka, Assistant Professor, International Relations, University of Waterloo,“Thank Goodness for NATO Enlargement,” INTERNATIONAL POLITICS v. 57, 2020, pp. 451-470, SpringerLink]

Even the use of so-called hybrid tactics may have limited efficacy in the Baltic region. The three Baltic countries have been subject to an intense Russian disinformation campaign since at least 2014. Nevertheless, local public opinion remains largely supportive of NATO and other defense policy measures aimed at boosting deterrence. One reason why these societies may be inoculated against Russian disinformation is that they have grown accustomed to seeing Russia in adversarial terms, thus making average citizens critical of pro-Kremlin narratives (Lanoszka 2019). In addition, the Baltic states have integrated their minority populations far better than is often assumed. Although many Russophones may still lack citizenship rights in Estonia and Latvia and so are more likely to experience political discrimination and economic hardship, they nevertheless retain key benefits associated with living in the European Union (Trimbach and O’Lear 2015). They may have sympathies for aspects of Russian foreign policy, but these sympathies do not translate into a preference to be reunited with Russia (Kallas 2016). Accordingly, Russia faces serious obstacles replicating what it did in Crimea. Russians living in Crimea were generally sympathetic to being part of Russkiy Mir (‘Russian World’), making them more willing to be the objects of an annexation effort (O’Loughlin, Toal, and Kolosov 2016, 761). Further, Russia does not have an existing military presence in the Baltic countries—as it did with the Black Sea Fleet stationed in Sevastopol—that it could leverage to achieve easy faits accomplis and dissuade potential challengers from organizing. In sum, NATO does not need to have a heavy footprint in the Baltic region to deter Russian aggression. Russia would have to overcome major operational challenges if it wished to undertake a successful conquest of the Baltic countries. Of course, none of this is to invite complacency about Baltic security. The Baltic states and Poland should deepen regional cooperation in order to ensure that no key policy diferences exist between them (Jermalavicius et al. 2018). They also face potential vulnerabilities at sea and so need to improve the resilience of their undersea and maritime infrastructure (Schaub et al. 2017). Still, the defensibility of the Baltic region helps illuminate why Russia resorts to disinformation campaigns, airspace incursions, vague nuclear threats, and other attempts at subversion. It cannot do much more lest it would provoke an unwanted response.

#### Hybrid war does not escalate—many checks

Sorensen & Nyemann, Royal Danish Defence College, scholars, ‘19

[Heine Sorensen and Dorthe Bach Nyemann, Senior Lecturers, Institute for Strategy, Royal Danish Defence College, “Deterrence by Punishment as a way of Countering Hybrid Threats – Why we need to go ‘beyond resilience’ in the gray zone,” Information Note, MCDC Countering Hybrid Warfare Project, 3—19, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/783151/20190304-MCDC_CHW_Information_note_-_Deterrence_by_Punishment.pdf>]

The Flipside of Deterrence by Punishment – the Fear of Escalation

**One of the** greatest reservation**s against communicating a willingness to take punitive actions concerns the risk of** escalation **and increased tension due to a more assertive** or offensive **posture. Yet when looking into possible responses – retaliation in cyberspace, for example – a number of** “self-dampening” mechanisms **appear to be** in place **that may be** applicable **to many types of responses**.30 **One example is the requirement to establish** some level of attribution of aggression on which to base a response. As discussed above, while attribution is rarely impossible, **it can be a time-consuming and technically-challenging endeavor. In a high-stakes scenario the** time **taken** to get attribution as right as possible **means there will be** plenty of time **to** think twice **about actions and consequences, and to** lean on diplomatic measures **in** parallel**. An example of a self-dampening mechanism related to the** cyber **domain is the** large investment **required to develop credible offensive capabilities. Moreover, an offensive cyber capability is a** transitory tool31. **The ability to access a computer system or network to cause harm or damage is** only temporary **and** dependent **on a** very rapid and ongoing patching **of vulnerabilities**. At the same time, wielding the cyber instrument despite the downside of “burning” the capacity might have a de-escalatory effect by communicating capability and credibility to the opponent with a view to discouraging future hostile attacks. **Targeting in any domain** – including cyberspace – **must also follow** relevant rules, law and due-process **which will** self-limit **the** range **of** targets **and** actions **available.**

**A final** “escalatory showstopper” **is related to the challenge of** identifying **and** developing targets **of adequate strategic significance –** not too much, not too little **– to achieve the desired effect. Responding to hybrid aggression by applying “middle range” punitive actions that are** proportionate **to the aggression threatened or suffered will also** self-limit **the escalatory potential. It is** unlikely **to be in the** interest **of** any **hybrid aggressor to pursue** a**n** escalatory spiral **above and beyond where they were looking to compete in the first place: on the hybrid level**. Nevertheless, one way to mitigate the risk of escalation – while enhancing civilian oversight and interagency coordination – would be to establish rules of engagement for punitive actions on the hybrid level32 . This would provide decision-makers with common guidelines to pursue punitive actions that fall below the “use of force threshold”. Moreover, this could actually bolster the credibility of punitive actions by signaling to hybrid aggressors the intent to take pre-prepared punitive actions when deemed necessary: in other words, a “playbook” for countering hybrid threats.

### Hybrid War Ans: Disinformation

#### The alternative is no news

Hurwitz ’17 [Justin Hurwitz, Assistnat Professor, Law, University of Nebraska, “Fake News Not-So-Real Antitrust Problem: Content Remains King,” Compeittion Policy International, 2017, <https://laweconcenter.org/wp-content/uploads/2018/01/CPI-Hurwitz.pdf>, accessed 10-5-21]

Nor are there vertical – or to use the antitrust newspeak, platform – concerns driving the problem of fake news. Facebook is a

platform-based distributor of information, including news. This means that news is (one of many) inputs into Facebook. Hubbard suggests

that Facebook’s gatekeeper position allows it to harm the traditional media in an effort to keep people on Facebook’s own site. She points,

in particular, to Facebook’s use of its proprietary in-app browser and Instant Articles feature, arguing that Facebook uses these to lock

users in to Facebook’s platform, denying third-party news sites valuable analytics and advertising revenue, and making it more difficult

for users to navigate away from Facebook.

As an initial matter, in-app browsers have become common. Facebook, Twitter, and Google News all use them. This suggests that

they have been implemented to address a technological problem – to make the mobile browsing experience better for users of each

platform. And, indeed, this is the case. Websites that have not been redesigned specifically for mobile platforms often do not work well.

Even websites that do have mobile versions often do not work particularly well. The user experience between those websites is often nonstandard, which inconveniences users and may encourage them to discontinue their use of both that website and the platform that sent

them there. By using an in-app browser – and especially by offering a standardized format for presenting news content across sites in that

browser – platforms can (at least in principle – I will not defend the quality of many in-app browsers, with the recognition that they are a

new and improving technology) offer users a superior experience. This means that they will make more use of a platform, yes, benefitting,

for instance, Facebook – but it also means that they will consume more content via that platform, benefitting, for instance, media outlets.

Importantly, mobile browsing, where we see these in-app browsers, is different from browsing in a desktop environment. When

a user is sent to a website for an article on a mobile device, they are unlikely to stay on that website once they are done with the article.

Rather, they are likely to exit out of the browser, which sends them back to whatever source sent them to the website initially. This means

that users are “locked in” to the Facebook platform no matter whether it uses an in-app or external browser.

Hubbard is exactly right that in-app browsers and Instant Articles are an effort to keep users engaged with the Facebook platform.

But the alternative is not users engaging more with news outlets’ platforms. The alternative is users getting frustrated with news outlets’ mobile experiences and finding more enjoyable ways to spend their time than waiting for poorly-rendered webpages to load. Facebook knows that if they can make articles quick and easy to access, more people will spend more time on their phones. This is why Facebook is willing to offer content providers a significant share of ad revenue. And, to the extent that publishers of any sort continue to produce content that Facebook users want to engage with, those publishers will continue to be able to demand such a share of revenue. Facebook has no incentive to deny its users access to content linked to via Facebook. To the contrary, it has every incentive to get them seamless access to that content, and is willing to pay to do so.

### Hybrid War Ans: Empirics

#### Empirics prove—Russia prefers keeping hybrid tactics at a low enough level to avoid escalation.

Ferris 18

(Research Fellow in the International Security Studies department at RUSI, specialising in Russia and Eurasia’s foreign policy. British IR think tank). Ferris, Emily. 2018. “Probing the Baltic States: Why Russia’s Ambitions Do Not Have a Security Dimension.” RUSI. November 21, 2018. <https://rusi.org/commentary/probing-baltic-states-why-russia%E2%80%99s-ambitions-do-not-have-security-dimension>. Accessed 2/9/19.

As a political and military reassurance, a recent NATO exercise in the Baltic region makes sense. But Russia’s real levers of influence over the Baltic states are not military, and NATO may not be the appropriate answer. On 7 November, NATO conducted military training drills with Poland which included, among others, relatively large contingents from the Baltic states of Estonia, Latvia and Lithuania. Anaconda 2018 was an exercise in political reassurance and an effort to test the Alliance’s emergency response and reinforcement procedures. However, it is not clear that military exercises of this kind reflect the real security needs of the Baltic states. While Baltic state leaders are apprehensive about Russia’s intent towards their countries, it is unlikely that Russia has serious territorial ambitions there. Russia certainly maintains a serious interest in gaining deeper involvement in political, intelligence and business processes in all three Baltic states, but it is not clear that this is a NATO issue that could be resolved by a military response. Military Engagement Unlikely Russia will not risk directly engaging with a NATO member, which would prompt a response from other member states. While it is one thing to militarily engage with a country like Ukraine that has never enjoyed NATO membership, it is quite another to test NATO’s mutual guarantee, underwritten by the US. Baltic state leaders have become increasingly concerned following Russia’s 2014 annexation of Crimea, which raised questions about changing borders in Europe. The Baltic states are particularly concerned by Russia’s military exercises, maintaining that they could be preparation for land invasions, but there is no evidence to suggest that this year’s Vostok exercises or last year’s Zapad training intended to take over Baltic territory. Russia has little desire to become embroiled in a conflict so close to its own borders, given its messy and expensive involvement in eastern Ukraine. Second and more importantly, Russia already exerts significant influence over the Baltic states, through its high penetration of the Baltics’ political and intelligence processes, as well as business networks. While Russia certainly has interests in probing the Baltic states’ capabilities, these are unlikely to take on an outright military dimension, such as an overt territorial aggression. Spheres of Influence Notwithstanding Russia’s unwillingness to engage militarily with the Baltics, Russia still considers these countries to be within its historic sphere of influence. The Russian authorities retain a strong interest in gathering intelligence on political and military processes there. Russia’s intelligence penetration of all three Baltic states is thought to be very high. Lithuania’s State Security Department published its National Threat Assessment in March, noting Russia’s active intelligence operations targeting Lithuania’s foreign and domestic policies, including attempts to influence the public in the run-up to the 2019 Lithuanian presidential elections. Estonia has also seen increasing Russian intelligence activity. There have been several high-profile spy swaps, and in September a senior Estonian army officer from the Ministry of Defence and his father were detained for spying on behalf of the Russian military intelligence (the GRU). Russia also allocates significant intelligence-gathering resources to assess the Baltic states’ military capabilities. All three Baltic states maintain that Russia works alongside Belarusian intelligence services to recruit informants, particularly from the Lithuanian military. The Baltics are also concerned by Russia’s military build-up in the exclave of Kaliningrad (near Lithuania), but the Russian authorities consider the Baltics’ cooperation with institutions such as NATO, including its consolidation of troops and hardware close to its borders, to be an aggressive act. Business as Usual? Russia also maintains significant influence in the Baltic business community, particularly in Latvia and Estonia. Despite Estonia’s strong anti-corruption stance, the beneficial owners of many businesses are thought to have close links to the Kremlin. Russian business interests still dominate the Latvian banking sector, which in the early 2000s became known as Russia’s ‘laundromat’ because of the banking system’s reputation for processing the proceeds of crime and corruption. In February 2018 allegations of widespread money laundering, funds of which were thought to originate in Russia, prompted the US Treasury Department to threaten to sanction one of Latvia’s largest banks, ABLV, which was eventually liquidated. All three Baltic states are attempting to reduce their reliance on gas and electricity from Russia and link to the EU power grid instead, but this is a long-term ambition that is unlikely to be fully operational before 2025. Lithuania has managed to reduce its reliance on Russian gas through its LNG port at Klaipėda and also imports gas from Norway – Russian state-controlled gas giant Gazprom has divested its shares in most of the Baltic gas companies. However, Gazprom still has a large stake in Latvias Gāze, Latvia’s state-controlled gas company, even though the gas market was officially liberalised in 2017. Russia has in the past used its control over gas and energy markets to pressure countries into political concessions, particularly Belarus, which remains a security concern for Latvia. Russian-Speaking Communities One of the most frequently discussed levers of Russian influence in the Baltics is through the significant Russian-speaking minorities in Estonia and Latvia – around a quarter of the population in Latvia. The Baltic states maintain that the Kremlin could influence this community by playing on their grievances, emphasising their political and economic marginalisation – many ethnic Russians do not have citizenship and are given ‘non-citizen’ status, preventing them from voting in national elections. As part of this, the Russian Duma (parliament) is in the process of passing a bill to simplify citizenship procedures for ethnic Russians living abroad. The bill will apply to countries that have ‘difficult’ political or economic situations such as an armed conflict (likely to refer to Ukraine), but also refers to the Baltic states, claiming that ethnic Russians’ rights are under threat there. While the bill is likely to be a measure to counter Russia’s demographic concerns by encouraging skilled migrants to return to Russia for work, it also indicates Russia’s ongoing attention to this community in the Baltics. However, these ethnic Russian communities are not a united movement seeking regime change in the Baltics. Aside from Russia’s ability to convey a narrative through the media, it is not clear that this translates into any cohesive action from the community that could have any security or fundamental political implications – pro-Russia demonstrations tend to be small and poorly attended. Moreover, despite Russian speakers’ grievances in Estonia and Latvia, as EU member states their standard of living remains higher than in Russia, and there is no widespread support for migration back into Russia. Ultimately, Russia has no desire to territorially expand into the Baltic states, but it does have several tools at its disposal to influence these states, which are likely to remain confined to the business and intelligence community. Notwithstanding their socio-political grievances, the Russian-speaking community in the Baltics does not presents a serious security threat to their own governments. While Russia often probes the Baltic states’ military and intelligence capabilities, this intelligence-gathering strategy is unlikely to escalate into open hostilities.

### Hybrid War Ans: Russia Cyber

#### They have zero interest in producing widespread damage

Lewis 18—(Senior Vice President at the Center for Strategic and International Studies, Ph.D. from the University of Chicago). Dr. James Andrew Lewis. January 2018, “Rethinking Cybersecurity: Strategy, Mass Effect, and States,” <https://tinyurl.com/y27xcqbb>, p. 7-11

Similarly, the popular idea that opponents use cyber techniques to inflict cumulative economic harm is not supported by evidence. Economic warfare has always been part of conflict, but there are no examples of a country seeking to imperceptibly harm the economy of an opponent. The United States engaged in economic warfare during the Cold War, and still uses sanctions as a tool of foreign power, but few if any other nations do the same. The intent of cyber espionage is to gain market or technological advantage. Coercive actions against government agencies or companies are intended to intimidate. Terrorists do not seek to inflict economic damage. The difficulty of wreaking real harm on large, interconnected economies is usually ignored. Economic warfare in cyberspace is ascribed to China, but China's cyber doctrine has three elements: control of cyberspace to preserve party rule and political stability, espionage (both commercial and military), and preparation for disruptive acts to damage an opponent's weapons, military information systems, and command and control. "Strategic" uses, such as striking civilian infrastructure in the opponent's homeland, appear to be a lower priority and are an adjunct to nuclear strikes as part of China's strategic deterrence. Chinese officials seem more concerned about accelerating China's growth rather than some long-term effort to undermine the American economy.6 The 2015 agreement with the United States served Chinese interests by centralizing tasking authority in Beijing and ending People's Liberation Army (PLA) "freelancing" against commercial targets. The Russians specialize in coercion, financial crime, and creating harmful cognitive effect—the ability to manipulate emotions and decisionmaking. Under their 2010 military doctrine on disruptive information operations (part of what they call "New Generation Warfare"). Russians want confusion, not physical damage. Iran and North Korea use cyber actions against American banks or entertainment companies like Sony or the Sands Casino, but their goal is political coercion, not destruction. None of these countries talk about death by 1000 cuts or attacking critical infrastructure to produce a cyber Pearl Harbor or any of the other scenarios that dominate the media. The few disruptive attacks on critical infrastructure have focused almost exclusively on the energy sector. Major financial institutions face a high degree of risk but in most cases, the attackers' intent is to extract money. There have been cases of service disruption and data erasure, but these have been limited in scope. Denial-of-service attacks against banks impede services and may be costly to the targeted bank, but do not have a major effect on the national economy. In all of these actions, there is a line that countries have been unwilling to cross. When our opponents decided to challenge American "hegemony," they developed strategies to circumvent the risks of retaliation or escalation by ensuring that their actions stayed below the use-of-force threshold—an imprecise threshold, roughly defined by international law, but usually considered to involve actions that produce destruction or casualties. Almost all cyber attacks fall below this threshold, including, crime, espionage, and politically coercive acts. This explains why the decades-long quest to rebuild Cold War deterrence in cyberspace has been fruitless. It also explains why we have not seen the dreaded cyber Pearl Harbor or other predicted catastrophes. Opponents are keenly aware that launching catastrophe brings with it immense risk of receiving catastrophe in return. States are the only actors who can carry out catastrophic cyber attacks and they are very unlikely to do so in a strategic environment that seeks to gain advantage without engaging in armed conflict. Decisions on targets and attack make sense only when embedded in their larger strategic calculations regarding how best to fight with the United States. There have been thousands of incidents of cybercrime and cyber espionage, but only a handful of true attacks, where the intent was not to extract information or money, but to disrupt and, in a few cases, destroy. From these incidents, we can extract a more accurate picture of risk. The salient incidents are the cyber operations against Iran's nuclear weapons facility (Stuxnet), Iran's actions against Aramco and leading American banks, North Korean interference with Sony and with South Korean banks and television stations, and Russian actions against Estonia, Ukrainian power facilities, Canal 5 (television network in France), and the 2016 U S. presidential elections. Cyber attacks are not random. All of these incidents have been part of larger geopolitical conflicts involving Iran, Korea, and the Ukraine, or Russia's contest with the United States and NATO. There are commonalities in each attack. All were undertaken by state actors or proxy forces to achieve the attacking state's policy objectives. Only two caused tangible damage; the rest created coercive effect, intended to create confusion and psychological pressure through fear, uncertainty, and embarrassment. In no instance were there deaths or casualties. In two decades of cyber attacks, there has never been a single casualty. This alone should give pause to the doomsayers. Nor has there been widespread collateral damage.

### Hybrid War Ans: Status Quo Solves

#### NATO is bolstering deterrence and ability to combat hybrid threats now

King, CSIS fellow, ‘19

[Iain King, Visting Fellow, Center for Strategic and International Studies, “NATO Is Not Brain Dead Yet,” THE HILL, 11—12—19, <https://thehill.com/opinion/international/470060-nato-is-not-brain-dead-yet/>]

It is true that Europe has witnessed some very bad defensive decisions in the past. A few military planners in the 1930s expected cavalry to have a combat role in the coming war. Others assumed that bomber aircraft would be decisive. Too much faith was placed in the Maginot Line, the robust concrete wall which defended against German tanks, until the panzers simply went around it. European defense is still vulnerable to strategic shocks today, and some of these have exposed flaws in earlier calculations by NATO. Take the Russian annexation of Crimea or the ongoing Russian use of hybrid attacks to destabilize neighbors and adversaries, including cybersecurity attacks and political meddling.

But like any credible military outfit, NATO has been industrious in its efforts to learn from these episodes and correct for the vulnerabilities they uncovered. Following Crimea, for example, NATO has made sure it can mobilize a well-equipped force swiftly, ready to meet and match any Russian forces trying to enter the Baltic states. NATO exercises have adapted to make hybrid attacks center stage, forcing military minds to think through their response to a complicated challenge. NATO has also been working hard to counter Russian efforts to spread lies online.

### Liberal Order Ans: 1NC

#### Claims about the liberal order are false

Staniland, Chicago professor, ‘18

[Paul Stnailand, Asosciate Professor, Political Seicne, University of Chicago, “Misreading the ‘Liberal Order’: Why We Need New Thinking in American Foreign Policy, LAWFARE, 7—29—18, <https://www.lawfareblog.com/misreading-liberal-order-why-we-need-new-thinking-american-foreign-policy>]

Pushing back against Trump’s foreign policy is an important goal. But moving forward requires a more serious analysis than claiming that the “liberal international order” was the centerpiece of past U.S. foreign-policy successes, and thus should be again. Both claims are flawed. We need to understand the limits of the liberal international order, where it previously failed to deliver benefits, and why it offers little guidance for many contemporary questions.

First, advocates of the order tend to skim past the policies pursued under the liberal order that have not worked. These mistakes need to be directly confronted to do better in the future.

Proponents of the order, however, often present a narrow and highly selective reading of history that ignores much of the coercion, violence, and instability that accompanied post-war history. Problematic outcomes are treated as either aberrant exceptions or as not truly characterizing the order. One recent defense of the liberal order by prominent liberal institutionalists Daniel Deudney and G. John Ikenberry, for instance, does not mention Iraq, Afghanistan, Vietnam, or Libya. Professors Stephen Chaudoin, Helen Milner, and Dustin Tingley herald the order’s “support for freedom, democracy, human rights, a free press.” Kori Schake writes that Western democracies’ wars are “about enlarging the perimeter of security and prosperity, expanding and consolidating the liberal order.” Historian Hal Brands argues that the order has advocated “political liberalism in the form of representative government and human rights; and other liberal concepts, such as nonaggression, self-determination, and the peaceful settlement of disputes.”

Other analysts have persuasively argued that these accounts create an “imagined” picture of post-World War II history. Patrick Porter outlines in detail how coercive, violent, and hypocritical U.S. foreign policy has often been. To the extent an international liberal order ever actually existed beyond a small cluster of countries, writes Nick Danforth, it was recent and short-lived. Thomas Meaney and Stephen Wertheim further argue that “critics exaggerate Mr. Trump’s abnormality,” situating him within a long history of the pursuit of American self-interest. Graham Allison—no bomb-throwing radical—has recently written that the order was a “myth” and that credit for the lack of great power war should instead go to nuclear deterrence. Coercion and disregard for both allies and political liberalism have been entirely compatible with the “liberal” order.

The last two decades have been a bumpy ride for U.S. foreign policy. Since 9/11, we have seen the disintegration of Syria, Yemen, and Libya, a war without end in Afghanistan, the collapse of the Arab Spring, the rise and resurgence of the Islamic State, and the distinctly mixed success of strategies aimed at managing China’s rise. At home, the growth of a national-security state has placed remarkable power in the hands of Donald Trump. Simply returning to the old order is no guarantee of good results. Grappling openly with failure and self-inflicted wounds—while also acknowledging clear benefits of the order—is essential for moving beyond self-congratulatory platitudes.

### Liberal Order Ans: 2NC

#### No authoritarianism impact—pushback now solves

Leong ’19 [Clarence Leong, journalist, “In an Age of Authoritarianism, the World Sees Glimmers of Hope,” CHRISTIAN SCIENCE MONITOR, 3—19—19, <https://www.csmonitor.com/World/Points-of-Progress/2019/0319/In-an-age-of-authoritarianism-the-world-sees-glimmers-of-hope>, accessed 9-21-21]

In the past year, citizens of Hungary, Poland, the Czech Republic, and Ethiopia have taken to the streets to demand accountability from their governments, while voters in Malaysia and the Maldives ousted corrupt governments at the ballot box. Countries with a strong civil society or decent-sized middle class continue to push back against autocrats, even though the headlines are more often about the threats to democracy.

That’s not to say democracy has nothing to worry about. A new paper published this month found that the world has been in “a wave of autocratization” since 1994, and as many as 75 democracies have seen a reversal to autocracy. Modern-day autocrats know better than to blatantly shore up power, but do so gradually and under a legal facade, making it harder to detect, researchers say. Autocrats pit authoritarianism against democracy, promoting it as a more efficient form of governance and spreading the technology that strengthens control. Social media amplifies the spread of misinformation, clouding voters’ judgment.

Global freedom, which is composed of political rights and civil liberties, has been in decline for the 13th year in a row, according to a new report from Freedom House. But the same report also notes significant improvement in accountability for corruption in Angola, Armenia, and other nations. Political participation in most parts of the world has seen a continuous upward trend, reports The Economist. And while autocrats threaten democracies, they are also “fueling a powerful counterattack,” Human Rights Watch notes in its latest annual report.

“Those who are bemoaning this authoritarian turn in the world were overstating the case,” says Steven Levitsky, a political scientist at Harvard and co-author of “How Democracies Die.” The euphoric expansion of democracy in the 1990s led to the over-optimistic belief that authoritarianism was a thing of the past, and now that expectation has been dashed, he says. But “there’s yet to emerge a real, viable, truly legitimate alternative to democracy in the world.”

That doesn’t discount the fact that people are disillusioned with traditional political parties and losing confidence in democracy. But rather than disengaging from it, that dissatisfaction is driving citizens to participate in political processes, according to The Economist. Voter turnout and membership of political parties rose, reversing a downward trend. A larger proportion of the world’s population is now willing to engage in lawful demonstrations. The Economist also notes a particularly striking area of progress coming from female participation in politics.

“Women have become much more active, not just in [the] U.S. but around the world,” says Steven Leslie, lead analyst at The Economist Intelligence Unit. “There is an ongoing surge of female participation in politics and in activities that are essential to democracy.” Barriers like discriminatory laws and socioeconomic obstacles are gradually being removed. In Rwanda and Ethiopia, half of the cabinet ministers are women. New legislation in Japan encourages gender parity in parliament. In the United States, the voters in the November midterms elected the highest number of women to Congress in history – though they still make up only 23.7 percent.

Still, the international atmosphere has become less favorable to the expansion of democracy. Not only is the totalitarian state of China spreading its influence, but cracks are appearing in decades-old alliances such as the European Union and NATO. In the EU, both Italy and Turkey saw their rankings in The Economist’s democracy index fall by at least 10 places. Meanwhile, on the other side of the Atlantic, the U.S. is becoming more isolationist, analysts say.

“America’s commitment to the global progress of democracy in its foreign policy has been seriously compromised,” says Sarah Repucci, senior director for research and analysis at Freedom House.

In one example, when the U.S. withdrew from the council on human rights at the United Nations, it left “a huge vacuum of power,” says Rosa Freedman, a professor of law, conflict, and global development at the University of Reading in England and author of several books on the U.N.

Despite the downward trends, however, countries are forming new alliances to put pressure on repressive regimes, reports Human Rights Watch. It points to the example of the EU and a group of Muslim-majority countries working together to create a mechanism at the U.N. to collect evidence on the ethnic cleansing of Rohingyas, which could be used in future trials of the Myanmar government. A group of Latin American countries led a resolution in the Human Rights Council to condemn the severe persecution of Venezuelans under President Nicolás Maduro.

Other human rights mechanisms have sprung up in unexpected places, adds Joseph Saunders, deputy program director at Human Rights Watch. For example, the organizing bodies of big sports tournaments, such as the World Cup and the Olympics, will scrutinize the bidders and hosts’ human rights records.

“These are obviously dark times,” says Mr. Saunders. “But [you] miss a large part of the picture if you don’t see the pushback that is also happening.”

#### There are too many other causes

Newton ’18 [Casey Newton, staff, “Internet Freedom Continues to Decline Around the World, a New Report Says,” THE VERGE, 11—1—18, <https://www.theverge.com/2018/11/1/18050394/internet-freedom-report-2018-freedom-house-chertoff>, accessed 11-2-21]

Digital authoritarianism is on the rise, according to a new report from a group that monitors internet freedoms. Freedom House, a pro-democracy think tank, said today that governments are seeking more control over users’ data while also using laws nominally intended to address “fake news” to suppress dissent. It marked the eighth consecutive year that Freedom House found a decline in online freedoms around the world.

“The clear emergent theme in this report is the growing recognition that the internet, once seen as a liberating technology, is increasingly being used to disrupt democracies as opposed to destabilizing dictatorships,” said Mike Abramowitz, president of Freedom House, in a call with reporters. “Propaganda and disinformation are increasingly poisoning the digital sphere, and authoritarians and populists are using the fight against fake news as a pretext to jail prominent journalists and social media critics, often through laws that criminalize the spread of false information.”

In the United States, internet freedom declined in 2018 due to the Federal Communications Commission’s repeal of net neutrality rules. Other countries fared much worse — 17 out of 65 surveyed had adopted laws restricting online media. Of those, 13 prosecuted citizens for allegedly spreading false information. And more countries are accepting training and technology from China, which Freedom House describes as an effort to export a system of censorship and surveillance around the world.

Of course, there are tradeoffs between freedom and security. The report is critical of Sri Lanka and India, which have periodically shut down or limited access to the internet in response to the outbreak of ethnic and religious conflict. In both cases, citizens were being murdered by mobs that had encountered misinformation spread through social media.

“Cutting off internet service is a draconian response, particularly at a time when citizens may need it the most, whether to dispel rumors, check in with loved ones, or avoid dangerous areas,” said Adrian Shahbaz, research director for technology and democracy. “While deliberately falsified content is a genuine problem, some governments are increasingly using ‘fake news’ as a pretense to consolidate their control over information and suppress dissent.”

The report also found:

\* Governments in 18 countries increased state surveillance between June 2017 and now, with 15 considering new “data protection” laws, which can require companies to store user data locally and potentially make it easier for governments to access.

\* Governments in 32 countries used paid commentators, bots, and trolls in an effort to manipulate online conversations. WhatsApp and other closed messaging apps are becoming more popular targets for manipulation, the authors write.

\* There were bright spots. The authors credit Armenian citizens’ use of social media, communications apps, and live-streaming services for making possible a peaceful revolution earlier this year. And in Ethiopia, a new prime minster released bloggers and activists from prison and pledged to ease restrictions on online communication.

### Liberal Order Ans: Doomed

#### GLO doomed

Mead ’21 [Walter Russell Mead, Professor, Foreign Affairs and Humanities, Bard College, “The End of the Wilsonian Era: Why Lilberal Internationalism Faled,” FOREIGN AFFAIRS, January / February 2021, Ebsco]

This task was complicated by the Cold War, but "the free world" (as Americans then called the noncommunist countries) continued to develop along Wilsonian lines. Inevitable compromises, such as U.S. support for ruthless dictators and military rulers in many parts of the world, were seen as regrettable necessities imposed by the need to fight the much greater evil of Soviet communism. When the Berlin Wall fell, in 1989, it seemed that the opportunity for a Wilsonian world order had finally come. The former Soviet empire could be reconstructed along Wilsonian lines, and the West could embrace Wilsonian principles more consistently now that the Soviet threat had disappeared. Self-determination, the rule of law between and within countries, liberal economics, and the protection of human rights: the "new world order" that both the George H. W. Bush and the Clinton administrations worked to create was very much in the Wilsonian mold.

Today, however, the most important fact in world politics is that this noble effort has failed. The next stage in world history will not unfold along Wilsonian lines. The nations of the earth will continue to seek some kind of political order, because they must. And human rights activists and others will continue to work toward their goals. But the dream of a universal order, grounded in law, that secures peace between countries and democracy inside them will figure less and less in the work of world leaders.

To state this truth is not to welcome it. There are many advantages to a Wilsonian world order, even when that order is partial and incomplete. Many analysts, some associated with the presidential campaign of former U.S. Vice President Joe Biden, think they can put Humpty Dumpty together again. One wishes them every success. But the centrifugal forces tearing at the Wilsonian order are so deeply rooted in the nature of the contemporary world that not even the end of the Trump era can revive the Wilsonian project in its most ambitious form. Although Wilsonian ideals will not disappear and there will be a continuing influence of Wilsonian thought on U.S. foreign policies, the halcyon days of the post-Cold War era, when American presidents organized their foreign policies around the principles of liberal internationalism, are unlikely to return anytime soon.

THE ORDER OF THINGS

Wilsonianism is only one version of a rules-based world order among many. The Westphalian system, which emerged in Europe after the Thirty Years' War ended in 1648, and the Congress system, which arose in the wake of the Napoleonic Wars of the early nineteenth century, were both rules-based and even law-based; some of the foundational ideas of international law date from those eras. And the Holy Roman Empire--a transnational collection of territories that stretched from France into modern-day Poland and from Hamburg to Milan-- was an international system that foreshadowed the European Union, with highly complex rules governing everything from trade to sovereign inheritance among princely houses.

As for human rights, by the early twentieth century, the pre-Wilsonian European system had been moving for a century in the direction of putting egregious violations of human rights onto the international agenda. Then, as now, it was chiefly weak countries whose oppressive behavior attracted the most attention. The genocidal murder of Ottoman Christian minorities at the hands of Ottoman troops and irregular forces in the late nineteenth and early twentieth centuries received substantially more attention than atrocities carried out around the same time by Russian forces against rebellious Muslim peoples in the Caucasus. No delegation of European powers came to Washington to discuss the treatment of Native Americans or to make representations concerning the status of African Americans. Nevertheless, the pre-Wilsonian European order had moved significantly in the direction of elevating human rights to the level of diplomacy.

Wilson, therefore, was not introducing the ideas of world order and human rights to a collection of previously anarchic states and unenlightened polities. Rather, his quest was to reform an existing international order whose defects had been conclusively demonstrated by the horrors of World War I. In the pre-Wilsonian order, established dynastic rulers were generally regarded as legitimate, and interventions such as the 1849 Russian invasion of Hungary, which restored Habsburg rule, were considered lawful. Except in the most glaring instances, states were more or less free to treat their citizens or subjects as they wished, and although governments were expected to observe the accepted principles of public international law, no supranational body was charged with the enforcement of these standards. The preservation of the balance of power was invoked as a goal to guide states; war, although regrettable, was seen as a legitimate element of the system. From Wilson's standpoint, these were fatal flaws that made future conflagrations inevitable. To redress them, he sought to build an order in which states would accept enforceable legal restrictions on their behavior at home and their international conduct.

That never quite materialized, but until recent years, the U.S.-led postwar order resembled Wilson's vision in important respects. And, it should be noted, that vision is not equally dead everywhere. Although Wilson was an American, his view of world order was first and foremost developed as a method for managing international politics in Europe, and it is in Europe where Wilson's ideas have had their greatest success and where their prospects continue to look strongest. His ideas were treated with bitter and cynical contempt by most European statesmen when he first proposed them, but they later became the fundamental basis of the European order, enshrined in the laws and practices of the EU. Arguably, no ruler since Charlemagne has made as deep an impression on the European political order as the much-mocked Presbyterian from the Shenandoah Valley.

THE ARC OF HISTORY

Beyond Europe, the prospects for the Wilsonian order are bleak. The reasons behind its demise, however, are different from what many assume. Critics of the Wilsonian approach to foreign affairs often decry what they see as its idealism. In fact, as Wilson demonstrated during the negotiations over the Treaty of Versailles, he was perfectly capable of the most cynical realpolitik when it suited him. The real problem of Wilsonianism is not a naive faith in good intentions but a simplistic view of the historical process, especially when it comes to the impact of technological progress on human social order. Wilson's problem was not that he was a prig but that he was a Whig.

Like early-twentieth-century progressives generally and many American intellectuals to this day, Wilson was a liberal determinist of the Anglo-Saxon school; he shared the optimism of what the scholar Herbert Butterfield called "the Whig historians," the Victorian-era British thinkers who saw human history as a narrative of inexorable progress and betterment. Wilson believed that the so-called ordered liberty that characterized the Anglo-American countries had opened a path to permanent prosperity and peace. This belief represents a sort of Anglo-Saxon Hegelianism and holds that the mix of free markets, free government, and the rule of law that developed in the United Kingdom and the United States is inevitably transforming the rest of the world--and that as this process continues, the world will slowly and for the most part voluntarily converge on the values that made the Anglo-Saxon world as wealthy, attractive, and free as it has become.

Wilson was the devout son of a minister, deeply steeped in Calvinist teachings about predestination and the utter sovereignty of God, and he believed that the arc of progress was fated. The future would fulfill biblical prophecies of a coming millennium: a thousand-year reign of peace and prosperity before the final consummation of human existence, when a returning Christ would unite heaven and earth. (Today's Wilsonians have given this determinism a secular twist: in their eyes, liberalism will rule the future and bring humanity to "the end of history" as a result of human nature rather than divine purpose.)

Wilson believed that the defeat of imperial Germany in World War I and the collapse of the Austro-Hungarian, Russian, and Ottoman empires meant that the hour of a universal League of Nations had finally arrived. In 1945, American leaders ranging from Eleanor Roosevelt and Henry Wallace on the left to Wendell Willkie and Thomas Dewey on the right would interpret the fall of Germany and Japan in much the same way. In the early 1990s, leading U.S. foreign policymakers and commentators saw the fall of the Soviet Union through the same deterministic prism: as a signal that the time had come for a truly global and truly liberal world order. On all three occasions, Wilsonian order builders seemed to be in sight of their goal. But each time, like Ulysses, they were blown off course by contrary winds.

TECHNICAL DIFFICULTIES

Today, those winds are gaining strength. Anyone hoping to reinvigorate the flagging Wilsonian project must contend with a number of obstacles. The most obvious is the return of ideology-fueled geopolitics. China, Russia, and a number of smaller powers aligned with them--Iran, for example--correctly see Wilsonian ideals as a deadly threat to their domestic arrangements. Earlier in the post-Cold War period, U.S. primacy was so thorough that those countries attempted to downplay or disguise their opposition to the prevailing pro-democracy consensus. Beginning in U.S. President Barack Obama's second term, however, and continuing through the Trump era, they have become less inhibited. Seeing Wilsonianism as a cover for American and, to some degree, EU ambitions, Beijing and Moscow have grown increasingly bold about contesting Wilsonian ideas and initiatives inside international institutions such as the un and on the ground in places from Syria to the South China Sea.

These powers' opposition to the Wilsonian order is corrosive in several ways. It raises the risks and costs for Wilsonian powers to intervene in conflicts beyond their own borders. Consider, for example, how Iranian and Russian support for the Assad regime in Syria has helped prevent the United States and European countries from getting more directly involved in that country's civil war. The presence of great powers in the anti-Wilsonian coalition also provides shelter and assistance to smaller powers that otherwise might not choose to resist the status quo. Finally, the membership of countries such as China and Russia in international institutions makes it more difficult for those institutions to operate in support of Wilsonian norms: take, for example, Chinese and Russian vetoes in the un Security Council, the election of anti-Wilsonian representatives to various un bodies, and the opposition by countries such as Hungary and Poland to EU measures intended to promote the rule of law.

Meanwhile, the torrent of technological innovation and change known as "the information revolution" creates obstacles for Wilsonian goals within countries and in the international system. The irony is that Wilsonians often believe that technological progress will make the world more governable and politics more rational-- even if it also adds to the danger of war by making it so much more destructive. Wilson himself believed just that, as did the postwar order builders and the liberals who sought to extend the U.S.-led order after the Cold War. Each time, however, this faith in technological change was misplaced. As seen most recently with the rise of the Internet, although new technologies often contribute to the spread of liberal ideas and practices, they can also undermine democratic systems and aid authoritarian regimes.

Today, as new technologies disrupt entire industries, and as social media upends the news media and election campaigning, politics is becoming more turbulent and polarized in many countries. That makes the victory of populist and antiestablishment candidates from both the left and the right more likely in many places. It also makes it harder for national leaders to pursue the compromises that international cooperation inevitably requires and increases the chances that incoming governments will refuse to be bound by the acts of their predecessors.

The information revolution is destabilizing international life in other ways that make it harder for rules-based international institutions to cope. Take, for example, the issue of arms control, a central concern of Wilsonian foreign policy since World War I and one that grew even more important following the development of nuclear weapons. Wilsonians prioritize arms control not just because nuclear warfare could destroy the human race but also because, even if unused, nuclear weapons or their equivalent put the Wilsonian dream of a completely rules-based, law-bound international order out of reach. Weapons of mass destruction guarantee exactly the kind of state sovereignty that Wilsonians think is incompatible with humanity's long-term security. One cannot easily stage a humanitarian intervention against a nuclear power.

The fight against proliferation has had its successes, and the spread of nuclear weapons has been delayed--but it has not stopped, and the fight is getting harder over time. In the 1940s, it took the world's richest nation and a consortium of leading scientists to assemble the first nuclear weapon. Today, second- and third-rate scientific establishments in low-income countries can manage the feat. That does not mean that the fight against proliferation should be abandoned. It is merely a reminder that not all diseases have cures.

What is more, the technological progress that underlies the information revolution significantly exacerbates the problem of arms control. The development of cyberweapons and the potential of biological agents to inflict strategic damage on adversaries--graphically demonstrated by the COVID-19 pandemic--serve as warnings that new tools of warfare will be significantly more difficult to monitor or control than nuclear technology. Effective arms control in these fields may well not be possible. The science is changing too quickly, the research behind them is too hard to detect, and too many of the key technologies cannot be banned outright because they also have beneficial civilian applications.

In addition, economic incentives that did not exist in the Cold War are now pushing arms races in new fields. Nuclear weapons and long-range missile technology were extremely expensive and brought few benefits to the civilian economy. Biological and technological research, by contrast, are critical for any country or company that hopes to remain competitive in the twenty-first century. An uncontrollable, multipolar arms race across a range of cutting-edge technologies is on the horizon, and it will undercut hopes for a revived Wilsonian order.

IT'S NOT FOR EVERYBODY

One of the central assumptions behind the quest for a Wilsonian order is the belief that as countries develop, they become more similar to already developed countries and will eventually converge on the liberal capitalist model that shapes North America and western Europe. The Wilsonian project requires a high degree of convergence to succeed; the member states of a Wilsonian order must be democratic, and they must be willing and able to conduct their international relations within liberal multilateral institutions.

At least for the medium term, the belief in convergence can no longer be sustained. Today, China, India, Russia, and Turkey all seem less likely to converge on liberal democracy than they did in 1990. These countries and many others have developed economically and technologically not in order to become more like the West but rather to achieve a deeper independence from the West and to pursue civilizational and political goals of their own.

In truth, Wilsonianism is a particularly European solution to a particularly European set of problems. Since the fall of the Roman Empire, Europe has been divided into peer and near-peer competitors. War was the constant condition of Europe for much of its history, and Europe's global dominance in the nineteenth century and early twentieth century can be attributed in no small part to the long contest for supremacy between France and the United Kingdom, which promoted developments in finance, state organization, industrial techniques, and the art of war that made European states fierce and ferocious competitors.

With the specter of great-power war constantly hanging over them, European states developed a more intricate system of diplomacy and international politics than did countries in other parts of the world. Well-developed international institutions and doctrines of legitimacy existed in Europe well before Wilson sailed across the Atlantic to pitch the League of Nations, which was in essence an upgraded version of preexisting European forms of international governance. Although it would take another devastating world war to ensure that Germany, as well as its Western neighbors, would adhere to the rules of a new system, Europe was already prepared for the establishment of a Wilsonian order.

But Europe's experience has not been the global norm. Although China has been periodically invaded by nomads, and there were periods in its history when several independent Chinese states struggled for power, China has been a single entity for most of its history. The idea of a single legitimate state with no true international peers is as deeply embedded in the political culture of China as the idea of a multistate system grounded in mutual recognition is embedded in that of Europe. There have been clashes among Chinese, Japanese, and Koreans, but until the late nineteenth century, interstate conflict was rare.

In human history as a whole, enduring civilizational states seem more typical than the European pattern of rivalry among peer states. Early modern India was dominated by the Mughal Empire. Between the sixteenth century and the nineteenth century, the Ottoman and Persian Empires dominated what is now known as the Middle East. And the Incas and the Aztecs knew no true rivals in their regions. War seems universal or nearly so among human cultures, but the European pattern, in which an escalating cycle of war forced a mobilization and the development of technological, political, and bureaucratic resources to ensure the survival of the state, does not seem to have characterized international life in the rest of the world.

For states and peoples in much of the world, the problem of modern history that needed to be solved was not the recurrence of great-power conflict. The problem, instead, was figuring out how to drive European powers away, which involved a wrenching cultural and economic adjustment in order to harness natural and industrial resources. Europe's internecine quarrels struck non-Europeans not as an existential civilizational challenge to be solved but as a welcome opportunity to achieve independence.

Postcolonial and non-Western states often joined international institutions as a way to recover and enhance their sovereignty, not to surrender it, and their chief interest in international law was to protect weak states from strong ones, not to limit the power of national leaders to consolidate their authority. Unlike their European counterparts, these states did not have formative political experiences of tyrannical regimes suppressing dissent and drafting helpless populations into the service of colonial conquest. Their experiences, instead, involved a humiliating consciousness of the inability of local authorities and elites to protect their subjects and citizens from the arrogant actions and decrees of foreign powers. After colonialism formally ended and nascent countries began to assert control over their new territories, the classic problems of governance in the postcolonial world remained weak states and compromised sovereignty.

Even within Europe, differences in historical experiences help explain varying levels of commitment to Wilsonian ideals. Countries such as France, Germany, Italy, and the Netherlands came to the EU understanding that they could meet their basic national goals only by pooling their sovereignty. For many former Warsaw Pact members, however, the motive for joining Western clubs such as the EU and NATO was to regain their lost sovereignty. They did not share the feelings of guilt and remorse over the colonial past--and, in Germany, over the Holocaust--that led many in western Europe to embrace the idea of a new approach to international affairs, and they felt no qualms about taking full advantage of the privileges of EU and NATO membership without feeling in any way bound by those organizations' stated tenets, which many regarded as hypocritical boilerplate.

EXPERT TEXPERT

The recent rise of populist movements across the West has revealed another danger to the Wilsonian project. If the United States could elect Donald Trump as president in 2016, what might it do in the future? What might the electorates in other important countries do? And if the Wilsonian order has become so controversial in the West, what are its prospects in the rest of the world?

Wilson lived in an era when democratic governance faced problems that many feared were insurmountable. The Industrial Revolution had divided American society, creating unprecedented levels of inequality. Titanic corporations and trusts had acquired immense political power and were quite selfishly exploiting that power to resist all challenges to their economic interests. At that time, the richest man in the United States, John D. Rockefeller, had a fortune greater than the annual budget of the federal government. By contrast, in 2020, the wealthiest American, Jeff Bezos, had a net worth equal to about three percent of budgeted federal expenditures.

Yet from the standpoint of Wilson and his fellow progressives, the solution to these problems could not be simply to vest power in the voters. At the time, most Americans still had an eighth-grade education or less, and a wave of migration from Europe had filled the country's burgeoning cities with millions of voters who could not speak English, were often illiterate, and routinely voted for corrupt urban machine politicians.

The progressives' answer to this problem was to support the creation of an apolitical expert class of managers and administrators. The progressives sought to build an administrative state that would curb the excessive power of the rich and redress the moral and political deficiencies of the poor. (Prohibition was an important part of Wilson's electoral program, and during World War I and afterward, he moved aggressively to arrest and in some cases deport socialists and other radicals.) Through measures such as improved education, strict limits on immigration, and eugenic birth-control policies, the progressives hoped to create better-educated and more responsible voters who would reliably support the technocratic state.

A century later, elements of this progressive thinking remain critical to Wilsonian governance in the United States and elsewhere, but public support is less readily forthcoming than in the past. The Internet and social media have undermined respect for all forms of expertise. Ordinary citizens today are significantly better educated and feel less need to rely on expert guidance. And events including the U.S. invasion of Iraq in 2003, the 2008 financial crisis, and the inept government responses during the 2020 pandemic have seriously reduced confidence in experts and technocrats, whom many people have come to see as forming a nefarious "deep state."

International institutions face an even greater crisis of confidence. Voters skeptical of the value of technocratic rule by fellow citizens are even more skeptical of foreign technocrats with suspiciously cosmopolitan views. Just as the inhabitants of European colonial territories preferred home rule (even when badly administered) to rule by colonial civil servants (even when competent), many people in the West and in the postcolonial world are likely to reject even the best-intentioned plans of global institutions.

Meanwhile, in developed countries, problems such as the loss of manufacturing jobs, the stagnation or decline of wages, persistent poverty among minority groups, and the opioid epidemic have resisted technocratic solutions. And when it comes to international challenges such as climate change and mass migration, there is little evidence that the cumbersome institutions of global governance and the quarrelsome countries that run them will produce the kind of cheap, elegant solutions that could inspire public trust.

WHAT IT MEANS FOR BIDEN

For all these reasons, the movement away from the Wilsonian order is likely to continue, and world politics will increasingly be carried out along non-Wilsonian and in some cases even anti-Wilsonian lines. Institutions such as NATO, the un, and the World Trade Organization may well survive (bureaucratic tenacity should never be discounted), but they will be less able and perhaps less willing to fulfill even their original purposes, much less take on new challenges. Meanwhile, the international order will increasingly be shaped by states that are on diverging paths. This does not mean an inevitable future of civilizational clashes, but it does mean that global institutions will have to accommodate a much wider range of views and values than they have in the past.

There is hope that many of the gains of the Wilsonian order can be preserved and perhaps in a few areas even extended. But fixating on past glories will not help develop the ideas and policies needed in an increasingly dangerous time. Non-Wilsonian orders have existed both in Europe and in other parts of the world in the past, and the nations of the world will likely need to draw on these examples as they seek to cobble together some kind of framework for stability and, if possible, peace under contemporary conditions.

For U.S. policymakers, the developing crisis of the Wilsonian order worldwide presents vexing problems that are likely to preoccupy presidential administrations for decades to come. One problem is that many career officials and powerful voices in Congress, civil society organizations, and the press deeply believe not only that a Wilsonian foreign policy is a good and useful thing for the United States but also that it is the only path to peace and security and even to the survival of civilization and humanity. They will continue to fight for their cause, conducting trench warfare inside the bureaucracy and employing congressional oversight powers and steady leaks to sympathetic press outlets to keep the flame alive.

Those factions will be hemmed in by the fact that any internationalist coalition in American foreign policy must rely to a significant degree on Wilsonian voters. But a generation of overreach and poor political judgment has significantly reduced the credibility of Wilsonian ideas among the American electorate. Neither President George W. Bush's nation-building disaster in Iraq nor Obama's humanitarian-intervention fiasco in Libya struck most Americans as successful, and there is little public enthusiasm for democracy building abroad.

# Case Answers: China

### China Ans: Rise—1NC

#### Multiple internal factors limit China’s rise—will distract leadership, stagnation is more likely

Mueller, Ohio State Adjunct Professor, ‘21

[John Mueller, Adjunct Professor, Political Science, Ohio State University and Senior Fellow, Cato Institute, “China: Rise or Demise?” POLICY ANALYSIS n. 917, 5—18—21, <https://www.cato.org/policy-analysis/china-rise-or-demise>, accessed 6-12-22]

Concerns about the security implications of China’s rise are not particularly justified. Moreover, China faces many problems. As Freeman puts it, “China has its hands full.” Among the problems: “environmental devastation, slowing growth, a rapidly aging population and shrinking labor force, enormous levels of industrial overproduction, accumulating local debt, a still‐​inadequate social safety network, and an increasingly oppressive political system.… It has an unfinished civil war with Taiwan and uneasy relations with fifty‐​five ethnic minority groups—8½ percent of its population—at least two of which are in a near state of rebellion.”79

Although China might eventually be able to handle these and other problems, they will arrest the attention of its leaders for a long time. And, in total, they might be taken to suggest that descent or at least prolonged stagnation might come about, rather than a continued rise.

### China Ans: Rise—2NC

#### No China rise—economically and strategically impossible.

Carey 20

(CEO and founder of the Lexington Institute, from 1990-1993, Carey was Executive Vice President of the international economic advisory firm Johnson Smick International, also served from 1989 through 1996 as an Intelligence Officer in the United States Naval Reserve and was a mobilized reservist for Operations Desert Shield and Desert Storm (to Navy Headquarters, Europe), as well as an Air Intelligence Officer in 1996, has lectured at the Naval War College, Marine Corps University, and George Washington University). Merrick Carey. “Has China's Rise Peaked?” RealClearDefense, July 13, 2020, <https://www.realcleardefense.com/articles/2020/07/13/has_chinas_rise_peaked_115460.html>.

Even though the Western mainstream view is that China is a military and economic dynamo that is quickly leaving America behind, the world may be turning against the Middle Kingdom, and Chinese leadership may be turning to a harsh brand of nationalism as a result. Its recent border clash with India in the high Himalayas and crackdown on free Hong Kong are the most recent manifestations of this. China's rise as a global economic power, and regional military power, is one of the fastest in history. China has grown faster than America for four straight decades. It has built the industrial and technological foundations for a rapid expansion of its military, to include world-class capabilities in space launch, and its own version of GPS. China's mercantilist economics have taken over entire sectors of other economies, including those of the United States. All this has occurred not just with U.S. acquiescence, but intentional facilitation. America first wanted China as a counterweight to Soviet Russia, and then aggressively helped China to get rich, with the expectation that self-government and democracy would follow in the Middle Kingdom. But the times may be-a-changin’. China's population is aging at a rate and scale that is historically unprecedented. That nation is expected to lose 400 million working age persons this century, and the number is already falling. There is an 18 percent gender imbalance in the country's population. China's birth rate never recovered from its multi-decade "one child" policy. India will likely pass China as the world's most populous country this decade. China has just backed off publishing its economic growth goal for the first time in decades. China is bullying South Korean and Japanese companies. Samsung and Sony are scaling back their operations in the People's Republic. Apple is a laggard, but is planning to move 20 percent of its Chinese supply-chain presence to India. India banned fifty-nine Chinese mobile apps after the above-mentioned border clash. Huawei has found itself on the Trump administration's blacklist, and its loss of Google on its smartphones has badly damaged sales outside China. The UK has announced plans for Huawei's complete removal from British telecom infrastructure by 2023. China's export markets are flat on their backs, and furious at China about the coronavirus. Europe is 16 percent of China's exports, and is an economic and financial wreck. America is 19 percent, the Trump attitude towards China is no secret, and those views are gaining steam with both parties on Capitol Hill. Chinese exports to America are falling rapidly, down 17 percent from the summer 2018 to January 2020. This will be dramatically accelerated by coronavirus. No one thought this economic decoupling could happen so fast. Chinese global direct foreign investment is also down from $260 billion in 2017 to $125 billion in 2019. Why would China be easing up now on its Belt and Road Initiative? On the military side, China's geographic circumstances can only be described as bottled up and vulnerable. China is almost surrounded by countries that are unfriendly. It only has one ally, North Korea, which is more of a client state. Japan, South Korea, Taiwan, Vietnam, Australia, and India are all on the spectrum from cool to hostile towards China. Most are allies or friendly with the United States. Many are armed with American high-tech weapons. To actually control the South China Sea, China would need to control both Subic Bay and Cam Rahn Bay. China is zero percent of the way there. The Philippines just reversed course on its threat to abrogate their Visiting Forces Agreement with the United States. Every South China Sea nation's maritime territory is blatantly infringed upon by the PRC's "Nine Dash Line" claims. This is not how to make friends. The America-India courtship is going well. China and Russia are temporary friends of convenience. Russia is strapped for cash, and the quality and quantity of its defense exports are mostly sub-par. The Chinese defense industry mainly builds Russian knock-offs. Russia is good at making fighters and air defense, but not much else. China's commercial aircraft are immature, and are not worthy of being considered for aerial refueling platforms. There is not much north or west of China, and it is not a good working alliance with Russia. Their power centers are a giant continent apart, and Russia's center of gravity has always been in Europe. Russia has never been able to project power effectively in her far east. This is not a good long-term symbiotic relationship. In order to secure her trade, China must project power from the Yangtze basin and Yellow Sea into the East China Sea. Waiting there are three potential adversaries with sophisticated Western militaries: South Korea, Japan, and Taiwan. Four if you want to count the United States. South Korea and Japan have great force generation land-based aircraft in Strike Eagles (F-15s) and Joint Strike Fighters (F-35s). Taiwan is getting lethal F-16 Vipers with AESA radars. There are 28,000 American troops on South Korean soil. China has no nuclear-powered aircraft carriers, and its conventional carriers are clunkers. Chinese land-based Flankers are much better than their carrier aircraft. The carrier-based J-15 Flanker, based on the Russian Su-33, is a bit of a joke. They cannot take off with full ordnance and fuel. Chinese press openly criticizes the J-15. They are 70,000-plus pound fighters taking off from a ski ramp with an obsolete carrier launch and retrieve system. The Chinese carriers are powered by old-fashioned oil-fired boilers. Chinese bombers are based on old Soviet-designed Tu-16 Badgers. They are more accurately described as "medium" bombers, as opposed to their "strategic" long-range American counterparts. Though recent models feature upgrades, these H-6 bombers are not ready to go toe-to-toe with Western air defenses or air superiority fighters. A move to serious American-type power projection would bankrupt a Chinese economy that is already in trouble. The scary power projection incentive or scenario for China is just not there. The eastern side of the first island chain is the wrong side for China. There China will find swarms of fourth and fifth generation land and sea-based fighters. Taiwan has an impressive military buildup underway. Taiwan has lots of airfields, rapid runway repair capabilities, and can maintain a high level of tactical operations even after a bombardment. Even the west side of the first island chain is a nasty problem set for China. Whether it is superior allied tactical aircraft or American attack submarines, it will have its hands full in a battle it might not win. China needs markets in Europe, oil from the Persian Gulf, and resources in Africa. All three of those are easily held hostage by the U.S. Navy alone, not to mention the naval capabilities held by American friends and allies along the Asian littoral. The Chinese economy would collapse within weeks without Persian Gulf oil. China's military challenges may not be surmountable, maybe for decades. Geography is just too hard for China.

#### Corruption limits China’s rise—undermines its economy

Mueller, Ohio State Adjunct Professor, ‘21

[John Mueller, Adjunct Professor, Political Science, Ohio State University and Senior Fellow, Cato Institute, “China: Rise or Demise?” POLICY ANALYSIS n. 917, 5—18—21, <https://www.cato.org/policy-analysis/china-rise-or-demise>, accessed 6-12-22]

Andrew Wedeman, a prominent student of the issue who heads the China Studies Program at Georgia State University, suggests that, in all, “corruption may be an intractable problem” as long as “people remain subject to temptation, and conditions and incentives make it possible and profitable to ignore regulations, accept bribes to expedite projects, or in other ways pursue acceptable goals through unsanctioned means.” Moreover, “it has the potential to erode public confidence in the regime and the legitimacy of party rule” even as it “tarnishes China’s image abroad and sometimes distorts and impedes efforts to meet critical challenges.” His essay on the subject is provocatively titled “Anticorruption Forever?”89

In his study of China’s crony capitalism, economist Minxin Pei argues that the process not only wastes “precious resources that could have been invested more productively” but also diverts energies and talents into sectors “that are unlikely to be the growth engines needed to upgrade the Chinese economy.” The result, he suggests, is likely to be “long‐​term economic stagnation.”90

#### China’s power is limited—belligerence is driving our foreign investment and technology

Mueller, Ohio State Adjunct Professor, ‘21

[John Mueller, Adjunct Professor, Political Science, Ohio State University and Senior Fellow, Cato Institute, “China: Rise or Demise?” POLICY ANALYSIS n. 917, 5—18—21, <https://www.cato.org/policy-analysis/china-rise-or-demise>, accessed 6-12-22]

Fingar and Oi point to another development that “bodes ill for China’s future”: it has alienated foreign firms. It has done so by stealing intellectual property, demanding transfers of technology as a condition for operating in China, and “generally failing to honor contracts and trade commitments.” As a result, they note, rather than building facilities in China, foreign companies have increasingly sought better opportunities in other countries.119 Notes Doug Bandow, “Even corporate America, long the strongest supporter of the Sino‐​American relationship, has grown frustrated, viewing the Chinese market as almost irredeemably biased against foreign firms.”120

Meanwhile, China’s authoritarian crackdown in Hong Kong, a region that once sported an attractive openness and a court system that was not corrupt, is scarcely likely to encourage international confidence and investment.121 Transparency International routinely ranks countries for perceived corruption. Its rankings from least to most for 179 countries in 2019 found that for what might be called “Chinese entities,” Singapore ranked at 4, Hong Kong at 16, Taiwan at 28, and China at 80. (The United States, for comparison, ranks at 23.) The Hong Kong ranking seems likely to change. And that could have substantial economic consequences. As one business executive puts it, “Businesses will inevitably change their perceptions of Hong Kong as a gateway to China that is protected by rule of law.… There will be foreign companies that say ‘we’ll just enter China directly, I’ve got no one‐​up going via Hong Kong,’ or they’ll just exit China completely.”122

The new national security law is unlikely to charm foreigners—including those in the vast Chinese diaspora—because China has applied it to anyone living anywhere on the planet. Thus, it appears that foreigners who, for example, call for independence for Hong Kong or advocate sanctions against China are subject to arrest and life imprisonment if the Chinese government can get its hands on them.123

### China Ans: Threat—1NC

#### China is not a trheat—multiple reasons

Mueller, Ohio State Adjunct Professor, ‘21

[John Mueller, Adjunct Professor, Political Science, Ohio State University and Senior Fellow, Cato Institute, “China: Rise or Demise?” POLICY ANALYSIS n. 917, 5—18—21, <https://www.cato.org/policy-analysis/china-rise-or-demise>, accessed 6-12-22]

However, even if it continues to rise, China does not present much of a security threat to the United States. China does not harbor Hitler‐​style ambitions of extensive conquest, and the Chinese government depends on the world economy for development and the consequent acquiescence of the Chinese people. Armed conflict would be extremely—even overwhelmingly—costly to the country and, in particular, to the regime in charge. Indeed, there is a danger of making China into a threat by treating it as such and by engaging in so‐​called balancing efforts against it.

Rather than rising to anything that could be conceived to be “dominance,” China could decline into substantial economic stagnation. It faces many problems, including endemic (and perhaps intractable) corruption, environmental devastation, slowing growth, a rapidly aging population, enormous overproduction, increasing debt, and restive minorities in its west and in Hong Kong. At a time when it should be liberalizing its economy, Xi Jinping’s China increasingly restricts speech and privileges control by the antiquated and kleptocratic Communist Party over economic growth. And entrenched elites are well placed to block reform.

That said, China’s standard of living is now the highest in its history, and it’s very easy to envision conditions that are a great deal worse than life under a stable, if increasingly authoritarian, kleptocracy. As a result, the Chinese people may be willing to ride with, and ride out, economic stagnation should that come about—although this might be accompanied by increasing dismay and disgruntlement.

In either case—rise or demise—there is little the United States or other countries can or should do to affect China’s economically foolish authoritarian drive except to issue declarations of disapproval and to deal more warily. As former ambassador Chas Freeman puts it, “There is no military answer to a grand strategy built on a non‐​violent expansion of commerce and navigation.” And Chinese leaders have plenty of problems to consume their attention. They scarcely need war or foreign military adventurism to enhance the mix.

The problem is not so much that China is a threat but that it is deeply insecure. Policies of threat, balance, sanction, boycott, and critique are more likely to reinforce that condition than change it. The alternative is to wait, and to profit from China’s economic size to the degree possible, until someday China feels secure enough to reform itself.

### China Ans: Threat—2NC

#### Any threat posed by China is grossly exaggerated

Mueller, Ohio State Adjunct Professor, ‘21

[John Mueller, Adjunct Professor, Political Science, Ohio State University and Senior Fellow, Cato Institute, “China: Rise or Demise?” POLICY ANALYSIS n. 917, 5—18—21, <https://www.cato.org/policy-analysis/china-rise-or-demise>, accessed 6-12-22]

\*\*edited for language

The current concern about China, and the hostility toward it, are sometimes said to constitute “a new Cold War.” There are, of course, considerable differences. In particular, during the Cold War, the Soviet Union—indeed the whole international Communist movement—was under the sway of a Marxist theory that explicitly and determinedly advocated the destruction of capitalism and probably of democracy, by revolutionary violence if necessary. China today does not harbor such cosmic goals, nor is it enamored of such destructive methods.214

However, the United States was strongly inclined during the Cold War to massively inflate the threat it imagined the Communist adversary to present, particularly militarily.215 The current “new Cold War” is thus in an important respect quite a bit like the old one: it is an expensive, substantially militarized, and often ~~hysterical~~ [panicked] campaign to deal with threats that do not exist or may, in the long term, possibly even self‐​destruct.

#### No threat, they make it worse

Mueller, Ohio State Adjunct Professor, ‘21

[John Mueller, Adjunct Professor, Political Science, Ohio State University and Senior Fellow, Cato Institute, “China: Rise or Demise?” POLICY ANALYSIS n. 917, 5—18—21, <https://www.cato.org/policy-analysis/china-rise-or-demise>, accessed 6-12-22]

Indeed, there is a danger of making China into a threat by treating it as such, by refusing to consider the unlikelihood as well as the consequences of worst‐​case‐​scenario fantasizing, and by engaging in endless metaphysical talk about rejuggling military hardware to somehow “balance” against China. In this respect, special consideration should be given to the observation that, as China expert Susan Shirk notes, provocative balancing talk, especially if military showmanship accompanies it, has the potential to be wildly counterproductive: “historically, rising powers cause war not necessarily because they are innately belligerent, but because the reigning powers mishandle those who challenge the status quo.”36

Similarly, Columbia University’s Richard Betts warns: “No evidence suggests that Chinese leaders will have an interest in naked conquest.… The most likely danger lies in the situation in which action China sees as defensive and legitimate appears aggressive to Washington.”37 “Unfortunately,” observes China scholar Thomas Christensen, “exaggerated rhetoric” from the United States has “seemingly confirmed nationalist Chinese narratives about U.S. efforts to encircle and contain China.”38 Historian Odd Arne Westad points out that China continually complains that “the United States is planning to undermine China’s rise through external aggression and internal subversion.”39 And after going over hundreds of relevant Chinese‐​language articles, Lyle Goldstein, research professor in the China Maritime Studies Institute at the U.S. Naval War College, finds “a plainly evident common theme.” Chinese specialists “are convinced that Washington seeks to contain and even derail China’s rise.”40

#### Any negative effects of China’s rise will be limited

Medin, Johns Hopkins M.A., ‘20

[John Theodore Medine, M.A., Government, Johns Hopkins University, “Rising Tensions: The effects of China’s Rise on the United States, China’s Regional Neighbors, and the International System,” M.A. Thesis, 2020, https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/62699/MEDIN-THESIS-2020.pdf?sequence=1&isAllowed=y]

The international system, which can be defined as the western-backed liberal system that has existed since the end of World War II, is being impacted in subtle ways due to China’s rise. China's rise will harm the current western-backed international system because China has utilized its newfound strength the erode the liberal norms and values which the system is based on. China has looked for ways to contribute to the international system while altering the system to suit its ideals of non-intervention in the domestic affairs of sovereign nations. China has used its growing influence to curtail and limit attempts by the international system to deal with a variety of issues, including human rights. It has also looked for ways to undermine the Washington Consensus, which advocates for political and economic reforms in nations, for its own Beijing Consensus that only focuses on the economic growth of nations. This new concept has further undermined the norms and values of the international system as other nations can look for aid and funding from an alternative source which is not as concerned about social and political reforms such as environmental protections, anti-corruption measures, and human rights. However, the international system is still principally controlled by the Western powers of the United States and the European Union who maintain a distinct advantage over China economically, politically, and militarily. Their extensive system of alliances, which have been cultivated over the last several decades, also means that the international system has a loyal following of supporters committed to its maintenance and continuance. China's rise will allow it greater power and flexibility to allow it to alter the international system along the edges. However, overall, the rise of China will have a limited adverse impact on the international system as China alters the system around the edges by looking for ways to erode the values and norms, such as human rights and democracy, using its influence. However, it will not be a severe threat to the existing global order or its institutions because it has an interest in maintaining the status quo and does not have the power to alter it drastically.

In conclusion, China’s rise will have a limited negative impact on the United States, China’s regional neighbors, and the international system. These impacts include unfair economic trade practices that hurt the United States and other nations around the world while continuing to fund its rise. This economic growth enables China to increasingly challenge the United States and bully its regional neighbors in pursuit of China’s national interests and the growing ability to withstand diplomatic pressure attempting to China’s bad behavior, such as its aggressive actions in the South China Sea and flagrant violations of human rights. China also uses this economic power to pressure other nations, fearful of economic repercussions, into altering key aspects of the international system to better suit China’s interests and condone bad behavior. However, the United States, China’s neighbors, and the international community have the power to limit and roll back these short-term negative effects. Policymakers and scholars are becoming increasingly aware that China is actively trying to alter the global order to suit its national interests and cannot be ignored. China’s current capabilities may not allow it to pursue its national interests aggressively, but if its capabilities increase, it will most likely change its behavior and show different motives. The United States and international community can continue to work constructively with China on a variety of issues of mutual interest such as counterterrorism and North Korea. However, they can no longer be afraid to push back against China’s actions. The top priorities should target China’s main source of power, its economy, by forcing China to end its long-standing unfair trade practices. It should also enforce the international norms and standards that the international system claims to stand by publicly calling out China for any of its offenses. Working constructively with China should not mean giving in to China’s demands as it so frequently has in the past. Now is the time for the United States and the international community to create a united front to firmly reject when China oversteps while the US and the international community have the upper hand.

### China Ans: Threat—Authoritarianism

#### China not exporting autho—split motives

Wong ’21 [Audrye Wong, “How to Not Win Allies and Influence Geopolitics: China’s Self-Defeating Economic Statecraft,” FOREIGN AFFAIRS, May / June 2021, <https://www.foreignaffairs.com/articles/china/2021-04-20/how-not-win-allies-and-influence-geopolitics>, accessed 9-21-21]

What does China want to do with all this newfound economic power? The opacity of China’s political system leads many to ascribe its behavior to a centralized decision-making process pursuing a coherent grand strategy, but Chinese policies are in fact often the product of competition and compromise among a tangle of actors—local governments, high-level bureaucracies, state-owned enterprises, private firms, and more. Consider the BRI. What began as a vague and sprawling plan has taken on a life of its own, at times hijacked by opportunistic government officials and companies seeking to feather their own nests. Many of the constituent projects are motivated less by some grand strategic blueprint than by the preferences of individual actors.

Another error is to assume that China’s actions are driven by a desire to export its own autocratic political system and statist economic system. True, Xi has grown increasingly repressive at home and assertive abroad, but China is still preoccupied more with safeguarding its own interests than with trying to remake other countries in its own image. Even though China seeks to reshape the international system to reflect its priorities, that is a far cry from trying to overturn the order altogether.

What really drives China’s economic statecraft is not grand strategic designs or autocratic impulses but something more practical and immediate: stability and survival. The Chinese Communist Party’s fundamental objective is to preserve the legitimacy of its rule.

China’s economic statecraft, then, is often employed to put out immediate fires and protect the CCP’s domestic and international image. China wants to stamp out criticism and reward those who support its policies. This is particularly true when it comes to issues involving national sovereignty and territorial integrity (such as Taiwan, Tibet, and the East China and South China Seas) and domestic governance (such as China’s treatment of the Uyghurs in Xinjiang and its handling of the covid-19 pandemic).

### China Ans: Threat—Cyber Espionage

#### Economic espionage is normal—the U.S. is the outlier in this regard

Mueller, Ohio State Adjunct Professor, ‘21

[John Mueller, Adjunct Professor, Political Science, Ohio State University and Senior Fellow, Cato Institute, “China: Rise or Demise?” POLICY ANALYSIS n. 917, 5—18—21, <https://www.cato.org/policy-analysis/china-rise-or-demise>, accessed 6-12-22]

International spying and stealing have been standard forever, and they are likely to become ever more extensive as the relevant technology improves. That is, as Hanania puts it, “most of the indictment against China involves things that every country does.”69 As Johnston points out, “the United States has been the only major power to make a clear, normative distinction between the legitimacy of cyber‐​enabled political‐​military espionage and the illegitimacy of cyber‐​enabled commercial espionage.” China, then, is following “the dominant behavioral norm on cyber commercial espionage,” and it is the United States that is the outlier. He also notes that American businesses in China find forced technology transfers to be much less of a problem than issues like the lack of transparency in the Chinese regulatory system.70

### China Ans: Threat—Economics Check

#### China not a threat—economics

Mueller, Ohio State Adjunct Professor, ‘21

[John Mueller, Adjunct Professor, Political Science, Ohio State University and Senior Fellow, Cato Institute, “China: Rise or Demise?” POLICY ANALYSIS n. 917, 5—18—21, <https://www.cato.org/policy-analysis/china-rise-or-demise>, accessed 6-12-22]

From time to time, China may be emboldened to throw its weight around in its presumed area of influence. Such weight‐​throwing is unpleasant to watch as well as counterproductive to China’s economic goals to the degree that it inspires hostility in the region, making the neighbors wary and pushing them closer to the United States.32 But, as even Friedberg and Walt acknowledge, China does not seem to harbor extensive conquest ambitions.33

Above all, China has become almost the quintessential trading state.34 Its integration into the world economy and its increasing dependence on it for economic development and the consequent acquiescence of the Chinese people are crucial. Armed conflict would be extremely—even overwhelmingly—costly to the country and especially to the regime in charge. And Chinese leaders seem to realize this. As Bell puts it, “there is little reason to think that the country has any interest in seriously damaging the United States, its largest trading partner and debtor.”35 The best bet is that this condition will essentially hold.

#### China will be peaceful—economics trumps other factors

Coco, University of Hong Kong researcher, ‘20

[Orazio Coco, Visting Lecturer, University of Hong Kong, and PhD, Sapienza University, “Contemporary China and the “Harmonious” World

Order in the Age of Globalization,” CHINESE JOURNAL OF GLOBAL GOERNANCE v. 6, 2020, pp. 1-19 https://brill.com/view/journals/cjgg/6/1/article-p1\_2.xml?language=en]

The question is whether China would risk losing its achievements and recognition of being part of the international leadership for a relevant ‘domestic’ matter of geographical territory. The answer can be found in history. Waging war does not bring popularity or more power. Conflicts do not bring progress and prosperity and certainly not a leadership role for the countries leading their nations to destruction and human losses. Europe has inexorably withdrawn from being an important geopolitical and military global leader after initiating and staging two World Wars. History has also taught us that the moral quality of leadership is the most qualified reassurance that discourages wars. In the age of nuclear powers such as China and the United States, the consequences of a conflict will be devastating for humanity, and they will be worse for the ideal process of progress and advancement of the involved nations. As far as China is concerned, as Chan argues, all the previously mentioned risks and weaknesses suggest that the current Chinese strategy does not seem to be one of a rising world hegemon but that of a strong country searching for a regional (Asian) leadership role rather than being an impatient newcomer determined to challenge or change the existing international order. 5 More Considerations about the Harmonious International (Socialist) Order As so far argued, China’s political role and economic relevance are strongly linked to the achievement of the ‘harmonious’ and peaceful global order. The fact that the entire idea of a ‘Great China’ is built on the fundamental assumption that only a world at peace can bring prosperity for the Chinese nation and give recognition to China as an important power in international society should not be underestimated. The emergence in the world of any kind of conflict that affects international political instability and economic volatility in the international markets does not support the long-term consolidation of the socio-economic results achieved by China in recent years. This awareness of the need for peace and harmony guides Chinese leadership in pursuing consistent policies in domestic and international affairs. Achieving this goal requires ‘orderliness’, that is, national and international order must be maintained and protected.

### China Ans: Threat—Liberal Order

#### There is no need to contain China, and it will buy into the global order

Mueller, Ohio State Adjunct Professor, ‘21

[John Mueller, Adjunct Professor, Political Science, Ohio State University and Senior Fellow, Cato Institute, “China: Rise or Demise?” POLICY ANALYSIS n. 917, 5—18—21, <https://www.cato.org/policy-analysis/china-rise-or-demise>, accessed 6-12-22]

It certainly seems that, although China may present some challenges to U.S. policy as it continues to grow, there is little to suggest a need to balance against or contain China—particularly through military means—to keep it in line. In fact, the chief problem may not stem from China’s quest for influence, as Washington’s alarmists would have it, but from the fact that a kleptocratic and increasingly authoritarian China may be descending into stagnation or perhaps even into something like demise. That’s, of course, not good news for China; but it is also not necessarily good news for the United States or the rest of the world either. Indeed, in 2016, President Barack Obama suggested that “we have more to fear from a weakened, threatened China than a successful, rising China.”180

As for the challenges provided by China, an observation by Chas Freeman is pertinent. He stresses that “China’s rise is a real, not imaginary, challenge to the status quo and to U.S. leadership” but adds that the rise “is mainly economic, not military and it can be peaceful or not, as our interaction with it determines.” China does not seem to have territorial ambitions (beyond integrating Taiwan at some point), and it does not have the wherewithal or, it seems, the ambition, to “run the world.” As Freeman continues, “History has given the Chinese a healthy apprehension about the damage war can do to their homeland. China is not in search of monsters to destroy beyond its still partially unsettled borders.”181 Fingar concludes that although China expects to play a more influential role in shaping the global order, “it does not (yet) aspire to lead it.”182 Or as Fu Ying, chairperson of the Foreign Affairs Committee of China’s National People’s Congress, puts it more bluntly, “China views the U.S.-dominated world order as a mess and this is why it does not want to take over. Why should China repeat the mistakes which the U.S. did?”183

The Cato Institute’s Colin Grabow suggests that China may eventually become “the responsible stakeholder that many have long urged it to be.” At any rate, “rather than reflexively viewing China’s economic initiatives as an affront to U.S. interests,” efforts should be made to “harness China’s emerging taste for global economic leadership.” And through cooperation, the two countries “could become successful partners in the promotion of trade and prosperity.”184 This seems a sensible course even if it might entail scaling back American claims to “leadership” in China’s neighborhood and ceding some of that role (such as it is) to Beijing.185

### China Ans: Threat—Spheres of Influence Ans

#### Spheres of influence arguments are bunk

Mueller, Ohio State Adjunct Professor, ‘21

[John Mueller, Adjunct Professor, Political Science, Ohio State University and Senior Fellow, Cato Institute, “China: Rise or Demise?” POLICY ANALYSIS n. 917, 5—18—21, <https://www.cato.org/policy-analysis/china-rise-or-demise>, accessed 6-12-22]

Many commentators have raised concerns about China’s often‐​expressed desire to have more “influence” in the world. They point, in particular, to an elaborate Chinese scheme—the Belt and Road Initiative—to establish sea and land lanes to maintain and enhance China’s ability to trade with the rest of the world. Unsurprisingly, many in the United States envision this as a key part of a diabolical plot by the Chinese to “rule the world.”46

However, it is absurd to obsess over something like the vacuous, if venerable, sphere of influence concept. The notion that world affairs are a process in which countries scamper around the world seeking to establish spheres of influence is at best decidedly unhelpful and at worst utterly misguided.47 But the concept continues to be embraced in some quarters as if it had some palpable meaning. For example, in 2017, the National Intelligence Council opined that “geopolitical competition is on the rise as China and Russia seek to exert more sway over their neighboring regions and promote an order in which U.S. influence does not dominate.”48

However, it is difficult to see whether American “influence” could be said to “dominate” anywhere. For example, on December 21, 2017, when the United States sought to alter the status of Jerusalem, the United Nations General Assembly repudiated the U.S. stand in a nearly unanimous vote that included many U.S. allies. That’s influence?49 Indeed, it is impressive that the hegemon, endowed with what Reich and Lebow aptly call a grossly disproportionate military capacity, has had such a miserable record of military achievement since 1945.50 The militarized application of American primacy and hegemony to order the world has often been a fiasco.51

### China Ans: Threat—Tech

#### No impact to emerging tech.

Hickman 20

(Peter L. Hickman, PhD from Arizona State University in International Relations and a Master of Military Operational Art and Science in Joint Warfare, Defense Legislative Fellow for a member of the House Armed Services Committee, former Requirements Manager on Air Combat Command HQ staff and the Chief of Weapons and Tactics at the 225th Air Defense Squadron; 5-12-2020, War on the Rocks, "The Future of Warfare Will Continue to Be Human," 9-15-2021) url: https://warontherocks.com/2020/05/the-future-of-warfare-will-continue-to-be-human/

The character of war continues to evolve, and there is no doubt that AI will significantly contribute to elements of that evolution for the foreseeable future. However, there are risks to an overestimation of the rate of technological change and the role of advanced tech in future victory. In spite of many exciting technological developments, history and data suggest that we are probably in an evolutionary rather than revolutionary period. Furthermore, at least since the beginning of the modern age technological overmatch has been neither necessary nor sufficient for victory, and is about as predictive as a coin toss.

In its understandable zeal for technological advantage, the military should remember enduring truths about warfare. The nuance of force employment is key to any battle, and an over-emphasis on technology risks allowing blind spots that our future adversaries will be sure to exploit. Though we should certainly strive for cutting edge technology, if that pursuit comes at the expense of force employment investments, we may be unknowingly entrusting future success to little more than a coin toss.

#### Their impact is hype.

Sechser 19 - (\*Todd S. Sechser \*\*Neil Narang & \*\*\*Caitlin Talmadge \*Department of Politics @ University of Virginia \*\*Department of Political Science @ University of California Santa Barbara \*\*\*Associate Professor in the Edmund A. Walsh School of Foreign Service and a core faculty member of the Security Studies Program; 8-1-2019, Taylor &amp; Francis, "Emerging technologies and strategic stability in peacetime, crisis, and war," 9-15-2021) url: https://www.tandfonline.com/doi/full/10.1080/01402390.2019.1626725

Yet the history of technological revolutions counsels against alarmism. Extrapolating from current technological trends is problematic, both because technologies often do not live up to their promise, and because technologies often have countervailing or conditional effects that can temper their negative consequences. Thus, the fear that emerging technologies will necessarily cause sudden and spectacular changes to international politics should be treated with caution. There are at least two reasons to be circumspect.

First, very few technologies fundamentally reshape the dynamics of international conflict. Historically, most technological innovations have amounted to incremental advancements, and some have disappeared into irrelevance despite widespread hype about their promise. For example, the introduction of chemical weapons was widely expected to immediately change the nature of warfare and deterrence after the British army first used poison gas on the battlefield during World War I. Yet chemical weapons quickly turned out to be less practical, easier to counter, and less effective than conventional high-explosives in inflicting damage and disrupting enemy operations.6 Other technologies have become important only after advancements in other areas allowed them to reach their full potential: until armies developed tactics for effectively employing firearms, for instance, these weapons had little effect on the balance of power. And even when technologies do have significant strategic consequences, they often take decades to emerge, as the invention of airplanes and tanks illustrates. In short, it is easy to exaggerate the strategic effects of nascent technologies.7

Second, even if today’s emerging technologies are poised to drive important changes in the international system, they are likely to have variegated and even contradictory effects. Technologies may be destabilising under some conditions, but stabilising in others. Furthermore, other factors are likely to mediate the effects of new technologies on the international system, including geography, the distribution of material power, military strategy, domestic and organisational politics, and social and cultural variables, to name only a few.8 Consequently, the strategic effects of new technologies often defy simple classification. Indeed, more than 70 years after nuclear weapons emerged as a new technology, their consequences for stability continue to be debated.9

### China Ans: Threat—A2 “Revisionist”

#### They’re too inwardly focused to be revisionist.

Zhao 18

(Professor of Chinese politics and foreign policy at the University of Denver's Josef Korbel School of International Studies). Suisheng Zhao. 4/25/18; A Revisionist Stakeholder: China and the Post- World War II World Order; <https://doi.org/10.1080/10670564.2018.1458029>.

Not Ready to Overhaul the World Order To some observers, Beijing is positioned to overhaul the world order. Warning about a ‘collision between geo-economics and geopolitics’, a harbinger of battles to come, one Western observer worried that the global system would not survive the rising competition between the US and China. 38 A Singaporean scholar predicted China’s victory, heralding the end of the American century and the arrival of the Asian century. 39 A Chinese scholar claimed that the UK, the US, and China represented three superpowers of yesterday, today, and tomorrow, respectively. The UK as the first modern superpower left rich Anglo- Saxon legacies of global governance. The US replaced the UK after World War II, starting Pax - Americana . Relying on the Bretton Woods System, NATO and so-called universal values, the US was determined to hold on to global dominance. China has to find an alternative path ( 另辟蹊径 ) to defend its national interests. 40 But China is not ready. First, as one Chinese scholar admitted, ‘China does not have the comprehensive national strength to change the current global order led by the US and other Western countries for more than 70 years’. 41 A fragile rising power much weaker than most outsiders think, China is a middle-income country, facing immense internal hurdles, such as the environmental destruction, rampant corruption, inequality, and huge local government debt, all of which have the potential to derail its rise. Preoccupied by mounting challenges, Chinese leaders have to fight an uphill battle to mobilize resources and internal support for the global leadership role. China is far from achieving the donor sta- tus of many OECD countries. For one prominent Chinese scholar, the most dangerous challenge is the extreme-leftist policy-line and ‘the false-large-empty’ ( 假大空 ) slogans, making international promises and setting strategic objectives beyond the reach of China’s national strength. 42 China’s international initiatives do not play a critical role in China’s rise but are the consequences of its rise. Although some scholars have claimed that the US power was declining so that the post-World War II order was suffering from an acute case of Anno Domini, they may have to recant their predictions. With the world’s largest concentration of capital and technology, the US remains the most powerful nation. China has faster GDP growth than the US, but its net national wealth, i.e. the resources available to pursue national interests, is still not in America’s league. From 2000–2012, Chinese net wealth jumped from $4.66 trillion to $21.7 trillion. American net wealth over the same period rose from $42.3 trillion to $67.5 trillion. From 2012 to 2017, while Chinese net wealth climbed to $29 trillion, American net wealth reached to over $93 trillion. Claiming that China is about to eclipse the US is untenable in the face of $64 trillion less in net wealth. The resource advantage rests overwhelmingly with the US. 43 China has pushed RMB internationalization. But the share of RMB in global payment is below 2% while US dollar share remains above 40%. RMB accounts for a scant 1% of global reserves while the US dollar accounts for over 60%. The drive to internationalize RMB has not gained momentum since its inclusion in the SDR basket in 2015. 44 Shortly before inclusion, China’s Central Bank announced a ‘market-oriented’ mechanism for setting the daily benchmark of the exchange rate, accompanied by 2% devaluation, the first since 1994, leading the onshore RMB to tumble by 4% in the subsequent two days. The Central bank intervened massively to halt the slide in the weeks after. Less than two months after RMB’s inclusion in the IMF basket, the central bank imposed new controls over capital outflow. 45 These difficulties have made the cost outweigh the benefits of RMB internationalization. Remaining the ‘indispensable nation’ of the world, the US cannot avoid the responsibility to provide public goods and security protection for its allies. Although President Trump has distanced Washington from its traditional allies and stepped back from global leadership, The American economy and geopolitics encourage a global outlook, imposing compelling imperatives on the superpower. Woven thickly into global value chains, protectionism calls for other countries’ retaliation against American producers and shifts burdens to American consumers. With checks and balances in the US constitution and the dynamism of the open society, economic liberals and internationalists in the US Government and across the states have been powerful countervailing forces against protectionism and disengagement. In spite of President Trump’s isolationist position, ‘American national interests endure. They include preventing any hostile power from dominating Asia, Europe, or the energy resources of the Middle East; sustaining an open international economic and political order, not subverted by spheres of influence that exclude the United States; protecting free access to the global commons, especially the maritime sea lanes that carry 90 % of global trade; nurturing alliances that magnify American power and influence; and promoting democracy and human rights, because the ultimate source of global security is a world in which power is bounded by law and pluralistic institutions’. 46 Second, China cannot provide shared values and other elements of soft power to common willing- ness on the part of other countries to align, and in some cases subordinate, their own narrow interests to those of the larger international community. China has made significant investments in developing its soft power with the opening of more than 500 Confucius Institutes across the world and carrying out extensive international branding campaigns. But China is not successful in projecting its values and ideals that others identify with and aspire to share. The US leadership comes with willing followers and trust through a network of alliances and other ties. For all of their differences with Washington and periodic resentment of its policies, many countries invested more confidence in the US than in any other nation. China does not possess the attributes that underpin US leadership. It lacks allies and inspires little trust in its own neighborhood. Its efforts to project soft power often fail to resonate abroad partly because China displays little empathy with the sensitivities of those living beyond its borders. 47 While US global influence has dropped due to President Trump’s policy, it still holds much more soft power than China. Against the background of seemingly retreating democracy, China’s authoritarian- ism appears to be more appealing to autocracies. But this has not been accompanied by serious and significant interest worldwide in China’s development model. Promoting globalization, the Chinese Government is doing the opposite by imposing controls on the inflow of information and outflow of capital, leading people to question the sincerity of its posited global leadership. A Chinese scholar admits that China might one day overtake the US in the size of economy but may never overtake the US influence and leadership in the world. 48 Another Chinese scholar finds that China is short of international discursive power ( 国际话语权缺失 ). China had never played a world leadership role in history. The traditional Chinese system ( 华夏体系 ) was only an East Asian system, not universal, and cannot automatically transform into modern discursive power. 49 Until China develops values that appeal universally, it misses one of the core features of global leadership. Beijing’s overreliance on its economic prowess as the key diplomatic instrument reveals the shortage of normative power. Despite its growing economic and military might, China’s efforts to use economic ties to influence other state’s behavior have only achieved limited success because money cannot buy loyalty. Influence does not simply derive from a country’s coffers. While closer economic ties are important, they are hardly sufficient to build strong trust between countries—especially those with conflicting security interests. This is clearly reflected in China’s relationship with Japan, characterized as hot economics and cold politics. It is reflected in China’s relations with North Korea, a country that is widely perceived as economically dependent on China for its own survival but has often taken actions against China’s strategic interests. To play a global leadership role, China has to build the ability to inspire other countries to share its vision. The leadership will not work itself out only through economic ties. Building common identity and value is equally, if not more, important. Unable to construct shared values, China may change nothing of substance in the global order. While China’s insistence on the Westphalian principles looks attractive to some countries where intense interventionism by the US often ends in chaos and chronic instability, many of China’s neighbors view China’s great power aspiration with a wary eye, worrying that, as Chinese power rises, China’s imperial past can produce an undue pressure on its leaders to restore the old Chinese hierarchical order. One reporter took note that at the 60th anniversary of the Bandung Conference that gave birth to the Five- Principles, only two notable leaders turned up. One was President Xi, who used the occasion to portray China as the leader of the non-western world. The other was Prime Minister Shinzo Abe, who suggested that the threat to the sovereignty of smaller countries no longer came from the West. 50 China’s power aspirations in a diverse and crowded neighborhood are checked by the presence and influence of the US and other regional powers. The Twenty-first century has seen a multipolarity rather than a Chinese hegemony. While China is rising, many surrounding states are also on the rise. China’s shift from espousing a peaceful rise to assertive behavior has made its neighbors nervous, motivating them to realign with the US and with each other to balance China. 51 survey found that more than 73 % of correspondents had little or no confidence that Beijing would do the right thing in contributing to global peace, security, and governance. 52 A regional Pax Sinica is not desirable for these countries. Historically, to bandwagon with a rising power is common practice due to potentially great relative gains. The most successful rising powers most often attracted the greatest number of bandwagoners. 53 It does not serve China’s interests to have tension with many neighbors simultaneously. China cannot rise successfully without winning the support of its neighbors or at least preempt their balancing motives. Third, China has benefited and continues benefiting from the US-led order. US treaty alliances, troops on the ground and naval predominance have maintained regional peace and facilitated commerce in Asia and beyond. Residing in a neighborhood with complicated power competition and historical animosities, China has to be measured and judicious. ‘The corollary of the decline of the West is not the rise of Asia. It is the erosion of Asia, at least as an idea, as rivalries within geographic Asia overtake the notion of regional cohesion that once bound these countries together’. 54 China often expresses concern over the US–Japan alliance. But the alliance is part of the regional security architecture that has prevented remilitarization of Japan. ‘Imagine what the regional security picture would look like to China if Japan were strategically independent from the United States’. 55 Without the US nuclear umbrella, Japan would have developed nuclear weapons a long time ago, prompting South Korea and others to develop their nuclear weapons. One Chinese scholar, therefore, suggested that ‘Chinese policymakers and analysts should not believe their own jingoistic rhetoric about a US in decline. Even if it’s true, a weak America isn’t good news for China’. 56

### China Ans: U.S. War—1NC

#### No China war

Shifrinson 19

(assistant professor of international relations at Boston University). Joshua Shifrinson. 2/8/19. The ‘new Cold War’ with China is way overblown. Here’s why. February 8, 2019. <https://www.washingtonpost.com/news/monkey-cage/wp/2019/02/08/there-isnt-a-new-cold-war-with-china-for-these-4-reasons/?noredirect=on&utm_term=.f8ca8195c4e4>

Is a new Cold War looming — or already present — between the United States and China? Many analysts argue that a combination of geopolitics, ideology and competing visions of “global order” are driving the two countries toward emulating the Soviet-U.S. rivalry that dominated world politics from 1947 through 1990. But such concerns are overblown. Here are four big reasons why. 1. The historical backdrops of the two relationships are very different When the Cold War began, the U.S.-Soviet relationship was fragile and tenuous. Bilateral diplomatic relations were barely a decade old, U.S. intervention in the Russian Revolution was a recent memory, and the Soviet Union had called for the overthrow of capitalist governments into the 1940s. Despite their Grand Alliance against Nazi Germany, the two countries shared few meaningful diplomatic, economic or institutional links. In 2019, the situation between the United States and China is very different. Since the 1970s, diplomatic interactions, institutional ties and economic flows have all exploded. Although each side has criticized the other for domestic interference (such as U.S. demands for journalist access to Tibet and China’s espionage against U.S. corporations), these issues did not prevent cooperation on a host of other issues. Yes, there were tensions over the past decade, but these occurred against a generally cooperative backdrop. 2. Geography and powers’ nuclear postures suggest East Asia is more stable than Cold War-era Europe The Cold War was shaped by an intense arms race, nuclear posturing and crises, especially in continental Europe. Given Europe’s political geography, the United States feared a “bolt from the blue” attack would allow the Soviet Union to conquer the continent. Accordingly, the United States prepared to defend Europe with conventional forces, and to deter Soviet aggrandizement using nuclear weapons. Unsurprisingly, the Soviet Union also feared that the United States might attack and wanted to deter U.S. adventurism. Concerns that the other superpower might use force and that crises could quickly escalate colored Cold War politics. Today, the United States and China spend proportionally far less on their militaries than the United States and the Soviet Union did. Though an arms race may be emerging, U.S. and Chinese nuclear postures are not nearly as large or threatening: Arsenals remain far below the size and scope witnessed in the Cold War, and are kept at a lower state of alert. As for geography, East Asia is not primed for tensions akin to those in Cold War Europe. China can threaten to coerce its neighbors, but the water barriers separating China from most of Asia’s strategically important states make outright conquest significantly harder. Of course, as scholars such as Caitlin Talmadge and Avery Goldstein note, crises may still erupt, and each side may face pressures to escalate. Unlike the Cold War, however, U.S.-Chinese confrontations occur at sea with relatively limited forces and without clear territorial boundaries. This suggests there are countervailing factors that may give the two sides room to negotiate — and limit the speed with which a crisis unfolds. 3. The Cold War had just two major powers The Cold War took place in a bipolar system, with the United States and Soviet Union uniquely powerful, compared with other nations. This dynamic often pushed the United States and the U.S.S.R. toward confrontation and contributed to more or less fixed alliances; moreover, it encouraged efforts to suppress prospective great powers, such as Germany. In 2019, it’s not at all clear we are back to bipolarity. Analysts remain divided over whether the U.S. unipolar era is waning (or is already over) — and, if so, whether we are heading for a new period of bipolarity, modern-day multipolarity or something else. Regardless, most analysts accept that other countries will play a central role in East Asian security affairs. Russia, for example, still benefits from legacy military investments, India is developing economically and militarily, and Japan is beginning to build highly capable military forces to complement its still-significant economic might. Even if these nations aren’t as powerful as the United States or China, their presence makes for more fluid diplomatic arrangements and more diffuse security concerns than during the U.S.-Soviet competition. The resulting security dynamics are therefore likely to look very different. 4. Ideology plays less of a role in U.S.-Chinese relations Many people see the Cold War as an ideological contest between U.S.-backed liberalism and Soviet-backed communism. But that’s not the whole story. The early 20th century saw liberalism, communism and fascism vie for ideological preeminence. With fascism defeated alongside Nazi Germany, the postwar stage was set for a struggle between communism and liberalism to reinforce the U.S.-Soviet contest. That each ideology claimed universal scope ensured that the ideologies served as rallying cries for Third World conflicts, which were subsequently associated with the U.S.-Soviet struggle. The respective “ideologies” of the United States and China do not favor this type of contest today. Indeed, analysts calling for a hard-line stance against China have faced difficulties even identifying a coherent Chinese ideological alternative. And while some researchers claim that a nascent ideological contest pitting an “autocratic” China against the “liberal” United States is emerging, this narrative ignores the political contests that shape Chinese politics (and have parallels in U.S. politics). Autocracies and democracies often cooperate. And on one important ideological issue — how they organize their economic lives — China and the United States have both embraced economic growth via trade, the private sector and semi-free markets.

# Case Ans: Solvency

### Solvency: Attribution Problems—1NC

#### NATO’s attribution problems undermine the plan’s effectiveness

Patrick, Council on Foreign Relations Senior Fellow, ‘18

[Stewart M. Patrick, James H. Binger Senior Fellow in Global Governance and Director of the International Institutions and Global Governance Program, CFR, “NATO's Deterrence Problem: An Analog Strategy for a Digital Age,” The Internationalist, Council on Foreign Relations, 8—18—18, <https://www.cfr.org/blog/natos-deterrence-problem-analog-strategy-digital-age>, accessed 3-20-21]

Cyber deterrence is inherently more challenging than nuclear or conventional deterrence because such attacks are difficult to definitively attribute to a particular actor. For example, it is easier to mask the source of a cyberattack on a power grid than it would have been for the Warsaw Pact to conceal a massive incursion into West Germany. This attribution problem could complicate NATO’s capacity to conclusively determine the source of a cyberattack and justify and conduct a timely conventional response, particularly if member states diverge in their perceptions. This dilemma could strain the foundations of collective defense and undermine any unified front against cyberattacks.

For NATO to commit to military action, all of its members would need certainty, beyond a reasonable doubt, about the identity of the perpetrator. This is particularly true in the case of Russia—a known sponsor of cyberattacks. Without conclusive proof, it might be a challenge to convince a distant country like Portugal or a dangerously close one like Estonia to join in a counterattack. Complicating matters, such post-attack decisions would need to be made quickly, given Russia’s precedent of using cyberwarfare as a precursor to kinetic invasion. The need for speed leaves little room for philosophical debates over what constitutes an act of war.

### Solvency: Attribution Problems—2NC

#### Cannot stop attacks—attribution problems

Lewis, CSIS analyst ‘09

[James Andrew Lewis, Senior Vice President and Director, Strategic Technologies Program, CSIS, “The "Korean" Cyber Attacks and Their Implications for Cyber Conflict,” Center for Strategic and International Studies, 10—23—09, <https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf>, accessed 3-20-21]

Cyberspace enables anonymous attacks. Identities are easily concealed or fabricated in cyberspace, and an astute opponent will of course make it look as if another was responsible for an attack. The use of botnets complicates attribution - the source of an attack, at the first iteration, will be innocent and unknowing third parties. Forensic work may eventually reveal the source of an attack, but a sophisticated opponent will be able to operate clandestinely and with a high degree of deniability. The “Confickr” worm is a good example of this difficulty. Confickr was a global malware that infected millions of computers.1 Many companies and governments made a coordinated effort to fend it off, but we still have no idea who launched Confickr, what their intent was, or even whether it has been removed from all infected systems.

#### Attribution problems undermine effective responses

Lewis, CSIS analyst ‘09

[James Andrew Lewis, Senior Vice President and Director, Strategic Technologies Program, CSIS, “The "Korean" Cyber Attacks and Their Implications for Cyber Conflict,” Center for Strategic and International Studies, 10—23—09, <https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf>, accessed 3-20-21]

Weak attribution and unpredictable collateral damage make deterrence ineffective in cyberspace. Deterrence is a threat of retaliation, but it is hard to credibly threaten unknown parties and counterproductive to threaten or damage the wrong party. The United States is widely recognized to have pre-eminent offensive cyber capabilities, but it obtains little deterrent effect from this.

In the absence of attribution, the response options for the United States to the July 4 events were extremely limited. We could not retaliate against an unknown attacker. Deterrence is the threat of violent retaliation. This threat changes the opponent’s calculus of the benefits and costs of an attack. But it is hard to convincingly threaten an unknown attacker, and weak attribution makes traditional deterrent concepts – those based on the threat of reprisal for an attack (either counterforce or countervalue) – largely irrelevant in cyberspace.

### Solvency: Cohesion Problems—1NC

#### Political problems threaten cohesion, undermine the plan’s effectivenss

Psychogiou, Finabel researcher, ‘22

[Vasiliki Psychogiou, Finabel research intern, “Cyberspace: Is NATO Doing Enough?” Finabel—European Army Interoperability Centre, Info Flash, 2—22, p. 3]

Undoubtedly, cyberspace has become a key playing field of NATO’s overall defence and deterrence posture. Yet, the question remains whether the Alliance is doing enough. NATO’s internal challenges can significantly underestimate its efforts to build a solid cybersecurity posture. NATO has traditionally focused more on its military character rather than on its political role to promote constructive internal dialogue among its members, to consult on defence and security-related issues to solve problems, build trust and, in the long run, prevent conflict. Thus, it is essential that NATO updates its political foundation and enhances its political cohesion under its common purpose, that is, the protection of the Euro-Atlantic area (NATO, 2021; NATO, 2020; Deschaux-Dutard, 2021; Brent, 2019).

Moreover, the Alliance has often been accused of being a monolithic structure rather than a hub of political dialogue (Shea, 2020). Disputes between its Allies have often impacted NATO unity on external matters. Driven mainly by national interests, these disputes have constrained NATO’s cohesion. Worries have also been expressed about the commitment of the United States to the defence of the European continent, the impact of the European Union’s development as a security actor on the future of NATO, the commitment of some European Allies to burden-sharing of defence, and the development of political inroads by NATO’s rivals into the Alliance territory (Reflection Group, 2020; Belkin, 2020; NATO, 2021; NATO, 2020; Deschaux-Dutard, 2021; Brent, 2019; Shea, 2020). All these issues have significantly challenged NATO’s decision-making, which needs political cohesion to shape decisions, including on cyberspace-related matters.

### Solvency: Cohesion Problems—2NC

#### Illiberal governments threaten cohesion

Psychogiou, Finabel researcher, ‘22

[Vasiliki Psychogiou, Finabel research intern, “Cyberspace: Is NATO Doing Enough?” Finabel—European Army Interoperability Centre, Info Flash, 2—22, p. 3]

Another major challenge emanates from undermining NATO’s fundamental principles from inside. Some allied governments have moved away from NATO’s fundamental freedoms (Ricketts, 2020). For instance, Poland, Hungary, and Turkey have undermined free speech, free press, and the independence of courts. These actions have threatened democracy, individual liberty and the rule of law, the foundation of the North Atlantic Treaty (Lute & Burns, 2019). Erdogan has aligned Turkey closer to Moscow rather than the United States or the European Union (Petrov, Schütte et al., 2020). As a result, NATO’s cohesion and credibility are at stake with important implications for its deterrence, defence and security posture in all domains, including cyberspace (NATO, 2021; NATO, 2020; Deschaux-Dutard, 2021; Brent, 2019; Shea, 2020).

### Solvency: Democracy Turn—1NC

#### Resilience-necessitated monitoring undermines democracy

Atkinson, eSchool Security Studies Professor, ‘18

[Carol Atkinson, PhD, IR, Duke University, Professor, Security Studies, eSchool of Professional Military Education, and Lt. Col. (ret.), USAF, “Hybrid Warfare and Societal Resilience: Implications for Democratic Governance,” INFORMATION AND SECURITY: AN INTERNATIONAL JOURNAL v. 39 n. 1, 2018, p. 71-72]

The cyber operations discussed earlier in this paper have the capacity to undermine fundamental ideas of democratic citizenship in a way that traditional military attacks do not. One of the key lessons learned from the strategic bombing campaigns in World War I, World War II, the Vietnam War, and other war theaters is that physical attacks against a population are more likely to result in a hardening of morale and increased patriotism rather than demoralization and surrender. Hybrid threats, particularly cyber threats, pose a conundrum for democratic governments trying to ensure that their societies are resilient. The ability of any democratic country to counter hybrid threats, in large part, depends on the willingness of its citizens to support government policies aimed at combating hybrid actors. In turn, some of the things that democratic governments would like to do to combat hybrid threats may undermine some of the basic freedoms that define what it means to be a democratic country. These basic freedoms include personal freedoms such as the right to privacy at home and the right to have private conversations and private correspondence that is not subject to government monitoring. On the one hand, government monitoring of personal conversations and personal activities is an action that is associated with the worst aspects of autocratic rule. On the other hand, if hybrid actors use cyber systems to cause damage then the only way to combat the threat seems to be through monitoring and using the same systems.

What is unique in the current era, and particularly in the case of hybrid threats, is that citizens of democratic countries have in some cases advocated, or been complicit in, he undermining of their own democratic rights and freedoms. Government officials have argued that only by limiting some rights and freedoms can hybrid threats be effectively countered. Many citizens are willing to acquiesce. U.S. citizens’ contradictory views on the U.S. National Security Agency’s (NSA) widespread collection programs that were revealed by Edward Snowden illustrate the conundrum. It is widely known that the NSA collection programs monitored and stored (and continue to do so) the data from billions of phone calls each day as well as email messages, instant messages, Facebook posts, contact lists, videos, chat, file transfers, on-line social networking information, and other internet data.

### Solvency: Democracy Turn—2NC

#### Resilience measures push people to give up their basic freedoms

Atkinson, eSchool Security Studies Professor, ‘18

[Carol Atkinson, PhD, IR, Duke University, Professor, Security Studies, eSchool of Professional Military Education, and Lt. Col. (ret.), USAF, “Hybrid Warfare and Societal Resilience: Implications for Democratic Governance,” INFORMATION AND SECURITY: AN INTERNATIONAL JOURNAL v. 39 n. 1, 2018, p. 72-73]

U.S. citizens are not alone in acquiescing to increasingly intrusive government surveillance and monitoring. The governments of France, Germany, United Kingdom, Netherlands, Austria, Denmark, Finland, Norway,38 and Switzerland 39 have all recently deliberated or passed laws allowing greater surveillance of their own populations. A recent analysis by journalist Hugh Eakin concluded, “the very qualities that have made Sweden and Norway successful models of advanced democracy may also have made their populations more susceptible to government spying. In Norway, the government committee that put forward the mass surveillance legislation now before parliament has argued that such measures ‘can be justified as necessary in a democratic society’.” 40 This is an argument that seems to resonate and be accepted by citizens across Western democracies. This gradual relinquishing of democratic freedoms is a result of hybrid warfare strategies. It is a phenomenon that requires much more attention from scholars and democratic citizens alike.

Conclusion

Hybrid warfare presents a conundrum for Western democracies and their citizens. Increasingly, these governments have argued that their ability to counter cyber threats and “irregular” agents such as terrorists depends on the government’s ability to monitor all forms of communication, information and social connections on the internet and through cellular networks. This paper has suggested that the willingness of citizens to support government surveillance programs will ultimately undermine the basic freedoms that define what it means to be a democratic country. Hybrid warfare has opened a new era for international politics and Western democracies as democratic governance is undermined not only by hybrid warfare threats, but also by actions taken by democratic governments to counter those threats.

### Solvency: Political / Tech Barriers—1NC

#### System architecture undermines resilience efforts

Hall & Sandeman, London School of Economics researchers, ‘22

[Jonny Hall, PhD Candidate, International Relations, London School of Economics and Political Science and Hugh Sandeman, Visiting Senior Fellow, LSE Ideas and Project Head of Global Strategies, “NATO’s Resilience: The First and Last Line of Defence,” Strategic Update, LSE IDEAS, 5—22, London School of Economics p. 10]

The Political Challenges of Resilience

A further set of challenges for NATO members regarding resilience policies revolve around efficiency and costs. The drive towards greater efficiency that underlies modern economies and societies can inhibit resilience. As Andrew Zolli and Ann Marie Healy note, “a seemingly perfect system is often the most fragile, while a dynamic system, subject to occasional failure, can be the most robust”.24

This is a consequence of individual actions having wider effects in more interdependent systems. Advances in information and communication technologies and the growth of crossborder economic interdependence, for example, have increased vulnerabilities to disruption.25 As Secretary General Stoltenberg put it, NATO members might be “more prosperous” in “today’s interconnected and digital world … but they are also … more vulnerable”.26 Hence there is the need, as underlined in the Strengthened Resilience Commitment, to work with the whole of government and non-governmental sectors to increase NATO resilience.27

### Solvency: Political / Tech Barriers—2NC

#### Resilience measures are expensive, will be resisted

Hall & Sandeman, London School of Economics researchers, ‘22

[Jonny Hall, PhD Candidate, International Relations, London School of Economics and Political Science and Hugh Sandeman, Visiting Senior Fellow, LSE Ideas and Project Head of Global Strategies, “NATO’s Resilience: The First and Last Line of Defence,” Strategic Update, LSE IDEAS, 5—22, London School of Economics p. 10-11]

However, creating resilience is almost inherently expensive. Unlike efficient systems that engage with existing environments, proactive resilience measures plan for worst-case scenarios that may not even emerge. This creates a dilemma for politicians who wish to be seen neither to over- nor underreact to potential shocks. Take the example of disease prevention in the United States. The 1976 “swine flu affair” was marked by a significant degree of government action, including $137 million spent on vaccine research and the costs of inoculating 40 million Americans before the “sorry debacle” was abandoned as unnecessary, as The New York Times put it.28 On the other hand, the Trump administration called for a 17 percent cut in funding for the Centers for Disease Control and Prevention (CDC) just two years before the COVID-19 pandemic.29 The Trump case is indicative of policies in the era of austerity that followed the 2008-2009 financial crisis, as NATO members have generally hedged their bets against hypothetical shocks by reducing funding. The problem of costsaving is acute given that, unlike during the Cold War, contemporary critical national infrastructure such as internet providers and mobile networks are principally run by private companies who are especially geared towards efficiency.30

#### Polarization undermines messaging efforts

Hall & Sandeman, London School of Economics researchers, ‘22

[Jonny Hall, PhD Candidate, International Relations, London School of Economics and Political Science and Hugh Sandeman, Visiting Senior Fellow, LSE Ideas and Project Head of Global Strategies, “NATO’s Resilience: The First and Last Line of Defence,” Strategic Update, LSE IDEAS, 5—22, London School of Economics p. 11]

To justify the costs and attention necessary to implement proactive resilience measures, a third challenge emerges for NATO and governments of alliance members: how to encourage whole-of-society resilience without adverse side effects. As highlighted by Secretary General Stoltenberg, the contemporary security environment means that “it is not enough to have strong militaries alone” as NATO also “need[s] strong societies”.31 This is necessary for defence and deterrence: cohesive societies will not only generate resilience in the face of adversity but may also discourage the belief by adversaries that hostile behaviour will prevail. But the required public mindset cannot be built without trust in the message that the authorities are trying to get across. If the messaging is regarded as opportunistic or politically motivated, the effort will fail. This is particularly true in an era of widespread political polarisation, given that “resilience is often a measure of the public’s confidence in … government”.32

### Solvency: Private Sector Blocks—1NC

#### Private sector is key and they say no

Collier, Oxford PhD candidate, ‘15

[James Collier, PhD Candidate, Cyber Security, University of Oxford, “NATO’s Role in the Cyber Domain Is Unclear,” Cybersecurity Intelligence, 11—6—15, <https://www.cybersecurityintelligence.com/blog/natos-role-in-the-cyber-domain-is-unclear-775.html>, accessed 3-21-22]

First, there are a number of flaws in the militarisation of the cyber domain. The majority of those with the necessary technical skills to respond to the cyber security challenges work outside of the military sector. In addition, a large proportion of the infrastructure within the cyber domain is privately owned and operated. This prevents NATO from making a substantial contribution to its protection. Crucially, NATO does not have any rights, or powers, to intervene in the private sector. Given NATO’s current lack of expertise in the area, private sector firms are unlikely to welcome NATO assistance.

### Solvency: Private Sector Blocks—2NC

#### Private actors are superior—the plan confounds those efforts

Rosenblum, former Assistant Secretary of Defense, ‘16

[Todd Rosenblum, former Acting Assistant Secretary of Defense for Homeland Defense and Amercas’ Security Affairs, “NATO and Cyberwar Strategy: Proceed with Caution,” THE CIPHER BRIEF, 7—6—16, <https://www.thecipherbrief.com/column_article/nato-and-cyberwar-strategy-proceed-with-caution>, accessed 3-21-22]

For example, attacks against domestic critical infrastructure constitute an unrefined and hugely expansive mission space. Should it be an alliance military mission? Should this come under NATO’s security umbrella? Expanding Article V protections to attacks against private sector operations may seem logical to some, but NATO should proceed with great caution before promising its security umbrella to cyber homeland security and resiliency. Asserting protection and response to attacks in this area, over-states NATO’s capacities and undermines alliance credibility.

There are a host of reasons why NATO must confine its ambitions to government network defense and response, and rethink whether domestic infrastructure protection really is – or should be – part of its writ.

First among the reasons is that the private sector owns and operates the vast majority of critical infrastructure and may not want NATO or even their own government’s help. The private sector has its own diverse perspectives, and the crisis management links between government and the private sector simply do not exist. Calling this a NATO mission makes essential coordination with the private sector exponentially harder. Differing national laws and ethos that define government–private sector cooperation makes it nearly impossible.

NATO members, like so many national governments, continue to minimize the reality that the private sector is at least as central as governments in cyber crisis management and response. Unlike traditional armed conflict, deterrence and crisis management is a joint venture with the private sector, no matter how often governments think they will be the tip of the spear.

The private sector is not only a co-equal branch in cyber crisis management but has different stakes than governments and multinational alliances. Information technology and other major companies are borderless, and responsive to global stakeholders and financial markets. Their interests often do not align with those of governments, and certainly not major military alliances. The private sector generally has superior capabilities than governments. Its decisions about what to do, when to do it, and how to do it, will take government views into account but will not be beholden to them.

Revisiting North Korea’s repeated attacks against Sony America’s networks throughout 2014 highlight how different and difficult crisis management is in the domestic digital domain. NATO will do well to remember how complicated this event was for the United States national security apparatus.

In brief, the North Korean state attacked the digital data stores of the American subsidiary of a Japanese company. The key actors through most of the crisis were all in the private sector, and Sony responses were framed more by the actions of its rivals and business partners in industry than anything said or done by government. Not surprisingly, individual business interests outweighed common cause. Private sector unity was not possible.

Of course the U.S. government played an important role late in the crisis when President Obama declared there to be a national interest in the situation and imposed sanctions on the North Korean state. But the central point is that critical decisions were made by the private sector, based on business needs, damage assessments, and capabilities.

Government was not able to manage this major crisis even though it involved a nuclear weapon state threatening physical strikes in the U.S. homeland. Events since, such as Apple’s refusal to cooperate with a court order to assist the government in accessing encrypted information on a terrorist’s iPhone, reinforces the reality that the relationship between government and industry is getting more distant, not closer. Apple probably would be even less likely to cooperate with a 28 nation military alliance than with its “home” government.

Just imagine how complex it would be for a 28 nation military alliance to assert response dominion against digital attacks by a known adversary against the networks controlling a member’s key infrastructure. What if the company(s) involved had deep business interests in the adversary nation and refused to work with the alliance in fashioning a response? What if its business interest compelled accommodation? What if it did not want to share its essential capabilities with government (or a large military alliance) fearing doing so would be a competitive disadvantage?

National security officials across the globe struggle with the idea that the private sector is not subservient to government in protecting their information technology interests and often is just as capable as government in intelligence gathering and response planning. Cohesion between the two worlds is not likely unless the private sector becomes an essential actor in this element of national security decision making space.

This is not to say industry can operate alone. Industry has many dependencies on government. Only governments can set laws and press treaty enforcement between states. Industry relies on government to provide emergency response assistance if digital strikes have a physical effect, such as a major power outage. Governments often hold key bits of information that can complete the operating picture environment.

The shared dependency between government and the public sector provide opportunity to remake decision-making processes heretofore made solely by government actors. Until we make more headway remaking these processes, NATO would be wise to constrain its ambitions to defending its own networks and improving its operational resiliency. It should set aside planning to protect and respond to digital strikes against privately owned domestic critical infrastructure.

NATO has more than enough challenges ensuring its communications integrity and updating war plans to fully accommodate for fighting in the digital domain. Let’s leave the hornet’s nest of what the alliance should do in response to attacks on domestic infrastructure and private companies to a more settled period.