# Aff – OCOs – Michigan Starter Packet

## 1AC

### Russian Cyberattacks Adv---1AC

#### Russia’s actions in Ukraine demonstrate their reliance on cyberattacks---they’ll escalate attacks against NATO

Cattler ’22 [David and Daniel Black; April 6; Assistant Secretary General for Intelligence and Security at NATO; Principal Analyst in the Cyber Threat Analysis Branch at NATO; Foreign Affairs, “The Myth of the Missing Cyberwar: Russia’s Hacking Succeeded in Ukraine—And Poses a Threat Elsewhere, Too,” https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar]

After Russia invaded Ukraine, many observers initially expected cyberattacks to steal the limelight as a major instrument in Russia’s arsenal. But after a month of fighting, a host of prominent scholars and analysts of cyberconflict have reached the opposite conclusion. Russia’s activities in cyberspace, they claim, have been paltry or even nonexistent. They have dismissed the role of cyber-operations, variously proposing that digital preparations for the invasion in Ukraine never occurred, were haphazard or lacked any real impact, or were mere continuations of Russia’s long-term cyber-activity against Ukraine that fell below the threshold of outright war.

This is a dangerous misdiagnosis. All available evidence indicates that Russia has employed a coordinated cyber-campaign intended to provide its forces with an early advantage during its war in Ukraine. The apparent disconnect between these observed incidents, on the one hand, and the public analysis that Russian cyber-operations have been minimal, on the other, is jarring. Preconceived notions of the role of cyberattacks on the battlefield have made it hard for analysts to see cyber-operations in Ukraine for what they are and for the role they play within Russia’s military campaign. Leaning on these preconceptions will only lead to future policy and intelligence failures. Cyberspace is still a nascent domain of operations, and events in Ukraine will have outsized implications not just for any appreciation of Russian cyberpower but for an understanding of the nature of cyberconflict itself.

OPENING SALVO

The belief that cyber-operations have played no role in Ukraine does not stem from a lack of real-world impact. To the contrary, the magnitude of Moscow’s pre-kinetic destructive cyber-operations was unprecedented. On the day the invasion began, Russian cyber-units successfully deployed more destructive malware—including against conventional military targets such as civilian communications infrastructure and military command and control centers—than the rest of the world’s cyberpowers combined typically use in a given year.

The cumulative effects of these attacks were striking. In the hours prior to invasion, Russia hit a range of important targets in Ukraine, rendering the computer systems of multiple government, military, and critical infrastructure sectors inoperable. Forensic analysis by Microsoft, the cybersecurity company Symantec, and the Slovak firm ESET has found that these attacks affected numerous government agencies, military institutions, civil emergency services, and a range of other critical infrastructure sectors such as defense industrial base manufacturers, information technology services, and energy companies directly relevant to Ukraine’s military capacity.

Cyber-enabled sabotage also knocked offline the satellite Internet provider KA-SAT, which Ukraine’s military, intelligence, and police units depend on. Victor Zhora, the deputy chief of Ukraine’s State Service of Special Communication and Information Protection, has characterized the satellite outage as “a really huge loss in communications in the very beginning of war.” U.S. defensive cyberspace operations prevented further Russian attacks from disrupting the railway networks that were being used to transport military supplies and help millions of Ukrainian citizens evacuate.

Russia continues to draw from its wartime arsenal of cybertools, deploying additional destructive malware on a weekly basis. Cities under siege from Russian shelling, including Kharkiv and Kyiv, have experienced cyber-enabled disruptions to Internet services. Ukraine’s national cyber-authorities continue to expose intrusion attempts by Russian and Belarussian cyber-units. All of this has occurred against the backdrop of a series of website defacements, denial-of-service attacks, and other destabilizing cyber-operations intended to produce chaos and further exhaust Ukraine’s cyberdefenses.

If observers see this cyber-offensive as a series of isolated events, its scale and strategic significance get lost in the conventional violence unfolding in Ukraine. But a full accounting of the cyber-operations reveals the proactive and persistent use of cyberattacks to support Russian military objectives. The misperception that Russia has been restrained or ineffective in the prosecution of its cyberwar on Ukraine likely stems from the fact that Russia’s cyber-operations have not had the standalone, debilitating effects that assessments before the war imagined they would have. But those assessments pose an unrealistic test of strategic value. No single domain of operations has an independent, decisive effect on the course of war. Nevertheless, the lack of overwhelming “shock and awe” in cyberspace has led to the flawed presumption that Russia’s cyber-units are incapable, and even worse, that cyber-operations have offered Russia no strategic value in its invasion of Ukraine.

THUNDER RUN

Analysts should assess the use of cyberpower in its proper context. Evaluating Russia’s cyber-operations in Ukraine is impossible without accounting for the multiple tactical and strategic errors that have bedeviled other aspects of Moscow’s military campaign. Russian planners expected a swift victory in Ukraine, but their strategy failed for multiple reasons: inadequate coordination and preparation, the underestimation of the strength and resilience of Ukraine’s military, and various intelligence lapses. Russia’s missteps and struggles have almost certainly hurt its ability to fully employ its cyber-program in support of its conventional forces.

But even with those limitations, Russian cyber-units successfully attacked a range of targets in accordance with Russia’s war plans. Russian cyberattacks on government and military command and control centers, logistics, emergency services, and other critical services such as border control stations were entirely consistent with a so-called thunder run strategy intended to stoke chaos, confusion, and uncertainty, and ultimately avoid a costly and protracted war in Ukraine. Indeed, Russian cyber-units have demonstrated their ability to succeed without a great deal of advance warning and direction, and despite the overarching difficulties hampering Russia’s military effort.

The reason for this relative success lies in the unique nature of competition and conflict in cyberspace. Unlike troop buildups or other forms of military mobilization that are infrequent and highly visible, cyber-operations are the result of operational cycles that occur covertly and continuously through peacetime and wartime. The targeting of sensitive networks during peacetime lets attackers lay the groundwork for malware intended for wartime use. The methods attackers use to establish initial footholds for espionage activities are indistinguishable from those that precede cyberattacks. For cyber-units, war does not fundamentally change the way they prepare or start to fight.

Russia’s cyberattacks prior to the invasion suggest methodical preparations, with the attackers likely gaining access to Ukrainian networks months ago. This stands in stark contrast to the evident lack of preparation across Moscow’s other military instruments, including on the ground, in the air, and in its frequently used influence operations through media and social media. Russian cyber-units did not need direct military orders to prepare for the invasion or to generate new capabilities for the war. The operational realities of cyberspace required them to be ready well in advance. Russian cyber-units will probably continue to be in a state of permanent readiness and capable of supporting tactical and strategic objectives on short notice, either in Ukraine or beyond, as the war persists.

The emerging consensus that claims Russian cyber-operations were ineffective misses the bigger picture. Russia’s strategy failed to capitalize on the full capabilities and numerous operational successes of its cyber-units. For instance, Russian cyber-units have not yet shut down electricity or Internet connectivity on a massive scale in Ukraine. That does not mean Russia is incapable of such attacks, as some observers have suggested, but that it envisioned a swift victory and did not see the need for such widespread, indiscriminate disruptions. In all likelihood, Russian military units were reliant on Ukrainian civil infrastructure for their planned seizure of Kyiv and could not risk blowback to their own operations. Russia is almost certainly capable of cyberattacks of greater scale and consequence than events in Ukraine would have one believe. Moscow has significantly improved its ability to conduct comprehensive cyber-operations in recent years and has actively invested in its cyber-capabilities, developing new and harder-to-detect variants of its more advanced malware and operational infrastructure.

NO RESTRAINT

The war in Ukraine is not over. Russia has been forced to change its operational approach, and Western intelligence points to Moscow shifting toward a strategy of attrition. With the likelihood that the conflict will become a protracted war, Russia will probably not exercise restraint in its use of additional disruptive and destructive cyber-actions. Russian President Vladimir Putin is most likely to double down on early cyber-successes and seek to further disrupt and undermine government, military, and civilian infrastructure, as well as defense industrial base enterprises. Russia’s recent attempts to strike the same targets it hit on the day of the invasion with additional destructive malware indicate this new phase of the conflict is well underway.

Although less visible than cyberattacks, cyber-enabled espionage—the theft of sensitive information, in this case from Ukrainian networks—is also likely to play a grisly role in the Russian offensive. Russia’s Federal Security Service has allegedly used personal information stolen from Ukrainian federal databases to draw up kill lists of people who could lead a Ukrainian resistance movement in the event of a Russian victory. And as the war carries on, Russia may be increasingly tempted to tap into the latent strategic potential of hacking collectives aligned with the Kremlin that specialize in ransomware and can unleash chaos at a moment’s notice.

Western policymakers should also be prepared for cyber-operations to spread beyond the confines of Ukraine. Several Russian cyber-operations since the invasion have already had spillover effects into NATO countries, affecting critical sectors and civilian Internet connectivity across Europe. Russia knowingly accepted the risk that its cyberattacks would cause collateral damage and has a history of similar reckless behavior. The U.S. Office of the Director of National Intelligence’s Annual Threat Assessment released in March judged that “Russia is particularly focused on improving its ability to target critical infrastructure … in the United States as well as in allied and partner countries.” Active Russian preparations for future cyber-operations indicate that this not an idle threat.

Cyber-operations have been Russia’s biggest military success to date in the war in Ukraine. They will continue to provide Moscow a flexible tool capable of hitting a range of targets in Ukraine and beyond. Disregarding their unprecedented use will only leave policymakers and analysts unprepared for what’s next. A clear-eyed view of the role cyberwarfare has played so far in Ukraine and a better understanding of its place in modern warfare are imperatives for NATO’s collective security and for managing the risks of escalation looming in cyberspace.

#### Multilateral responses are crucial to counter Russian attacks---otherwise they’ll shut down the grid

Aldanova ’22 [Dina; May 30; Master’s Candidate at Georgetown University’s Eurasian, Russian, and East European Studies Program; National Interest, “Will Russia Launch a New Cyber Attack on America?,” <https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/will-russia-launch-new-cyber-attack>]

International cooperation to this degree is not an asset that Russia benefits from. With the support of NATO Cooperative Cyber Defense Center of Excellence’s research and development projects, expertise, and training, U.S. retaliation to a potential Russian cyber attack could be not only detrimental but even more profound as a multilateral response. Based on all this, the fear of retaliation could indeed prevent Putin from engaging in offensive cyber operations against the United States.

Finally, Putin has lost the upper hand in launching an attack by surprise. For instance, Russia invaded Georgia during the Olympics Games in Beijing in 2008, and Ukraine during the Sochi Winter Olympics in 2014. When Putin waged war on Ukraine in 2022—incidentally, immediately following the Beijing Winter Olympic Games—the West anticipated it. Putin invaded Ukraine anyway. He is unlikely to act recklessly in this way again, considering the failures the Russian military has experienced since the invasion. Furthermore, knowing that the United States and European allies have shielded up, Putin has no incentive to strike. Nevertheless, would Putin wait for a more favorable moment? Or scale back a potential attack, for instance, by meddling in the U.S. midterm elections in November?

It would be misleading, however, to underestimate Russian cyber capabilities or Putin’s mind games and lose vigilance. In 2020, despite denying its involvement, Russia evidently hacked U.S. software company SolarWinds. By installing malware into the company’s updated Orion software program, the attack affected thousands of customers, a hundred companies such as Microsoft and Intel, and some federal agencies like the Treasury Department, the Pentagon, and the Cybersecurity and Infrastructure Security Agency. Cyber experts acclaimed the code used as phenomenal. More astonishingly, if not for a performance assessment and proper investigation, the attack could have easily gone unnoticed. For over six months, Moscow tracked emails and other traffic of sensitive information. Could there already be a similar malware in U.S. networks?

Now, on the brink of a new Cold War, the United States must keep its guard up on cybersecurity. Although there are significant factors that challenge the probability of an imminent Russian cyber-retaliation, the United States should not disregard the potential for malicious activity in the near future. It needs to keep a sober view and not act hastily. Setting priorities for the long run, the United States needs to continue advancing cyber mechanisms that detect sensitive activity like the Solar Winds hack, and invest more in training and education about cyber hygiene for government agencies, private companies, and the public. It should not neglect to regularly test offline backups, run software updates, report incidents, use multifactor authentication, block unusable domain IP addresses, and assess third-party risks.

Although Putin’s intentions are far from clear, his decision to pursue a cyberattack on the United States’ critical infrastructure that would instantly shut down electricity or disrupt clean water supply, the offense might come unexpectedly, and soon. Cornered with sanctions and burdened by the bitterness of defeat, Putin might act furiously. The United States and Western allies need to be vigilant and maintain strong lines of communication about any malicious activity. With a strong multilateral front in the West, Russia will have fewer incentives to engage in cyber warfare.

#### Extinction

Weiss ’19 [Matthew and Martin; May 29; National Sales Director at United Medical Instruments, UMI and Research assistant at the American Jewish University; Neurosurgeon at UCLA-Olive View Medical Center; Energy, Sustainability, and Society, “An assessment of threats to the American power grid,” vol. 9]

In testimony before a Congressional Committee, it has been asserted that a prolonged collapse of this nation’s electrical grid—through starvation, disease, and societal collapse—could result in the death of up to 90% of the American population [1].

There is no published model disclosing how these numbers were arrived at, nor are we able to validate a primary source for this claim. Testimony given by the Chairman of the Congressional EMP Commission, while expressing similar concerns, gave no estimate of the deaths that would accrue from a prolonged nationwide grid collapse [2].

The power grid is posited to be vulnerable to geomagnetic storms generated by solar activity, electromagnetic pulses (EMP, also referred to as HEMP) produced by high altitude nuclear detonations, cyberattack, and kinetic (physical) attack. Evidence for and against the validity of each of these threats follows below. Much of the knowledge on these matters is classified. The studies for and against EMP, other than for limited testing of a few components of the infrastructure by the EMP commission, are based not on physical demonstrations but mathematical models and simulations. Moreover, the underlying physics and technology involved—the electrical engineering and materials science—is likely beyond the understanding of the reader, and certainly beyond that of these writers. With these limitations in mind, we proceed.

The electrical grid

HV (high voltage) transformers—transmitting voltages of greater than 100 kV—are what make it possible to send electricity over great distances to thousands of substations, where smaller transformers reduce the voltage.

HV transformers are the weak link in the system, and the Federal Energy Regulatory Commission (FERC) has identified 30 of these as being critical. The simultaneous loss of just 9, in various combinations, could cripple the network and lead to a cascading failure, resulting in a “coast-to coast blackout” [3].

If the HV transformers are irreparably damaged it is problematic whether they can be replaced. The great majority of these units are custom built. The lead time between order and delivery for a domestically manufactured HV transformer is between 12 and 24 months [4], and this is under benign, low demand conditions.

The first practical application of the transformer was invented in the USA by William Stanley, but largely as a consequence of American trade policy (“It doesn’t make any difference whether a country makes potato chips or computer chips”- attributed to Michael Boskin, Chairman of President George H W Bush’s Council of Economic Advisors) [5] there is little manufacturing capability remaining in the USA. Worldwide production is less than 100 per year and serves the rapidly growing markets of China and India. Only Germany and South Korea produce for export.

Ordered today, delivery of a unit from overseas (responsible for 85% of current American purchasing) would take nearly 3 years [6]. The factory price for an HV transformer can be in excess of $10 million—too expensive to maintain an inventory solely as spares for emergency replacement.

Potential mechanisms of collapse

Geomagnetic storms

Geomagnetic storms are due to coronal mass ejections (CMEs)—massive eruptions of plasma expelled from the sun’s corona. Plasma is the fourth fundamental state of matter, consisting of free electrons and positively charged ions. The sun, like all stars, is plasma.

Coronal mass ejections often occur with solar flares, but each can also take place in the absence of the other. The latter emits radiation in all bands of the electromagnetic spectrum (e.g., white light, ultraviolet light, X-rays, and gamma rays) and unlike CMEs, affect little more than radio communications.

CME’s take several days to reach the Earth. The radiation generated by solar flares on the other hand arrives in 8 min.

Coronal mass ejections carry an intense magnetic field. If a storm enters the earth’s magnetosphere, it causes rapid changes in the configuration of the earth’s magnetic field. Electric current is generated in the magnetosphere and ionosphere, generating electromagnetic fields at ground level. The movement of magnetic fields around a conductor, i.e., a wire or pipe, induces an electric current. The longer the wire, the greater the amplification. The current induced is akin to DC (direct current), which the electrical system poorly tolerates. Our grid is based on AC. The excess current can cause voltage collapse, or worse, cause permanent damage to large transformers.

The current flowing through HV transformers during a geomagnetic disturbance can be estimated using storm simulation and transmission grid data [7]. From these results, transformer vulnerability to internal heating can be assessed.

The largest recorded geomagnetic storm occurred Sept 1–2, 1859—the Carrington event, named after the English amateur astronomer, Richard Carrington. Auroras were seen as far south as the Caribbean. Campers in the Rocky Mountains were awakened shortly after midnight by “an auroral light so bright that one could easily read common print. Some of the party insisted it was daylight and began preparation for breakfast” [8]. Telegraph wires transmitted electric shocks to operators and ignited fires.

In May 1921, there was another great geomagnetic disturbance (GMD), the railroad storm. The National Academy of Sciences estimates that if that storm occurred today, it could cause 1–2 trillion dollars damage and full recovery could take 4–10 years [9].

The basis for this assertion is a presentation made by J Kappenman of Metatech, the Goleta California engineering consulting firm, given as part of the NAS Space weather workshop titled “Future Solutions, Vulnerabilities and Risks”, on May 23, 2008. The simulation asserts that a 1921 intensity storm could damage or destroy over 300 transformers in the US, and leave 130 million people without power [10]. Elsewhere, Kappenman states that in a worst case situation, geomagnetic disturbances could instantly create loss of over 70% of the nation’s electrical service [11].

In March 1989, a geomagnetic storm caused collapse of the power grid in Quebec, leaving 6 million without power for 9 h. NERC (the North American Electric Reliability Council), a self-regulated trade organization formed by the electric utility industry, asserts that the blackout was not due to overheating of transformers from geomagnetically induced current, but to the near-simultaneous tripping of seven relays, and this is correct [12]. The rapid voltage collapse (within 93 s) likely prevented transformer thermal damage. The same storm, however, destroyed a major transformer at the Salem nuclear plant in New Jersey [13]. The 1989 Hydro-Quebec storm was 1/10th the intensity of the 1921 Railroad Storm [14].

A report for Lloyd’s in 2013 states a Carrington-level extreme geomagnetic storm is almost inevitable in the future. Using its own models and simulations, it puts the US population at risk at between 20 and 40 million, with the outages lasting up to 1–2 years [15].

Because of geography and ground conductivity, the risk of a transformer sustaining damage is 1000 times greater in some US counties than in others. The highest risk is to the counties along the corridor between Washington DC and New York [16].

The first written account of a solar storm is possibly in the book of Joshua. Written reports of aural sightings by Greeks and Romans begin in 371 BC.

A Carrington-level storm narrowly missed the earth in 2012 [17]. NASA has produced a video on the CME [18]. Formerly considered a 1 in 100-year event, the likelihood of a Carrington intensity storm striking the earth has most recently been placed at 12% per decade [19].

Mitigation

The EMP Commission, in its 2008 report, found that it is not practical to try to protect the entire electrical power system or even all high-value components. It called however for a plan designed to reduce recovery and restoration times and minimize the net impact of an event [20]. This would be accomplished by “hardening” the grid, i.e., actions to protect the nation’s electrical system from disruption and collapse, either natural or man-made [21]. The shielding is accomplished through surge arrestors and similar devices [22]. The cost to harden the grid, from our tabulation of Congressional EMP figures, is $3.8 billion.

There has been no hardening of the grid

The commission and organization that are responsible for public policy on grid protection are FERC and NERC. FERC (The Federal Energy Regulatory Commission) is an independent agency within the Department of Energy. NERC, the self-regulatory agency formed by the electric utility industry, was renamed the North American Electric Reliability Corporation in 2006.

In June of 2007, FERC granted NERC the legal authority to enforce reliability standards for the bulk power system in the USA. FERC cannot mandate any standards. FERC only has the authority to ask NERC to propose standards for protecting the grid.

NERC’s position on GMD is that the threat is exaggerated.

A report by NERC in 2012 asserts that geomagnetic storms will not cause widespread destruction of transformers, but only a short-term (temporary) grid instability [23]. The NERC report did not use a model that was validated against past storms, and their work was not peer-reviewed.

The NERC report has been criticized by members of the Congressional EMP commission. Dr. Peter Pry asserts that the final draft was “written in secret by a small group of NERC employees and electric utility insiders….. The report relied on meetings of industry employees in lieu of data collection or event investigation” [22].

NERC, in turn, criticizes Kappenman’s work. NERC states that the Metatech work cannot be independently confirmed [24]. NERC reliability manager Mark Lauby criticized the report for being based on proprietary code [24]. Kappenman’s report, however, received no negative comments in peer review [24].

The NERC standards

The reliability standards and operational procedures established by NERC, and approved by FERC, are disputed [25]. Among the points are these:

1. The standards against GMD do not include Carrington storm class levels. The NERC standards were arrived at studying only the storms of the immediate prior 30 years, the largest of which was the Quebec storm. The GMD “benchmark event”, i.e., the strongest storm which the system is expected to withstand, is set by NERC as 8 V/km [26]. NERC asserts this figure defines the upper limit intensity of a 1 in 100-year storm [26]. The Los Alamos National Laboratory, however, puts the intensity of a Carrington-type event at a median of 13.6 V/km, ranging up to 16.6 V/km [27]. Another analysis finds the intensity of a 100-year storm could be higher than 21 V/km [28].

2. The 15–45 min warning time of a geomagnetic storm provided by space satellites (ACE and DSCOVR) will be insufficient for operators to confer, coordinate, and execute actions to prevent grid damage and collapse.

Testimony of Edison Electric Institute official Scott Aaronson under questioning by Senator Ron Johnson in a hearing before the Senate Homeland Security and Governmental Affairs Committee in 2016 encapsulates some of the issues. Video of the exchange is available on the web [29]. The Edison Electric Institute (EEI) is the trade association that represents all US investor-owned electric companies.

Johnson: Mr. Aaronson, I just have to ask you – the protocol of warning 15–30 min – who is going to make that call? I mean, who is going to make that for a massive geomagnetic disturbance, that nobody knows how many of these transformers are going to be affected. Who is going to make that call to shut them off line – to take them off line – so those effects do not go through those wires and destroy those large transformers that cannot be replaced?

Aaronson: So, the grid operators are tightly aligned. We talked about the fact that there are 1900 entities that make up the bulk electric system. There are transmission operators and so on…

Johnson (interrupting): Who makes the call? Who makes the call – we are going to shut them all down in 30 min, in 15 min?

Aaronson: It’s not as simple as cutting the power. That’s not how this is going to work but there is again, there is this shared responsibility among the sector.

Johnson: Who makes the call?

Aaronson: I do not know the answer to that question [29].

Mr. Aaronson’s is Managing Director for Cyber and Infrastructure Security at EEI.

Congressman Trent Franks, R Az introduced HR 2417, the SHEILD Act, on 6/18/2013. The bill would give FERC the authority to require owners and operators of the bulk power system to take measures to protect the grid from GMD or EMP attack. The costs would be recovered by raising regulated rates.

Franks states he had been led to believe that his bill would be brought to the House floor for a vote. But he states House Energy and Commerce Committee Chairman Fred Upton R, Mich., let it die in committee. He has been unable to get an explanation from Upton [30].

Between 2011 and 2016, Mr. Upton has received $1,180,000 in campaign contributions from the electric utility industry [31].

The electric utility industry is heavily involved in campaign donations. During the 2014 federal election cycle, the electric utility industry made $21.6 million in campaign contributions [32]. The electrical utility industry is particularly involved in state politics. For instance, in Florida, between 2004 and 2012 electric utility companies donated $18 million into legislative and state political campaigns. In that state, the electric utilities employ one lobbyist for every two legislators [33].

Electric utility revenue in 2015 was 391 billion dollars [34].

Electromagnetic pulse

Of the scenarios that might lead to electrical network collapse, EMP has received the widest public attention. It has been the subject of television series, films, and novels. HEMP (for high altitude) is the more accurate acronym, but as media and the public use EMP, we will use both interchangeably.

The issue has become highly politicized. The most prominent article in the media against EMP as a threat is by Patrick Disney, “The Campaign to Terrify You about EMP” published in the Atlantic in 2011. “From Newt Gingrich to a Congressional ‘EMP Caucus’, some conservatives warn the electronic frying blast could pose gravely underestimated dangers on the U.S…..Ballistic missile defense seems to be the panacea for this groups concern, though a generous dose of preemption and war on terror are often prescribed as well” [35].

As of 2009, Mr. Disney was acting Policy Director for the National Iranian American Council (NIAC). NIAC has been accused of acting as a lobby for the Islamic Republic of Iran [36].

Mr. Disney is quoted as stating his strategy, in advancing an Iranian interest, is to “create a media controversy” [36].

The campaign to discredit EMP has been largely successful. To a very large part of the body politic EMP is identified as a cause limited to the far right.

A high-altitude electromagnetic pulse (EMP) is produced when a nuclear device is detonated above the atmosphere. No radiation, blast, or shock wave is felt on the ground, nor are there any adverse health effects, but electromagnetic fields reach the surface.

An EMP has three components, E1 through E3, defined by speed of the pulse. Each has specific characteristics, and specific potential effects on the grid. E1, the first and fastest component, affects primarily microelectronics. E3, the later and slower component, affects devices attached to long conductive wires and cables, especially high-voltage transformers.

A single nuclear blast will generate an EMP encompassing half the continental USA [37]. Two or three explosions, over different areas, would blanket the entire continental USA.

The potential impact of an EMP is determined by the altitude of the nuclear detonation, the gamma yield of the device, the distance from the detonation point, the strength and direction of the earth’s magnetic field at locations within the blast zone and the vulnerability of the infrastructures exposed. The E1 gamma signal is greatest for bursts between 50 and 100 km altitude. E3 signals are optimized at busts between 130 and 500 km altitude, much greater heights than for E1 [38]. Higher altitude widens the area covered, but at the expense of field levels. The 1963 atmospheric test ban has prevented further testing.

E1 and its effects

The E1 pulse (“fast pulse”) is due to gamma radiation (photons), generated by a nuclear detonation at high altitude, colliding with atoms in the upper atmosphere. The collisions cause electrons to be stripped from the atoms, with the resultant flow of electrons traveling downward to earth at near the speed of light. The interaction of the electrons with the earth’s magnetic field turns the flow into a transverse current that radiates forward as an intense electromagnetic wave. The field generates extremely high voltages and current in electrical conductors that can exceed the voltage tolerance of many electronic devices. All this occurs within a few tens of nanoseconds.

The Congressional EMP Commission postulated that E1 would have its primary impact on microelectronics, especially SCADAs (Supervisory Control and Data Acquisition), DCSs (digital control systems), and PLCs (programmable logic controllers). These are the small computers, numbering now in the millions, that allow for the unmanned operation of our infrastructure.

To assess the vulnerability of SCADAs to EMP, and therefore the vulnerability of our infrastructure, the EMP Commission funded a series of tests, exposing SCADA components to both radiated electric fields and injected voltages on cables connected to the components. The intent was to observe the response of the equipment, when in an operational mode, to electromagnetic energy simulating an EMP. “The bottom line observation at the end of the testing was that every system tested failed when exposed to the simulated EMP environment” [6].

E1 can generate voltages of 50,000 V. Normal operating voltages of today’s miniaturized electronics tend to be only a few (3-4) volts. States the EMP Commission: “The large number and widespread reliance on such systems by all the nation’s critical infrastructures represent a systemic threat to their continued operation following an EMP event” [39]. A scenario seen in films is all automobiles and trucks being rendered inoperable. This would not be the case. Modern automobiles have as many as 100 microprocessors that control virtually all functions, but the vulnerability has been reduced by the increased application of electromagnetic compatibility standards. The EMP Commission found that only minor damage occurred at an E1 field level of 50 kV/m, but there were minor disruptions of normal operations at lower peak levels as well [40].

There is a self-published post (J. Steinberger, Nobel laureate physics, 1988) disputing the potential effects of E1 [41]. This is an isolated opinion.

Shielding against E1 could theoretically be accomplished through the construction of a Faraday cage around specific components or an entire facility. The cage is composed of conductive materials and an insulation barrier that absorbs pulse energy and channels it directly into the ground. The cage shields out the EM signals by “shorting out” the electric field and reflecting it.

To be an effective Faraday cage, the conductive case must totally enclose the system. Any aperture, even microscopic seams between metal plates, can compromise the protection. To be useful, however, a device must have some connection with the outside world and not be completely isolated. Surge protective devices can be used on metallic cables to prevent large currents from entering a device, or the metallic cables can be replaced by fiber optic cables without any accompanying metal. The US Military has taken extensive measures to protect (“harden”) its equipment against E1. “On the civilian side, the problem has not really been addressed” [42].

E3 and its effects

E3 is caused by the motion of ionized bomb debris and atmosphere relative to the geomagnetic field, resulting in a perturbation of that field. This induces currents of thousands of amperes in long conductors such as transmission lines that are several kilometers or greater in length. Direct currents of hundreds to thousands of amperes will flow into transformers. As the length of the conductor increases, the amperage amplifies.

The physics of E3 are similar to that of a GMD, but not identical. GMD comes from charged particles showering down from space creating current flow in the ionosphere. These currents create magnetic fields on the ground. A nuclear burst on the other hand generates particles which create a magnetic bubble that pushes on the earth’s magnetic field producing a changing magnetic field at the Earth’s surface. A geomagnetic storm will have substorms that can move over the Earth for more than 1 day, while the E3 HEMP occurs only immediately following a nuclear burst.

There are three studies on the potential effects of a HEMP E3 on the power grid.

The first study, published in 1991, found there would be little damage [43]. Although supporting the utility industry’s position, it has not been subsequently cited by either NERC or the industry. The study is criticized for expressing a smaller threat intensity [44]. The second, published in 2010 by Metatech, calculated that a nuclear detonation 170 km over the USA would collapse the entire US power grid [45]. The third study, by EPRI (an organization funded by the electric utility industry) published in February 2017, asserts that a single high-altitude burst over the continental USA would damage only a few, widely scattered transformers [46]. The study is disputed for underestimating threat levels and using erroneous models [44].

These results are incompatible. One’s interpretation of the studies on E3 (and GMD) is based largely on the credibility one gives to the underlying Commission or Institute, and not the published calculations.

FERC has decided not to proceed with a GMD standard that includes EMP [47]. It will be recalled the GMD standard is 8 V/km. The EMP Commission, utilizing unclassified measured data from the Soviet era nuclear tests, found an expected peak level for E3 HEMP for a detonation over the continental USA would be 85 V/km [48].

The position of the electric utility industry is that E3 from a nuclear detonation is not a critical threat [49]. Others have come to a different conclusion. Israel has hardened her grid [50]. She perceives herself to face an existential threat, and it is not the Sun.

The electric utility industry states the cost of hardening the grid against EMP is the government’s responsibility, not the industry’s [51].

Cyberattack

The vulnerability from a cyberattack is exponentially magnified by our dependence on SCADAs.

In 2010, a computer worm attacking SCADA systems was detected. Although widely spread, it was designed to only attack SCADA systems manufactured by Siemens for P-1 centrifuges of the Iranian nuclear enrichment program. The attack destroyed between 10 and 20% of Iranian centrifuges. Iran’s program was likely only briefly disrupted [52]. In December 2015, a cyberattack was directed against the Ukrainian power grid. It caused little damage as the grid was not fully automated.

There is an argument that the cyber threat is exaggerated. Thomas Rid states that viruses and malware cannot at present collapse the electric grid. “(The world has) never seen a cyber- attack kill a single human being or destroy a building” [53]. The electric utility industry offers a similar perspective. In testimony on cybersecurity before the Senate Homeland Security and Governmental Affairs Committee, its representative states that “There are a lot of threats to the grid…..from squirrels to nation states, and frankly, there have been more blackouts as a result of squirrels (gnawing wire insulation) then there are from nation states” [54].

Others however express concern [55]. Moreover, in a report by the Department of Defense in 2017, it is noted that “the cyber threat to critical US infrastructure is outpacing efforts to reduce pervasive vulnerabilities.” [56] That report notes that “due to our extreme dependence on vulnerable information systems, the United States today lives in a virtual glass house” [57].

On March 15, 2018, the Department of Homeland Security issued an alert that the Russian government had engineered a series of cyberattacks targeting American and European nuclear power plants and water and electric systems [58]. It is reported these attacks could allow Russia to sabotage or shut down power plants at will [59].

The ability to operate a system in the absence of computer-driven actions is fast disappearing. The electric power industry spends over $1.4 billion dollars annually to replace electromechanical systems and devices that involve manual operation with new SCADA equipment [60]. With modest increases in efficiency come exponential increases in vulnerability. The extent to which reduced labor costs (and perhaps reduced energy costs) are passed on to the public is uncertain.

#### They’ll target NATO’s undersea cables

Kello ’22 [Lucas and Monica Kaminska; April 14; Associate Professor of International Relations at Oxford University and co-Director of the interdisciplinary Centre for Doctoral Training in Cyber Security in the Department of Computer Science; postdoctoral researcher at The Hague Program on International Cyber Security at Leiden University; Lawfare Blog, “Cyberspace and War in Ukraine: Prepare for Worse,” <https://www.lawfareblog.com/cyberspace-and-war-ukraine-prepare-worse>]

Some observers have noted the absence of major cyber incidents during Russia’s invasion of Ukraine. The situation does not afford complacency, however. Despite the few breakdowns—so far—in cyberspace beyond Ukraine, their risk has increased rather than diminished. The apparent lull in international cyber activity related to the war is likely illusory; it portends a deterioration in the security of computer systems and networks in Russia and in the nations that sanctioned it or armed Ukraine. Below we explain why.

The central premise of our argument is that Russia and NATO member states will want to avoid a direct military clash at nearly all costs (Putin’s desire to protect his regime from imminent collapse might be an exception). If anything, the tragedies of the war in Ukraine reveal the enormous economic and human costs of conventional battles involving the Russian military behemoth. Although the risk of an accidental or unwanted war between Russia and NATO is always present and has increased, both sides will want to reduce it. That is how to interpret Russian President Vladimir Putin’s recent allusion to nuclear war: He rattled the atom in order not to have to use it. Similarly, President Joe Biden’s warning about the certainty of “World War 3” if Russia attacked NATO was a rhetorical device to reduce its chances. Both sides have signaled that they wish to avoid an epochal war among them; they threaten it in order not to fight it. This is conventional deterrence thinking at its finest. Familiar red lines are reinforced so that all sides can see them plainly amid the crisis.

Far less clear are the lines of response to offensive cyber activity within the realm of “unpeace”: actions that are not physically violent or fatal like war but whose harmful effects on national security are too great to be considered normal peacetime competition. The line between unpeace and war is clear because the boundary of war is easily recognizable. The lower line between unpeace and peace, however, is largely unclear; nations have not painted it, although many Western states seem to assume that existing international laws and norms of restraint apply to forms of conflict less than war.

War in Ukraine will present Western nations with response dilemmas in cyberspace. One concern is the risk of breakdowns in Western cyberspace: It has risen dramatically owing to the intense economic and diplomatic showdown with Moscow (as Lucas Kello warned in a speech at U.S. Cyber Command on March 10). Our logic here is simple: There is an implied symmetry between, on the one side, the effects of economic and financial sanctions against the Russian economy and financial sector and, on the other, the effects of cyberattacks against economic and financial targets in the sanctioning nations.

A large coalition of Western and Western-aligned states (such as Japan and South Korea) have levied economic and financial sanctions against Russia. The country is now possibly the most heavily sanctioned nation in the world—even more so than North Korea under the reclusive Kim Jong Un’s rule. The sanctions go far beyond the targeted financial penalties that the U.S. Treasury Department has applied to individuals and organizations such as the Russian Internet Research Agency, which it deemed responsible for previous hacking activities, or those imposed after the SolarWinds incident. They far surpass, too, the scope and effects of the United Kingdom’s diplomatic and financial penalties in response to the Russian Main Intelligence Directorate’s (GRU) poisoning operation (with the banned chemical agent novichok) against its former agent Sergei Skripal in Salisbury in 2018. The current sanctions regime against Russia is particularly potent because it has included an extraordinary freeze on central bank assets and the expulsion of some of Russia’s largest banks from the global interbank payments system, SWIFT. Hundreds of multinational and mostly Western companies have exited the Russian market or suspended their operations there. The ruble has undergone dramatic price drops not seen since the 1998 financial crisis, which has inflicted economic pain on the general Russian population. The net result of these economic dislocations is an expected drop in Russian gross domestic product of 15 percent in 2022—a decline that would reduce the Russian economy to its size in 2007 at current prices.

Against the backdrop of Russia’s economic meltdown, the Kremlin’s retaliatory options within the diplomatic and economic realms are limited. Russia has so far responded, among other measures, with a ban on ruble loans to citizens of “unfriendly” states, closed its domestic airspace to Western airplanes and demanded payment for Russian gas in rubles. These punitive instruments have not hit very hard—if only because Russia’s strongest measure, the closing of oil and gas exports to Europe and North America, would severely curtail its remaining source of hard currency (hence why Russia has avoided this measure). The United States, the United Kingdom, the European Union and other Western players can wield the potent club of economic sanctions because of their dominant position within the global financial system (for example, the role of the dollar, the pound and the euro as world reserve currencies). Russia does not enjoy such a position of dominance; it will seek punitive options elsewhere.

Cyberspace offers attractive alternative options. Hackers and security planners in Moscow must be assessing how to mirror some of the sanctions’ economic and financial effects through disruptions in Western cyberspace. Scenarios are not hard to imagine. They include, for example, an interruption of computers that support stock trading at the NASDAQ or the London Stock Exchange (the Moscow Exchange index has lost almost 50 percent of its value since its February high); the processing of payments at SWIFT (from which Russian banks were recently ejected); or the data servers of JPMorgan Chase, Deutsche Bank and other banks that have dialed down their Russian operations.

Then there are the asymmetric options: acts of unpeace whose effects transcend the economic realm without crossing the lines of war. Forensic evidence shows that Russia has burrowed itself deeply within key U.S. networks. The intelligence community’s 2022 Annual Threat Assessment cautioned that Russia was honing its ability to target underwater cables and industrial control systems. Reports of Russian GRU hackers penetrating the U.S. electrical grid are commonplace. Perhaps the clearest indication of the growing risk of breakdowns in cyberspace was President Biden’s public warning on March 21 that the West should expect them.

But that is not all. Beyond the intentional effects of Russian cyberattacks are their unintentional effects. During a military invasion that appears to be failing on many fronts, Russian cyber operations are likely to be at least as brazen and indiscriminate as in the past. An illustrative case is the “NotPetya” wiper malware that the GRU unleashed upon Ukrainian businesses in 2017 but whose cascading effects disrupted commercial operations in many countries (notably interrupting the activities of the global shipping giant Maersk). A more recent example is the hack (likely by Russian state agents) of Viasat, a U.S. satellite internet provider used by the Ukrainian military and police. What is particularly significant is that the operation’s effects, like NotPetya’s, spread far beyond Ukraine. It affected thousands of wind turbines in Germany—which are still not fully operational—and disconnected tens of thousands of European internet users.

There is also the case of Finland and Sweden. Russia’s invasion of Ukraine is driving the two traditionally neutral states firmly toward NATO membership. They will face a period of critical vulnerability spanning their formal request for accession (which is expected in the coming months) and their actual accession (which requires ratification among the alliance’s 30 member states). Russia’s motives to disrupt the joiners’ information space will rise even as collective defense guarantees to protect them are still being worked out.

If and when these scenarios (or their variants) materialize, the history of cyber conflict suggests that the United States and its partners will struggle to mount a forceful response. Although they often promised to respond decisively, they traditionally failed to do so. Rather, Western nations—in particular, the United States—have been risk averse in their reactions. Officials are wary of responding in kind for fear of engaging in escalating tit-for-tat cyber exchanges in a domain marked by an inherent potential for collateral damage and blowback.

More broadly, officials struggle to interpret the legal vagaries of unpeaceful conflict—where are its red or “pink” lines?—which delays decision-making in the aftermath of major incidents. Hence they struggle to figure out how to impose costs outside of cyberspace for actions within it. In the current crisis, Western nations are fast running out of those options. The sanctions box of penalties is almost exhausted. At any rate, it is not clear that imposing them without communicating clear criteria for their lifting is an effective punishment tool (as Daniel Drezner argued). Moreover, levying sanctions for cyber activity while simultaneously imposing them for military activity risks muddling the signaling to Moscow. Where exactly, flustered Kremlin analysts might wonder, are the response thresholds for different conflict domains?

Therefrom arises another policy dilemma: whether to relax the reluctance to impose costs within Russian cyberspace. With the sanctions toolbox emptying and the aversion to direct military measures prevailing, a viable pathway to affect Russian interests—whether in response to future cyberattacks or events on the ground—might be found in cyberspace.

An intensification of conflict in cyberspace will likely require a reduction of risk aversion in the response calculus. Western nations should not reinforce the perception in Moscow that missile strikes in Kyiv are unacceptable but the interruption of banking operations in Manhattan or Frankfurt is tolerable—a perception that far predates the Ukraine war and which has lived too long. And not just the hawks in Moscow will be watching. Observers in other capitals such as Beijing or Tehran will also bear witness. Western officials will want to teach them that computer breakdowns back home will elicit unacceptable penalties.

More than ever before in the history of cyber conflict, the United States and its partners—long reluctant cyber warriors—might find cyber operations a more attractive option for strategic action abroad. Examples are not hard to conjure. Similar to past actions by U.S. Cyber Command, the operations might involve takedowns of servers of Russian information warfare outfits and hacking units (like within the GRU) or the disruption of criminal ransomware groups (which have recently shifted their resources toward patriotic activities). More boldly, they might entail the interruption of computer networks that support Russian financial or commercial operations that circumvent sanctions.

In sum, the absence of breakdowns in cyberspace likely marks a period of false stability. After Nazi Germany invaded Poland in 1939, it took eight months—the “phony war” period—for conflict to break out in earnest on the Western front. Unlike 1939, the current prospect of direct war involving large nations is low. But we expect that, like then, the conflict will eventually spread to other fronts. The common desire to avoid a direct war on the ground has increased the risk of lesser but still consequential conflict in cyberspace (although unprecedented warnings and multiple CISA alerts, such as this one, about sophisticated attack tools could already be having a deterring effect). After the aggressor shifts its focus from immediate tactical objectives to broader strategic gains, it may want to pursue them there. The Ukraine war will probably shape the next chapters in the annals of cyber conflict. Western security planners should be active authors in the saga. Beyond shoring up defenses, they should prepare their responses now.

#### Nuclear war

Clark ’16 [Bryan; 2016; Senior Fellow with the Center for Strategic and Budgetary Assessments; Bulletin of Atomic Scientists, “Undersea cables and the future of submarine competition,” vol. 72]

Given the likely economic and military impacts of cable breaks, the ability to threaten or protect submarine cables and their shore landings will be increasingly important in future conflicts. In a crisis, an aggressor could use multiple coordinated attacks on cables to compel an opponent to back down or employ them as part of an opening offensive to cut off the defender’s military forces from national commanders, intelligence data, and sensor information. Cable attacks could also be highly destabilizing, since they could prevent a nuclear-armed opponent from controlling and monitoring its strategic weapons and early-warning systems. In response, the country targeted could choose to place its nuclear weapons in a higher alert condition – or initiate a preemptive attack.

#### Russian cyberattacks cause NC3 entanglement--

Whyte ’22 [Christopher; March 31; assistant professor of homeland security and emergency preparedness in the L. Douglas Wilder School of Government and Public Affairs at Virginia Commonwealth University; World Politics Review, “Cyber and Nuclear Threats Make for a Dangerous Mix in Ukraine,” <https://www.worldpoliticsreview.com/articles/30439/cyber-and-nuclear-make-for-a-dangerous-mix-in-the-ukraine-war>]

To say that the world is closer to the brink of nuclear war today than at any time since the Cuban Missile Crisis of 1962 feels less controversial by the day. United Nations Secretary-General Antonio Guterres recently told media representatives that the “prospect of nuclear conflict, once unthinkable, is now back within the realm of possibility.”

Certainly, Russian President Vladimir Putin has been signaling a willingness to at least consider the nuclear option. In late February, he raised the readiness level of Russia’s nuclear response force, stating that Western interference in the ongoing war in Ukraine will result in “consequences greater than any you have faced in history.” And despite calming messaging from the Biden administration, further Russian mobilizations—including the deployment of nuclear missile launchers to Siberia and nuclear submarines to the Barents Sea for supposed “drills”—have continued to stoke public fears over nuclear weapons’ use. Even Russia’s recent pledge not to use nuclear weapons in Ukraine has done little to calm fears about the potential use of tactical nuclear devices, with many claiming the statement is nothing more than an attempt to bolster Moscow’s negotiating position.

Amid these rising nuclear tensions, there is one dimension of potential escalation that has not yet received much public attention: that of a cyber-enabled nuclear event. It’s time for policymakers to consider whether cyber operations affecting elements of nuclear command, control and communications, or NC3, systems could prompt nuclear escalation in the current crisis.

Experts across the West have been scrambling to place Putin’s threats, both tacit and explicit, in strategic and political context in order to gauge the possibility of a nuclear escalation leading to nuclear war. Others still have more narrowly—and perhaps more realistically—focused their analysis on what strong nuclear threats mean for fraught international engagement with Russia, and on whether Putin is likely to authorize the use of any nuclear weapons at all.

On the digital side of things, experts on cyber conflict have thus far narrowly focused their attention on the non-nuclear aspects of tactics being employed in the war. Scholars rightly predicted that the “cyber blitzkrieg” anticipated by many pundits was unlikely, pointing out that, contrary to popular portrayals, cyber instruments actually make for poor tools of coercion and battlefield augmentation. By contrast, the entry of so many nonstate and semi-state cyber forces into the conflict on both sides, including nearly 300,000 volunteers coordinated by the Ukrainian government and a pro-Russia equivalent calling itself “Killnet,” was less expected.

Even given so much robust analysis of the ongoing war, the nuclear tie-in has remained curiously underexamined. This is particularly concerning given the manner in which scholars have in recent years suggested that the logic of cyber warfare could undermine the logic of nuclear deterrence under highly specific circumstances.

Overall, experts are right to dismiss the threat of a so-called “cyberwar,” a fantastical scenario that contradicts what we know about the strategic and operational functions of cyber instruments. But could cyber operations affecting elements of NC3 prompt nuclear escalation in the current crisis? Perhaps.

The conflicting logics of cyber and nuclear warfare, when considered in the context of the present crisis, suggest real reasons to be concerned about the possibility of a cyber-enabled nuclear escalation.

Off the bat, it’s important to remember that several elements involved in that question could present themselves in a range of ways. Nuclear escalation itself could take a number of forms, from additional escalatory rhetoric or mobilization to the actual use of a nuclear weapon.

Likewise, a cyber operation impacting NC3 systems—which essentially comprise the networks of intelligence sensors, communications systems, other early warning assets and arms control mechanisms that underlie a country’s nuclear deterrent forces—could be an actual attempt to interfere with a nation’s deterrent capability by means of disrupting or taking over an element of its command system. That could be perceived by the targeted party as a prelude to a preemptive strike. But it could also be something as simple as an exploratory probe not intended to subvert system functions. Significantly, these different attacks could be hard to differentiate from the defensive perspective and so misinterpretation is entirely possible.

While countries like Russia and the United States have historically reacted with caution to nuclear provocations, uncertainties borne of the current crisis might diminish that inclination. Such uncertainties could also encourage Russian leaders to lend less weight to the cyber attribution problem—that is, the difficulty inherent in identifying the party responsible for a cyber-attack that, even under ordinary circumstances, complicates efforts to organize an appropriate response.

Even more concerning than the uncertainties bound up in interpreting certain cyber actions is the oft-cited and well-documented vulnerabilities of most states’ NC3 systems. Scholars have noted that NC3 weaknesses are widespread and, at times, quite glaring. There’s little doubt that American or Russian second-strike capabilities could be made to function effectively in the event of a nuclear war. But both sides’ reliance on a blend of new and legacy technologies to coordinate a complex detection, analysis and strike apparatus for nuclear weapons virtually guarantees errors in how these systems function as a whole. For example, in the past, American forces have lost contact with launch systems for hours due to faulty circuitry. At other times, they have detected false launches because legacy machinery was mishandled by operators.

These base conditions are cause for at least minimal concern. Both the probability of either side’s NC3 systems being vulnerable to some form of cyber compromise and the possibility that either side might mistakenly believe its NC3 is being targeted by hostile foreign cyber operations clearly create the potential for a cyber-enabled nuclear event where perceived cyber-preemption against NC3 leads directly to either coercive or real military escalation.

Admittedly, the stakes of nuclear weapons’ use suggest that escalation is not an especially likely outcome most of the time, even given these known issues. But unique circumstances might change this calculus. In particular, the conflicting logics of cyber and nuclear warfare, when considered in the context of the present crisis, suggest real reasons to be concerned.

Nuclear and cyber forces are polar opposites with regard to their operational features. The former relies on open signaling to “warn” adversaries about potential consequences in order to generate a deterrent effect. The latter typically banks on secrecy, exploiting the element of surprise to avoid giving an opponent the opportunity to upgrade their defenses. The combination of the two creates unusual commitment problems, where the coercive brinksmanship usually on display in nuclear contests might be absent as one side tries to use cyber instruments to neutralize the other’s NC3. Importantly, with cyber in the mix, the side that detects cyber activity targeting NC3 will likely also notice that the attempted breach was done in secret, creating new uncertainties over how they might respond to such an attack.

In addition to the potential weaknesses of NC3 systems, the unique political dynamics currently on display in Moscow, where Putin seems to be both isolated and dependent on politicized intelligence that has effectively undermined his decision-making, complicates this game of nuclear chicken. Given the difficult intelligence assessments and operational decisions that any government trying to reconcile cyber and nuclear logics in real-time will be required to make, this is worrisome to say the least.

And Russia’s many obvious logistical failures in launching its invasion are cause for further concern. After all, objectively assessing the risks of cyber-enabled nuclear interference requires having the ability to locate potential NC3 compromises and to mitigate any that are found. This means robust intra-service communication and deployment of expertise, neither of which has been on prominent display in Moscow when it comes to the invasion of Ukraine.

The range of cyber forces arrayed against Putin’s government in the current crisis also represents a potential source of further uncertainty that could produce cyber-prompted nuclear escalation. In addition to Ukraine’s cyber forces, which are active against Russian targets of all stripes, Kyiv has benefited from massive Western support for its operations in cyberspace, including from hacktivist elements to hundreds of thousands of volunteers that are being coordinated by Ukrainian state auspices.

Added to this is the fact that, in addition to military equipment, Kyiv has been receiving non-battlefield aid from NATO member states, particularly those that are most geographically proximate, including Poland, Slovenia and the Czech Republic. There is clearly a narrow situation here in which Russian leadership, under the current internal political conditions, may see possible Western intention in cyber events involving NC3 or related systems.

#### Escalation is likely---accidents, fog of war, and wargame simulations prove

Schneider ’22 [Jacquelyn; March 7; Hoover Fellow at the Hoover Institution at Stanford University; Foreign Affairs, “The Biggest Cyber Risk in Ukraine? How Russian Hacking Could Threaten Nuclear Stability,” <https://www.foreignaffairs.com/articles/ukraine/2022-03-07/biggest-cyber-risk-ukraine>]

Why the apparent restraint? It is almost impossible to know exactly why (or if) the Russians have indeed held back. Perhaps cyber-operations have been attempted and failed; perhaps Russian President Vladimir Putin has held his cyber-capabilities in reserve, saving them for later. Or maybe cyber-operations have taken place, but their effect—which is often virtual and not clearly attributed—will take longer to materialize.

What is known is that the conflict is far from over, and the next question becomes whether cyber-operations could play a larger role as the war turns more violent. It is likely that the next stage of conflict will more than ever be defined by planes, tanks, artillery, and soldiers. It seems unlikely, given the amount of indiscriminate damage currently being inflicted by Russia, that cyber-operations will escalate the violence of the campaign within Ukraine. That said, could cyber-operations lead to horizontal escalation, drawing NATO into the fight, for example? Or, given that the United States and Russia are the world’s largest nuclear powers, could cyber-operations escalate to the worst possible outcome—nuclear war? Recent wargaming research suggests that cyber-exploits into nuclear command and control may be enticing for states looking to neutralize a nuclear escalation threat in the midst of a conventional war, and that actors may underestimate the danger of these exploits and vulnerabilities to nuclear stability.

GETTING PULLED IN

One way cyber-operations could lead to escalation is by pulling the United States or NATO into the conflict. Mark Warner, the Democratic senator from Virginia, warned in late February that potential Russian cyberattacks on critical infrastructure in Ukraine could have accidental spillover effects on NATO countries—for instance if a Russian cyberattack on Ukrainian energy infrastructure caused an outage in a NATO neighbor like Poland. This could inadvertently trip Article 5 of NATO’s founding treaty, which states that an armed attack against one member state will be considered an attack against them all. This would be uncharted waters for NATO, which only recently publicly stated that cyberattacks might invoke Article 5 and is still ambiguous about what types of cyberattack—which range from virtual outages to data manipulations to physical damage (in extremely rare circumstances)—might be serious enough for NATO to respond with conventional retaliation.

The Biden administration has warned that the United States would respond to cyberattacks on U.S. critical infrastructure, such as the country’s electrical grid or water supply (although officials stopped short of saying how the United States would respond). So far, the United States has answered previous cyberattacks with either sanctions, law enforcement actions, or the confiscation of cryptoassets. None of these options seem likely to deter Putin at this point, and so the Biden administration may find itself in an unprecedented position of having few credible options to threaten Russia. It is certainly possible that Putin, facing a conventional war that he thinks he might lose, could attack critical infrastructure in the United States or other NATO countries in the hope that their citizens will push their governments to abandon Ukraine. The financial sector, in particular, would seem to be a logical target for Russian cyberattacks, given the damage that Western economic actions have already done to the Russian economy.

It is difficult to create widespread and long-lasting effects with cyberattacks, however, and the financial sector is the best equipped and most advanced cyber-defender in the world. Plus, research I’ve conducted with Sarah Kreps, director of the Cornell Tech Policy Lab, finds that the American public views cyberattacks as qualitatively different from conventional means of warfare—more akin to economic sanctions than bombs. Thus, cyberattacks are unlikely to provoke the kind of retaliation or emotional response that would pull the United States or its NATO allies into a war with Russia. What’s more, the United States can probably withstand the short-term damage to critical infrastructure that a Russian cyberattack might create, and such attacks might actually increase resolve to support Ukraine. This means a deliberate choice by Russia to use cyberattacks against the United States or NATO to “escalate to dominate”—deliberately ratcheting up the pressure to force Washington to back off—would likely fail.

A more troubling scenario involves accidental escalation from cyber-operations—that is, when critical infrastructure is unintentionally damaged by a cyberattack or when a cyberattack is misattributed to Russia (or the United States). This is especially dangerous for civilian infrastructure that also serves military or security purposes—for example, harming a refugee train by using a cyberattack targeting railroads also used to move troops and supplies to the front. Plus, a jumble of actors has jumped into this space, from criminal syndicates to cyber-militias to hacker collectives such as Anonymous. That increases the chances that one of these players will target civilian infrastructure, and misattribution to either Russia or the United States could needlessly trigger retaliation.

WHEN CYBER GOES NUCLEAR

By far the most dangerous form of escalation is the possibility that a cyber-operation increases the likelihood of nuclear war. How likely is such a scenario? No one may know if Russia has a cyberweapon that can target nuclear weapons (or, for that matter, whether the United States does), but there are theories and some data about how the cyber-realm might affect nuclear stability.

American policymakers have generally recognized that attempting to interfere with nuclear command, control, and communications could lead to dangerous incentives for states to launch nuclear weapons preemptively. Threats to nuclear command and control, for example, could leave states so fearful about their second-strike capability (the ability to launch a nuclear weapon in retaliation against an attacker) that in the midst of a conflict they would feel compelled to use nuclear weapons preemptively. Some scholars have warned that attacks against nuclear command-and-control systems could make it impossible to control nuclear war and keep it limited, leading to inadvertent nuclear Armageddon. Despite these fears about the dangers of attacking nuclear command and control, there was never an agreement between the United States and the Soviet Union (and subsequently Russia) to not attack each other’s nuclear command, control, and communications.

Would Russia, or even the United States and its allies, launch a cyberattack against an enemy’s nuclear command-and-control system if they could? And how might that capability affect nuclear instability? Beginning in 2017, my team at the Naval War College and the Hoover Institution ran a wargame that explored this very question. It took place over three years and included 580 players from across the world—predominantly nuclear, cyber, and military experts ranging from former heads of state to military officers to industry leaders. In our simulations, we found that teams who were told they possessed cyber-exploits against nuclear command-and-control systems overwhelmingly used them. Because cyber-operations can be denied and are covert and virtual, players appeared to believe that they did not pose too great a risk of escalation. The tools seemed too valuable not to use, especially because they have a quick expiration date, with vulnerabilities quickly patched once discovered.

#### Cyber-attacks trigger retaliation and false readings---nuclear war.

Klare ’19 [Michael; November 19; Professor Emeritus of Peace and World Security Studies at Hampshire College, Senior Visiting Fellow at the Arms Control Association; Arms Control Today, “Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation” <https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation>]

Yet another pathway to escalation could arise from a cascading series of cyberstrikes and counterstrikes against vital national infrastructure rather than on military targets. All major powers, along with Iran and North Korea, have developed and deployed cyberweapons designed to disrupt and destroy major elements of an adversary’s key economic systems, such as power grids, financial systems, and transportation networks. As noted, Russia has infiltrated the U.S. electrical grid, and it is widely believed that the United States has done the same in Russia.[12](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote12) The Pentagon has also devised a plan known as “Nitro Zeus,” intended to immobilize the entire Iranian economy and so force it to capitulate to U.S. demands or, if that approach failed, to pave the way for a crippling air and missile attack.[13](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote12)

The danger here is that economic attacks of this sort, if undertaken during a period of tension and crisis, could lead to an escalating series of tit-for-tat attacks against ever more vital elements of an adversary’s critical infrastructure, producing widespread chaos and harm and eventually leading one side to initiate kinetic attacks on critical military targets, risking the slippery slope to nuclear conflict. For example, a Russian cyberattack on the U.S. power grid could trigger U.S. attacks on Russian energy and financial systems, causing widespread disorder in both countries and generating an impulse for even more devastating attacks. At some point, such attacks “could lead to major conflict and possibly nuclear war.”[14](https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation#endnote14)

These are by no means the only pathways to escalation resulting from the offensive use of cyberweapons. Others include efforts by third parties, such as proxy states or terrorist organizations, to provoke a global nuclear crisis by causing early-warning systems to generate false readings (“spoofing”) of missile launches. Yet, they do provide a clear indication of the severity of the threat. As states’ reliance on cyberspace grows and cyberweapons become more powerful, the dangers of unintended or accidental escalation can only grow more severe.

#### Only US-Russia nuclear war causes extinction

Bostrom ’2 [Nick; Oxford philosophy professor; “Existential Risks: Analyzing Human Extinction Scenarios and Related Hazards,” nickbostrom website]

A much greater existential risk emerged with the build-up of nuclear arsenals in the US and the USSR. An all-out nuclear war was a possibility with both a substantial probability and with consequences that might have been persistent enough to qualify as global and terminal. There was a real worry among those best acquainted with the information available at the time that a nuclear Armageddon would occur and that it might annihilate our species or permanently destroy human civilization.[4] Russia and the US retain large nuclear arsenals that could be used in a future confrontation, either accidentally or deliberately. There is also a risk that other states may one day build up large nuclear arsenals. Note however that a smaller nuclear exchange, between India and Pakistan for instance, is not an existential risk, since it would not destroy or thwart humankind’s potential permanently. Such a war might however be a local terminal risk for the cities most likely to be targeted. Unfortunately, we shall see that nuclear Armageddon and comet or asteroid strikes are mere preludes to the existential risks that we will encounter in the 21st century.

#### Developing an integrated OCO doctrine among NATO allies solves cyberconflict

Lewis ’15 [James; October; Director and Senior Fellow, Strategic Technologies Program, Center for Strategic and International Studies; "THE ROLE OF OFFENSIVE CYBER OPERATIONS IN NATO’S COLLECTIVE DEFENCE,” Tallin Paper No. 8, A NATO CCDCOE Publication on Strategic Cyber Security, https://www.ccdcoe.org/uploads/2018/10/TP\_08\_2015\_0.pdf]

The central question for NATO’s cyber doctrine is how the lack of an articulated offensive cyber capability affects its ability to deter or defend. Put another way, can any military force credibly claim to have advanced capabilities if it does not include offensive cyber operations in its arsenal? Offensive capabilities, unlike NATO’s current defensive posture, involve deliberate intrusions into opponent networks or systems with the intention of causing disruption, damage or destruction. The question of NATO and offensive cyber capabilities touches on a range of sensitive political issues that militate against any change in policy in the near term.

The US has always been overly secretive about its offensive cyber capabilities, even after a flood of media leaks have made the most sensitive doctrine publicly available. This secrecy has carried over into NATO, and is unhelpful in that it increases the likelihood of opponents miscalculating as they consider the risks of using force or coercion against NATO members or interests. A lack of public discourse on offensive cyber operations undercuts the legitimacy of NATO operations by failing to build public understanding, and leaves NATO open to charges of sinister plots, since denial of offensive capabilities is not credible when two NATO members are world leaders in cyber operations.

Parallels between cyber operations and nuclear strategy are usually misleading, but cannot always be dismissed. The parallel for NATO is that cyber attack is a “weapon” with both strategic and tactical uses, which only a few NATO members possess. Unlike nuclear weapons, however, the procedures for integrating offensive cyber operations into NATO’s defensive actions are not at all obvious, if they exist. NATO will need to describe how the cyber capabilities possessed by a few of its members will support NATO’s defensive activities, and NATO’s credibility in defence requires some public discussion on the use of offensive cyber operations.

There has been a confusing debate over the merits of cyber deterrence, but one conclusion that we can draw from this discussion is that both the contribution of cyber operations to deterrence and the ability to deter cyber attack work best when embedded in a larger military force structure. Adding offensive cyber capabilities to NATO’s force structure and response doctrine will increase its deterrent capabilities – by how much is unclear, but what is clear is that a failure to add cyber capabilities will erode a credible deterrent as cyber operations are increasingly embedded into military operations.5

Beyond deterrence, two other factors point to the need for additional consideration of NATO’s public posture on offensive cyber operations. The first is that cyber techniques are essential for the kinds of combat operations that NATO forces may carry out in the future. No modern air force would enter into combat without electronic warfare (EW) capabilities; as cyber and EW merge into a single activity, air operations will require cyber support. The same is true for special forces operations. Offensive cyber capabilities will shape the battlefields of the future.

Second, NATO’s potential opponents will use cyber techniques in new ways, in what some have called “hybrid warfare”.6 These include countries traditionally of concern to NATO, but cyber threats could also come from new actors, such as Iran or North Korea, and proxy or non-state actors such as the Syrian Electronic Army. These nations and groups, using cyber techniques, now have new ways to strike NATO countries.

Military doctrine is changing as opponents seek to circumvent US military power and use a blend of political action and “influence operations”, special forces, proxies and irregular units, unconventional tactics and cyber techniques to apply force to gain their ends. Cyber techniques for political action and “influence operations” are not intended to destroy or disrupt, but rather to put coercive political pressure on targets. This new style of warfare will challenge planning for mutual defence. For these reasons, the need for more than defensive or technical cyber capabilities will increase.7

#### NATO OCOs key to win cyberwar---prevents nuclear meltdowns and financial collapse

Iftimie ’20 [Ion A.; May; PhD, Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business; NDC Policy Brief, “NATO's needed offensive cyber capabilities,” no. 10]

Cyber as a hybrid threat to, and enabler of, military operations

All future military confrontations are expected to be fought with cyber weapons. These offensive cyber capabilities in the hands of adversaries pose a significant threat to the military forces and critical infrastructure of NATO member states; and the Alliance recognizes that cyber-attacks (as hybrid threats) can be as damaging as conventional ones. This is because malicious cyber activities against computers that control physical processes can be as dangerous as threats that are purely physical in nature and could lead to explosions, nuclear meltdowns, blackouts, or financial crises. As put by NATO Secretary General, “in just minutes, a single cyberattack can inflict billions of dollars’ worth of damage to our economies, bring global companies to a standstill, ~~paralyze~~ our critical infrastructure, undermine our democracies and ~~cripple~~ our military capabilities”.4

Over the past decade, Allies have identified a steep increase in cyber activities targeting the critical infrastructure sectors that NATO military operations rely upon. Directly or indirectly, these malicious cyber activities can also disrupt the Alliance’s logistics and forward operations. NATO’s commitment to “operate and defend itself ”5 in the cyber domain as effectively as in the geographic domains came, thus, as a direct recognition of cyber as a hybrid threat to both the Allies and the Alliance.

Compared to the air, land and sea domains, the cyber domain is not constrained by national borders (although certain physical aspects of it might be located within them). This distinction between the cyber and the geographic domains is important to note, because NATO was founded in response to external military threats without the right to intervene in internal security matters, where member states maintain the monopoly over the use of force. In the cyber domain, the distinction between internal and external security threats is harder to ascertain. When integrating offensive cyber capabilities into its defence and deterrence mandate, NATO would inevitably tackle certain aspects inherent to internal security; and yet, not legally infringe on the sovereignty of the Allies as long as effects amounting to force or intervention are not employed against the physical systems residing in these nations.6 Operating in the cyber domain requires, thus, that member states better integrate their offensive cyber capabilities into NATO operations not just to win future wars, but also to avoid elements of friction between Allies, which may arise from unilateral cyber effects to defend critical infrastructure.

NATO’s adversaries in the cyber domain

Warfare in the cyber domain is already conducted against NATO member states by both state and nonstate actors. It is also conducted by NATO member states against these external threats. Within the Alliance, however, offensive cyber effects are not yet part of the mission planning process and integration of national offensive cyber capabilities into joint NATO operations is voluntary. Integrating these national offensive cyber capabilities into NATO operations, thus requires, not only a clear understanding of these capabilities, but also agreement on the cyber threat environment, characterized by the intent and capabilities of NATO’s current and/or potential future adversaries.

State adversaries in the cyber domain include Russia, China and/or Iran. These are countries known to be building offensive cyber capabilities specifically for the purpose of using them against NATO member states.7 In Russia’s case, cyber attacks were conducted against the critical infrastructure of NATO member states and partner nations, as for example against US energy infrastructure in 2017 (including against a nuclear powerplant near Burlington, Kansas)8 or against the Ukraine power grid in December 2015. China has also been conducting persistent cyber espionage using offensive cyber capabilities against core military and critical infrastructure of NATO member states for years. For this reason, the US Secretary of Defense, Mark T. Esper, remarked at the 2020 Munich Security Conference that the 5G Huawei infrastructure is a serious threat to NATO.9 Lastly, Iran’s offensive cyber capabilities have also been observed during multiple attacks against the critical infrastructure of NATO partner nations in the Middle East.

NATO adversaries in the cyber domain also include non-state actors, such as terrorist organizations. The US and the UK have conducted several successful offensive cyber operations against those entities. These offensive cyber operations had a significant force multiplier effect, in conjunction with conventional actions on the ground, at sea, in the air and from space, that contributed to the defeat of Daesh in both Iraq and Syria.10 Today, most Allies are building offensive cyber capabilities needed to deny adversaries the freedom of maneuver in the cyber domain.

The use of area denial weapon systems in the cyber domain

Anti-Access/Area Denial (A2/AD) weapon systems have traditionally been used by NATO and its member states to prevent an adversary's freedom of maneuver on land, sea or air. In the geographic domains, these capabilities include land mines, missiles (cruise, ballistic, surface to air, anti-ship, etc.), submarines, electronic warfare, and even Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) weapons. In the cyber domain A2/AD is achieved through offensive cyber operations.

Those operations have already been used for the purpose of achieving A2/AD by NATO member states in the cyber domain. This is the case of the US-led Operation Glowing Symphony (OGS), where "the United States Cyber Command reportedly acquired administrator passwords to [Daesh] websites. The passwords enabled deletion of digital content, including videos used for recruitment, from cyber infrastructure located in at least five countries outside actively hostile areas of Iraq and Syria. Similar digital content reportedly resided on cyber infrastructure in as many as 30 other States. Changing the passwords reportedly locked IS administrators out of the web- sites". OGS restricted Daesh's freedom of maneuver on networks physically residing in Iraq and Syria (which were controlled by the terrorist group), but also worldwide, where a NATO member state (the US) achieved denial of service effects against Daesh.

OGS disrupted Daesh propaganda through content removal from servers residing in multiple countries and through restricting access to physical infrastructure needed to store digital data. Combined with operational successes against ISIL on the ground, OGS actions resulted in propaganda efforts being significantly reduced on several global social media plat-forms, including Twitter. One particular offensive cyber operation acted, ipso facto, as an A2/AD platform where a NATO member state restricted access to physical networks critical for Daesh recruitment, training, radicalization, fundraising, and command and control.

Integrating offensive cyber capabilities into NATO's mandate for cyber deterrence and defence

Operationalizing warfighting capabilities in the cyber domain, beyond the traditional geographic domains, requires a new way of fighting in the 21st century, challenging the deterrence and defence mandate of the Alliance.

Speaking at the Cyber Defence Pledge Conference in London in May 2019, NATO Secretary General highlighted that for deterrence to have full effect against state and non-state adversaries, NATO and its member states must be ready to use the full range of capabilities at their disposal, to include national offensive cyber capabilities. Deterrence is the act of diminishing an adversary's intent by highlighting the excessive costs for the said adversary if it proceeds with an undesired action. In NATO's case, deterrence is achieved by highlighting to an adversary the excessive costs delivered through military means in the event of an attack against Allies. For deterrence to be successful, the adversary must believe that NATO is ready and willing to impose these excessive costs across all operational domains, to include the cyber ■UK

domain. This may call for Allies to develop offensive cyber capabilities and integrate them with NATO operations in order to collectively impose a high enough cost to deter adversaries from aggressive behaviour. To avoid escalation to total war and cyber fratricide during the fog of war, Allies must also agree on a list of Flexible Deterrent Options meant to allow for a gradual increase

of pressure in the cyber domain, and then hopefully limiting the scope and intensity of conflict in this do-main. NATO Flexible Deterrent Options in the cyber domain could include (as presented in Figure 1):

• Increasing NATO's readiness posture through cyber education, training and exercises;

• Deploying NATO Cyber Rapid Reaction teams to conduct defensive cyber operations and protecting critical infrastructure of NATO member states and/or that NATO operations rely upon;

• Increasing public awareness of malicious cyber activities and the potential for conflict in the cy-ber domain;

• Taking steps to gain the support of all NATO member states in response to the cyber threat and in accordance with commitments of the 2016 Cyber Defence Pledge and the 2018 Brus-sels Summit;

• Triggering Article 4 of the Treaty to enhance information-sharing and mutual assistance in the cyber domain;

• Making official statements addressing violations of international law in the cyber domain;

• Alerting and deploying offensive cyber opera-tions forces;

• Imposing cyber sanctions;

• Conducting offensive cyber operations to achieve A2/AD effects in the cyber domain;

Offensive cyber operations have already been used for the purpose of achieving A2/AD by NATO member states

• Triggering Article 5 of the Treaty; and

• Conducting offensive cyber operations in com-bination with other maneuver forces across all operational domains.

12 Cyber sanctions are defined here as "the actual or threatened restriction of digital transactions to affect a behavioural change by a NATO adversary through the introduction of psychological pressure against its political leaders and populace"; see A. Iftimie, "Cyber sanctions: weapo- nizing the embargo of flagged data in a fragmented internet", Journal of Information Warfare, Vol.19, No.1, 2020, p.52.

NATO Cyber Rapid Reaction teams are already equipped to conduct defensive cyber operations in support of member states if called upon. A mandate of cyber defence and security implies, however, that NATO also starts to engage in active military measures to deny, degrade, disrupt, deceive, or destroy an adversary's offensive cyber capabilities. This requires the development of not only offensive cyber A2/AD capabilities by Allies, but also the restructuring of the NATO command structures, policies, processes

To avoid escalation to total war and cyber fratricide during the fog of war, Allies must also agree on a list of Flexible Deterrent Options

(procurement, intelligence, operations, etc.) and engagements needed to integrate them by the Alliance. NATO coordination with both national and regional entities charged with cyber security aspects will, in particular, need to be enhanced. Many agreements already exist in the realm of defensive cyber at national and regional levels (as seen with the 2016 NATO-EU Technical Arrangement on Cyber Defence), but political consensus among Allies is missing on whether they should be expanded to incorporate the collective use of offensive cyber A2/AD capabilities.

Conclusion

The lack of integrated offensive cyber A2/AD capabilities undermines both the unity of the Alliance and its mandate of defence and deterrence. On the former, the lack of coordination between Allies during unilateral cyber operations could lead to friction when resulting effects infringe on Allied cyber-physical infrastructures. It could also lead to cyber fratricide, when failure to properly attribute Allied digital personas occurs during these military operations. On the latter, while most Allies are developing offensive cyber capabilities, some remain unable to face the growing number of cyber threats unilaterally.

Successful defence and deterrence in the cyber domain calls, thus, for ready collective offensive cyber A2/AD capabilities that, when integrated with NATO operations, would complement national and/ or regional responses to malicious cyber activities. If and when this integration occurs, NATO Flexible Deterrence Options would also need to be agreed upon in order to signal cyber adversaries that Allies will re-spond with one voice if attacked in the cyber domain. Ultimately, political consensus within the Alliance would still need to be built on the type of needed collective offensive cyber capabilities (such as for A2/ AD purposes) and on how to integrate them into NATO's existing operations and missions.

#### Nuclear meltdowns cause extinction

Nadesan ’14 [Majia; September 13; professor of communication at ASU, their interdisciplinary research examines the ethical implications of societal governing logics and risk-management strategies; “The Nuclear Energy Paradigm Collides with Earth Changes and Technospheric Breakdown,” The Millenium Report, themillenniumreport.com/2014/09/will-fukushima-become-an-extinction-level-event]

As Technospheric Breakdown Accelerates, Nuclear Power Generation Mishaps will Increase and Intensify

There is really no way around this eventuality. As all the nuclear power plants age, they will succumb to the micro-stresses which inevitably occur in such an ever-deteriorating environment. Most people are unaware of the true depth and breadth of technospheric breakdown since it is a concept rarely taken up by academia or the media. The following excerpts provide a wider perspective of this unavoidable byproduct of the Industrial Revolution.

Technospheric breakdown is something that occurs everywhere around the globe, 24/7, without interruption, and with tremendous repercussions. Let’s start with anything that has been manufactured in the factories of the modern world or built on the surface of the Earth. Simply put, everything is in the constant state of breaking down, degeneration, deterioration.

What does this really mean when we say that every bridge is slowly breaking down, every road is in greater disrepair with each passing day, every reservoir is gradually degrading, every office building, every factory, every school, every home, etc. most of which adhered to very low building standards in the first place?

What does it mean when the infrastructure for every sewer system, municipal water division, electrical grid, airport, railway station, etc. is in a slow but sure process of degrading and breaking down. So, unfortunately, is every nuclear power plant across the planet. (Cosmic Convergence)

What makes this ongoing process of physical degradation so insidious is that it almost always occurs subliminally. Through a gathering array of various forces throughout post-modern civilization, there does exist a sort of conspiracy of circumstances which has greatly magnified the effects of technospheric breakdown. The completed marriage between the industrial base of the Western powers and the financial class throughout the world has guaranteed that this slow motion collapse will continue unabated. How so?

Because so many corporate decisions are made according to their impact on the bottom line, many inferior nuclear power plants have been constructed around the globe. Likewise, because the mega-banks and investment houses are now dictating to a financially-strapped Nuclear Energy Industry, substandard nuclear reactors have been designed, engineered and continue to be put into operation across the planet. One only has to take a close look at the websites dedicated to decommissioned nuclear reactors or cold shutdowns or partially closed nuclear power plants or emergency actions taken at various nuclear power generation sites to grasp just how precarious a position the entire industry is currently in.

Unknown to even many of the nuclear engineers who address these issues ‘in the office’, or who fix the cascade of problems at nuke plants themselves, is the notion of slow motion, subclinical, pernicious technospheric breakdown. It often manifests in ways where cause and effect cannot be easily established because of some of the unseen forces produced by atomic fission. With that said, it should be noted that a chapter could easily be dedicated to this particular issue alone, so significant is it to the future of nuclear power generation

Then there is the problem of nuclear wastes and natural rights, yes?

No one has articulated this point better than Albert Bates in his definitive essay entitled The Karma of Kerma: Nuclear Wastes and Natural Rights (Bates, A.K., 1988)

This extremely lucid and illuminating, sober and sane treatment of the greatest ongoing environmental disaster of our times lays bare the most basic legal and human rights issues which converge around the production, treatment and storage of nuclear wastes. Were the governments of the world to read and take to heart its simple and straightforward thesis, the current incarnation of nuclear energy production would have been abandoned years ago:

The disposal of radioactive substances in a manner that anticipates their eventual partial release into the human environment imposes a health burden upon future generations that cannot be justified by any moral or legal rationale. Like an irresistible force meeting an immovable object, the concept of the greater good for the many in the present generation runs against the concept of the inalienable rights of each individual in future eras. At present, in matters involving nuclear power, our governmental agencies have taken the side of the irresistible force. But when federal agencies venture to tread beyond of the scope of the foundation principles with which the federal government was fashioned, they endanger more than human lives. At risk in the nuclear waste debate are long-held concepts of ordered liberty. (Bates A. K., 1988)

Fukushima has illustrated exactly why this elegantly stated legal concept of human rights and moral imperative is so pertinent to the public discourse. When massive amounts of radioactive wastewater are dumped into the Pacific Ocean, not only human life will be adversely affected. Marine life has been negatively impacted in ways that will take decades to observe and comprehend. The outright destruction of the environment in and around Fukushima and the Pacific Ocean must also be considered in any meaningful assessment of collateral damage.

Perhaps even more than Chernobyl, Fukushima has allowed the global community to view the whole event through the lens of legal responsibility and ethical outcomes so that new international standards can be written and implemented regarding nuclear waste conveyance and disposal. If nothing else, this discussion has raised awareness about the most nagging issue concerning the NEP. Whereas the human rights aspect confers the legal right to not be contaminated by nuclear radiation has barely been addressed by those responsible for it consequences, it now enjoys a prominent place throughout the worldwide debate.

Accidents and mishaps, manmade and natural disasters happen. Things are fixed fairly quickly in this postmodern age, and life goes on. Whether these events occur in a full-blown war zone or in the wake of a hurricane, the affected population usually does everything it can to rebuild and move on.

However, when these events take place in or near nuclear power plants, life doesn’t just go on. It often stops. Depending on the circumstances and seriousness of a nuclear event, sometimes life stops in that area for a long time.

Our civilization has now been given three unmistakable wakeup calls since the advent of the nuclear power generation era. First there was Three Mile Island in Pennsylvania, then there was Chernobyl in the Ukraine, and lastly the world is still reeling from the specter of possibilities which are presented by Fukushima.

Surely it is not by chance that these three flagrant examples of nuclear Perfect Storms occurred around the globe affecting major nations and populations centers. Each of these disasters has served to wake up whole swaths of humanity to the dangers and risks which are associated with the current Nuclear Energy Paradigm. To ignore, or deny, or refute the obvious lessons which all three nuclear catastrophes have given to humankind would be folly of the highest order.

The global impact of Fukushima, which has disseminated radionuclides (radioactive contaminants) by air and by way of the largest of the seven seas, stands as dramatic testimony to all that can go wrong — seriously wrong — with the current nuclear energy business model and method of power generation. Can it get any worse than Fukushima? That we are compelled to even ask this question speaks volumes about the true state of the affairs on that 25 square mile patch of land and contiguous sea which surround the Fukushima Daiichi nuclear disaster site.

Given this inescapable testament of nuclear folly, it is now incumbent upon the community of nations to rally around the obvious necessity of terminating the current form of the Nuclear Energy Paradigm. Why? Because when a “China Syndrome” occurs anywhere in the world, it will inevitably affect the entire planet. In other words, an INES Level 7 (Wikipedia, International Nuclear Event Scale) nuclear catastrophe does not respect borders. Nor does it discriminate between the young and old, healthy and sick, or those who live close to ground zero from those who live far away.

Therefore, any nation that chooses to set up a nuclear energy-producing operation from this point forward has an inviolable responsibility to its neighbors, as it does to the rest of the world. Likewise, those nations have a moral obligation to proceed in a manner that guarantees its neighbors will not be exposed to the consequences of its nuclear accidents, even when they are caused by duel natural disaster events as we saw at Fukushima.

Just as Europe was contaminated with radiation from Chernobyl (Yablokov, A.V., 2009), and North America has been contaminated from Fukushima, it is understood that once a nuclear catastrophe spirals out of control, the genie of radioactive contamination cannot be put back in the bottle. The entire Pacific Rim, in fact, has varying degrees of exposure to the radioactive waste water being conveyed by the ocean from Fukushima, as does the Western Hemisphere to seaborne radioactive isotopes like Cesium-137 and airborne isotopes such as Iodine-131(Center for Marine and Environmental Radiation).

Consequently, Japan is responsible for the damage wrought to the largest ocean on Earth. Have they acknowledged this? Have they approached the nations both near and far which have been affected by their cavalier and irresponsible approach to siting reactors up and down their seismic shorelines? Has the United Nations even addressed this extremely important issue known as national accountability? Or territorial sovereignty?

Conclusion

It doesn’t get very much more weighty than the ‘fallout from Fukushima’. All of the affected nations have been curiously silent on this issue. It is almost as though a conspiracy of silence has descended upon the concerned countries because of how unpredictable and intractable the nuclear containment problems have been at the Daiichi plant.

At the end of the day the current race of humanity will look back on the Fukushima Nuclear Disaster as the defining moment for both the industry and the underlying paradigm. If they haven’t already, the various stakeholders will be forced to re-evaluate the integrity of their nuclear enterprises around the globe. Hopefully, they will begin to take aggressive preemptive measures to address whatever needs to be addressed at every nuclear site still in operation.

If a decisive response is not formulated and implemented on a global scale, in light of the hard lessons learned from Fukushima, the current planetary civilization will be compelled to face up to these fatal flaws in most unpleasant ways, which will continue to manifest with each major Earth change. In a similar way, the inherent defects of the NEP will only be accentuated as technospheric breakdown accelerates. The profound and fundamental shortcomings which pervade the entire nuclear energy industry can no longer be hidden or ignored.

After all, it was the dangerous combination of willful blindness and feigned ignorance which got the world into this position in the first place.

“Does anyone in their right mind believe that nuclear power plants can ever be designed, engineered or constructed to withstand 9.0 earthquakes followed by 15 meter high tsunamis? Sorry if we offend, but such a display of so deadly a combination of ignorance and arrogance must represent the very height of hubris. Particularly in view of the inevitable consequences which have manifested at Fukushima, how is it that so few saw this pre-ordained and disastrous outcome, except by willful blindness?”

#### Economic collapse causes nuclear war---loose nukes and terrorists.

Mann ’14 [Eric; 2014; special agent with a United States federal agency, a special assistant for a U.S. Senator and served as a presidential appointee for the U.S. Congress, Graduate Degree in Homeland Security at Georgetown; “Austerity, Economic Decline, and Financial Weapons of War: A New Paradigm for Global Security,” https://jscholarship.library.jhu.edu/bitstream/handle/1774.2/37262/MANN-THESIS-2014.pdf]

The conclusions reached in this thesis demonstrate how economic considerations within states can figure prominently into the calculus for future conflicts. The findings also suggest that security issues with economic or financial underpinnings will transcend classical determinants of war and conflict, and change the manner by which rival states engage in hostile acts toward one another. The research shows that security concerns emanating from economic uncertainty and the inherent vulnerabilities within global financial markets will present new challenges for national security, and provide developing states new asymmetric options for balancing against stronger states.

The security areas, identified in the proceeding chapters, are likely to mature into global security threats in the immediate future. As the case study on South Korea suggest, the overlapping security issues associated with economic decline and reduced military spending by the United States will affect allied confidence in America’s security guarantees. The study shows that this outcome could cause regional instability or realignments of strategic partnerships in the Asia-pacific region with ramifications for U.S. national security. Rival states and non-state groups may also become emboldened to challenge America’s status in the unipolar international system.

The potential risks associated with stolen or loose WMD, resulting from poor security, can also pose a threat to U.S. national security. The case study on Pakistan, Syria and North Korea show how financial constraints affect weapons security making weapons vulnerable to theft, and how financial factors can influence WMD proliferation by contributing to the motivating factors behind a trusted insider’s decision to sell weapons technology. The inherent vulnerabilities within the global financial markets will provide terrorists’ organizations and other non-state groups, who object to the current international system or distribution of power, with opportunities to disrupt global finance and perhaps weaken America’s status. A more ominous threat originates from states intent on increasing diversification of foreign currency holdings, establishing alternatives to the dollar for international trade, or engaging financial warfare against the United States.

### NATO Cohesion Adv---1AC

#### Allied disagreements over procedures for offensive cyber operations undermine trust and confidence in NATO---establishing memoranda of understanding minimizes allied friction, and allies will say yes if the US offers meaningful intelligence

Smeets ’19 [Max; October 14; Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich, co-founder and Director of the European Cyber Conflict Research Initiative (ECCRI.eu), an organization promoting the interdisciplinary study of cyber conflict and statecraft in Europe and beyond, also an Affiliate at Stanford University Center for International Security and Cooperation; Lawfareblog, “NATO Allies Need to Come to Terms With Offensive Cyber Operations,” <https://www.lawfareblog.com/nato-allies-need-come-terms-offensive-cyber-operations>]

U.S. Army Cyber Command, Fort Belvoir, Va. (Source: U.S. Army Cyber Command/Bill Roche)

In May 2008, the U.S. Department of Defense and the German Ministry of Defence signed a memorandum of understanding concerning “Cooperation on Information Assurance and Computer Network Defense.” Computer network defense (CND) refers to actions taken on computer networks to monitor and protect those networks. It is not the only memorandum the U.S. Department of Defense has signed with allies on cyber defense.

In late 2016, U.S. Cyber Command operators wiped Islamic State propaganda material off a server located in Germany. The German government was notified in some fashion but not asked for advance consent, causing much frustration. While U.S. Cyber Command’s reported action may have violated Germany’s sovereignty, it didn’t explicitly violate the memorandum. It wasn’t an act of CND; it was a computer network attack (CNA), seeking to disrupt, deny, degrade or destroy.

This reveals an uneasy situation within cyber cooperation: Allies do not agree on the appropriate procedures and boundaries for offensive cyber operations. More specifically, there is no agreement on when military cyber organizations can gain access to systems and networks in allied territory to disrupt adversarial activity. As I have argued previously, this issue may end up causing significant loss in allies’ trust and confidence. My proposed solution: NATO allies should establish memoranda of understanding on offensive cyber effects operations in systems or networks based in allied territory.

Objectives of Out-of-Network Operations in Allied Networks

Allied states may operate in each other’s systems or networks in at least three ways: as an observer, gathering intelligence on adversarial activity in others’ networks; as a passerby, transiting through allied systems and networks to access a certain adversarial target; or as a disrupter, seeking to cause friction for an adversary’s operation within an ally’s network or system. The German case discussed above is the only publicly known case of a state acting as a disrupter in an allied network. But we can expect that more of these cases will be publicly disclosed in the future.

It has now been widely discussed that the U.S. Cyber Command has undergone a significant shift in strategic thinking away from deterrence toward persistent engagement and defend forward. Following these recent changes in strategic thinking, U.S. Cyber Command seeks to cause friction “wherever the adversary maneuvers,” operating “globally, continuously and seamlessly.” In a similar vein, NSA director and Cyber Command head Gen. Paul Nakasone writes in an article for Joint Force Quarterly: “We must … maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries.”

While one may expect adversaries to maneuver in allied networks, the U.S. is currently the only NATO state that makes causing friction in allied networks a necessary and explicit component of its strategy. Other military cyber organizations could follow in the near future.

And we already see countries moving in this direction. On Aug. 1, the Communications Security Establishment Act (CSE) came into force in Canada. According to the Canadian government, “CSE could be authorized to proactively stop or impede foreign cyber threats before they damage Canadian systems or information holdings, and conduct online operations to advance national objectives.” The Canadian government does not explicitly talk in its latest strategy about the need to operate “globally, continuously and seamlessly” or to cause friction “wherever the adversary maneuvers.” In that regard, it needs to do more strategic thinking—as other countries do—on the exact role of cyber operations on allied networks in the military context.

But the proposed memorandum of understanding on cyber offense addresses exactly this possibility.

The Goal of the Memorandum of Understanding

The goal of the proposed memorandum is to reduce discord among the allies; enhance trust, transparency and confidence between allies; and improve the effectiveness of disrupting and deterring adversaries’ operations in cyberspace.

The scope of the memorandum should include (a) developing a common notification equity framework for out-of-network operations that seek to achieve cyber effects in allied systems or networks; (b) identifying procedures for communicating the consideration and conduct of offensive cyber effects operations between states against systems or networks in allied territory; and (c) identifying technical solutions and administrative documentation required for the continuous exchange of information on offensive cyber operations.

In writing the memorandum, states first and foremost should agree on the equities involved in permitting signatories to conduct cyber effect operations in each other’s networks—and the relative weight of those equities. Equities that should be considered include (a) the ability of an actor to take action to negate known threats on or to the other parties’ networks and systems; (b) the likelihood that an action will negate known threats; (c) the imminence and scale of the threat; (d) the risk of collateral damage; (e) whether the computer system or network is government owned or privately owned; and (f) the certainty that the system or network will be used to achieve strategic effects by the adversary.

There are three open questions about the memorandum of understanding.

I. Should the Proposed Memorandum Be NATO-Wide or Bilateral?

There are benefits of negotiating a NATO-wide agreement, including ensuring it contributes to the defense of all NATO members’ networks and enhances resilience across the alliance. It could also guard against the potential that persistent engagement and defense forward might be exploited by adversaries, as I argued previously:

Adversaries don’t randomly choose which intermediate nodes to direct their operations through. If Russia has the choice to go through a network that would raise some serious diplomatic friction between the U.S. and a U.S. ally, or operate through a network that would cause no diplomatic friction for the U.S., what would it prefer? It would make sense for adversaries to operate through the networks of exactly those countries with which the U.S. has a strong relationship but that do not want the U.S. to operate within their networks causing any effects.

#### The plan reduces tensions between NATO allies with divergent cyber policy preference---that enables cohesive cybersecurity policy

Smeets ’21 [Max; Aug 6; senior researcher at the Center for Security Studies (CSS) and Affiliate at Stanford University Center for International Security and Cooperation and Research Associate at the Centre for Technology and Global Affairs, University of Oxford; Hague Center “NATO allies’ offensive cyber policy: A growing divide?,” https://hcss.nl/report/nato-allies-offensive-cyber-policy-a-growing-divide]

NATO allies have made slow but steady progress when it comes to crafting policy to deal with cyber security challenges. Yet this progress has not always been made in a collaborative fashion. Especially when it comes to the development and deployment of offensive cyber capabilities, NATO allies are increasingly diverging in policy. This is a worrying development and deserves more attention than it has so far received.

Steady progress

Member states agree on the critical need for a coherent cyber policy. Almost all NATO allies have developed both a cyber security strategy and a cyber defense strategy.[1] Some states have published updated versions over the years to reaffirm cyber security as an issue of national security importance, to tweak institutional responsibilities, or to articulate changes in the threat landscape. In addition, since 2018, most NATO allies have established a military cyber organization (either a command or unit) with a mandate to conduct cyber effect operations – that is, cyber operations intended to disrupt, deny, degrade and/or destroy.[2] There is also shared recognition that international law applies in cyberspace, although allies have yet to spell out the legal procedures for operating in this new “domain of warfare.”

These developments have been both reflected in, and aided by, policy progress made at the inter-governmental level. At the Prague Summit in 2002, NATO for the first time recognized that the Alliance should “Strengthen our capabilities to defend against cyber attacks.”[3] In 2008, at the Bucharest Summit, there was another milestone development, when NATO adopted a “Policy on Cyber Defense,” aiming to “protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack.”[4] In the same year, the Cooperative Cyber Defence Centre of Excellence – a NATO accredited international research institution – was established in Tallinn, Estonia. In 2016, at the Warsaw Summit, cyberspace was officially recognized as a “domain of operations” and allies made a Cyber Defense Pledge to enhance their cyber defenses.[5] The 2018 Brussels Summit and 2020 London Summit reiterated NATO’s commitment to implement the Cyber Defense Pledge and operationalize the Cyber Operations Center, responsible for situational awareness and the centralized planning of cyber operations and missions.[6] In January 2020, the Allied Joint Doctrine for Cyberspace Operations was published “to plan, execute and assess cyberspace operations (CO) in the context of allied joint operations.”[7]

Steady divergence

Yet when it comes to the direction of allies’ cyber policy, growing differences are apparent – especially in the development and deployment offensive cyber capabilities. First, even though most states now have – or are in the process of – establishing a cyber command, operational capabilities vastly differ across states. Whereas some governments are increasingly allocating significant resources to conduct cyber operations – and are now starting to benefit from these investments – the majority of allies still run their cyber commands on a budget of a few million a year –an amount that is insufficient for effective operations in the cyber domain.

Secondly, until a few years ago, NATO members’ strategic visions were largely aligned. National cyber strategies shared a common threat focus on operations that could potentially cause major societal havoc, such as taking down the power grid. Allies’ national strategies were also largely unified in their vision to address this threat, discussing the need for deterrence, resilience, and norms. However, this changed with the publication of the US Department of Defense’s strategy on Defend Forward and US Cyber Command’s vision on Persistent Engagement.[8] The United States emphasizes the need to cause friction “wherever the adversary maneuvers,” operating “globally, continuously and seamlessly” (potentially) below the threshold of armed attack. “We must…maneuver seamlessly across the interconnected battlespace, globally, as close as possible to adversaries and their operations, and continuously shape the battlespace to create operational advantage for us while denying the same to our adversaries,” in the words of NSA director and Cyber Command head Gen. Paul Nakasone.[9] Whereas deterrence is about changing your adversary’s cost-benefit calculus, Persistent Engagement is about taking the opportunity away from the adversary to act.[10]

Third, NATO member positions on how international law applies – particularly the obligations of states vis-a-vis sovereignty – are now more divergent than a decade ago. Whereas countries like the Netherlands and France are located on the side of the “sovereignty as a rule” camp, the United Kingdom has taken the position that a remote cyber operation by one state into another’s cyber systems or network does not violate the latter’s sovereignty.

Where to go from here?

The divergence in cyber policy across NATO member states is problematic. Allies disagree on both the goals of cyber policy and the ways and means to achieve them. This can cause tension between allies, especially when it comes to the necessity and legitimacy of operating on each other’s national systems and networks.

Some may argue that these differences result from differences in maturity. Some states simply have not caught up with the latest developments, goes the argument. This assumes a single path to cyber maturity or that the dynamics of cyberspace pull all states in the same direction. It suggests that – even without major policy coordination – allies’ cyber policies will converge over time. But a more persuasive understanding of the current trend is that even though states can learn from each other’s institutional progress, differences do not merely stem from states “lagging behind.” These states are on a different policy path. This means it requires dedicated and sustained policy attention to, at a minimum, coordinating the different policies of states – and potentially bring them closer together.

What can be done to ensure that this divergence in cyber policy does not cause further friction between allies?[11]

I have previously proposed a NATO Memorandum of Understanding (MoU) to reduce discord among the allies; the goal would be to enhance trust, transparency, and confidence between allies and to improve the effectiveness of disrupting and deterring adversaries’ operations in cyberspace.[12] The main purpose of the MoU would be to reach an agreement on the equities involved in permitting signatories to conduct cyber effect operations in each other’s networks—and the relative weight of those equities.

#### Russia will exploit divisions between NATO members to instigate nuclear crises---extinction.

Kulesa ’18 [Lukasz; February 2018; Research Director at the European Leadership Network; European Leadership Network, “Envisioning a Russia-NATO Conflict: Implications for Deterrence Stability,” <http://www.jstor.com/stable/resrep17437>]

Escalation: Can a NATO - Russia conflict be managed?

Once a conflict was under way, the “fog of war” and rising unpredictability would inevitably set in, complicating the implementation of any predetermined theories of escalation, deescalation and inter-conflict management. The actual dynamics of a conflict and the perceptions of the stakes involved are extremely difficult to predict. Simulations and table-top exercises can give only limited insights into the actual decision-making processes and interactions.

Still, Russian military theorists and practitioners seem to assume that a conflict with NATO can be managed and controlled in a way that would bring it to a swift end consistent with Russian aims. The Russian theory of victory would seek to exploit weak points in an Alliance war effort. Based on the conviction that democracies are weak and their leaders and populations are risk-averse, Russia may assume that its threats of horizontal or vertical escalation could be particularly effective. It would also try to bring home the notion that it has much higher stakes in the conflict (regime survival) than a majority of the NATO members involved, and thus will be ready to push the boundaries of the conflict further. It would most likely try to test and exploit potential divisions within the Alliance, combining selective diplomacy and activation of its intelligence assets in some NATO states with a degree of selectivity in terms of targets of particular attacks.

Any NATO-Russia conflict would inevitably have a nuclear dimension. The role of nuclear weapons as a tool for escalation control for Russia has been thoroughly debated by experts, but when and how Russia might use (and not merely showcase or activate) nuclear weapons in a conflict remains an open question. Beyond catch phrases such as “escalate to de-escalate” or “escalate to win” there are a wider range of options for Russian nuclear weapon use. For example, a single nuclear warning shot could be lethal or non-lethal. It could be directed against a purely military target or a military-civilian one. Detonation could be configured for an EMP effect. A “false flag” attack is also conceivable. These options might be used to signal escalation and could significantly complicate NATO’s responses.

Neither NATO nor its member states have developed a similar theory of victory. Public NATO documents stipulate the general goals for the Alliance: defend against any armed attack and, as needed, restore the full sovereignty and territorial integrity of member states. It is less clear how far the Alliance would be willing to escalate the conflict to achieve these goals, and what mechanisms and means it would use while trying to maintain some degree of control over the conflict.

The goals and methods of waging a conflict with Russia would probably have to be limited in order to avoid a massive nuclear exchange. Such limitations would also involve restrictions on striking back against targets on Russian territory. But too narrow an approach could put too much restraint on NATO’s operations: the Russian regime’s stability may ultimately need to be threatened in order to force the leadership into terminating the conflict. NATO would thus need to establish what a proportional self-defence response to Russian actions would involve, and to what extent cyber operations or attacks against military targets in quite different parts of Russia would be useful as tools of escalation to signal NATO’s resolve. Moreover, individual NATO Allies, especially those directly affected by Russia’s actions, might pursue their individual strategies of escalation.

With regards to the nuclear dimension in NATO escalation plans, given the stakes involved, this element would most likely be handled by the three nuclear-weapon members of the Alliance, with the US taking the lead. The existence of three independent centres of nuclear decision-making could be exploited to complicate Russian planning and introduce uncertainty into the Russian strategic calculus, but some degree of “P3” dialogue and coordination would be beneficial. This coordination would not necessarily focus on nuclear targeting, but rather on designing coordinated operations to demonstrate resolve in order to keep the conflict below the nuclear threshold, or bring it back under the threshold after first use.

Relying on concepts of escalation control and on lessons from the Cold War confrontation might be misleading. The circumstances in which a Russia-NATO conflict would play out would be radically different from the 20th century screenplay. Moreover, instead of gradual (linear) escalation or salami tactics escalation, it is possible to imagine surprizing “leap frog” escalation, possibly connected with actions in different domains (e.g. a cyberattack against critical infrastructure). Flexibility, good intelligence and inventiveness in responding to such developments would be crucial.

Conflict termination

Russian and NATO assumptions regarding conflict termination would most likely not survive the first hours of an actual conflict. Both sides are capable of underestimating the resolve of the other side to prevail in a conflict and the other side’s willingness to commit the necessary resources and endure the costs, especially once both sides start committing their political capital and resources and the casualties accumulate.

#### NATO cohesion checks numerous existential crises.

Gallagher ’19 [Mike and Colin Dueck; January 2019; Representative for Wisconsin’s Eighth District in the U.S. House of Representatives; Professor in the Schar School of Policy and Government at George Mason University; National Review, “The Conservative Case for NATO,” <https://www.nationalreview.com/2019/01/nato-western-military-alliance-bolsters-american-interests/>]

The conservative case for NATO is not that it strengthens liberal world order. Rather, the conservative case for NATO is that it bolsters American national interests. In an age of great-power competition, as identified by the Trump administration, America’s Western alliance provides the U.S. with some dramatic comparative advantages. The United States, Canada, and their European allies have a number of common interests and common challenges with regard to Beijing, Moscow, terrorism, cyberattacks, migration, nuclear weapons, and military readiness. NATO is the one formal alliance that allows for cooperation on these matters. It is also the only alliance that embodies America’s civilizational ties with Europe — a point forcefully made by President Trump when he visited Poland in 2017. Properly understood, NATO helps keeps America’s strategic competitors at bay, pushing back on Russian and Chinese influence. In all of these ways, the U.S. alliance system in Europe is a bit like oxygen. You may take it for granted, but you’ll miss it when it’s gone.

#### The plan restores faith in NATO’s credibility across domains---that spurs allied challenges to Chinese aggression in cyberspace

Odgaard ’22 [Liselotte; April 25; Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich, co-founder and Director of the European Cyber Conflict Research Initiative (ECCRI.eu), an organization promoting the interdisciplinary study of cyber conflict and statecraft in Europe and beyond, also an Affiliate at Stanford University Center for International Security and Cooperation; Washington Quarterly, “NATO’s China Role: Defending Cyber and Outer Space,” 45:1]

Looking to the future, NATO’s success in establishing transatlantic mechanisms for cyber and outer space safeguards and consultation will be crucial to allow NATO a key role in taking on the China challenge in ways that help restore faith in NATO’s credibility as a provider of collective defense in all domains. It will also assist NATO in straddling the chasm between member states prioritizing threats from either China, Russia, the Middle East, or North Africa, since cyber and space threats potentially stem from all of them, and the effectiveness of cyber and space defense mechanisms do not necessarily depend on geographical origin.

Cyber and space would allow NATO a key role in the China challenge without prioritizing China

Improved communication between NATO and the EU will be essential for NATO to successfully address the military aspects of cyber and space threats. The framework for permanent EU-NATO relations, Berlin Plus, was concluded in March 2003. It allows for the exchange of classified information, the EU’s use of NATO assets and capabilities for EU-led crisis management operations, and the establishment of consultation arrangements.31 Due to disagreements over responsibilities and jurisdiction, however, meaningful coordination did not take place until July 2016. On this occasion, NATO and the EU issued a joint declaration stating their intention to work together on security and defense responses to unprecedented challenges emanating from the South and East of the Euro-Atlantic area.32 During Biden’s visit to Brussels in June 2021, NATO promised to strengthen cooperation with the EU on promoting peace and stability including protecting critical infrastructure, strengthening resilience, maintaining a technological edge, and addressing challenges to a rules-based order.33 The EU-US summit statement from the same visit merely reaffirms support for robust NATO-EU cooperation and promises to strengthen the partnership.34 At the level of policy implementation, it is clear when talking to NATO and EU officials that usually they do not coordinate their strategies and tactics for countering China challenges.35

The EU-US summit statement’s negligible mention of cooperation with NATO indicates that the ball is in NATO’s court if strengthening NATO-EU coordination is to take place. French and German concerns about entrapment are a major barrier to meaningful NATO-EU cooperation. The area of cyber and space security may allow NATO to work around this roadblock. In line with the EU’s practice of supporting the efforts of groups of member states to take the lead on issues where EU institutions cannot trump sovereignty, in the area of cybersecurity the EU has decentralized implementation to work around national resistance. This has allowed the EU to respond collectively and effectively to cyberattacks in Europe, primarily through bolstering capacities and law enforcement cooperation.36 However, the EU is not yet a globally influential and effective cyber-power because differences among member states over issues such as whether to prioritize tech sovereignty or Europe’s global tech competitiveness prevent the EU from acting in unison on the global stage.

The first US-EU TTC meeting held in September 2021 was an important step in strengthening the EU’s global position in cooperation with the United States, and hence called into question whether NATO has a role to play in cyber security.37 The next couple of years will demonstrate whether the EU and the US are able to focus on becoming mutually supportive global cyber security guardians by cooperating on strengthening investment screening, export controls, and rebalance global supply chains in semiconductors. The successful implementation on both sides of the Atlantic of the recommendations of the TTC working groups will determine if transatlantic cooperation positions the US and the EU as global partners in guarding cyber space. In part, this will depend on the EU’s ability to forge common positions that meet the US halfway on issues such as tech sovereignty and data privacy, points of contention through which transatlantic relations have been marred by conflict.

The potential convergence of transatlantic views on cybersecurity leaves room for NATO to play a significant role because the EU is a civilian and economic, rather than military, set of institutions. The NATO summit in Brussels in 2018 carved out a role for NATO which the EU cannot fulfill, allowing NATO members to integrate their sovereign cyber capabilities into NATO operations and missions.38 However, compared to the EU’s major role in cyber, NATO’s role is negligible. As EU civil-military cooperation ramps up in enhancing Europe’s autonomous defense profile while allowing US companies a role in this effort, the union looks set to become an even more dominant actor in transatlantic cyber defense. Because NATO is a military organization, it has the procedures and instruments to position itself in a key role in coordinating and implementing the military aspects of cyber defense between the US and Europe. The multinational cybersecurity effort which is confronting the global threat posed by Chinese state-sponsored cyberattacks involves NATO, the EU, Australia, New Zealand, and Japan, and sets NATO off to a good start in enhancing its profile in countering Chinese challenges to transatlantic cybersecurity.39 However, it remains to be seen if it manages to deliver mechanisms that succeed in integrating allied responses in the military sector in a way that complements US and EU cyber defense initiatives.

In outer space, the EU is also increasingly active, recognizing the need to deepen investments in areas such as satellite navigation, earth observation, space situational awareness, and secure communications, which are all central to enhanced space security. The EU has established the EU Agency for the Space Programme, which has oversight over everything the EU does in orbit as a bloc. Moreover, the EU uses the European Space Agency (ESA) as technical advisor and industrial procurement agent. This setup allows the EU to become more agile, dynamic, and innovative in space as rapid industrialization is taking place with US entrepreneurs and well-funded Chinese space programs in leading roles.40 In the pipeline are a next generation of Europe’s satellite-navigation system, Galileo, and an extension of the scope and capabilities of its Copernicus-Sentinel spacecraft, which monitors the state of the planet. The EU focuses on ensuring that Europe has independent space capabilities, but it does not develop instruments such as space weapons systems.41

In the outer space realm, NATO has tremendous potential for playing a key role in developing instruments in the military sector that involve European and US space capabilities. NATO’s decision to declare outer space an operational domain at the London summit in 2019 is a first step in allowing NATO an active role in addressing growing anti-satellite threats from China and Russia.42 With the US as the leading power in outer space and with the EU developing its space platforms to enhance situational awareness and security, NATO has the tools to work out a common transatlantic definition of the anti-satellite challenges that need to be addressed. The establishment of mechanisms that ensure coordination across military NATO commands regarding intelligence gathering and the interface between cyber and space defense, as well as civilian and military occurrences and initiatives, would potentially strengthen the ability of allies to counter anti-satellite threats considerably. As with cyber, NATO must first integrate the space issue into all its organizational and operational structures, and secondly, develop mechanisms that focus on coordination between US and European capacities on the basis of a common understanding of the challenges to be addressed.

NATO has the tools to work out a common transatlantic definition of anti-satellite challenges

NATO’s Role in the Global Commons

NATO can only be as effective as its member states allow it to be. NATO reflects the state of transatlantic relations: are US and European security outlooks sufficiently compatible such that the alliance is able to address threats from China collectively? This question is reflected in how well they manage to define common challenges and establish mechanisms that allow them to address these challenges together. NATO was a natural center of security focus for Washington when Europe was the main arena for US-Soviet deterrence. Today, the Indo-Pacific competes for US attention and resources as competition with China has moved to the center stage of US security and defense priorities.

The strategic shift in US priorities does not mean that Europe cannot continue to remain a significant influence on global security dynamics. The EU has demonstrated its continued relevance in the security realm, not merely by relying on its role as a major trade bloc, but also by reforming the interplay between member states and EU institutions to avoid being paralyzed by consensus requirements, which apply in most areas outside the trade sector. This is done by providing platforms for member states to start initiatives. If successful in attracting support within the union, the initiatives are consolidated by supportive mechanisms and programs.43

NATO is not the EU and hence should not duplicate its methods. The EU is driven by the urge to secure the continued influence of its member states on major global issues. NATO’s raison d’être is to facilitate transatlantic cooperation in the military sector to counter common threats and challenges. Coordination is complex at a time when US and European security outlooks are drifting apart in terms of threat perceptions and priorities. At the same time, fears of entrapment stifle NATO’s efforts to update its relevance, principally because key members such as France and Germany are not interested in NATO taking on China as a threat.

Nevertheless, NATO’s agreement to define China as a challenge promises opportunities for positioning the alliance in a key role in transatlantic relations. Because cyber and space encompass threats from other adversaries such as Russia and Iran, these domains are a good place to start taking on China as they do not require that China be singled out as a threat. By taking on the responsibility for coordinating US and European definitions of cyber and outer space threats in the military sector, integrating these domains in all organizational and operational NATO structures, devising mechanisms for the member states to address cyber and outer space threats, and by facilitating intelligence exchange and management of the vulnerabilities produced by civil-military interaction and overlapping interfaces between the cyber and space sectors, NATO can demonstrate its continued relevance for transatlantic security in an era where threats are increasingly global and transcend geographical boundaries. There’s no time like the present.

#### NATO can proactively dissuade Chinese hybrid efforts---solves espionage and cyber-backed IP theft

Speranza ’20 [Lauren; July 8; director for trans-Atlantic defense and security at the Center for European Policy Analysis; Foreign Policy, “China Is NATO’s New Problem,” https://foreignpolicy.com/2020/07/08/china-nato-hybrid-threats-europe-cyber]

Over the past decade, Chinese companies have invested billions of dollars throughout Europe—buying up critical infrastructure and increasing Beijing’s political clout across the continent. As Chinese firms, often with strong ties to the state and Chinese Communist Party (CCP), acquire parts of sensitive ports, pipelines, and telecommunication networks, China’s incursions into Europe’s security umbrella are drawing serious concern.

But NATO, long worried about Russia, has largely been silent on China. Now, that is changing. NATO Secretary-General Jens Stoltenberg recently called on the alliance to stand up to Beijing’s “bullying and coercion,” underscoring how China’s rise is fundamentally shifting the global balance of power. It’s apparent that NATO can no longer ignore the threat. If the alliance hopes to remain competitive, it will need to develop a new strategy for dealing with Beijing.

First, NATO needs a common assessment of China’s hybrid threats—a mix of diplomatic, economic, security, information, and technological actions designed to quietly undermine democratic states and institutions to Beijing’s benefit while avoiding a traditional conflict. While China’s conventional military threat in the Indo-Pacific is far from NATO’s borders, its hybrid activities are happening in the alliance’s own backyard.

Cyber-espionage, intellectual property theft, infiltration of critical infrastructure, debt manipulation, and disinformation are prime examples. While these threats may seem to fall outside of NATO’s purview, they pose serious security risks for the alliance. For instance, China’s desire to invest in Lithuania’s Klaipeda Port may not look like a problem for NATO on its surface. But its investments have worrying strings attached that give China operating control over the infrastructure. That control could decrease allies’ willingness to move military forces—including sensitive technologies—through the port and its surrounding networks. This could lead to disrupted planning and fewer military exercises, decreasing NATO’s ability to defend the Baltic States during a crisis with Russia. This could also open the door for pragmatic collaboration between China and Russia to undermine trans-Atlantic security.

Allies need to forge a shared understanding of these risks through information-sharing and dialogue—no small feat for countries that do not see eye to eye on China. Some are even willing to ignore such vulnerabilities, due to economic benefits or disenchantment with trans-Atlantic institutions. The United States has a critical role to play in getting allies on the same page and setting common goals for countering China’s hybrid activities.

Second, NATO needs to focus on public diplomacy. NATO has an important role to play in the battle against the CCP’s global narratives, which Beijing promulgates through hybrid activities. To defend the trans-Atlantic values on which the alliance is built—freedom, democracy, rule of law, and human rights—NATO should clearly communicate China’s violations of these principles and its propaganda efforts to cover them up. (These include, among others, human rights abuses against ethnic Uighurs in Xinjiang and violations of the U.N. Convention on the Law of the Sea in the South China Sea.) NATO should also enhance its outreach to key partners in the Indo-Pacific, such as Australia, Japan, New Zealand, and South Korea, which can serve as important counterweights to Chinese influence in the region. Effective public messaging also means getting serious about attributing the blame for attacks, as the European Commission recently did over Chinese disinformation around COVID-19, to raise the pressure on Chinese officials. Trans-Atlantic countries have struggled to shape China’s behavior because they cannot prove malign intent or agree to call out Beijing for its subversive efforts. Allies should develop clearer guidelines—what needs to be proved, by whom, and to what degree—to enable collective attribution. NATO is strongest when it speaks with one voice. It should use that voice to demand transparency and change from China.

Third, the alliance should step up its counteroffensive. China’s hybrid actions intentionally blur the lines between what is legally permissible, politically inappropriate, and downright escalatory.

This makes it difficult for leaders to determine appropriate responses, producing a reactionary approach thus far. But an intensifying geostrategic competition has already begun. To compete in this environment, the trans-Atlantic community needs a more proactive approach. Rather than waiting for China to invest in the next major European port, allies should coordinate legislation to prevent the riskiest Chinese acquisitions. And rather than waiting for more Chinese cyberintrusions, allies should collaborate on responsible, targeted offensive cyberactions. Over time, this would help dissuade China from manipulating investments in critical infrastructure, conducting cyber-espionage, and other hybrid activities. While adopting a more offensive posture remains controversial among certain allies, it is gaining traction across Europe and is strongly supported in Washington. Although NATO, as a defensive alliance, should not implement such a counteroffensive, policymakers should leverage it as the primary forum to coordinate actions among willing nations.

Fourth, NATO needs to deepen its cooperation with other key players, such as the European Union and the private sector. Where NATO lacks the mandate and means, the EU and multinational businesses play critical roles in developing, implementing, and enforcing the legislation and financial incentives necessary to counter Chinese hybrid threats. Complementary to that, NATO and its allies can focus on providing intelligence, defending cyberspace, developing capability targets for new technologies, conducting exercises and contingency planning, informing resilience requirements for secure infrastructure, and bolstering deterrence. Despite the political obstacles that impede more formal NATO-EU cooperation, allies should look to the European Centre of Excellence for Countering Hybrid Threats in Helsinki to bring together NATO and EU staff, national officials, and industry voices in one place to align their counter-hybrid policies for China.

The Chinese government’s manipulative efforts around the coronavirus have thrust China’s hybrid activities to the center of trans-Atlantic debates. Policymakers need to seize the moment and respond by “using NATO more politically,” in Stoltenberg’s words. NATO is first and foremost about its nations. In the fight against China’s hybrid threats, these nations bring much more to the table than military power alone. They have access to a broad range of tools—military, political, economic, technological, and information—which the alliance can use to its collective geopolitical advantage in the competition with China. What NATO needs now is a strategy to leverage those tools in a coordinated manner. That will go a long way in solving NATO’s China problem.

#### It’s an existential threat to US power and the Western security architecture---deterring cyber aggression is key

Fleming ’18 [T. Casey; Feb 5; Chairman and Chief Executive Officer of BLACKOPS Partners Corporation, the leading intelligence, think tank, cybersecurity and asymmetrical hybrid warfare advisors to senior leadership of the world’s largest organizations; “Top Threat to Business, National Security and the American Dream: Detailing the New Global Competitive Model Based on Cyber and Asymmetrical Hybrid Warfare,” https://smallwarsjournal.com/jrnl/art/new-global-competitive-model-based-cyber-and-asymmetrical-hybrid-warfare]

Over the past three decades, as the US military trained in conventional, nuclear, and counterinsurgency warfare, the Chinese Communist Party (CCP) engaged and perfected over forty methods of warfare intended to permanently destabilize and weaken the US both economically and militarily. At the same time, China rapidly grew its economy and military without the required time or investment in innovation. The result is that the US is hemorrhaging its economic strength and relevance at the rate of $5 trillion in lost total value each year, or one-third of the U.S. Gross Domestic Product (GDP).

General (Ret.) Keith Alexander, former Director of the National Security Agency (NSA) and Commander of US Cyber Command, referred to China’s theft of American innovation and intellectual property as “the greatest transfer of wealth in history.”

Over time, a weakened US economy directly reduces the strength and effectiveness of the US military. Further, when a country is manipulated by an adversary to lose one-third of the value of its economy each year, it is at war. What does this mean for US citizens? A cumulative and shocking permanent reduction in quality of life to those organizations that "don't know what they don't know."

Asymmetrical Hybrid Warfare

Clear and Present Existential Threat

Over the past thirty years, the US government and private sector have advanced their policy of full-cooperation, including substantial financial and technological investment in China, under the belief that they were moving towards a more democratic, free-market society while China played intentional misdirection and deception. In 1986, month number three, the Communist Party of China (CCP) officially declared Asymmetrical Hybrid Warfare (AHW) against the US and its western allies in its nation-state Program 863. This strategy commits all of China with its strict Communist military rule to engage in any and all methods to become on par with, surpass, and dominate the West at any and all cost. China’s ultimate objective is to harvest and perpetuate the Chinese Dream through the extraction and extinguishing of the American Dream, the American way of life and ending Western dominance. The Chinese strategy is that a er 200 years of Western global dominance, it is their destiny to reverse roles with the US and to relegate it to a forced supplier with a much lower quality of life. To underscore this strategy, China refers to the last century as “the century of great humiliation.” It must also be emphasized that AHW strategy is rooted in Unrestricted Warfare or “war without rules.”

Death by a Thousand Cuts

The Modern Battlefield is Everywhere

AHW has been established as the future of modern warfare and business strategy across the globe. It is ultimate warfare that has many forms: economic warfare, transaction warfare, industrial warfare, drug warfare, and propaganda warfare, to name only a few. Each method is characterized by the non-utilization of military or conventional warfare that is typical of aircraft, ships, troops, and weapons. While China continues to aggressively develop and expand its military, it does so with the belief that if it must resort to the use of conventional or nuclear warfare, it has ultimately failed at achieving the enemy’s capitulation through the combined methods of AHW. In the business sector, AHW has become the “New Global Competitive Model” where the “winner takes all.” Soon, China will dictate transactions and pricing based on its market dominance. As businesses rush to move to “digital transformation” and “Big Data,” each must perform a 180° cybersecurity transformation based on sensitive data protection and adversarial motives as a means to survive. Currently, AHW is the primary focus of our adversaries: China is, by far, the most successful at methodically executing all AHW methods, while Russia, North Korea, Iran, and India engage in relatively few methods at present. The strategy is to continuously inflict damage or cuts to every facet of American society just below the pain threshold where we choose not to act. We believe that China has achieved an estimated 750 cuts towards “death by a thousand cuts.” (Sun Tzu)

Definition

AHW is characterized as unconventional, non-military, multi-method strategic warfare based on deception and void of any rules between countries where economic and military power, strategy and tactics differ significantly. The attacking country exploits inherent weaknesses through numerous uneven and seemingly unrelated AHW methods that are designed to destabilize the unwitting target country for ultimate and complete economic and military submission. Extensive use of misinformation and plausible deniability are used to deceive and deflect suspicion of the strategy or its methodical advancement. Hybrid warfare is a military strategy that blends conventional warfare, asymmetric warfare, irregular warfare, offset warfare, non-linear warfare, and cyber warfare. AHW is rooted in unrestricted warfare (war without rules where “everything is fair play”) which is also described as “anything warfare.” Source: BLACKOPS Partners Corporation

Culture Disparity as a Strategic Weapon

It is important to note the striking contrast between the two cultures of the US and Communist China. It is this great divide that has contributed to China’s manipulation and acceleration of AHW against the US. The CCP believes its “legalism” philosophy of supreme law and people are superior to America’s constitutional democracy underpinned by justice, religion, a Creator, and “all men are created equal.” Since 1949, the CCP have controlled all aspects of China’s commerce, military, and daily life where intellectual property is state-owned, all data is controlled, and it is the national duty of all citizens to support the regime, including all aspects of espionage. The Communist culture is further defined not by “winning vs. losing”; rather, “living vs. dying.” It is this extreme belief that underscores China’s support for AHW in its conflict with the US. Another distinction is that the CCP controls every business transaction with US companies. In many cases, the CCP resembles a powerful organized crime faction, through its shell business partnerships and facades. There is no distinction between China’s organized crime, military, or government. This places every US business partnership or transaction with China at extreme risk.

Critical Role of Intelligence

China’s uncompromising commitment to AHW demonstrates a national objective to destroy the US and its Western allies. The critical nucleus that drives the AHW strategy is the complete dependence on stolen innovation, intellectual property (IP), sensitive data, and military secrets - namely intelligence. For over thirty years, China has orchestrated the most impressive and sophisticated strategy with an intricate global network of espionage and industrial theft to fuel AHW. In recent years, an emboldened China has demanded the complete surrender of all intellectual property during the process of contracting current international business transactions. Conversely, intelligence plays a critical role for the US to gauge the executional success of AHW, changes in strategy, and individual and cumulative damages.

Cyber Warfare as the Key Accelerator

China has successfully intertwined Cyber warfare as the key AHW accelerator due to its relatively minimal investment and the difficulty of attributing actions to a specific actor. At the same time, cybersecurity remains fundamentally broken in the US and the West due to failed cyber strategies, lack of awareness of AHW, lack of accountability, overconfidence, and over-dependence on inherently fallible cybersecurity products. This is made clear by the “new normal” of the increased trend in number, frequency, and resulting total damages from cyberattacks.

Current estimates place global cyber losses at $6 trillion by 2021, with expectations that this will increase further in the future, according to Cybersecurity Ventures. Cyber warfare and cybersecurity have become a “whole of society” challenge that requires a unified, elevated strategy and 180° approach to combat the morphing threat. As we examine today’s cybersecurity environment, we are looking through the wrong end of the telescope. It is only in the context of AHW that we can begin to fully understand cybersecurity’s critical role for successful defense, protection, and resolution. We have learned to treat cybersecurity first and foremost as a human problem and a senior leadership challenge, not solely an IT issue.

#### China’s political revisionism will cause existential great-power war AND obliterate the LIO.

Wang ’19 [Fei-Ling; October 24; Professor at the Sam Nunn School of International Affairs, Ph.D. from the University of Pennsylvania; The Cipher Brief, “The China Order: A Challenge for the U.S. and the World,” <https://www.thecipherbrief.com/column_article/the-china-order-a-challenge-for-the-u-s-and-the-world>]

It is no longer hard to see that the rising power and the mounting pugnaciousness of the People’s Republic of China (PRC) have become a comprehensive challenge for the United States. China’s Machiavellian policies and actions at home and abroad have turned an otherwise naturally complementary Sino-American economic relationship into a near zero-sum, if not already a zero-sum, competition for market, jobs, technology, and financial primacy. Beijing now openly flexes its new muscles in its neighborhood and beyond to resist, reduce, and replace American leadership and presence everywhere possible, seeking to undermine the U.S.-led international economic order and American-anchored collective security arrangements. The PRC has been burning billions, for example, hoping to replace the U.S. dollar with the over-printed Chinese Renminbi (RMB). Extraordinarily heavy extraction of its own economy, the world’s second largest, and its enormous foreign currency reserve resulting from the gross imbalance in U.S.-China trade have enabled the PRC to massively expand its military. That military is already the world’s second largest; its navy, for example, is projected to soon surpass the U.S. Navy in fleet tonnage. At the same time, massive but opaque spending sprees has allowed the PRC to actively procure power and proxies even inside the United States, positioning Beijing to reshape international opinions and norms more easily than ever.

What is less known, perhaps, is that the rising PRC state also seeks an overhaul of the very world order that has enabled the greatest advances of human civilization over the past few centuries – the Westphalian system of nation-states. This world order was codified in the 17th century, expanded to a global scale in the 20th century, and now is in its post-World War II and post-Cold War iteration — the so-called America-led Liberal International Order (LIO). The rise of Chinese power, under the autocracy of the Chinese Communist Party (CCP), is not just contesting U.S. national security and American global leadership but also the existing world order. Never since the heyday of the Cold War has the world seen such a full challenge to the United States and to the Westphalian system.

The CCP is leading the PRC toward a Chinese Dream of a world order in its own image, which I call the China Order. The China Order is a millennia-old political tradition and ideology that mandates a unitary, authoritarian (often totalitarian), omnipotent and omnipresent government for the whole known world. This alternative world order has had a variety of euphemisms in the long history of China: from tinaxia yitong (unification of all under heaven) and shijie datong (world’s grand harmony) in the imperial past, to Mao Zedong’s world solidarity for Communist revolution only forty years ago, to now Xi Jinping’s community of common human destiny. The China Order has powerfully revived to guide rising PRC power, under the banner of a Chinese version of globalization, ingeniously taking advantage of the various calls in our time for global governance to address transnational issues such as climate change, inequality, epidemics, and terrorism.

This China Order is normatively and practically at fundamental odds with the LIO version of the Westphalia system that enshrines comparison and competition among nations coexisting with equal sovereignty. The China Order has been widely addictive to the powerful and ambitious in history, whether they have been ethnically Han or not. It has been highly effective in practice, in great part because it became deeply legitimized and internalized in elite Chinese culture over many centuries. The China Order is now the sole acceptable model of the world under the authoritarianism known as the Qin-Han polity that the PRC now practices. But under this world order, as documented by The China Order (#ad), human civilization is socio-economically very suboptimal and hopelessly stagnant, inevitably shortchanging the lives of just about everyone, especially nonelites, as the tragic and often catastrophic history of Eastern Eurasia under the China Order before the nineteenth century amply demonstrates.

Since 1949, when the PRC restored traditional Chinese autocracy under the guise of imported Marxism-Leninism, the CCP has been ceaselessly and callously fighting its own people internally and the United States and American allies externally to preserve its monopoly over power. Only sheer exhaustion and near collapse could force the CCP to slow down and retreat, at home and abroad. External powers have influenced and facilitated the rise of PRC power, but have so far failed to transform the Qin-Han autocracy and its China Order ideal, thus remaining unable to change Beijing’s world views and global pursuits. Various, often false, rationalizations have justified the continuation of American/Western engagement with the PRC, which has greatly enriched and enabled the CCP to persist in its consolidation of power. Beijing’s push for power is nothing personal; it is a brand of authoritarianism just happens to be anchored in the remarkably persistent belief that failing to achieve control over the whole known world would spell the loss of the “mandate of heaven” and political extinction. Thus, the CCP is driven (or doomed) to methodically and opportunistically seek ever greater influence.

The rise of China, or more precisely the ever-greater power of the PRC state, represents a shift of the distribution and concentration of power in the international system (conceptually known as power transition) and an effort to reorder the units in the system and change the system’s governing norms. Chinese leaders have already openly claimed that they are now moving to the center of the world stage, leading a revolutionary change in the world order, upending the Peace of Westphalia established “four hundred years ago,” in the words of PRC leaders This points to a systemic change of world politics and a choice for all of us at the grandest possible scale: a scale that could reshape nations and redirect the path of human civilization. The PRC’s challenge is therefore greater than the struggle between the two European ideologies of Capitalism and Communism. The confrontation between the U.S.-led LIO and the PRC-dreamed China Order transcends these often vaguely defined civilizational clashes.

If the PRC challenge, the rise of an unscrupulous, ever more resourceful and determined PRC state, is not managed well and promptly, the United States will have to face a much worse choice in the not too distant future between tragic capitulation and a desperate war for its national security and world leadership and for the way in which humankind is organized worldwide. In the age of many kinds of weapons of mass destruction, this will be a harrowing decision.

Of course, one may argue that the grandiose China Dream of a China Order may be just another pretentious way for the CCP to invoke traditional, nationalist, and populist ideals to justify its autocratic governance of the Chinese people forever, similar to the splendid slogans and missions fabricated by many other dictators. Perhaps the highly insecure CCP leadership is fighting for its survival, not world domination. However, words have consequences. Propaganda and dilution often greatly mesmerize and mislead the pretenders themselves. More importantly, the CCP has been steadily following up its words with action and money for years (basically nonstop since 1949); it has just pledged over 10 times the total sum of the Marshall Plan (in today’s dollars) for its Belt and Road Initiative alone, for instance.

As the logic of the China Order dictates, the rising Chinese power will not stop short of unseating the United States and reordering the world, unless Beijing’s Qin-Han polity is transformed and/or the ever richer and more powerful PRC is checked. The alternatives, American capitulation or world war, are horrific to contemplate, but not necessarily impossible. Unlike in Hollywood, the “good” guys do not always win necessarily in the real world. A mighty autocracy that tightly controls one-fifth of humankind, willfully spends a disproportionately larger portion of the fruits of the world’s second largest economy, and vows (even if only hypocritically) to reform and reorder the world under its leadership, is and will always be a mortal challenge to the national security of the United States. America’s global position and way of life, world peace, and the overall world order all rest on how the PRC challenge is managed—soon.

#### Extinction---rogue tech, bio arms-racing, and climate change.

Harari ’18 [Yuval; September 26; Professor of History at Hebrew University of Jerusalem; "We need a post-liberal order now," https://www.economist.com/open-future/2018/09/26/we-need-a-post-liberal-order-now]

If the liberal order is collapsing, what new kind of global order might replace it? So far, those who challenge the liberal order do so mainly on a national level. They have many ideas about how to advance the interests of their particular country, but they don’t have a viable vision for how the world as a whole should function. For example, Russian nationalism can be a reasonable guide for running the affairs of Russia, but Russian nationalism has no plan for the rest of humanity. Unless, of course, nationalism morphs into imperialism, and calls for one nation to conquer and rule the entire world. A century ago, several nationalist movements indeed harboured such imperialist fantasies. Today’s nationalists, whether in Russia, Turkey, Italy or China, so far refrain from advocating global conquest.

In place of violently establishing a global empire, some nationalists such as Steve Bannon, Viktor Orban, the Northern League in Italy and the British Brexiteers dream about a peaceful “Nationalist International”. They argue that all nations today face the same enemies. The bogeymen of globalism, multiculturalism and immigration are threatening to destroy the traditions and identities of all nations. Therefore nationalists across the world should make common cause in opposing these global forces. Hungarians, Italians, Turks and Israelis should build walls, erect fences and slow down the movement of people, goods, money and ideas.

The world will then be divided into distinct nation-states, each with its own sacred identity and traditions. Based on mutual respect for these differing identities, all nation-states could cooperate and trade peacefully with one another. Hungary will be Hungarian, Turkey will be Turkish, Israel will be Israeli, and everyone will know who they are and what is their proper place in the world. It will be a world without immigration, without universal values, without multiculturalism, and without a global elite—but with peaceful international relations and some trade. In a word, the “Nationalist International” envisions the world as a network of walled-but-friendly fortresses.

Many people would think this is quite a reasonable vision. Why isn’t it a viable alternative to the liberal order? Two things should be noted about it. First, it is still a comparatively liberal vision. It assumes that no human group is superior to all others, that no nation should dominate its peers, and that international cooperation is better than conflict. In fact, liberalism and nationalism were originally closely aligned with one another. The 19th century liberal nationalists, such as Giuseppe Garibaldi and Giuseppe Mazzini in Italy, and Adam Mickiewicz in Poland, dreamt about precisely such an international liberal order of peacefully-coexisting nations.

The second thing to note about this vision of friendly fortresses is that it has been tried—and it failed spectacularly. All attempts to divide the world into clear-cut nations have so far resulted in war and genocide. When the heirs of Garibaldi, Mazzini and Mickiewicz managed to overthrow the multi-ethnic Habsburg Empire, it proved impossible to find a clear line dividing Italians from Slovenes or Poles from Ukrainians.

This had set the stage for the second world war. The key problem with the network of fortresses is that each national fortress wants a bit more land, security and prosperity for itself at the expense of the neighbors, and without the help of universal values and global organisations, rival fortresses cannot agree on any common rules. Walled fortresses are seldom friendly.

But if you happen to live inside a particularly strong fortress, such as America or Russia, why should you care? Some nationalists indeed adopt a more extreme isolationist position. They don’t believe in either a global empire or in a global network of fortresses. Instead, they deny the necessity of any global order whatsoever. “Our fortress should just raise the drawbridges,” they say, “and the rest of the world can go to hell. We should refuse entry to foreign people, foreign ideas and foreign goods, and as long as our walls are stout and the guards are loyal, who cares what happens to the foreigners?”

Such extreme isolationism, however, is completely divorced from economic realities. Without a global trade network, all existing national economies will collapse—including that of North Korea. Many countries will not be able even to feed themselves without imports, and prices of almost all products will skyrocket. The made-in-China shirt I am wearing cost me about $5. If it had been produced by Israeli workers from Israeli-grown cotton using Israeli-made machines powered by non-existing Israeli oil, it may well have cost ten times as much. Nationalist leaders from Donald Trump to Vladimir Putin may therefore heap abuse on the global trade network, but none thinks seriously of taking their country completely out of that network. And we cannot have a global trade network without some global order that sets the rules of the game.

Even more importantly, whether people like it or not, humankind today faces three common problems that make a mockery of all national borders, and that can only be solved through global cooperation. These are nuclear war, climate change and technological disruption. You cannot build a wall against nuclear winter or against global warming, and no nation can regulate artificial intelligence (AI) or bioengineering single-handedly. It won’t be enough if only the European Union forbids producing killer robots or only America bans genetically-engineering human babies. Due to the immense potential of such disruptive technologies, if even one country decides to pursue these high-risk high-gain paths, other countries will be forced to follow its dangerous lead for fear of being left behind.

An AI arms race or a biotechnological arms race almost guarantees the worst outcome. Whoever wins the arms race, the loser will likely be humanity itself. For in an arms race, all regulations will collapse. Consider, for example, conducting genetic-engineering experiments on human babies. Every country will say: “We don’t want to conduct such experiments—we are the good guys. But how do we know our rivals are not doing it? We cannot afford to remain behind. So we must do it before them.”

Similarly, consider developing autonomous-weapon systems, that can decide for themselves whether to shoot and kill people. Again, every country will say: “This is a very dangerous technology, and it should be regulated carefully. But we don’t trust our rivals to regulate it, so we must develop it first”.

The only thing that can prevent such destructive arms races is greater trust between countries. This is not an impossible mission. If today the Germans promise the French: “Trust us, we aren’t developing killer robots in a secret laboratory under the Bavarian Alps,” the French are likely to believe the Germans, despite the terrible history of these two countries. We need to build such trust globally. We need to reach a point when Americans and Chinese can trust one another like the French and Germans.

Similarly, we need to create a global safety-net to protect humans against the economic shocks that AI is likely to cause. Automation will create immense new wealth in high-tech hubs such as Silicon Valley, while the worst effects will be felt in developing countries whose economies depend on cheap manual labor. There will be more jobs to software engineers in California, but fewer jobs to Mexican factory workers and truck drivers. We now have a global economy, but politics is still very national. Unless we find solutions on a global level to the disruptions caused by AI, entire countries might collapse, and the resulting chaos, violence and waves of immigration will destabilise the entire world.

This is the proper perspective to look at recent developments such as Brexit. In itself, Brexit isn’t necessarily a bad idea. But is this what Britain and the EU should be dealing with right now? How does Brexit help prevent nuclear war? How does Brexit help prevent climate change? How does Brexit help regulate artificial intelligence and bioengineering? Instead of helping, Brexit makes it harder to solve all of these problems. Every minute that Britain and the EU spend on Brexit is one less minute they spend on preventing climate change and on regulating AI.

In order to survive and flourish in the 21st century, humankind needs effective global cooperation, and so far the only viable blueprint for such cooperation is offered by liberalism. Nevertheless, governments all over the world are undermining the foundations of the liberal order, and the world is turning into a network of fortresses. The first to feel the impact are the weakest members of humanity, who find themselves without any fortress willing to protect them: refugees, illegal migrants, persecuted minorities. But if the walls keep rising, eventually the whole of humankind will feel the squeeze.

#### And, effective cybersecurity’s key to protect NATO space assets

Unal ’19 [Beyza; July; Former Deputy Director, International Security Programme at Chatham House; Research Paper, “Cybersecurity of NATO's Space-based Strategic Assets,” https://www.chathamhouse.org/2019/07/cybersecurity-natos-space-based-strategic-assets-0/3-analysis-space-dependent-capabilities]

Summary

• All satellites depend on cyber technology including software, hardware and other digital components. Any threat to a satellite's control system or available bandwidth poses a direct challenge to national critical assets.

• NATO's missions and operations are conducted in the air, land, cyber and maritime domains. Space-based architecture is fundamental to the provision of data and services in each of these contexts. The critical dependency on space has resulted in new cyber risks that disproportionately affect mission assurance. Investing in mitigation measures and in the resilience of space systems for the military is key to achieving protection in all domains.

• Almost all modern military engagements rely on space-based assets. During the US-led invasion of Iraq in 2003, 68 per cent of US munitions were guided utilizing space-based means (including laser-, infrared- and satellite-guided munitions); up sharply from 10 per cent in 1990-91, during the first Gulf war. In 2001, 60 per cent of the weapons used by the US in Afghanistan were precision-guided munitions, many of which had the capability to use information provided

by space-based assets to correct their own positioning to hit a target.

• NATO does not own satellites. It owns and operates a few terrestrial elements, such as satellite communications anchor stations and terminals. It requests access to products and services - such as space weather reports and satellite overflight reports provided via satellite reconnaissance advance notice systems - but does not have direct access to satellites: it is up to individual NATO member states to determine whether they allow access.

• Cyber vulnerabilities undermine confidence in the performance of strategic systems. As a result, rising uncertainty in information and analysis continues to impact the credibility of deterrence and strategic stability. Loss of trust in technology also has implications for determining the source of a malicious attack (attribution), strategic calculus in crisis decision-making and

may increase the risk of misperception.

1. Introduction

Space is a vital part of national and international infrastructures. Since the launch of the first artificial satellite, Sputnik 1, in 1957, humanity has used space for the purposes of communication, monitoring the environment, collecting intelligence, conducting vital scientific experiments, and providing data for global positioning, navigation and time keeping. Countries are increasingly dependent on global satellite capabilities for national and international infrastructures, which include systems governing the navigation of aircraft and ships, military manoeuvres, financial transactions, the internet and telecommunications.

Strategic space capabilities are generally composed of three elements: a space segment, a ground segment, and a user segment - also known as an uplink, a downlink and a crosslink - that transmit telemetry data. Military commanders, staff and senior decision-making cadres within NATO receive mission-significant data through products - e.g. space imagery and weather maps - and services - e.g. satellite communications and position, navigation and timing (PNT) data - provided by member states with space capabilities. Although emerging technologies such as artificial intelligence (AI) and the Internet of Things (IoT) could be force multipliers for space capabilities, increased prevalence of cyber means may also challenge the integrity of data carried through these technologies.

Most countries either own satellites or have a stake in space-based assets for meteorological purposes and communications. The functioning of all satellites is dependent on cyber technology, including software, hardware and other digital components. Any threats that could impact a satellite's controls, reliability, or bandwidth availability would pose a direct challenge to national critical assets. If cyberthreats are not effectively addressed, vulnerabilities in the strategic infrastructure could result in severe consequences for international security. Cyber vulnerabilities strike at the heart of the key technologies in strategic doctrines and military planning. In the event of crisis escalation, such as in Ukraine, the Middle East or in South Asia, the assumption is that weapons systems will perform as planned. But this should not be taken for granted. It is mission-critical for NATO to manage, preserve and protect space capabilities, inter alia, by means of agreements and policies. Understanding space vulnerabilities and ensuring that mitigation measures and redundancies are in place, will help to protect NATO's space capabilities.

NATO's missions and operations are conducted in four areas: air, land, cyber and sea. Space-based architecture is fundamental to the provision of data and services to all domains. Therefore, any vulnerability in space infrastructure will likely spread to other domains. The critical interdependency between space and other domains increases the threat of cyber risks, which disproportionately affect mission assurance. Investing in mitigation measures and in the resilience of space systems are key priorities in protecting all domains.

Since NATO relies on the space-based assets of its member states and allies, any consideration of mitigation measures - such as systems redundancy and increased technical resilience - would require the consent and involvement of all parties.

There is an urgent need to study and address cyber-related challenges to strategic assets within NATO and its key member countries, particularly the cyberthreat to space-based command and control systems. It is difficult to define what constitutes a country's strategic military assets. Depending on where they are deployed, even short- to medium-range ballistic missiles or tactical nuclear weapons may be viewed as strategic assets.

There is an urgent need to study and address cyber-related challenges to strategic

assets within NATO and its key member countries.

Strategic military systems depend heavily on space-based assets for navigation and targeting, timing, positioning, command and control, operational monitoring, intelligence gathering and reconnaissance, among other functions. However, the increasing vulnerability of space-based assets, ground stations, associated command and control systems, and the personnel who manage the systems, has not yet received the attention it deserves. This is particularly true in regard to the so-called 'New Space' revolution: the growing role of the private sector in space. For example, during the Iraq war of 2003-11, there was a 560 per cent increase in the US reliance on commercial satellites for military purposes.

Policy influencers and policymakers are struggling to grasp the full impact of cyber vulnerabilities in the context of both space-based assets and strategic systems. Just as with physical attacks on space-based assets - such as anti-satellite weapon (ASAT) strikes - cyberattacks have the potential to wreak havoc on strategic weapons systems and undermine deterrence by creating uncertainty and confusion. Cyberthreats pose a significant and complex challenge due to the absence of a warning and speed of an attack, the difficulty of attribution, and the complexities associated with carrying out a proportionate response. Given the progress made in the areas of strategic conventional weapon systems - for example, the development of advanced cruise missiles and hypersonic glide vehicles - it is essential for NATO and its allies to be able to rely upon space-based systems for early observation and detection; this may enable them to identify and attribute activities and to launch effective, calibrated responses. Cyber technology and innovation are accessible across much of the world, levelling the field and creating opportunities for states outside the NATO alliance - such as China, Russia and North Korea, for example - to instigate high-impact attacks on allied-owned strategic assets.

This research paper will first introduce the cyber risks to strategic systems, through an evaluation of threats, vulnerabilities and consequences. The paper aims to frame the problem by analysing ongoing incidents, and to conduct an analysis of threats and resilience measures in order to offset the risks. Second, it will discuss cyber risks for specific space-dependent strategic weapons systems. Third, it will explore mitigation measures against such cyber risks, through examining NATO's capability development approach, which is known as DOTMLPF-I (doctrine, organization, training, materiel, leadership, personnel, facilities, and interoperability).

2. Cyber Risks to Space-based Strategic Systems

Risk is a product of probability and consequence. However, since estimating the probability of a cyberattack is unreliable at best, this paper focuses on the qualitative nature of potential threats, vulnerabilities and their impacts. Without knowing the actual likelihood of an event happening, it is still possible to assess threats and likely degree of exposure, which can identify potential resilience measures. In essence, the priority of NATO and its allies should be the readiness of their forces to identify potential threats and defend critical assets, rather than the likelihood of cyberattacks on space-based strategic systems. This approach minimizes risk by taking preparedness, resilience and continuity into the equation. Furthermore, it does not require detailed knowledge of an adversary's motivation and capability.

Cyberattacks are a different beast to traditional forms of aggression. Whereas electronic attacks use physical means (such as jamming or 'spoofing') to interfere with the transmissions of radio frequency signals and cause reversible damage, cyberattacks employ digital manoeuvres to target data and access systems in order to cause permanent damage. Electronic warfare methods can physically cut out communication signals that go to satellites (upstream) and come back from satellites (downstream). The attacker could send fake signals (spoofing) and trick the system without the knowledge of the receiver. In a cyberattack, however, an adversary would be able to gain full access to satellites as well as data, enabling them to cause permanent damage.

Spoofing information through cyber means is a more sophisticated form of jamming. In times of conflict, global positioning system (GPS) digital spoofing - which involves digital interception and manipulation - permits the transmission of false information without the awareness of either the transmitter or the receiver. This approach could be used to disorient troops or even control their deployment. In order to mitigate risks, military forces should have the means to validate information integrity and detect spoofing and manipulation of data. One possible approach would be to educate and train personnel in alternative navigation methods as a minimum requirement for those working for NATO and its allies.

Cyberthreats to strategic systems

Cyber research is a fast-moving and constantly evolving area of science, and the scope of cyberthreats that countries face is on the rise as malicious actors find new ways to infiltrate weapons systems.

The use of electronic warfare methods and cyberattacks in peacetime illustrates the blurred lines of engagement between nations even in the absence of conflict. According to Norwegian military and NATO officials, Russia persistently jammed civilian GPS signals during NATO's 2018 Trident Juncture exercise in Europe's High North region, which highlights the growing threat. In November

2018, NATO Secretary-General Jens Stoltenberg stated that electronic warfare and cyberattacks were increasingly being used in operations. It was also reported that NATO officials believed Russia is testing this capability through its large-scale exercises, such as Zapad 2017, which was conducted jointly with Belarus in September 2017.

According to the Consultative Committee for Space Data Systems (CCSDS), the most common cyberthreats to the space segment, ground segment and space-link communication segment include data corruption/modification; ground system loss; interception of data; jamming; denial of service; masquerade (spoofing); replay; software threats; and unauthorized access. There is also crossover between offensive and defensive activities in cyberspace and space, given that - technologically - offence is easier and more cost-effective than defence. Furthermore, space-related personnel are vulnerable to cyberthreats. Social engineering is becoming an important tool when used by adversaries, and - whether it occurs deliberately or unwittingly - the potential for people to constitute the weakest link in cyber defence is an increasing reality.

The nature of cyber activities must evolve from being purely defensive to include active, persistent engagement, in order to disrupt attackers of western critical space-based capabilities. Given the importance of space-based systems to critical infrastructure that supports NATO military capabilities, it would be prudent to assume that an adversary is already active in these networks and focus on resilience measures. This increases urgency for advanced techniques, such as AI and machine learning (ML), to identify and respond to modern threats.

Both China and Russia prioritize electronic warfare, cyberattacks and superiority within the electromagnetic battlespace as part of a strategy to achieve victory in future operations. Available doctrine from these nations highlights a key focus on preventing adversarial satellite-based communication systems from impacting their operational effectiveness - a focus shared in US military planning and policy.

Russian space capabilities and their cybertechnologies pose particular threats to NATO. For its navigational system, Russia relies on its own satellite system GLONASS (Global Navigation Satellite System), rather than the US-provided GPS or the EU's Galileo system. As part of a series of improvements to its communications technology and GLONASS, Russia is designing new navigation satellites, which are claimed to be highly accurate and longer lasting. Russia has been testing its capabilities in a hybrid context in Syria and in Ukraine, particularly relying on capabilities for jamming GPS signals to ground remotely piloted aircraft. It is reported to have conducted denial-of-service attacks on radio and telephone equipment, and to have attempted to steal encrypted military data.

It is likely that several countries - such as the US, Russia and countries within

the EU - will in future possess working quantum communications satellites.

China, too, is improving its space capabilities by investing in new areas of research, such as quantum communications satellite technology, which provides a new way to encrypt information transmitted between satellites, increasing the difficulty of hacking information. In this regard, China's Micius satellite, the first of its kind when it was launched in 2016, may eventually be able to provide a quantum cryptography service. Other countries are following suit and it is likely that several countries - such as the US, Russia and countries within the EU - will in future possess working quantum communications satellites. The European Space Agency, for instance, signed a contract with Luxembourg-based SES Techcom SA to develop a quantum cryptography telecommunication system (to be known as QUARTZ). With this agreement, quantum communications have opened a new dimension in cryptography. Quantum capabilities are likely to make existing asymmetric-based, traditional cryptographic-based protection obsolete. The EU, the UK and the US are all investing heavily in a range of quantum technologies - including communication devices, computers and imaging enhancers.

Vulnerabilities to strategic systems

When analysing risk, understanding system vulnerabilities is as important as understanding the threat landscape. Threats alone would not pose a risk if there were no known vulnerabilities for an adversary to exploit. Similarly, system vulnerabilities would not always result in risk, especially in peacetime, when there is no incentive to attack or infiltrate.

In the military domain, some of the major system vulnerabilities include the use of commercial companies for military purposes; 'back-doors' in encryption; and the supply-chain security of satellites. This list can also be extended to include physical, personnel and procedural vulnerabilities. Risks also arise from the dual-use aspect of most of the space-related technology - where the technology can be used for both civilian and military purposes. For instance - whether fixed or mobile units - communications satellites and broadcasting satellite services have both civilian and military utility. Similarly, the utilization of satellite imagery capability in the civilian sphere for earth observations, environmental monitoring, and the provision of oceanographic and cartographic data, also extends to the military domain. There is an increasing need to apply higher-grade military hardening and cyber protection specifications to civilian capabilities that have the potential to be used in support of military applications.

These capabilities aside, terminals located in ground stations constitute a critical vulnerability, as a terminal is an access point to a satellite and is usually not protected by authentication in order not to hinder operational actions. Terminals house software systems that can be compromised and require patching and upgrading. Moreover, software embedded in weapons systems (such as precision-guided munitions) could also be compromised.

At times, NATO allies procure equipment and software to be integrated into their national defence architecture, which becomes part of the overall NATO capability. The commercial supply chain is embedded in nearly every aspect of military equipment. This may not necessarily be a particular vulnerability, as long as commercial equipment is designed to military standards and is secure. However, if military standards are not met, items procured from commercial industry with design flaws may expose NATO's systems to additional vulnerabilities.

While the absence of data is easy to detect, the manipulation of data or erosion of confidentiality at such an interface is potentially more difficult to discern.

Civil satellites, operated by private companies, may be used to fulfil specific missions in locations where NATO allies do not have their own space equipment. Ground stations constitute further elements that are relevant for the data flow. From a cybersecurity point of view, each interface could present a vulnerability and could become a weakness, as an interface typically requires manual processes to establish its operation, and/or the administration of the components involved. Adversaries infiltrating ground- or space-based systems could exploit weak software implementation, or the incompatibility of network or data transfer protocols in the chain. While the absence of data is easy to detect, the manipulation of data or erosion of confidentiality at such an interface is potentially more difficult to discern. Vulnerabilities can stem from:

• A higher number of data exchange interfaces used between the military and civil sectors;

• The fact that each actor has its own isolated view of its data network, protected by its own security standard;

• The use of old and proprietary IT hardware and software; and

• The failure or inability to conduct regular software updates to remove known vulnerabilities. In such an environment, it seems difficult to ensure security of the information delivered.

Space-specific risks for the NATO alliance and for key NATO countries

Space systems, which include both satellites and ground stations, as well as related space products and services, provide mission-critical information both for NATO's member states and for the alliance as a whole. NATO relies on space-based assets for almost all of its operations and missions. Some of the critical missions that rely on space assets include: defence of NATO's territory and the neighbouring regions; peacekeeping missions; humanitarian assistance and disaster relief; counterterrorism; and conflict prevention activities.

NATO does not own satellites. It owns and operates a few terrestrial elements, such as satellite communications (SATCOM) anchor stations and terminals. It requests access to products and services but does not have direct access to satellites, leaving it up to its allies to determine whether they provide access to their satellite capabilities. NATO has established memoranda of understanding with allies for possible use of space products and services.

Originally, in the US, space systems used by the military were separated from commercial and civilian assets in terms of their development and operation. One of the reasons for this separation was to protect the military structure against physical and cyberthreats. Military space system safety and security requirements were also higher and more stringent than in the commercial sphere (for example, requirements to invest in survivability enhancement mechanisms in order to resist jamming, or special design approaches for military space architecture). In recent years commercial methods, for instance the capture and analysis of satellite imagery, have been shown to be as effective as military means. As a result, NATO uses a mix of military, civilian, commercial, and national/multinational assets to conduct its operations. The joint use of these assets, however, comes with an acceptance of inherent risk, not only to the countries that provide such capability but also to the alliance as a whole. In response, the European Defence Agency, through its Governmental Satellite Communications (GOVSATCOM) development programme, decided to build an intermediary class of satellites between commercial SATCOM and military SATCOM, with security requirements able to address the needs of critical missions, including crisis management.

There is increased dependence on space-based systems in modern military engagement. During the US engagement in Iraq in 2003, 68 per cent of munitions were guided utilizing space-based means (including laser-, infrared- and satellite-guided munitions); this percentage had risen sharply from 10 per cent in 1990-91, during the first Gulf war. In its operations in Afghanistan in 2001, 60 per cent of the weapons used by the US were precision-guided munitions: these included bombs, missiles, and other weapons, many of which had the capability to correct their own positioning to hit the target, using space-derived information.

Cyber vulnerabilities undermine confidence in strategic systems; they increase uncertainty in information and analysis, which impacts the credibility of deterrence and strategic stability. Loss of trust in technology also has implications for attribution and strategic calculus in crisis decision-making and may increase the risk of misperception.

This dependency on space-based technology has major implications for the way NATO conducts warfare today, and how it will do so in the future. For instance, in order to conduct precision strikes or earth observation through the use of unmanned aerial vehicles (UAVs - such as military drones), systems rely on so-called 'beyond-line-of-sight' (BLOS) communication via satellites - especially

in times of crisis and conflict, since ground-based line-of-sight communications are vulnerable to physical attacks. Yet, cyberattacks on space technology or on the UAVs may lead them to misinterpret commands, or to lose contact with the command centre and fail in operation.

#### Space war causes nuclear conflict

Gallagher ’15 [Nancy, interim director of the Center for International and Security Studies at Maryland, “Antisatellite warfare without nuclear risk: A mirage,” <http://thebulletin.org/space-weapons-and-risk-nuclear-exchanges/antisatellite-warfare-without-nuclear-risk-mirage>]

But even if the norm against attacking another country’s satellites is never broken, developing and testing antisatellite weapons still increase the risk of nuclear war. If, for instance, US military leaders became seriously concerned that China or Russia were preparing an antisatellite attack, pressure could build for a pre-emptive attack against Chinese or Russian strategic forces. Should a satellite be struck by a piece of space debris during a crisis or a low-level terrestrial conflict, leaders might mistakenly assume that a space war had begun and retaliate before they knew what had actually happened. Such scenarios may seem improbable, but they are no more implausible than the scenarios that are used to justify the development and use of antisatellite weapons. Reducing danger. One way to moderate the nuclear risks associated with antisatellite weapons is to realistically assess arguments that attacking satellites would be an easy way to achieve major military advantages without creating unanticipated or uncontrollable consequences. For example, unclassified analysis by Jaganath Sankaran, a research scholar at the Center for International and Security Studies at Maryland, suggests that the practical limitations of Chinese ballistic missiles and launch facilities would make it much harder for China to attack critical US satellites during a crisis than it would be for Washington to respond in ways that denied Beijing any military advantage from such an attack. As more such studies are conducted and given serious consideration, policy makers will be less likely to invest heavily in antisatellite capabilities or to take pre-emptive action against purported antisatellite threats. Another important way to reduce risk is to strengthen both the norms and the legal rules that protect satellites. The most straightforward way to accomplish this would be to prohibit using anything, including other space objects, to damage or destroy satellites that are not themselves being used as space weapons; and to prohibit any testing of methods for damaging or destroying such satellites. Currently, the biggest threat to established norms and legal protections comes from people who cite anticipatory self-defense—during a crisis or at the outset of hostilities—as a justification for disabling or destroying satellites, launch facilities, or ground stations. Almost as dangerous are those who argue that, once war begins, anything in space becomes fair game and therefore should be targeted. Although it might be legal in the midst of a war to attack satellites used for command, control, communications, and intelligence, it doesn't follow that attacking satellites would be smart strategy.

#### US-NATO security cooperation is vital to alliance cohesion

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

The United States still struggles to find effective policies for deterring cyberattacks. Suggestions run the gamut from more widespread use of indictments and economic sanctions, despite their lackluster record of success, to less traditional but more risky policies that emphasize the asymmetric advantage America has in conventional military power. Most of the discussion of cyber deterrence focuses on preventing a single catastrophic or cascading cyberattack that would threaten lives (like disruptions to electricity transmission or clean water)—or our way of life—altering election outcomes or grinding global finance to a halt. Yet the reality is that in the event of such an attack, the response would likely not come from the U.S. alone but from the NATO alliance in concert. NATO’s cyber-defense mandate has evolved over time to update its collective defense commitment under Article V of the North Atlantic Treaty for the era of cyberattacks. In the latest effort to collectively impose costs on adversaries, the 2018 NATO Summit saw a commitment from heads of state and government “to integrate sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions, in the framework of strong political oversight.” The newly updated White House National Cyber Strategy likewise envisions working together with a “coalition of like-minded states” to “ensure adversaries understand the consequences of their malicious cyber behavior.” Therein lies the rub. Both formal alliances, such as NATO, and more ad hoc arrangements, such as what the Cyber Deterrence Initiative imagines, will require members to share intelligence and eventually, to the best of their ability and perhaps in different domains, contribute to joint action against a presumably well-armed foreign aggressor. States including the United States, the United Kingdom, the Netherlands, Estonia, and Denmark have publicly declared their willingness to lend sovereign offensive cyber effects to deter, defend against and counter the full spectrum of threats. Sharing intelligence and information is a key element of NATO’s core decision-making process enshrined in Article 4 of the Washington Treaty. Political consultations are part of the preventive diplomacy between member states, but they are also an avenue to discuss concerns related to the security threats member states face. These consultations can be a catalyst for reaching a consensus on policies to be adopted or actions to be taken—including those on the use of sovereign cyber effects to support a NATO operation. The alliance has a track record of collective action and cooperative security measures. For example, Operation Active Endeavour helped to deter, disrupt and protect against terrorist activity in the Mediterranean in the aftermath of the 9/11 terrorist attacks, in solidarity with the United States. For the seventh time, the Atlantic Council’s Cyber Statecraft Initiative will be among the organizations privileged to organize an event on the sidelines of the Feb. 15–17 Munich Security Conference. This year in particular, the Atlantic Council’s event, “Defending Human Dignity: Limiting Malicious Cyber Activity Through Diplomacy,” will complement the topics high on the agenda of the main conference, such as transatlantic collaboration, the consequences of a resurgence of great power competition and the future of arms control. In the United States, the greatest failures of response and deterrence to foreign aggression in cyberspace have not been caused by a lack of intelligence, capability or imagination. Rather, U.S. policy has been serviceable in theory but impotent in practice because of an inability to translate technical findings and intelligence into public support for sufficiently tough responses ordered by elected political leaders. North Korea’s repeated operations targeting U.S. companies and critical infrastructure have been met with public skepticism over their culpability, limiting the strength of retaliatory options needed to deter further events. Chinese cyber economic espionage continued for years despite widespread knowledge of China’s activities because political leaders found it difficult to confront Beijing without undermining U.S. companies in return. Russian information operations did not sow enough doubt to mislead experts, but they succeeded in exacerbating the partisan polarization of an already-divided electorate and its leaders. That inability to translate the findings of cyber experts into public sentiment and therefore political action has sidelined America’s cyberwarriors, by far the most technologically advanced and well-resourced in the world. Imagine the political response of an ally that is asked to burden-share in response to cyber aggression but is probably much closer to any resulting kinetic fight than the United States. Now imagine the response of that ally when it’s being asked to take causus belli on faith: The United States is presenting attribution for a cyberattack elsewhere in the world, but perhaps is depending on the ally lacking critical details due to classification, and is presenting that information alongside a request for help that might well put the ally in the crosshairs of its own cyberattack or lethal action. How can allies with different capabilities to collect, analyze and understand intelligence be part of a consensus on using sovereign cyber effects to support a NATO operation? How can a commander achieve a common operational picture to authorize the use of sovereign effects in a NATO operation if all the allies are not on the same page with respect to critical attribution and other technical information needed for a use of effect in an operation? We all know what a tank looks like on a shared satellite image, but if you ask three cyber experts to interpret the attribution for a set of indicators, you are likely to get at least four answers. For most U.S. allies in Europe and elsewhere, there is simply a dearth of technical know-how within the government when it comes to cyber attribution and operations. This is already a challenge for the United States, with a massive defense budget, Silicon Valley innovation and an educated workforce to pull into government service. But for many U.S. allies, tech-savvy public servants will have long fled for the private sector, nongovernmental organizations (NGOs) and academia before reaching ministerial positions. To its credit, the U.S. National Cyber Strategy does propose capacity-building measures to support allies. This means building up law enforcement, intelligence, and military operational and investigative capability. But even with successful capacity-building programs, many nations could, in a crisis, end up in the same place the United States is—with good options stuck on the shelf while political leaders and their electorates lack a critical mass of informed voters to trust, understand and act on expert findings. For countries weighing whether to risk their own blood and treasure in support of an ally’s cyber attribution findings, this hurdle could well prove insurmountable if not addressed well before a crisis emerges. Many such countries will no doubt recall being burned when placing too much confidence in U.S. technical and human sources without an ability to evaluate the evidence for themselves, as with the Iraq weapons of mass destruction findings. The private sector will probably play a crucial role in providing intelligence to support alliance responses to cyberattacks, especially as a stopgap over the next few years. FireEye and its peer competitors and partners regularly produce analyses of major world cyber events—many that fly below the radar of Western leadership, in fact—sometimes at a near-government quality and often covering much of the same “classified” evidence. More important, private-sector analysts are accustomed to writing for impact with both their technical counterparts, like chief information security officers (CISOs) and threat hunters, and nontechnical stakeholders such as boards of directors, CEOs and other persons controlling the purse strings. In this sense, unclassified, private-sector and NGO-driven cyber threat intelligence can become the lingua franca of discussions. Relying on commercial reporting generated by international teams, rather than declassified government-generated reports, both broadens the audience enough to make alliance discussions feasible and mitigates against disparities in terminology across national lines—the tendency of even closely integrated allies to describe cyber “attack,” “information operations,” and attribution findings with different implicit assumptions or implications. Long-Term Thinking In the long run, though, the U.S. and its more technologically advanced allies—such as its fellow Five Eyes (Australia, Canada, New Zealand and the U.K.), France and Japan—will have to make important policy changes in the interests of furthering alliance cooperation in cyberspace: a willingness to sometimes risk sensitive sources and methods in order to get cyber threat intelligence into the hands of other countries better positioned to take policy action, an end to classifying public information like IP addresses solely because of their acquisition via classified means, and greater transparency on their own decision-making. Government cyber leaders within the alliance should consider taking another page out of the private-sector playbook as well: running cyber-crisis exercises that involve more than the IT department. In the commercial world, the more successful practice runs involve leaders at both the CISO level and some presence from nontechnical teams that would weigh in during a crisis, such as communications and legal. The best exercises involve executives, too, who despite their busy schedules must see for themselves how their companies would survive and respond during a potentially ruinous cyberattack, and work through the minutiae of leading a response themselves. The experience and confidence is invaluable if ever called on during a real-life crisis, and the organizational introspection by involving decision-makers at all levels is irreplaceable. Military-to-military cyber training as part of cross-country force standardization and joint operational planning could pull in more senior national leadership, beyond battlefield commanders, and be coupled with increased funding for foreign affairs-led training for nontechnical leaders. The private sector could also meaningfully contribute during NATO consultations when developing Allied Joint Publications to make sure that definitions and requirements for threat intelligence incorporate the best practices of NATO member countries’ private sectors. If a U.S. diplomat reaches out to his or her counterpart in an allied country to ask for assistance responding to malware that’s damaging critical infrastructure, and that counterpart has to ask what malware is, the response isn’t going to happen. \*\*\* NATO’s essential and enduring purpose is to safeguard the freedom and security of all its members by political and military means. Tolerating cyberattacks, especially those deliberately targeting civilians and the political legitimacy of governments—without the alliance having the capability to jointly discuss attribution and have the confidence to act and assist one another—undermines this core purpose of the alliance. Likewise, pursuing only deterrence and response without an active role for the alliance in reaching peaceful diplomatic agreements with potential adversaries abrogates member responsibilities to their citizens but is impossible without a common language and operational picture to discuss enforcement of such agreements. The U.S. is stronger with allies, and with attention to these issues its cybersecurity can be too.

#### Expanding authority for DOD security cooperation with NATO over OCO’s both enables effective US cyberposture and restores NATO cohesion

Hansen ’21 [Dave and Morgan Musser; March 11; career US Army intelligence officer currently serving at the NATO Allied Rapid Reaction Corps, works in US Air Force Special Operations Command as an MC-130J pilot serving on Joint Special Operations Air Component; Foreign Area Senior Noncommissioned Officer serving as a regional planner in Stuttgart, Germany; The Civil Affairs Association, “The Rhetoric vs the Reality: Understanding NATO’s Capacity to Address Russian Gray-zone Conflict,” Eunomia Journal]

Despite these challenges, the NATO toolbox does include a variety of instruments, such as the imposition of sanctions. And while the Alliance has made clear it neither limits punishment to similar cyber-attacks nor excludes them, it keeps the option open to use the full range of Allied capabilities to deter and counter gray-zone actions. At the 2018 Brussels Summit, Allies expressed their determination “to employ the full range of capabilities, including cyber, to deter, defend against, and to counter the full spectrum of cyber threats, including those conducted as part of a hybrid campaign.”[33] Thus, NATO could retaliate in a proportional manner, but it does not necessarily have to do so by granting the authority to mirror Russian activity, especially considering Russia employs tactics that violate the norms of the liberal international order. Corruption, illicit finance, elections in­terference, debt traps, the restriction of free speech, spreading false narratives, territorial aggression, and ex­tra-legal operations are all areas NATO may rightfully choose to not engage.

From a technical standpoint, should an adversary proliferate computer viruses to shut down power grids, countering with a cyber-attack may not stop/prevent the attacker’s imminent capacity to reengage. Despite an open-ended potential for graduated response options, NATO policy on gray-zone activities, particularly in cyber and information remain wholly constructed around a defensive posture. Unfortunately, defensive actions do not adequately address either the safeguarding of personal data that Russian or other malign actors might use in cyber-enabled information warfare or the economic incentives that drive users toward such behavior.

Considering US cyber capacity, DoD’s stepped-up current posture of “persistent engagement” bodes well for active cyber defense.[34] However, questions remain as to whether it effectively enables operations to be deployed fast enough to address the ever-changing threat profiles and to manage escalation potential. Moreover, the approach requires the tight coupling of strategic ends—typically identified in an interagency policy process—and operational effects. It remains unclear if the current NATO collective defense strategy is able to deliver that coupling for US capabilities, which can create risks of unintended escalation or self-defeating effects not understood by well-meaning policymakers. Finally, significant gaps remain in intelligence and warning for cyber incidents across NATO, as well as normative frameworks to guide responsible use.[35]

Some efforts to resolve gray-zone conflict remain in their infancy. For example, in 2016, Finland instituted the European Centre of Excellence for Countering Hybrid Threats in Helsinki with participation open to EU member states and NATO.[36] However, the Hybrid CoE provides only an analytical framework for the assessment of current and future hybrid warfare situations and their practical implication. The development of the Hybrid CoE is a model that could be applied in other regions for building capacity, and interoperability, and its existence is an important step forward for EU and NATO members to informally address vulnerabilities. However, this effort holds no authority or capacity to engage a response.

Holistically, despite a number of declarations, increased force presence in Eastern Europe, and newly formed information-sharing centers, NATO’s actions remain pursuant to conventional forms of military deterrence or research. None specifically counter gray-zone activity or prevent Russia from targeting weaker nations. From a military deterrence standpoint, there clearly appears to be a functional mismatch between NATO’s traditional hard deterrence and the hybrid actions it wishes to remedy. Integrating multiple elements of national security remains unaddressed.

Authorities

One of the key challenges often plaguing US and NATO response to gray-zone conflict is “authorities.” This problem is two-fold. The first are the challenges internal to the US regarding perceived inadequate or dispersed authorities to effectuate coherent activity. The second are insufficient authorities inside the NATO Alliance – partly a function of the political bureaucracy within NATO itself, arguably slow to elicit timely and relevant responses. Much of the literature on countering gray-zone activity recognizes the need for an interdependent system.[37] Critics have additionally pointed to several issues which include the lack of a holistic methodology for dealing with Russia’s gray-zone behavior.[38] But without a formalized methodology for defining and assigning policy priorities and actions, effective long-term strategies for deterring, competing against, and responding to competitors’ use of state-controlled forces will likely be limited.

Limitations precluding a real-time, multi-agency approach to address adversarial actions are especially salient in the information and cyber domains. Within the US government, responsibilities and authorities are spread across numerous entities, to include DoD, DoS, and Treasury. There is no unity of effort and no specific organization has lead for synchronizing the employment of all instruments of national power.[39] Within DoD, most of the capabilities reside inside the force structure of geographic and functional combatant commands (CCMD) and are tasked through unified combatant command (COCOM) au­thority. Authorities quickly cut across both functional and geographic lines. This may slow defining roles and responsibilities. Also, several offensive capabilities are either compartmentalized due to the technology behind them or, considering their effect, may yield undesirable strategic impact. Therefore, authorities for their use – specifically in the information and cyber domains are often retained at the SECDEFs level (or above). This can dramatically impact the speed of response. To fix this, some authorities (and associated risk acceptance) might be delegated down to Ambassador level, such that in a steady-state environment, permission might be granted to create effects in the information environment, while retaining country-team level and multi-agency awareness.

Additional challenges with authority are a result of ambiguity in US law. Both Title 10 and Title 22 authorities grant DoD and DoS authorities to support, train, and partner with forces, with legal checks and controls on human rights and ac­countability measures. However, there is no clear de­lineation over whether building/countering US local partners should be under Title 10 or Title 50 (Central Intelligence Agency) authorities. As a result, the question of who owns long-term proxy strategy and operational development remains unanswered in the US interagency.[40] This “authorities dilemma” is even more convoluted within the NATO alliance. The United States’ aspirational model for countering Russia’s gray-zone activity via whole-of-government approach, is not well-suited for a multinational security-based alliance.

Opportunities and Recommendations

There are several observably difficult challenges in how the US and NATO approach gray-zone competition, as a military, as individual nations, and as Allies. Such challenges do come with opportunities. The Department of Defense cannot abruptly restructure itself to engage in all gray-zone activities, nor should it necessarily want to. What the Alliance does have however, includes asymmetric advantages of transparency through its rule of law. The system of alliances and partners can work to extend democratic principles, acknowledge humanitarian concerns, prevent violent conflict, identify and stymie political and economic ex­ploitation, and support free and fair media outlets.[41] Thus, developing methods that directly compete in the gray-zone can exist outside the development of like-capabilities. Likewise, NATO cannot immediately establish a multi-agency organization, built to compete across a spectrum of gray-zone activities, empowered to lead, synchronize, and coordinate diverse capabilities across the conflict continuum.[42] Authorities still must be reconfigured down and across to appropriate levels to enable proportionality, when directed.

The good news for US DoD is that it may not have to embark on a complicated restructuring in order to counter Russia’s malign actions. DoD’s current approach places war-fighting authorities under CCMDs. There are certainly numerous challenges in synchronizing prior­ities, resources, and actions to leverage a broad toolset and eliminate the stovepipes. Indeed, specific capabilities such as information warfare, or offensive cyber, are neither geographically nor functionally lim­ited.[43] Yet while true, just because some gray-zone actions cross geographical and functional lines, this does not inherently mean the response is hindered. While broad oversight may be an enabler, lack of it is not an inhibitor and it does not mean that a Combatant Command is disabled.

In fact, Russia’s activities are often geographically focused — making them ripe for inclusion into CCMD Campaign Plans. Under the current structure, the geographic Combatant Commands are arguably best postured to compete against Russia’s gray-zone activities, taking full advantage of supporting the coordinated activities of USCYBERCOM as well as the expertise of US SOCOM. Specific authorities could be granted now for implementation by US forces in support of NATO objectives to reduce Russia’s information position, as well as granting authorities for the leveraging of the information environment to the benefit of both US and NATO strategic interests.

While a US whole-of-government approach with a singular lead organization is a lofty ideal, this is simply not practical in the short term. There are actions that can be taken to establish a unified purpose, and to ensure that reform priorities for competing in the gray-zone are formed around making the most of available US strengths by mitigating current gaps in the ability to execute national interest-based strategy via campaign plans. If NATO is to deal effectively with such competition, then it too must refocus its own military strategy and forces to give gray-zone and hybrid conflicts at least equal standing with traditional deterrence. At present, NATO has only recognized cyberspace as a domain of operations since 2016. While an important first step in combating gray-zone activities in the information domain, the information centers standing up are limited to situational awareness, along with some planning and coordination tools.[44]The Alliance has yet to refocus its security strategy to address the impact of gray-zone activity across global, regional, and national levels.

Delegated authorities and packaged measures will need to be tailored and based on a better understanding of the strategic intent behind the use of gray-zone tools. This can help the military better engage in the debate and develop capabilities to support Allies in countering non-military threats, such as using special operations, information, and psychological operations. A focused approach with delegated authority would vastly improve NATO’s efficiency in influencing the cost-benefit analysis of potential aggressors in what has now become the modern theatre of operations. In short, if opponents increasingly act in the gray area, NATO must be efficiently enabled to defend, attribute, and respond. The initial structure is in place, but the operationalization of strategy and authority for appropriate comprehensive tools lags.

Defeating Russia’s sophisticated strategy requires strategic competence and a concerted effort to restore confidence in democratic principles, institutions, and processes, along with remediating the vulnerabilities Russia exploits. To compete properly, NATO must articulate clear guidance for its threshold warfare deterrence posture, with options that realistically allow forces to respond to Russian gray-zone behavior. Management of these threats must be an ongoing endeavor, requiring a change in mindset from the deliberate sequential planning processes associated with classic forms of conflict to a more dynamic approach of continuously updated situational awareness, driving political discussion, option development, decision-making, and measured response under political control.

To do this effectively, NATO will have to progress from crisis-response operations to reinvigorate both its military strategy and forces and ensure gray-zone and hybrid conflicts are prioritized along with higher levels of warfare. This may include refocusing its current security strategy to address the overall impact of Russian civil competition at all levels by fully integrating its military, political, and economic strategies and operations. How much of (and when) technological capacity should be delegated down must ultimately be considered and reviewed, along with how NATO integrates response capabilities into the multi-national environment. These gaps must be bridged to enable multinational teaming. Without them, NATO’s plans for deterrence, defense, and dialogue run the risk of becoming reactive, or even outmaneuvered.

Many gray-zone operations will not require the actual use of military force. Some will be entirely civil or economic – using non-military means to achieve strategic or tactical objectives. This will inevitably require ‘whole-of-government’ capacity within NATO structures in a way that NATO is presently not organized or enabled to perform. If NATO members agree that the trend of cyberspace is the most active battlefield, then it is crucial the Alliance has a threat preparation and mitigation plan that is continuously monitored, assessed, and adjusted, with deterrence mechanisms built-in. Presently they are not. The significance to NATO is clear. NATO must overhaul its deterrence strategy, to include options far more nuanced than tactical overmatch, by re-evaluating the role of its military as a deterrent, through increased sub-Article 5 capacities. This might even include support from the private sector and international organizations, with emphasis on a comprehensive approach.

Conclusion

Since its inception, NATO has been more than just a military alliance. It has embraced a political role, unifying Allies behind a common strategic vision. Future uncertainties demand NATO must continue to adapt. Given the significant changes in the security environment since Russia’s incursion into Georgia and Crimea, this presents an opportunity to determine the character of the Alliance’s military capabilities vis-à-vis gray-zone warfare. Future decades will certainly be different than the world the Alliance inhabited during the Cold War. NATO’s cohesion resides in the ability and will to act collectively against shared threats. This is the lifeblood that ensures the vitality, credibility, and durability of NATO. It becomes increasingly important in a sharpened competitive environment requiring collaboration and effective networks. Therefore, the distinctive capabilities required to counter gray-zone warfare must be seriously contemplated.

#### Only CBMs over OCO’s can mitigate tensions from inevitable cyber policy divergences

Zhang ’21 [Yiran; March 4; graduate student at Renmin University, China; Association for Political Risk Analysis, “The Looming NATO Offensive Cyber Policy’s Challenges of Harmonizing Deterrence and Decision-making,” https://www.aprascpo.org/post/the-looming-nato-offensive-cyber-policy-s-challenges-of-harmonizing-deterrence-and-decision-making]

The purpose of policy in NATO offers a broad directive multilaterally agreed by all allied states which guides the Alliance in their coordination, action, strategy, amongst other aspects. While NATO’s conventional capabilities such as nuclear weapons, are traditionally instructed by its policies, they themselves have evolved and been adapted to better suit the circumstances of contemporary challenges. Similarly, in confronting new challenges with emerging technologies and an ever-change landscape of different domains of warfare, the Alliance, starting from its first recognition of the need to bolster cybersecurity and cyber defence at the Prague Summit in 2002, has made continuous efforts in shaping and reshaping its policy in cyberspace (Davis, 1).

However, unlike other capabilities in the conventional sense, NATO has yet to announce and adopt a cyber offensive policy, as its current cyber policy is based mainly on cyber defence and cyber deterrence. In the meantime, not only have allied states suffered substantial cyberattacks by Russia with the wake-up call conflict that is the 2007 cyberwar on Estonia, other NATO adversaries and select allies have also been developing increasingly sophisticated cyber offensive capabilities, in short starting an arms race to gain superiority in this domain.

For the Alliance to remain credible, it needs to achieve and maintain the two-pronged aspects of the allies’ political commitment to collective defence, as well as its military capability, which is the insurance to the former (Jonson 2). Its credibility in cyberspace is currently maintained by a number of allied states each with their own national cybersecurity capabilities and some with cyber offensive policies. Yet, for NATO to adopt similar cyber capabilities and coordinate them across its allies, it would require an institution-wide policy to guide it. But is an offensive cyber policy for NATO politically feasible?

The present paper examines this question by first 1.) explaining NATO’s institutional lenience towards allied offensive cyber capabilities in recent times despite its policy only in the defensive arena, and addressing areas of strength and deficiency in the Alliance’s comprehension and coordination without an offensive policy. Secondly, 2.) areas of allied rift and agreement are identified by discussing issues surrounding cyber offensive policies with previous research into the Alliance’s deterrence purpose and its decision-making and strategic challenges. Finally, it will conclude by 3.) proposing general recommendations for NATO’s approach in considering an offensive cyber policy.

Offensive Capabilities under a Defensive Policy

Like NATO’s many conventional assets, in terms of offensive cyber tools, it is precisely because its allies have agreed to not conduct offensive cyber operations as NATO that it relies on the contribution of such capabilities from allies who possess them to volunteer them to the Alliance (NATO Cyber Defence Factsheet). ​The strictly defensive policy does not stop allies’ decision to conduct offensive cyber operations individually or with each other, and as long as these possibilities are willingly offered by allies, NATO can play a coordination role in aligning the offensive operation from allied state(s) with the Alliance’s collective defence ones (Freedberg). With the decision to integrate offensive capabilities into a defensive policy, NATO has already signalled its interest in strengthening its own offensive capabilities by building its cyber command with the ability to conduct its own cyber attacks (Emmott). From a capability standpoint, this command will have coordination and capacity-building functions for NATO allies to develop offensive capabilities on an institutional level together rather than relying on the United States’ command.

The benefits of having offensive cyber capabilities have also been widely studied; and it is generally considered that cyberspace is more offensive-focused and those superior offensive capabilities including demonstrating strategic, operational, and tactical versatility and precision to paralyze the adversary gives one the upper hand (Saltzman 42-44). Developing a certain capability does not necessarily mean that the Alliance’s cyber policy will definitively expand to include offensive operations, but it will increase the Alliance’s credibility in deterring possible cyber risks from adversaries. On one hand, NATO’s cyber defence policy is in line with its founding identity as a collective defence alliance; on the other hand, in other domains where capabilities are matched with their respective policies and doctrines, NATO allies receive clear guidance across the board on the conditions of proliferation or nonproliferation of these capabilities whether the response takes place on land, in the sea, or air. It may be then advantageous for NATO to provide a clear direction to allies on its cyber policy involving both its defensive and offensive capabilities upon the refinement of the latter.

Another key consideration is the ascension of cyber to being on the same level as other operational domains at the Wales Summit in 2014, insinuating that a cyberattack could trigger Article 5 (Oolup 28). Considering the event of NATO’s response to entail kinetic measures, cyberattacks successfully operated to a targeted and effective extent may not cause physical destruction but other types of large-scale damage, such as information loss or political undermining (Roggeveen). For NATO to thus engage adversaries in such an event, multiple levels of cyber aggression need to be addressed separately to provide proportional and appropriate offensive responses. Furthermore, contrary to claims which often point out an engagement in cyberwar can escalate a conflict to other domains, scholars have also found that although offensive cyber capabilities are not particularly effective in deterring military action of an adversary unless the threat of proliferation comes from credible actors, they are useful in compellence while the secrecy of their operation can potentially de-escalate a conflict by saving the adversary face (Smeets & Lin 55). Given the strategic value and the complexity of possessing cyber offensive capabilities, a NATO-level multilateral policy would distribute the knowledge of such advantages and disseminate strategic bargaining power amongst allies in a way that does not clash with collective defence goals.

One may speculate that NATO’s integration of allied offensive capabilities is beneficial until the performance of natively-researched and developed tools reach a highly advanced and well-funded level to supplement and even match its defensive capabilities, because strategically speaking, the supremacy of defence capabilities should precede offensive ones in anticipation of adversary attack. According to research in the theory of cyber offence-defence balance, the race to develop effective offensive capabilities globally may contribute to the destabilization of the international security system, especially when these actors do not possess adequate defensive ones (Shaheen 77). This guiding theory informs the historical reluctance of NATO towards an offensive cyber policy, although the offence-defence balance also suffers from an interpretation of traditional warfare’s narrative of escalation and destabilization. Therefore, for NATO to better coordinate allies' offensive cyber operations, a guiding policy may aid crucial posturing and strategy of its engagements in both low-intensity and high-intensity contexts, instead of for NATO to coordinate each operation individually. By extension of this forecast based on NATO’s current stance on cybersecurity, a multilateral offensive policy may be on the horizon with time and political will but its negotiation and agreement face significant issues politically, technically, and strategically. The following summary will provide an overview of popular political and strategic challenges connecting to the consensus-based direction and deterrence-based foundation of the Alliance in the formulation of a NATO-level cyber offence policy.

Reforming the Deterrence Doctrine

The Alliance seeks to contribute its overall defence and deterrence posture using cyber capabilities, and offensive cyber capabilities announced by a guiding policy may signal clearly to the adversaries of NATO’s posture and credibility. The integration of cyber offensive capabilities and policy with other domains of warfare may provide strategic benefits to the Alliance by upping its credible firepower. Though without integration into physical force in this coercive sense, deterrence-by-punishment posturing in cyberspace through retaliatory measures may also legitimize offensive cyber operations’ use and may present risks towards collective cooperative security amongst allies and even potentially undermining political policies (Burton, 8).

The preference for deterrence-by-denial as a result of the consideration for these important risks is additionally problematic, as the passive strategy runs counter to some allied states’ political will to establish a more proactive policy (Ibid.). Out of the number of NATO allies who have volunteered their offensive capabilities to the Alliance, the United Kingdom expresses the most obvious intent in using its capabilities for both deterrence and operational means as stated in its National Cyber Security Strategy (HM Government 25). Evidence of the UK’s political will for a more proactive policy and posture can be seen in the policy prioritization of its national investment into cyber offensive capabilities and its demonstration of offensive operations in Russia and the Middle East. It is explicit in its national policy in identifying exactly the deterrence aims that UK is aiming to accomplish with its offensive operations, while the US also takes a preemptive approach in using offensive capabilities in deterrence and in gaining other types of advantages across domains to ensure US superiority (Oolup 40).

Comparatively, European Union allies seem to favour the more passive policy as it suffers similar coordination and policymaking problems like NATO. That being said, the European Parliament welcomed the European Commission’s cyber package, in which reinforcements to European offensive and defensive capabilities at both civilian and military levels are recommended to be implemented due to the EU’s fragmentation in joint defence strategies and member states’ lag in exchanging knowledge and warnings about cyber attacks (European Parliament). This need for a joint policy and the approval of an EU-wide cyber package including offensive capabilities may signal more political will for an interoperable NATO policy as well as bolster collective deterrence and security. As the allies of differentiated capabilities debate on the value of offensive cyber deterrence in their national policies with discretion for the inapplicability of nuclear-era deterrence theory to cyberspace, the decision-making and organizational fashion of NATO inflame internal political complexities and may discourage consensus.

Testing Alliance Consensus and Decision-making

The Alliance’s decision-making principle of consensus further complicates the negotiations and agreement of a NATO offensive cyber policy. The above-mentioned nuclear example almost exclusively concerns kinetic and state-level physical destruction of massive proportions. The dire consequences of the extremity of possible nuclear proliferation are enough to establish credibility, deterrence, and is a comparatively simpler way in getting its 30 member states on board, especially in the context of Cold War bipolarity.

Cyberspace as a domain of war contains a myriad of vested technical issues including the difficulty of attributing attacks to specific adversaries. Even though this is one the most prominent difficulties according to a variety of research in cybersecurity, more recent analyses published by NATO's Cooperative Cyber Defence Centre of Excellence have suggested that the attribution gap is gradually decreasing in size due to heavy research and development investment into web tracing and identification designs largely spearheaded by the US (Burton 11). A dynamic understanding of deterrence in cyberspace as formerly suggested by taking into consideration social and historical context will also alleviate the traditionally ‘impossible’ problem of attribution. While such technical capabilities play a crucial role in swaying the allies’ considerations and decisions, the political and strategic issues of simply conceptualizing an offensive cyber policy are examined in closer detail here.

Trust and Transparency

The transparency and capability-sharing quality of NATO may give way for disagreement amongst allies. Although the Alliance’s communication on a strategic and policy level is transparent, it still possesses enough opaque room to maneuver on an operational and tactical level. Furthermore, the problem of American supremacy in cyber capabilities and NATO’s reliance on its critical perspective may displease EU member states like France in their pursuit of strategic autonomy aside from its prevailing aversion to today's American leadership. A new demand for cross-alliance intelligence-sharing on offensive cyber capabilities can also exacerbate internal trust issues with the US. The global surveillance disclosures from 2013 onwards revealed allied surveillance and spying activities which damaged confidence in NATO (Smeets; 2018). Discussion of further integrated intelligence-sharing strategy under an offensive cyber policy can create tension between Five Eyes states (Canada, the US, and the UK) and other NATO allies.

Doctrine Diversity

Another overarching aspect with the potential to determine allies’ reception and leniency towards an offensive cyber strategy is the diversity of threat perception among NATO allies. The diversity across allied standards in defining the parameters of cyberattacks and the lack of overarching offensive cyber policy could result in strategic ambiguity and discourage retaliation (Arts 2). These differences stem from varied threat perceptions and cyber norms. Nationally, both threat perception and cyber norms are influenced by the state’s experience with malicious cyberattacks and its media and public opinion; and externally, the state’s engagement in bilateral and multilateral engagements are the most effective ways in which threat perception and cyber norms are shaped (Lewis 575). This hints at the political interest of near-Russia states like Estonia and Finland to possess well-rounded cyber norms and threat perception. Conversely, policy engagements on offensive capabilities would also shape NATO allies’ understanding as a whole. Without multilateral definitions, allies like Luxembourg and Iceland who have not experienced similar events do not benefit from harmonized knowledge and may not find justification to prioritize the strengthening of cyber capabilities when allocating funds from the common NATO budget. Not to mention the financial commitment issue affects trust in the Alliance overall as well.

Recommendations and Conclusion

The present memo provided an overview of the most pressing issues related to a possible NATO offensive cyber policy with a particular focus on the Alliance’s fundamental deterrence purpose and its policymaking structure. Since supporting volunteered cyber offensive operations on a case-to-case basis does not provide overarching guidance to NATO allies on cyber threats and norms even though offensive capabilities can conceivably function as a credible and powerful deterrent, allies have different understanding of NATO’s evolving offensive cyber leniency’s specific rules of engagement, aim, intended effects etc. But the Alliance’s decision-making structure and cyberspace’s technical complexity offers a wide range of challenges to allies as identified previously.

Going forward, NATO allies need to first revise its cyber deterrence approach to modernize its offensive cyber capabilities framework. Then, it needs to draw on the new cyber deterrence framework to work with specialized allies such as Estonia and the UK to examine the wide range of existing threat perceptions and cyber norms in the Alliance. Lastly, confidence-building measures between the US and NATO need to be strengthened upon commencing extended intelligence-sharing schemes. The achievement of these goals will give a clearer image of the allies’ political will, renew commitments for harmonization and interoperability of the Alliance’s offensive capabilities, and by extension boost its security cooperation.

### Plan

#### The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization in the area of offensive cyber operations.

## Case

### China Hybrid War---2AC

#### Chinese hybrid war ends the LIO, collapses NATO cohesion, and grants China tech supremacy

Varner ’20 [Joe; April 3; former Canadian director of policy in the minister of national defence's office and a consultant on defence policy, strategic intelligence and military operations; Diplomat Online, “The dynamic Russia-China duo: Russia and China are actively working to subvert NATO security in an era of political war,” https://diplomatonline.com/mag/2020/04/the-dynamic-russia-china-duo-russia-and-china-are-actively-working-to-subvert-nato-security-in-an-era-of-political-war/

China’s strategic objectives in Europe are geared to maintaining Chinese economic, political and military power and keeping the Chinese Communist Party in power at home. The goal is not just access to markets, but to split European Union members from one another to prevent unified positions against China and to break NATO and EU cohesion. It is important to note that China’s intention is to replace the post-Second World War (1939-1945) Liberal rules-based order and security architecture with its own Beijing-centric order. China has been hostile to NATO since its embassy was accidentally bombed by NATO forces during the Kosovo War (1998-1999). The Chinese Communist Party’s goal is to separate the United States from NATO and NATO states from one another. There is one major difference between the Russian and Chinese approach to subverting NATO. China still wants access to the EU’s economies, whereas Russia’s view is dominated by an environment of total great-power conflict.

Chinese attempts to subvert Europe include divide-and-rule tactics with Southern and Central European countries. China has negotiated bilateral deals with several EU countries, including the 17+1 group of Albania, Bosnia and Herzegovina, Bulgaria, Croatia, the Czech Republic, Estonia, Greece, Hungary, Latvia, Lithuania, Macedonia, Montenegro, Poland, Romania, Serbia, Slovakia and Slovenia. Eleven of these countries are EU member states and four others are candidates. Taking a page from Russia’s attempt to undermine NATO’s southern flank, in 2017, China stated it was ready to discuss Turkey’s membership in the Shanghai Cooperation Organization (SCO), whose members are China, Russia, India, Pakistan, Kazakhstan, Kyrgyzstan, Tajikstan and Uzebekistan.

As well, Greece and Italy have fallen into the big money-big debt trap of China’s Belt and Road Initiative. Chinese Shipping giant, COSCO, has taken the controlling share of the Greek port of Piraeus and it is said that China wants to build a high-speed rail link between Belgrade and Budapest and then onward to the western part of the continent. The Port of Piraeus is the main sea port of Athens, the largest port in Greece and one of the largest in Europe. In the past decade, Chinese companies have acquired controlling shares in 13 ports in Europe, including in Greece, Spain and Belgium. Together, these facilities handle about 10 per cent of Europe’s shipping-container capacity. In fact, China has gained access to Europe’s three largest ports: respectively Euromax in Rotterdam, of which it owns 35 per cent; Antwerp in Belgium, of which it holds a 20-per-cent stake; and Hamburg, Germany, where it is to build a new terminal. China’s People’s Liberation Army (Navy) warships have already paid a friendly port visit to Piraeus in Greece. Gary Roughead, a former U.S. chief of naval operations, warned that “Chinese port operators will be able to monitor U.S. ship movements closely, be aware of maintenance activities, have access to equipment moving to and from repair sites and interact freely with our crews over protracted periods.”

China is leveraging tensions in the Western alliance over U.S. economic policies, including U.S. sanctions on European countries and Washington’s trade war with China, climate change, multilateralism and the Iran nuclear deal. Beijing also builds networks among European politicians, businesses, media, think-tanks and universities to create layers of active support for Chinese policies and interests as well as a means to shut down and silence commentary from critics and dissidents. China has targeted specific European countries’ vulnerabilities to increase its economic presence, including Greece’s economic crisis and disenchantment among the countries that represent the poor cousins of the EU, those discontented with European Union conditions for investment, such as Serbia, and the United Kingdom post-Brexit. All the while, China is using its investment and new presence to acquire foreign technology through legal and illegal means, with the objective of dominating the innovation industries of the future. The U.S. Department of Defense has warned that China has sought to acquire, legally and illegally, Western technology in order to modernize its economy and build weapons to rival the strength of Western militaries by striking further, harder and faster. Chinese espionage and cyber espionage to gain access to foreign military and industrial secrets is well known. The Chinese government continues its partnership with Russia in Europe, where the two countries have similar strategic objectives and can work together to weaken and degrade U.S. and NATO interests.

### NC3 Entanglement---2AC

#### Yes NC3 entanglement---ensures nuclear escalation

Gompert ’19 [David and Martin Libicki; July 16; Distinguished Visiting Professor at the US Naval Academy and US Principal Deputy Director of National Intelligence from 2009 to 2010; Maryellen and Richard L. Keyser Distinguished Visiting Professor in Cyber Security Studies at the US Naval Academy; Global Politics and Strategy, “Cyber War and Nuclear Peace,” 61:4, p. 45-62]

Warfare against computer networks, not unlike nuclear warfare, tends to be ‘offence-dominant’ in that the efforts, resources and time it takes to defend or restore networks generally surpass what it takes to corrupt or crash them. After all, networks are generally meant to be accessible to facilitate the sharing of information and collaborative work. The growing importance of computer networks, both civilian and military, has given rise to sophisticated efforts to hack into them. Given the pay-offs, cyber-war capabilities are rapidly being developed, diffused and used. This does not necessarily portend a threat to NC3 networks, which are singularly hard to penetrate. Yet the consequences of infected NC3 are dire enough to warrant concern.

At the behest of those who sponsor them, hackers can upset stability by working to induce, prevent or delay the launch of nuclear weapons.12 Directly inducing nuclear launch is extremely difficult and improbable, mainly because launch orders go through human authorities. Moreover, it would take a character from Dr. Strangelove to see the advantage of launching a nuclear weapon without authority.13 Somewhat less difficult and improbable is to create false information that persuades authorities to launch weapons, particularly in the heat of a crisis. We know that indications-and- warning assets, such as satellites and over-the-horizon radar, have mistaken test alerts for real ones.14

Preventing launch or detonation could obviously have huge advantages for the side on which those weapons would otherwise fall. This is some-what more likely than inducing launch, but still very difficult because cyber attacks generally cannot disable weapons by issuing bad instructions unless the weapons are already capable of disabling themselves based on bad instructions. Delaying nuclear launch may be the least unlikely outcome: early-warning systems could be compromised or launch operations delayed by confusion; commands necessary to launch weapons could be tampered with; and false messages could be inserted to override true messages or persuade operators to distrust true messages. Delaying enemy missile-launch could expose retaliatory forces to destruction or cause the enemy to consider a truce.

While a wide variety of non-state actors engage in cyber war, states remain the most proficient actors. Few of them would have the ability to interfere with NC3 in the ways just described. However, the world’s three leading cyber powers are, not coincidentally, the same as the leading nuclear powers. Cyber war is being used for a variety of geopolitical purposes by Russia, and it is being integrated into warfare capabilities and operations by the United States and China. (All three powers engage in cyber espionage, but that’s a different matter.) This state of affairs presses us to ask whether the mutual deterrence that underpins strategic-nuclear stability among the Big Three could be weakened by the offensive cyber-war potential of those same powers.

Again, nuclear stability depends on fear of retaliation devastating enough to overwhelm any justification for a first strike. Of interest here is whether cyber warfare directed against an enemy’s NC3 could allay that fear by reducing the certainty or efficacy of retaliation. The answer to that question depends on which of the big nuclear powers one considers. Because it has the most survivable retaliatory forces, and because neither Russia nor China has BMD or the equivalent of global conventional strike, the United States has the least reason to worry about the strength of its strategic deterrent.

Nevertheless, any cyber attack on its NC3 would be cause for grave concern. The diversity of the US deterrent elements mitigates the risks of Russian or Chinese cyber attack on US NC3. At the same time, because it functions as the central nervous system of the US nuclear infrastructure, loss of NC3 could undermine US deterrence. Consequently, the United States would react strongly to any trace of Russian or Chinese interference with its ability to control and operate its nuclear systems. In fact, the US 2018 Nuclear Posture Review indicates that attacks on its NC3 systems could result in nuclear retaliation.15

A US cyber threat to Russia’s NC3 could be an even greater danger to nuclear peace. Context matters in this regard. Even in the absence of such a threat, the Russians worry more than the United States does – even more than they should – about the survivability and credibility of their strategic nuclear deterrent. Since the early 2000s, when the United States withdrew from the 1972 Anti-Ballistic Missile Treaty, the Russians have dismissed American assurances, however valid, that US BMD is aimed at the likes of North Korea and Iran. US technical briefings and political pledges have not mollified the concerns of Russians consumed by the belief that BMD would expand and improve to the point that a large percentage of Russia’s retaliatory force could be intercepted. When combined with their fear that a highly accurate US nuclear first strike could destroy much of Russia’s predominantly land-based deterrent force on the ground, including missiles in silos, the Russians have long seen American BMD as a threat to strategic equilibrium.

Moreover, as noted, the Russians are fearful of US capabilities to decimate their nuclear deterrent with non-nuclear strike forces. Lastly, US anti-satellite capabilities could potentially take out Russian warning systems and space-based communications. Russia’s lack of such capabilities, as well as effective BMD and global precision-strike, has compounded its fears – not so much that the United States would launch a disarming first strike as that it could use this advantage as leverage in a crisis or even peacetime.

The Russians’ view of US anti-deterrent capabilities and intentions may be exaggerated. But it is a strongly held one, as evidenced by Russia’s modernisation programmes for strategic-offensive forces. Despite a struggling economy, declining state revenues and competing demands on the defence budget, Russia is investing in at least two strategic-nuclear delivery systems that are expressly intended to penetrate US BMD: a transoceanic nuclear torpedo aimed at US coastal cities; and a hypersonic, manoeuvrable ‘glide’ vehicle. The alarm that these have caused in some US circles overlooks the fact that they are inherently second-strike weapons developed in response to US BMD.

In addition to deploying new second-strike systems, however, Russia could resort to nuclear launch-on-warning. This doctrine, inherited from Soviet days, calls for launch of a retaliatory attack when an incoming strike is observed by warning sensors. It is unclear whether launch-on-warning is stabilising or destabilising: it could be the former if it makes a surprise disarming first strike virtually impossible; it could be the latter insofar as it compresses decision time to a few minutes. In any case, US interference with Russia’s NC3 could be interpreted in Moscow as a precursor to nuclear or non-nuclear attack on its deterrent, augmented by BMD and anti-satellite operations. In this context, cyber war could disturb strategic equilibrium and even threaten nuclear peace.

### Undersea Cables---2AC

#### Russia will slash cables.

Sunak ’17 [Rishi; 2017; Member of Parliament for Richmond (Yorkshire); Policy Exchange, “No Shortcut to a European Deterrent,” <https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>]

The prospect of a Russian intelligence ship lurking near American waters – armed with submersibles capable of cutting undersea cables - might seem more at home in a Tom Clancy novel than the pages of The New York Times. Yet in late 2015, American military and intelligence officials spoke openly of a sustained pattern of Russian submarines and vessels “aggressively operating” near cables, highlighting that the vital lines of communication are vulnerable to attack by Russian naval forces. It was reported that US officials were “monitoring significantly increased Russian activity along the known routes of cables”

.55 This specific incident sits against a backdrop of Russian maritime activity which a senior European diplomat has described as “comparable to the Cold War”.56 Indeed, on the other side of the Atlantic, Norway has asked for the aid of NATO allies in locating Russian submarines near its coasts. Media in countries including Finland and Poland57 have also covered what is recognised to be a real threat to NATO countries from Russian interference with their undersea communications infrastructure.

In summary, it is clear that: Russia is investing and enhancing its maritime capabilities, it is increasingly willing to be aggressive in deploying that capability in various theatres and means, and it has a specific interest and track record (Crimea) in disrupting communications infrastructure as an asymmetric method of aggression to offset any relative weakness in hard assets.

Russia is investing in its naval capacity

The collapse of the Soviet Union inevitably led to a decline in the military capabilities of its successor state, the Russian Federation. Investment in modernisation and research were lacking, meaning that the Russian military fell behind the expanding technological capabilities of the West. In 2000, the once formidable Russian Northern Fleet was described as “I’m worried every day about what the Russions may be doing.”58 Rear Admiral Frederick J. Roegge, Commander Submarine Force, US Pacific Fleet “It would be a concern to hear any country was tampering with communication cables.”59 Commander William Marks, US Navy Spokesman 55 New York Times (2015) Russian Ships Near Data Cables Are Too Close for U.S. Comfort 56 Ibid. 57 Giles, K. (2016) The Next Phase of Russian Information Warfare. NATO Strategic Communications Centre of Excellence 58 New York Times. (2015) Russian Ships Near Data Cables Are Too Close for U.S. Comfort 59 Ibid. The Threats to Undersea Cables policyexchange.org.uk | 29 Undersea Cables: Indispensable, insecure being “a greater threat to the environment than the West” – more dangerous for its decaying nuclear power sources than its combat ability.61 Concurrently, the military-industrial complex lacked the capacity to mass produce state-of-the-art capabilities like Unmanned Aerial Vehicles, and many vessels fell into disrepair.

This, however, began to change following the election of Vladimir Putin in 2000. Since this time, the military has undergone an extensive programme of rearmament.63 Furthermore, despite the unfavourable economic context, the Russian Government continues to give spending high priority to the military, and in particular its maritime assets. Indeed, the State Armament Plan 2007-15 set out the explicit aim of constructing “the world’s second largest [navy] by 2027”. Moreover, the modernization of the military is not only increasing its capability but is also reorienting it toward an offensive rather than defensive military force.

Some aspects of the rearmament plan have proved far too ambitious to realise. A project to commission six aircraft carriers by 2020 is still yet to commence, and delivery of new vessels is behind schedule due to economic realities. Yet one area in which the Russian navy must be taken very seriously is in its subsurface capabilities.

Submarine capabilities are of particular importance because this is one area where the West’s advantage is not overwhelming64 – Russian submarines are becoming more advanced as new, modern and quieter vessels begin to narrow the gap between Russian and NATO undersea forces. Several modern classes of new submarine vessels have begun entering service, further increasing Russia’s maritime capability. At the same time, the West’s ability to engage in anti-submarine warfare has eroded since the end of the Cold War.

65 Russia’s auxiliary submarines, often referred to as deep sea underwater stations, are also a threat. Military analysts believe that these craft are Year 2016 2015 2014 2013 2012 2011 2010 Billion Roubles 3,972 4,026 3,222 2,783 2,505 2,029 1,760 % GDP 4.64 4.98 4.13 3.92 3.74 3.40 3.54 Table 1: Russian defence expenditure since 201062 “This is another example of a highly assertive and aggressive regime seemingly reaching backwards for the tools of the Cold War, albeit with a high degree of technical improvement. Are “equipped to be able to manipulate objects on the seafloor and may also carry sensitive communications intercept equipment in order to tap into undersea cables or otherwise destroy or exploit sea floor infrastructure.”

66 Furthermore, while the submarine fleet is of great concern, one class of Russian surface vessel in particular is notable for its capability to interfere with cables through the deployment of submersible craft.68 The Yantar-class intelligence ship carries two submarines designed for underwater engineering missions. The craft are thought to be capable of cutting cables or tapping them for information.

### Solvency---2AC

#### US pressure to integrate OCO’s into NATO strategy is vital to challenging Russian cyber ops---US intel sharing demonstrates good faith attempt to integrate allies

Lonergan ’22 [Erica and Mark Montgomery; January 25; assistant professor in the Army Cyber Institute at West Point and research scholar at the Saltzman Institute of War and Peace Studies at Columbia University; Retired Rear Admiral, US Navy, and senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies; Army Cyber Institute’s contribution to the series, “Compete and Win: Envisioning a Competitive Strategy for the Twenty-First Century, “Pressing Questions: Offensive Cyber Operations and NATO Strategy,” https://mwi.usma.edu/pressing-questions-offensive-cyber-operations-and-nato-strategy/]

NATO members are in the midst of a crisis. With Russia massing troops along its border with Ukraine and moving additional forces to Belarus ostensibly to conduct joint military exercises, policymakers fear that Russia is on the precipice of invading Ukraine and taking additional territory by force—similar to Russia’s annexation of Crimea in 2014. But, even if Russian President Vladimir Putin ultimately chooses not to launch a direct, conventional invasion of Ukraine, it is highly likely that he will continue to pursue Russian strategic objectives in the gray zone short of war. The crisis over Ukraine underscores the challenges NATO faces in competing with Russia in the gray zone—especially in cyberspace.

Russia has no such limitations in the gray zone. In addition to traditional forms of irregular warfare, such as the use of plausibly deniable proxy forces (Putin’s “little green men”), Russia has long relied on cyber operations to subvert and undermine rival governments while avoiding actions that would cross a threshold prompting an overwhelming retaliation. Indeed, in tandem with Russia’s conventional military buildup, Ukrainian government agencies were struck with a spate of website defacements. Microsoft also revealed that it had discovered destructive malware in some Ukrainian government systems, which Ukrainian officials have linked to the Belarusian group GhostWriter. Belarus has close ties to Russia, and observers have speculated that Belarus may have been operating in cyberspace on Russia’s behalf.

While Ukraine is not a NATO member, the current situation underscores the enduring strategic challenge the alliance faces in addressing the cyber threat posed by Russia and other actors. In particular, because cost imposition is an integral part of any deterrence strategy (and has been part of NATO’s conventional deterrence strategy), the alliance has begun to explore how it could incorporate offensive cyber operations as a component of its cyber deterrence posture. But, while NATO took important steps to address cyber defense, it took nearly a decade after Russia’s 2007 cyberattack against Estonia to begin to seriously address the issue of offensive cyber operations. Moreover, NATO cyber policy has traditionally focused on cyber operations in a warfighting context—a focus that comes at the expense of considering cyber operations below the level of warfare. As the recent cyberattacks against Ukraine illustrate, the gray zone just beneath the threshold of armed conflict is where NATO faces its most significant cyber threats. With NATO in the middle of conducting a comprehensive initiative, NATO 2030, to strengthen the alliance, it should incorporate an assessment of the role of cyber operations in routine competition.

Offensive Cyber Operations in NATO Strategy Above and Below the Level of Warfare

Historically, NATO’s cyber posture has largely focused on defense and resilience—and this continues to form the bulk of NATO’s approach. The alliance maintains that its “main focus in cyber defence is to protect its own networks (including operations and missions) and enhance resilience.” At the 2014 Wales summit, NATO endorsed the Enhanced Cyber Defence Policy, which affirmed that cyber defense is part of collective defense and that the alliance would incorporate cyber defense into its planning and operations. In 2016, NATO members pledged to improve their cyber defenses through training, education, exercises, and information sharing.

But the seeds were also planted in 2016 for NATO to consider a potential role for offensive cyber operations. That year, the alliance recognized cyberspace as a domain of military operations, comparable to land, sea, and air. At the 2018 Brussels summit, NATO began to more seriously consider offensive cyber operations. Specifically, NATO created the Cyberspace Operations Centre to coordinate requests for member states to provide offensive cyber effects through the Sovereign Cyber Effects Provided Voluntarily by Allies process. Following the 2018 summit, then-Secretary of Defense James Mattis stated in a press conference that five states—the United States, the United Kingdom, Denmark, the Netherlands, and Estonia—were contributing cyber forces to “help NATO fight in this important domain.” More recently, in June 2021, NATO convened in Brussels and committed to a Comprehensive Cyber Defence Policy. A key feature of the new policy is the prominent role of offensive cyber operations. In Brussels, member states committed to “employ the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats.”

NATO’s shift to incorporating offensive cyber operations into existing strategy and policy has focused on integrating offensive effects into conventional military plans and operations in the context of a conflict. While NATO’s updated strategy is a positive development, its limited focus on conflict scenarios for employing cyber power fails to accurately account for the cyber threat environment NATO faces—particularly the mismatch between the alliance’s clear distinction between wartime and peacetime and the approach of adversaries like Russia, who adopt a competition-conflict continuum. Additionally, the focus on employing offensive cyber during a high-end conventional fight is also not consistent with how several NATO members are already engaged in gray zone offensive cyber operations.

The primary threat to NATO allies in the cyber domain is not from high-end, decisive cyberattacks. Instead, cyber threats more frequently and effectively manifest as gray zone tactics designed to have a corrosive effect without rising to the level of warfare. There are numerous examples of this type of threat. For instance, in July 2021, NATO publicly condemned a range of malicious cyber behavior, including the Microsoft Exchange hack (which NATO attributed to China) and ransomware attacks targeting critical infrastructure. Russia has leveraged cyber and disinformation operations to interfere in democratic elections in the United States in 2016, 2018, and 2020; France in 2017; and Germany in 2017 and 2021—to name just a few examples. Russia also conducted distributed denial-of-service cyberattacks against government websites in Montenegro during the lead-up to, and following, Montenegro’s ascension to NATO in 2017. And when NATO forces were positioned in the Baltics beginning in 2017 as part of NATO’s enhanced forward presence, two threat actors, GhostWriter and Secondary Infektion, conducted a range of disinformation campaigns.

Additionally, the reality is that several NATO members are already speaking publicly about offensive cyber operations below the level of warfare and their statements and actions have an effect on the entire alliance. In particular, NATO member nations have not reached a political consensus about the role of offensive cyber operations. In 2018, the US Department of Defense and US Cyber Command issued new strategy and policy documents that articulated a role for the military in conducting offensive cyber operations below the level of armed conflict outside of US-controlled cyberspace (part of the “defend forward” strategy), and there has been some reporting about US offensive cyber operations. For instance, in 2018 the United States disrupted the Russian-linked Internet Research Agency from interfering in the midterm elections. And, more recently, in December 2021 General Paul Nakasone, commander of US Cyber Command, publicly acknowledged that the military played a role in disrupting ransomware groups targeting critical infrastructure. The United States has also worked with other NATO allies, such as Estonia and Montenegro, to conduct “hunt forward” cyber operations on allied and partner networks to uncover and disrupt malicious cyber activity.

Other NATO allies have also been more transparent about offensive cyber operations. In 2020, the United Kingdom announced a significant investment in its National Cyber Force, its organizational arm for offensive cyber operations, and its 2022 National Cyber Strategy emphasized the role of offensive cyber operations. In November 2021, General Nakasone and the director of Government Communications Headquarters—the UK government’s principal signals intelligence agency—stated jointly that the two governments were collaborating to “impose consequences” in cyberspace to disrupt adversary operations. The Netherlands has also publicly alluded to conducting offensive cyber operations.

Next Steps: Addressing Challenges and Mitigating Risks

Given the threat environment facing NATO, as well as the activities of several NATO members, the alliance should deliberately—but purposefully—consider incorporating offensive cyber operations below the level of armed conflict into its deterrence strategy. Any effort to explore a role for offensive cyber operations should also consider the challenges and risks that may come with doing so. A central challenge is that, at the political level, NATO allies lack consensus on the appropriate application of offensive cyber power—especially below the level of armed conflict. Addressing these disagreements among member states is essential because conducting offensive cyber operations often requires maneuvering through or operating on networks controlled by an ally or allies. Right now, NATO members do not collectively agree on the protocols and processes for partner actions in allied networks—and they also disagree on how to define sovereignty in cyberspace, or when an offensive cyber operation would rise to the level of an armed attack.

Offensive cyber operations for NATO also present real interoperability challenges. The role of intelligence in cyber operations is likely to complicate NATO planning processes. Even close allies are likely to be wary about sharing sensitive intelligence for a number of reasons. For instance, they may be averse to sharing information gleaned from signals intelligence collection or because a member state may be using the same exploits for both offensive action and their own espionage—including intelligence collection against allies. Or, allies may simply be worried that sensitive information may become exposed. On top of this, it’s challenging to adjudicate intelligence requirements among allies and to deconflict intelligence and military priorities. It is also not clear whether the alliance has established consensus thresholds that specify the conditions and timeline under which a state would have to notify others of its activities on their networks—if at all.

The alliance should account for, and address, these issues as NATO explores the prospect of incorporating offensive cyber operations below the level of armed conflict into existing NATO simulations and exercises that span the strategic, operational, and tactical levels. A number of important questions about how to coordinate offensive cyber operations and define roles and responsibilities remain unanswered. For instance, how could allies improve intelligence sharing to conduct more rapid attribution, enabling one state or the alliance to respond to adversary cyber activity? What are the conditions under which allies should consider dividing responsibilities for cyber campaign planning and developing accesses and capabilities against strategic targets in, for example, Russia? If some allies are responsible for offensive cyber operations against certain targets, what are the information-sharing and notification requirements?

#### Cyber capacity-building key to effective defense

Maigre ’22 [Merle; April 6; senior cybersecurity expert at e-Governance Academy in Estonia; served as director of the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE)in Tallinn; German Marshall Fund of the United States; “NATO’s Role in Global Cyber Security,” https://www.gmfus.org/news/natos-role-global-cyber-security]

Another course of action for NATO in cyber security is to increase its cyber capacity-building efforts for partner countries of strategic importance, reinforcing NATO’s commitment to partners and projecting stability in NATO’s neighborhood. This kind of cyber capacity-building could include various types of support, ranging from strategic advice and cyber institution-building in defense sectors to education and training or advice and assistance in cyber defense. The objective should to be to enable capacity-building activities for military actors, along with the provision of training, equipment, and infrastructure for security purposes. This would allow NATO to improve the capacities of partners to address crises, prevent conflicts, and cater for their own security and stability by themselves, to the benefit of their population.

As one example, NATO could fill a gap in capacity-building for partner countries by bringing together military Computer Emergency Response Teams (CERTs) to share information on incident management dynamics, a key factor in modern cyber defense. While partner countries can receive support from donors in establishing mechanisms and processes to exchange information between civilian CERTs, such cooperation and communication channels are much less developed in the military domain due in large part to the high sensitivity of the information. There is a need to extend the information-sharing practices used in civilian circles to partner countries’ military CERTs. Building cyber-security capacity should focus on partners’ ability to respond to and recover from cyber incidents.

### AT: Norms Fail

#### The only barrier to effective cyber arms control is American antipathy---the plan can successfully generate international pressure

Mette Eilstrup-Sangiovanni 17 {Dr Mette Eilstrup-Sangiovanni is Senior University Lecturer in International Relations and a Fellow of Sidney Sussex College. 7-21-2017. “Why the World Needs an International Cyberwar Convention.” https://link.springer.com/content/pdf/10.1007%2Fs13347-017-0271-5.pdf}//JM

The arguments presented in this article should not be read as a statement of ingenuous optimism. Negotiating an ICWC will be fraught with difficulty given the diverse interests at stake, and the task will not be accomplished overnight. Nonetheless, I argue, most standard objections to embarking on a process of international negotiation (including difficulties of verifying compliance and problems of rapid technological change) fail on closer inspection. In the end, the main barrier to an international agreement on governing cyberconflict may be opposition by powerful (mainly) western states, whose desire to exploit current strategic advantages in the cyber-domain leads them to reject a treaty. For example, many observers judge that America’s enduring hostility towards binding international rules for cyberspace is driven largely by its technological superiority in the realm of tactical electronic warfare, which provides a strong incentive to maintain maximum freedom of action in this domain (see Baruah 2013; Clarke and Knake 2010; Sanger 2015; Lindsay 2015, 46, 61–62; Sanger 2015; Goldsmith 2011). Not only would America be reluctant to bargain away its ability to exploit current tactical advantages, but as the world’s strongest cyber power, American decision-makers may fear that by accepting binding international constraints on the conduct of cyber warfare, they would be trying their own hands while allowing other nations to rapidly catch up (see Singer and Friedman 2014). Such reservations are too shortsighted. Given the current global rush to invest in offensive cyber power, America’s unrivaled position in the cyber domain may well be temporary. For now, however, America’s leading position provides a unique opportunity to shape international rules and norms for cyber conflict. By assuming a global leadership role, Washington might succeed in encouraging other states to accept constraints on the use of cyber offensive power before these states acquire significant offensive capabilities of their own.39 During the 1950s and 1960s, American leaders were sufficiently foresighted to see that they could exploit US superiority in the realm of nuclear technology to shape international rules regarding nuclear arms control. By promising self-restraint and by offering to share civilian nuclear technology, Washington succeeded in persuading other states to accept the norm of an international nuclear hierarchy and thereby prevented an uncontrolled global nuclear arms race. A similar opportunity is currently spurned in the cyber domain. The arguments presented in this article suggest it is time US policy-makers change course and give their support to negotiating an ICWC.

#### Proportionate response solves.

Dougherty 17 -- Jill Dougherty, CNN, citing Michael N. Schmitt, chairman of the US Naval War College's international law department. [NATO cyberwar challenge: Establish rules of engagement, 11-7-16, https://www.cnn.com/2016/11/07/politics/nato-cyber-centre-international-law/index.html]

But under international law, does President Barack Obama have the legal right to retaliate?

Schmitt of the Naval War College maintains that Obama "unambiguously" does have the right to respond, but Schmitt would not use the term "retaliate."

"In international law, we don't do tit for tat," he said. "What we may do is engage in what is called -- and this is a legal term -- 'counter measures.' "

Counter-measures are operations that would otherwise be unlawful but can be used if the purpose is to stop another state from violating the law.

So the US could hack back against the Russians? The answer is yes, Schmitt said, as long as Washington reasonably believes Moscow is going to continue to hack it.

Counter-measures don't have to be cyber-related. The US, for example, could prevent Russian ships from transiting its territorial waters until Russia stops its cyber breaches.

The response, however, must be "proportionate." Shutting down a Russian electric grid would only be permissible if it didn't cause more harm to Russia than its hacking caused the US -- a tricky thing to measure.

As the US considers itself a law-abiding country, it most often tries to follow accepted international law of war principles. It could, however, ignore those internationally accepted principles or interpret

#### Actions create defensive norms.

Machiels 19 -- Maaike Machiels, master’s degree in administration of law from Hasselt University. [Active Cyber Defence and NATO - NATOs innovative offensive strategy towards Russia and China, 11-1-19, https://atlantic-forum.com/content/active-cyber-defence-and-nato-natos-innovative-offensive-strategy-towards-russia-and-china]

2. NATO’s position in Cyber Defence

International law is created by and for states. According NATO’s Cyber Defence Pledge, the Alliance’s mandate has always been essentially defensive, relying on its Allies’ cyber capabilities to execute operations. (Legal) protection of critical infrastructure and related offensive strategies always remained a sovereign national prerogative, while NATO’s cornerstone was to build a resilient cooperation, founded on information-sharing, education, and risk management, to counter any negative consequences resulting from cyber attacks. To date, NATO’s priority lies with improving its own institutional infrastructure and computer networks, whilst supporting and bolstering resilience and defence capabilities through multinational projects.[vii] Nonetheless, future NATO policies should take a stance regarding the behaviour of Allies when being attacked by an aggressor state, and NATO has to reconcile its own agenda with the approaches of its members.[viii]

NATO has proven to be concerned with the rapid evolution of cyber space and cyber threats thanks to its many endeavours during the last years. The inclusion of cyber attacks in Article 5, the embodiment of NATO’s collective self-defence, incited further action in the cyber field. For instance, NATO provides adequate resources to its Allies through institutions such as the NATO Cyber Defence Centre of Excellence, the NATO Cyber Rapid Reaction Teams, the NATO Computer Incident Response Capability, and cooperation with national CERT (Computer Emergency Response Teams). The resilience strategy of NATO’s cyber defence strategy is reflected in the outcomes of the Warsaw Summit and the Brussels Summit. Moreover, NATO has fostered cyber interoperability with the EU, the UN, the OSCE, and industrial stakeholders as well as sponsored national cyber initiatives.

Current Challenges

The preamble of the North Atlantic Treaty emphasizes NATO’s guiding purposes and principles: freedom, civilisation, democracy, individual liberty, the rule of law, and the preservation of peace and security. In light of the emergence of Russia and China as possible adversaries in a future cyber conflict, the importance of these fundamental principles when engaging in cyber warfare was questioned during the Munich Security Conference in February 2019.[ix] On the one hand, cyber policy strategies concerning critical infrastructure are a national prerogative. On the other, these national strategies do not necessarily coincide with other states, nor are they governed by one institution; therefore, they remain very much unregulated on the international scale.[x] Despite states’ dominant role in cyber defence, two newly emerging infrastructure networks are nonetheless worth addressing on the NATO level: Chinese 5G networks and GPS networks mainly threatened by Russia.

2. Critical Infrastructural Challenges

Chinese 5G Networks

Huawei’s innovative 5G network will provoke a major evolution in global economics, (cyber) security, and policy-making.[xi] Among other benefits, 5G networks promise faster data speed, enhanced artificial intelligence and machine learning in the global market, and will thus conquer a major position in all corners of the ‘internet of things’ across the globe. Huawei, holding the world’s largest market share, has completely surpassed other ‘5G pioneers’ such as Ericsson, Nokia, and ZTE.[xii] Huawei’s dominance, acquired through government support, investment in education and technological innovation, attractive selling prices, large-scale contracting, and unrivalled competition, have aided Chinese economic and governance models in penetrating Western, democratic societies.[xiii]

Western economic powers and alliances fear China’s prevalence in the global market. Even though a 5G-breakthrough is an enormous (economic) goal rather than merely a security risk, several NATO Allies[xiv] have attempted to diminish China’s influence on their national networks, including completely banning Huawei’s services. This measure is based on a multitude of legitimate concerns.

Firstly, exclusively relying on one vendor, in this case a society driven by national interest instead of individual human rights, might facilitate China’s illegal meddling in Western societies’ data. China is known for its cyber espionage and mass surveillance practices[xv] and does not refrain from publicly identifying itself as an adversary of Western democracies.[xvi] Even more so, China signed a deal with Russian’s telecom giant MTS to launch 5G-generation in 2019–2020. This bilateral agreement further distances China from any democratic cooperation with Western democracies and solidifies its economic position against the ‘rest of the globe’. Likewise, by co-opting Russia, China might pose a greater military threat to the heart of the Alliance.

Secondly, Huawei has refrained from divulging any information regarding its internal functioning or its relationship with the government, Chinese military, or intelligence service. In spite of many public allegations, Huawei has brushed these off by stating it is the most audited technology company in the world.[xvii] This lack of disclosure renders any transparency impossible between democratic states and Chinese companies.

Thirdly, smart technology paves the way for potential surveillance over the entire planet. States with a weaker human rights protection, such as Serbia, Turkey, and Russia, have been subjected to mass surveillance through the purchase of Huawei’s cameras with facial recognition software, thereby endangering its citizens’ human rights and subjecting its own government to political meddling.[xviii]

The purchase of 5G networks by some NATO Allies illustrates a dual approach towards external cyber powers: states benefit from the advantages of global trade, on the one side, and avoid a possible adversary in future cyber conflict, on the other.[xix] These differences in policy-making might cause fractures within the Alliance and renew debates concerning fundamental Western values.[xx] National policies, financial and technological resources are strongly nuanced and differ amongst each other,[xxi] and there is no consistency between national policies on the threat Huawei poses. The UK, not lacking resources for cyber defence, established the “UK Huawei Cyber Security Evaluation Centre”. This centre, with newly erected centres in Germany and Belgium to follow, is a rigorous supervision mechanism overseeing Huawei’s operation in the national context and aims at holding Huawei accountable for any breaches in national cyber space. Two-thirds of NATO’s allies, nonetheless, lack the necessary resources to establish such oversight mechanisms and are dependent on richer third countries, such as the UK.[xxii] Concerns regarding sensitive information sharing between NATO and Allies might raise tensions and obstruct (bilateral) agreements.

Apart from its Allies, NATO itself might suffer damages. NATO depends on the critical infrastructure of its Allies to execute national operations and missions. Therefore, any threat to critical national infrastructure affects NATO by extension. Even more so, any threat to its Allies is a threat to NATO’s founding values. NATO must ensure (military) safety outweighs economic benefits.

GPS networks

Space-based assets should be awarded a major position in future debates about the protection of critical infrastructure of NATO Allies. To some extent, data stemming from other critical infrastructure is highly dependent on terrestrial networks, such as the reliance of telecommunications on GPS satellites. This interoperability might lead to a cascading effect, where not only the attacked server suffers damages but all linked networks representing different aspects of society.[xxiii] Therefore, a cyber strategy proportional to the scale and gravity of the cyber threat should be in place.

Space-based assets encompass cyber elements that depend on navigation and (geo)location in which the global position system (GPS) is the most important—and hackable—tool, because its data flows through satellites, ground stations, and land pipes.[xxiv] Even though critical terrestrial infrastructure goes far and beyond GPS satellites, this article will remain limited to illegitimate interference in GPS systems as this might pose an equal threat to NATO and its Allies.

GPS systems not only transmit data between terrestrial satellites but operate through ground stations, connecting landlines and user terminals. All these tools may be endangered by cyber threats. Apart from the multitude of possible targets, cyber threats themselves are multifaceted. Cyber threats to GPS systems might range from causing rather minor disturbances in the satellite’s network, such as monitoring data patterns, to severe cyber attacks, such as inserting corrupted data, loss of data, widespread disruptions, or permanent loss of a satellite. On top of that, military and commercial assets cannot strictly be distinguished. For example, military GPS signals are often deployed in commercial aviation. Accordingly, cyber threats to military targets might cause (collateral) damage to civilians, as well. This peculiar predicament is especially concerning for NATO, as the organization relies on Allies’ military GPS infrastructure. Considering society’s equal reliance on military and commercial infrastructure, a nation-state lacking considerable resilient GPS networks exposes not only its government and military to cyber threats but also its citizens. An undemocratic foreign power’s, such as Russia’s or China’s, dominance over civil aviation might threaten the individual human rights of the buyer nation’s own citizens, no matter its economic advantages.[xxv]

Like China, Russia is known for its unlawful interferences in Western democracies’ cyber space and being the aggressor of cyber attacks on (military) institutions, companies responsible for vital national infrastructure, and citizens. Russia claims to dispose of assets that are capable of disrupting cyber space or that might deny space-based assets to adversaries in future warfare as a form of military boycott.

Another reason to prioritize cyber defence for GPS networks is their inherent two-fold vulnerability. Firstly, several supply chain elements of GPS networks in commercial use are barely traceable. In combination with the lack of a coherent global supervision mechanism, data leaks, breaches, or weaknesses in the supply chain are often not addressed nor can military security standards be enforced.[xxvi] Secondly, NATO expressed its desire to include space as a domain of warfare during the London Summit end 2019. Even though many applaud the inclusion of space into modern warfare categories, the principles of international humanitarian law will have to be reshaped to be pragmatically useful for space warfare. For instance, scholars will have to investigate how the principle of distinction can govern an attack on a satellite with dual (civilian-commercial and military) use.

Moreover, the threat to national cyber space reflects a threat to NATO as an organization. NATO has no satellites of its own, with the exception of stationary ground satellite communications.[xxvii] When it wants to conduct a military operation, NATO is obliged to solicit its member states or GPS equipment and software. In brief, NATO remains highly reliant on its allies for all space-sourced data, information, and services, and the present security of space capabilities is ultimately in the hands of states. Consequently, a cyber attack on a national satellite might equally affect cyber space in a member state and in NATO itself.

3. Conclusions and Recommendations

The Brussels Summit of 2018 and the Cyber Command Structure of 2023

During the Brussels Summit in 2018, NATO recognised the complex and rapidly changing nature of cyber space and ventured in the direction of developing an ‘overarching space policy’, which was finally approved on 27 June 2019. NATO Secretary General Jens Stoltenberg emphasized the defensive nature of NATO’s operations in which NATO needs to be a forum to share information, support allies, and increase interoperability. Apart from solely addressing ‘space’ as a vulnerable factor, the outcome of the Brussels Summit introduced a New Cyber Operations Centre in Belgium that will serve to strengthen the cooperation between NATO and its Allies by assimilating NATO’s resources within the needs of Allies’ operations.[xxviii] This newly founded centre will operationalise the new Cyber Command Strategy starting from 2023.

Recognising the rising cyber threat from non-democratic countries in an enhanced, economically dependent and interconnected globe, NATO wishes to integrate member states’ cyber capabilities into NATO operations. These operations will be coordinated by the Cyber Command Centre in Belgium and will remain under one general, unified command of the Supreme Headquarters Allied Powers Europe (SHAPE). The Supreme Allied Commander Europe (SACEUR), thus enabled by a crafted and pragmatic operations’ toolbox, will offer an immediate and ‘real-time’ response to cyber threats, much like the pre-existing agreements on air defence and ballistic missiles. The purpose is to go beyond pure protection and prevention of attacks on Allies’ and NATO infrastructure and to acquire a full understanding of NATO’s cyber space, in particular its vulnerabilities. This will be a reliable tool for commanders and to deter possible future adversaries from attacking.

NATO’s newfound ability to interfere directly with adversaries’ operations, manipulate infrastructure through malware, shut off power networks, and stop an attack before it happens will affect the calculations of hostile actors, particularly whether or not the potential cost of the attack outweighs strategic gains.[xxix] In brief, this command structure implies a major policy shift from NATO’s past, purely defensive mandate to granting NATO the capacity to launch offensive attacks.

However, while applauding NATO’s awareness of the emerging threats and its recognition of a swift, unified response, a multitude of challenges must be overcome in order to render the command structure operational. To date, NATO lacks cyber warfare principles, thereby lacking any legal ground to derive hands-on rules regulating NATO’s offensive attacks and diminishing its ‘immediate reaction’ capacity.[xxx] Besides lacking cyber warfare principles, NATO’s general policies are absolutely a conditio sine qua non that determines how to respond offensively. So far NATO remains dependent on US policy and steers its operations on a case-by-case analysis, which will not be effective under a general command structure. Therefore, a formalized general command is absolutely vital to offer top-down guidance to Allies.[xxxi]

As cyber threats penetrate all layers of society, a holistic command structure should go beyond unifying purely military responses and enlarge its scope to the private sector, because the private sector’s strong online presence, for instance, might contribute to combating misinformation.[xxxii]

Conclusions and recommendations

Even though NATO recognizes the absolute necessity of a unified, formal, immediate, and holistic command, the enforcement of this command structure remains rather utopian. Following the formation of such a command, NATO will have to develop a general policy plan to carry out its new command structure mandate. This section will, while concluding the previous sections, reflect on a few policy recommendations that should be taken into account before 2023.

### AT: Say No---2AC

#### US leadership solves---intel sharing causes allied buy-in

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

When it comes to intelligence sharing, some allies fear that infiltration and attacks against countries with lower resilience could potentially compromise information shared by other member states. Pushback against greater transparency is especially strong on the part of the United States, which owns a large share of NATO’s intelligence capabilities, making it a critical player in alliance intelligence operations from a tactical as well as strategic perspective.[33] Due to the country’s outsized role in this field, NATO’s intelligence adaptation is largely dependent on U.S. inclinations to share capabilities and information with other allies.[34] Although efforts to protect intelligence by minimizing sharing may be justified, elevating the role of the United States in NATO’s cyber policy without increasing transparency could potentially limit tactical effectiveness.

#### Allies will grow more supportive as cyber threat increases

Lété & Dege ’17 [Bruno Lété, International Relations Master’s, a transatlantic fellow at the German Marshall Fund. Daiga Dege, PhD Researcher in Russia and NATO cyber operations at Tallinn University, International Relations Master’s at Latvijas Universitate, “NATO Cybersecurity: A Roadmap to Resilience, the German Marshall Fund,” No. 23, https://www.gmfus.org/publications/nato-cybersecurity-roadmap-resilience]

Consider Offensive Cybersecurity

NATO now recognizes a serious cyber-attack as a potential Article 5 trigger. But the doctrine and crisis management conditions enshrined in NATO’s cyber policy puts the emphasis on a defensive posture only. As such, the Alliance fails to recognize cyber as a force multiplier that could be of importance to the defense of NATO nations. Russia for instance considers offensive cyber capabilities to be an integral part of its military power and especially as a way to make up for its relative lack of conventional forces compared to NATO. The rise in connectivity, smartphone proliferation, cloud computing, growth of application development, and other technological advances open new avenues to attackers and force defenders to cover an ever-increasing number of fields. In the long run, NATO’s defensive approach is not sustainable. It is time for NATO to start a debate on offensive cybersecurity and map the feasibility of coordinating counter strikes, and to establish a significant offensive cyber capability. NATO could center this debate on projecting offensive cyber warfare capabilities as a means of deterrence, similar to the perceived value of nuclear weapons to deter attacks against NATO.

Offensive security will allow the Alliance to better control the virtual battlefield. There are valuable cyber capabilities worth attaining, including the ability to conduct reconnaissance and surveillance, intercept communications, or deny resources and access. NATO may find increasing support to have a conversation on offensive cyber security with its allies. As member states are increasingly preoccupied with defense and deterrence issues in cyber-space they will show more receptivity to cooperation with NATO on developing centralized offensive cyber capabilities.

### AT: Assurance Link---2AC

#### Allies want more assertive cyber postures, NOT less.

Schneider & Herr 18 -- Jacquelyn Schneider, Cyber Conflict Studies Professor at the U.S. Naval War College. Trey Herr, visiting fellow at the Hoover Institution. [Sharing is Caring: The United States’ New Cyber Commitment for NATO, 10-10-20, https://www.cfr.org/blog/sharing-caring-united-states-new-cyber-commitment-nato]

Given the recent blockbuster headlines about alleged Chinese snooping on server hardware sold to major technology companies and the latest joint-denunciation of Russian cyber operations, you could be forgiven for having missed an important NATO-related development. The Associated Press reports that the U.S. Defense Department will announce a new commitment to use offensive and defensive cybersecurity capabilities on behalf of NATO allies.

The new commitment is notable given how cybersecurity has long been treated as an exceptional domain of operations, and cyber capabilities reserved as strategic national assets to be shared with only the closest of allies. With this announcement, the Pentagon is suggesting that cyber capabilities might be used alongside conventional weapons with allies and indeed, equal weight appears to be given to offensive and defensive operations. Perhaps most significantly, the announcement moves NATO partners closer to what has been a tight coterie of U.S.-favored signals intelligence partners such as the United Kingdom, New Zealand, Australia, and Canada.

The DoD announcement is a sign of the continued, if nascent, normalization of cybersecurity under the current administration and in Europe. Even where offensive cyber operations may not rise to the level of war, they provide decision-makers with options to influence the geopolitical environment. This aligns with recent trends in the U.S. military to integrate cyber capabilities into maneuver units and large exercises, and reflects the shift towards more risk acceptant and offensive measures to counter cyberattacks found in the 2018 DoD Cyber Strategy.

Moving cyber capabilities into the same strategic frame as conventional weapons, especially with NATO, reflects a shift in institutional cyber arrangements within the United States and the growing power of the military relative to the intelligence community. For the United States, cyber capabilities have always had a complicated relationship with the intelligence community, in particular the National Security Agency (NSA). When Cyber Command stood up in 2010 as a sub-unified combatant command within the Department of Defense, it moved into the NSA’s headquarters, staffed its management ranks with longtime NSA employees, borrowed networks and technical capabilities, and to this day shares a dual-hatted commander. In the immediate years after the command was created, it was logical that the structure of partnerships with allies looked more like the special signals intelligence relationships formed around the NSA rather than traditional alliance networks in NATO and Asia. The recent announcement aligns cyber operations more closely with Department of Defense missions, which are more likely to posture capabilities for deterrent effects, than intelligence missions, which view capabilities as assets to be carefully husbanded.

Treating cybersecurity capabilities more like conventional arms and less like national assets also helps drive the integration of cyber operations into the planning and execution of a broader array of conventional military missions. Early cyber operations were largely conventional espionage and surveillance activities supercharged by the spread of computing and the internet. In the United States, this led to the creation of large and complex software tools, carefully guarded by the intelligence community as national assets (sometimes unsuccessfully). The DoD’s announcement indicates a move towards treating at least some of these capabilities, along with their supporting infrastructure, more like conventional armaments and making them available for broader use; a model closer to Central or Special Operations Command and less like the National Security Agency.

The Pentagon’s new commitment also reflects changes in how Europe talks about cybersecurity and characterizes the Russian threat. The last two years have seen a trend toward more open discussion of offensive cyber operations and the possibility of the alliance adopting more assertive postures to counter cyber operations against its members. After years of devastating ransomware attacks and cyber-enabled information attacks, NATO members are more willing to explore cyber triggers to Article 5. They have also been more willing to articulate the cyber threat against the alliance. In addition to last week’s denunciation by Dutch, UK, and U.S. authorities, Russian state actors are widely suggested to be responsible for an increasingly brazen series of operations, including targeting German government ministries, French and British TV stations, and more.

### AT: Attribution Fails---2AC

#### Attribution’s not a barrier.

Jeremy **Rabkin &** John **Yoo 17**. Rabkin is a Professor of Law at the Antonin Scalia Law School, George Mason University; Yoo is currently the Emanuel S. Heller Professor of Law at the University of California, Berkeley. 09/12/2017. “CHAPTER 6 Cyber Weapons.” Striking Power: How Cyber, Robots, and Space Weapons Change the Rules for War, Encounter Books.

Many commentators worry that, whatever their immediate destructiveness, cyber attacks remain especially dangerous because they are hard to track. The Internet is an immensely complex web of connections. Messages are routed automatically through available channels in this dense network. They may go halfway around the world before they are delivered to a neighboring state or a neighboring country. A sender who wants to disguise the origins can take control of a computer in a distant country and make it appear that this was the source of the hack. It is very difficult to respond when there is doubt about the source of an attack. Analysts call this the “attribution problem.” Even sober officials are concerned that attribution may interfere with the normal incentives behind deterrence. General Michael Hayden, former Director of the National Security Agency, warned in a 2011 essay that, “casually applying concepts from physical space like deterrence, where attribution is assumed, to cyberspace, where attribution is frequently the problem, is a recipe for failure.”26 A more recent study, Cybersecurity and Cyberwar, asserts that among “dimensions that make the cyber arena so challenging to secure . . . the most difficult problem is that of attribution.”27 The trouble with cyber intrusions is that they are spectral. We often can’t tell where they have come from. We often don’t know where they may go next. Cyber attacks may not be inherently more destructive than conventional weapons. But they are harder to identify. For alarmists, the attribution problem makes cyber warfare especially tempting for reckless governments or for terrorists. In Clarke’s scenario, the president considers whether to retaliate for the cascade of horrors falling on American cities by ordering cyber command to “turn out the lights in Moscow” or “hit Beijing.” But the president is paralyzed because it is not clear whether Russia or China is actually the power responsible for all of those attacks.28 There is some ground for this concern. Cyber attacks can be routed through a chain of computers in different countries.29 Tracing the proximate source of an attack does not always indicate where it was actually planned, directed, or launched. Computers in the chain may be redirected, without the collaboration or even the awareness of their own operators. They can be made to perform certain commands in robotic fashion, working as “botnets.” Determining who should finally be blamed for a cyber attack can prove a considerable technical challenge. In the episodes mentioned previously, such as the disruption of Estonian government websites, the Stuxnet disruption of Iran’s nuclear program, the disruption of computers at Saudi Aramco, and the vandalism at Sony Pictures, no government officially acknowledged responsibility.30 When no attacker claims credit for a cyber attack, its attribution may be disputed. Residual uncertainties, however, need not prove an obstacle to deterrence. As in clandestine operations, non-avowal is not always about confusing the intended target. Israel’s spy agency, Mossad, has tracked enemies to foreign capitals and killed them. It rarely acknowledges responsibility. Deniability gives diplomatic cover to host nations, which can claim to be “concerned” without having to strain their own relations with Israel. It may also make the intended targets and their organizations less certain about their safety and freedom to operate. The possibility of obscuring responsibility for lethal attacks has not emboldened governments to use assassination regularly around the world. Past a certain point, other states will insist on tearing off the pretense that they have “no idea” who may be responsible.31 As with kinetic attacks using bombs and bullets, attribution in the cyber realm is not an all or nothing enterprise. Analysts can assemble information that can identify the source of an attack with a fair degree of probability. They can compare characteristics of one attack with those of other attacks known to be associated with particular countries. Government agencies can assemble evidence from other sources (regarding the capacities and intentions of foreign powers) to compare with assessments by cyber specialists.32 A state that is suspected of involvement can be pressed to cooperate with the investigation and much may be learned from how it responds, or how it does not.33 Concern over the attribution problem also ignores the purpose of the inquiry. Attribution is not for etiological analysis in a medical sense, let alone for adjudication of criminal guilt. If an attack causes enough damage, an investigation for national security purposes can proceed under the standard of a “preponderance of the evidence” or reasonableness, rather than the criminal justice system’s “beyond a reasonable doubt.” Furthermore, the United States can hold nations liable for cyber attacks that originate on their territory. Just as they do with terror networks or militia groups, governments sometimes protect or work through hacker gangs, which commit cyber mischief to extort payments, perpetrate scams, or steal valuable information. The United States and other nations have long maintained the right to use force to stop attacks emanating from foreign countries, and to hold accountable the governments that refuse to stop them. In the wake of the 9/11 attacks, for example, the U.N. Security Council authorized an invasion of Afghanistan, even though the Taliban leadership was not accused of plotting the attacks. In the cybersphere, the United States could reasonably extend this claim to countries whose territory serves as a base for cyber attacks, which the host government will not help to control.34 The supposedly severe problem of attribution has not made cyber weapons attractive to the very actors most often desirous of secrecy. Terrorists groups depend on their ability to conceal their attacks and disguise their operations as normal civilian activity. Judging from experience to date, terrorists have not carried out destructive cyber attacks. A study by political scientists tracked “cyber incidents” between 2001 and 2011.35 Almost all occupied the low end of the spectrum of destructive impact. Whether it was the “Cyber Gaza” group attacking websites in Israel or the “Syrian Electronic Army” (loyal to Assad) attacking websites in the U.S., the damage involved resembled vandalism more than serious injury.36 And in the twenty interstate conflicts where cyber incidents occurred, traditional terror attacks (involving on-the-ground violence aimed at killing or wounding human beings) were almost 600 times more frequent than these cyber incidents.37 “Terrorists” rely on “violence that instills a sense of fear and horror,” writes a defense analyst. “To that end, terrorist attacks tend to be extremely violent, bloody, and photogenic. They want to hurt or kill their victims in a way that disturbs as many people as possible and is seen by as many people as possible.”38 Cyber attacks do not lend themselves to this strategy. Nor have terrorist groups been able or willing to invest the considerable resources required to execute the most fearful sorts of cyber attacks.39

### Allies Like The Plan---2AC

#### The U.S. push bends allies to support America’s position---asymmetrical power ensures they’ll fall in line.

Sperling ’19 [James and Mark Webber; 2019; Professor of Political Science at the University of Akron, Ph.D. from the University of California at Santa Barbara; Professor of International Politics at the University of Birmingham, Ph.D. from the University of Birmingham, Master of Social Science from the University of Birmingham, B.A. from the University of Warwick; International Studies, “Trump's Foreign Policy and NATO: Exit and Voice,” vol. 45, p. 516-517]

Institutional effects

Three specific institutional effects associated with NATO illustrate more precisely why voice is preferred to exit. In this section we survey these as trends over time as they affect the US. We then turn to the policy of the Trump administration to show how the proclivity for voice has persisted.

Institutional pull

The first of these effects is institutional pull, the enduring attractiveness of NATO to the US. We have already alluded to NATO’s institutional qualities, but of note here is how these have been bent to American design. That advantage is an enduring consequence of the asymmetry of power that has characterised the Alliance since its formation in 1949. NATO’s functioning in the Cold War, Robert Osgood argued, was premised on the fact that ‘no group of allies’ was capable of acquiring ‘independently of the United States, an adequate military basis for protecting its vital interests’. 39 That state of affairs has persisted. The end of the Cold War resulted in a significant drawdown of US forces in Europe, but as of September 2018 there were still approximately sixty-four thousand active US service personnel on the continent. In fact, with the end of US combat missions in Iraq and Afghanistan, a Cold War pattern has reasserted itself: US troops are again concentrated in East Asia and Europe (Japan, Germany, South Korea, and Italy being the top four locations of US forces overseas). 40

NATO operations – both in and beyond Europe – have also reflected America’s military weight. Interventions in Bosnia, Kosovo, and Libya would simply not have been possible if run by European allies. NATO’s reaction to the 2014 Ukraine crisis prompted an upscaling of European effort but European forces have remained constrained by years of under-investment. One recent study has suggested that ‘the major European allies would be hard-pressed to provide one combat-capable brigade at short notice’, whereas the US even in Europe ‘is set to have three combat brigades … present at all times’. 41 France, the UK, Germany, and some other allies may have developed niche capabilities in cyber, special operations, and drones, but in these regards also none can match the US in the scale and sophistication of military effort. NATO, in effect, has been the institutional means by which these differences have been accommodated. Allied defence planning has been one long exercise aimed at obtaining European interoperability with America’s quantitative and qualitative military advantages. That NATO’s Supreme Allied Commander Europe (SACEUR) has always been an American (the post being double-hatted with that of the Commander-in-Chief of US forces in Europe) is further evidence of European deference to American military power and priorities.

NATO is attractive to the US not simply because it is a collection of supplicant allies, but because it harnesses those allies in a predictable and sophisticated manner. NATO is the mechanism that ensures military interoperability of European and Canadian forces with those of the US, embeds a sophisticated command and planning structure that favours US oversight of the European theatre of operations, and shapes the national security priorities of its members consistent with American strategic objectives. Recognising these virtues, the US has an interest in NATO’s sustainment. It has, therefore, pursued policies that, while attuned to US interests, are also designed to add credibility to NATO itself. For instance, NATO nuclear sharing is an arrangement less to do with ‘the deterrence of adversaries’ and more with ‘catalyz[ing] agreements about broader strategy’ among allies. 42 In Afghanistan, NATO-ISAF was eventually folded into a US-led command structure and so the alliance and American fortunes were conjoined in the anti-Taliban campaign. 43 The US military response to the 2014 Crimea crisis was similarly framed by a NATO position aimed at deterring further Russian aggression.

#### Consultation over doctrinal ambiguities resolves allied fears

Jens Ringsmose 17, Director, Institute for Military Operations, at the Royal Danish Defence College and Professor II at the Royal Norwegian Air Force Academy, 5/15/17, "Now for the Hard Part: NATO’s Strategic Adaptation to Russia", Survival, Global Politics and Strategy, Volume 59, Issue 3, https://www.tandfonline.com/doi/full/10.1080/00396338.2017.1325603

In light of this, the fundamental challenge for NATO in its Russia policy is to avoid the temptation to become overly obsessed with hardware issues: budget numbers, force structures, fill rates, reaction times, command posts and so on. These issues matter, but their importance ultimately pales in comparison with the detente challenge and the question of what NATO hopes to achieve politically with its hardware. The best thing NATO allies could do is to recognise the magnitude of this challenge and decide to proceed with internal dialogue and close consultation. Inversely, the worst thing NATO allies could do is ignore the need for internal alignment, allow internal consultations to wither, and instead channel energies into a punishing debate on burden-sharing numbers that Europe is bound to lose, leaving open the possibility that some individual allies will seek bilateral terms with Russia. This would be tantamount to having launched a two-stage rocket for no good purpose.

Ultimately, the state of NATO’s strategic affairs, and the effectiveness of its policies and plans, will depend on the allies’ sense of unity. Solidarity and cohesion are at the heart of any strong alliance, and, indeed, NATO did act cohesively and with remarkable solidarity in response to the Ukraine crisis. This has been the case from Wales to Warsaw. However, the story continues, and NATO must now take its deterrence policy to the next level, where considerable difficulties await. We have examined these in terms of follow-on forces, command-structure review and the purpose of detente. We have argued that doctrinal approaches to these difficulties define a likely road to ruin, and that the path forward must involve a combination of adequate force and clarified political ambition. Three factors will ultimately determine the likelihood and quality of this combination: the strength of US leadership; Europe’s ability and willingness to take responsibility for the health of the Atlantic partnership; and Russia’s approach to Europe.

The Atlantic Alliance was always at its best when the United States accepted the burden of leadership and provided strategic direction. For this reason, there are no allies in Europe calling for US disengagement or a retreat to an offshore position. The real concern in Europe is that the United States will remain engaged but heavily focused on burden-sharing, while simultaneously pursuing bilateral great-power diplomacy with Russia. This would see the European allies punished economically and kept in the dark on the big political issues. The extent to which the United States is motivated to maintain processes of political consultation within NATO as a foundation for military cooperation and common missions remains unclear. Certainly, such consultations appear to be low on the Trump White House’s list of priorities. However, to solve the intricate problems of reforming NATO’s force and command structures and developing its detente policy, there is no way around sustained and in-depth consultations.

#### European allies fear Russian hybrid threats---clarifying decision-making increases assurance

Stephanie Pezard 17, PhD, political science, Graduate Institute of International and Development Studies, Geneva, Senior political scientist, RAND, "European Relations with Russia: Threat Perceptions, Responses, and Strategies in the Wake of the Ukrainian Crisis", RAND, https://www.rand.org/pubs/research\_reports/RR1579.html

While Russia’s neighbors see Russia as capable of and potentially willing to carry out a conventional attack against them, they do not necessarily see such an attack as likely. Officials and analysts interviewed tend to describe Russia’s behavior—such as its stationing of nuclear capable missiles in Kaliningrad and overflying Polish airspace—as “bullying,” “intimidation,” or “posturing” rather than an indication of an imminent invasion. A more immediate fear is that Russia could employ hybrid warfare—defined as a combination of various types of operations, from conventional to irregular or psychological warfare, to influence the domestic politics of potential target countries. Our Polish and Swedish interlocutors, for instance, were concerned about Russian propaganda in Estonia or Latvia and that Russia’s attempt to influence and mobilize Russian minorities in Estonia and Latvia could exacerbate tensions in the Baltic region. With an eye on this threat, Estonia and Latvia are training their forces to respond rapidly to any provocation from Russia. While they have more effective internal security services and border guards than Ukraine had, they are also aware that Russian capabilities relative to the Baltic countries give it a time-space advantage that it could exploit in any number of scenarios.

European countries, particularly eastern NATO members, are concerned that the Alliance is ill equipped to respond to the current crisis with Russia. French and Polish officials interviewed pointed out that NATO’s current decisionmaking mechanism would be inadequate, in particular, if Russia were to test Article 5 “from underneath,” i.e., with actions under the threshold of conventional war or that can be “plausibly denied” by Moscow. While the NATO International Staff interviewed maintained that NATO was on a path to strengthen its capability to deter Russia’s ability to threaten the security of NATO members, the current efforts may not be sufficient to bring the Alliance to the necessary level of preparedness in the face of the new Russian threat. U.S. and European officials interviewed emphasized the critical importance of U.S. leadership in NATO and recognized the importance of U.S. military presence for maintaining security in Europe. Yet, the appreciation for the U.S. role in Europe does not come without reservations, with generally positive perceptions of the United States being complicated by a legacy view of the United States as imperialist by some segments of society in several countries, such as Germany and Sweden.

### AT: Article 5 Key---2AC

#### Ambiguity is better in the cyber domain – adversaries test redlines and undermine alliances by circumventing escalation thresholds

Kulesa 19 [Łukasz Kulesa is the deputy head of research at the Polish Institute of International Affairs (PISM). "The Future of Deterrence: Effectiveness and Limitations of Conventional and Nuclear Postures." https://carnegieeurope.eu/2019/11/28/future-of-deterrence-effectiveness-and-limitations-of-conventional-and-nuclear-postures-pub-80440]

NATO needs to be careful about defining and signaling its redlines. Making these boundaries too specific could embolden adversaries to intensify their actions below NATO’s declared threshold of response. Being deliberately ambiguous and raising the fear of retribution may be more useful for encouraging adversaries’ self-restraint.

At the same time, NATO should aim to deter specific types of particularly threatening unconventional activities. These include major and sophisticated cyber attacks against allies’ military forces and critical military and civilian infrastructure, proxy military and special forces operations, and state-sponsored terrorism. NATO could declare that such activities may lead it to invoke Article 5 and respond in various ways, including asymmetrically (for example, the response to a cyber attack may not involve only cyber capabilities).

The alliance must be able to identify early whether and when unconventional and hybrid gray-zone actions have become a more substantial and coordinated campaign. In such a case, NATO should aim to deter the adversary from escalating further. This requires increasing the alliance’s capacity to share early-warning intelligence and pool national intelligence-gathering, investigation, and attribution capabilities. NATO should not shy away from attributing ongoing operations to state adversaries, relying on national data as needed. The alliance and its members should be prepared to use direct channels of communication and other means to deliver immediate deterrence signaling in specific cases.

On the Southern flank, NATO faces state actors that use unconventional tactics and proxy forces (for example, Iran and Syria); state collapse and the emergence of ungoverned spaces in Libya, Yemen, and parts of the Sahel; and the activities of a range of nonstate actors, from loose groups to terrorist and criminal networks to highly organized quasi-state structures like Hezbollah. Cooperation with regional partners in addressing these threats will be vital. NATO’s primary task, as elsewhere, should be to deter states in the region from using unconventional tactics against NATO and its allies, using signaling and attribution tools. When possible, the alliance should aim to affect the calculus of nonstate actors to prevent them from harming alliance interests. This may not work with jihadist groups but may be possible with actors motivated by political or economic interests.

#### Effective OCOs solve war but clarifying Article 5 greenlights aggression.

Bigelow '19 [Brad; June 2019; Principal advisor to Assistant Chief of Staff for Communications, Information Services and Cyber Defence for planning, delivery and operation of CIS and CD capabilities throughout Allied Command Operations and NATO Crisis Response Operations, MS in Space Systems Engineering from the US Air Force Institute of Technology; "What are Military Cyberspace Operations Other Than War?” https://ccdcoe.org/uploads/2019/06/Art\_10\_What-Are-Military-Cyberspace-OperationsOther-Than-War.pdf]

Establishing a military capability to conduct OCO below the level of conflict may be one key to realizing the unique benefits of cyberspace as an operational domain. Gregory Rattray and Jason Healey have argued that: “It may be that the future of cyber conflict is not equivalent to larger, theatre-level warfare but only to select covert attacks which could range across a wide set of goals and targets.” In part, this argument draws upon the substantial base of experience showing that offensive operations between nations using conventional forces are relatively rare and usually condemned by other states (Rattray & Healey, 2010). But conventional offensive operations are also quite visible, are easy to attribute, and raise higher risks of escalation, which is why they have traditionally been seen as “a last resort and a temporary state” (Maurer, 2012).

OCO below the level of conflict, on the other hand, demonstrates the potential for states to exploit “grey zones”—areas where “international law principles and rules that are poorly demarcated or are subject to competing interpretations” (Schmitt, 2017). The willingness to operate in this “grey zone” is clearly demonstrated in the 2018 DOD Cyber Strategy, which states that in the U.S. “the Department seeks to pre-empt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident regardless of whether that incident would impact DoD’s warfighting readiness or capability.” In the United Kingdom, Defence Minister Sir Michael Fallon called for “new doctrine to clarify our response within NATO to anonymous cyber activity which often takes place now in that grey zone below the previously understood threshold of war” (Fallon, 2017). A similar appetite is demonstrated in the Netherlands’ Defence Cyber Strategy 2018, which states an intent to focus Defence support for civil authorities “on the vital infrastructure through closer collaboration with the responsible security partners” such as the National Cyber Security Centre (NCSC) (Netherlands Ministry of Defence, 2018). And in Germany, Defense Minister Ursula von der Leyen has stated that the Bundeswehr’s cybersecurity forces are permitted to “offensively defend” their networks if attacked (Somaskanda, 2018).

NATO heads of state and governments have also recognized the value in leaving some amount of “greyness” in the “grey zone,” as Jonatan Vseviov, the permanent secretary of the Estonian Ministry of Defence, explained in an interview: “there is a good level of what I would call ‘constructive ambiguity’ built into the wording of the Washington Treaty and also Article 5…. We don’t want to give anybody a list of attacks that would trigger Article 5 because that would obviously mean that we automatically also create a list of potential attacks that would not trigger Article 5” (Mehta, 2018). The willingness of nations to consider use of OCO capabilities below the level of conflict is also a recognition that, as Michele Flournoy and Michael Sulmeyer have written, “for all the increasingly vehement warnings about a cyber Pearl Harbor, states have shown little appetite for using cyberattacks for large-scale destruction. The immediate threat is more corrosive than explosive” (Flournoy & Sulmeyer, 2018). All of which suggests that OCO can fulfil the vision proposed by Bernard Brodie at the dawn of the nuclear age: “Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them” (Brodie, 1946).

From a doctrinal standpoint, however, the importance of recognizing OCO as a type of military operation that can be carried out not only in “war”—large-scale armed conflicts—but below the level of crisis, in the context of jus ad bellum, is that such capabilities cannot be employed in any context unless they are ready at the time of need. For conventional forces to be ready to act on short notice, they have to exist. They have to be equipped, armed, trained, sustained, able to move, informed about their potential adversaries, positioned to able to engage within their required readiness timelines—even though they may never need to move past that point of readiness and actually engage in battle. The same is true for cyberspace forces.

#### Focusing on delineating Article V activation is worse by promoting a reactive and defensive approach

Lewis 15 – James A. Lewis, senior vice president and director of the Technology Policy Program at the Center for Strategic and International Studies, “The Role of Offensive Cyber Operations in NATO’s Collective Defence,” 2015, https://ccdcoe.org/uploads/2018/10/TP\_08\_2015\_0.pdf

New military technologies are destabilising. Computers used for attack are one such technology. NATO has made considerable progress in its efforts to integrate cybersecurity into its planning processes, but while it may have gone as far as the political environment allows, it needs to do more. NATO’s September 2014 summit established that cyber defence is part of the Alliance’s core tasks of collective defence, crisis management, and cooperative security. Consistent with its long history as a defensive organisation, the policy emphasised “prevention, detection, resilience, recovery.”2

Cyber defence has become a central component of NATO planning, given the success of Russia and others in compromising NATO networks. US intelligence sources assess that any unclassified NATO network that is directly connected to the internet should be considered potentially compromised and that cyber espionage is the principle threat to NATO systems over the next three years. They also assess that Russia, given its record of effective cyber collection, poses the greatest espionage threat to NATO computer networks.3 The vulnerable state of many NATO members’ national networks makes defence a priority, but it cannot be the only priority. Discussion within NATO has focused on a defensive role and on the issue of when a cyber incident could trigger the collective defence provision of Article 5 of the North Atlantic Treaty. NATO’s Computer Incident Response Capability (NCIRC), co-located with Allied Command Operations (ACO), is responsible for defending NATO networks. NATO is improving its cyber defence and helping member states improve their own cyber defences through information sharing, training, and if necessary, the deployment of rapid reaction cyber defence teams. These topics are essential for planning purposes, but leave NATO in a reactive mode when it comes to cyber warfare.4

The central question for NATO’s cyber doctrine is how the lack of an articulated offensive cyber capability affects its ability to deter or defend. Put another way, can any military force credibly claim to have advanced capabilities if it does not include offensive cyber operations in its arsenal? Offensive capabilities, unlike NATO’s current defensive posture, involve deliberate intrusions into opponent networks or systems with the intention of causing disruption, damage or destruction. The question of NATO and offensive cyber capabilities touches on a range of sensitive political issues that militate against any change in policy in the near term.

The US has always been overly secretive about its offensive cyber capabilities, even after a flood of media leaks have made the most sensitive doctrine publicly available. This secrecy has carried over into NATO, and is unhelpful in that it increases the likelihood of opponents miscalculating as they consider the risks of using force or coercion against NATO members or interests. A lack of public discourse on offensive cyber operations undercuts the legitimacy of NATO operations by failing to build public understanding, and leaves NATO open to charges of sinister plots, since denial of offensive capabilities is not credible when two NATO members are world leaders in cyber operations.

Parallels between cyber operations and nuclear strategy are usually misleading, but cannot always be dismissed. The parallel for NATO is that cyber attack is a “weapon” with both strategic and tactical uses, which only a few NATO members possess. Unlike nuclear weapons, however, the procedures for integrating offensive cyber operations into NATO’s defensive actions are not at all obvious, if they exist. NATO will need to describe how the cyber capabilities possessed by a few of its members will support NATO’s defensive activities, and NATO’s credibility in defence requires some public discussion on the use of offensive cyber operations.

There has been a confusing debate over the merits of cyber deterrence, but one conclusion that we can draw from this discussion is that both the contribution of cyber operations to deterrence and the ability to deter cyber attack work best when embedded in a larger military force structure. Adding offensive cyber capabilities to NATO’s force structure and response doctrine will increase its deterrent capabilities – by how much is unclear, but what is clear is that a failure to add cyber capabilities will erode a credible deterrent as cyber operations are increasingly embedded into military operations.5

#### The combination of ambiguity and increased offensive coordination is key

Brantly 16 – Aaron Brantly, assistant professor of political science at Virginia Tech, “Ambiguous Deterrence,” 1/23/16, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136127/ambiguous-deterrence/

The ratification of a pledge for joint defense in case of a major cyber-attack at the 2014 NATO Summit is a major step forward. Under this pledge a significant cyberattack on any NATO nation would be constitutive of an attack on all of them. While it is hoped that the vague framing and uncertain capabilities of each NATO member will facilitate deterrence through ambiguity, it should be noted that deterrence only works when that ambiguity is backed up by a command structure capable of a timely and organized response.

As President Obama and other NATO leaders are redefining and reinvigorating strategy for the alliance it should be noted that the problem lies less in an ability to pledge for mutual defense than it does in the ability to organize and provide for that same defense. As recently as February 2013 the Government Accountability Office released a report on National Strategy, Roles, and Responsibilities and found that many of the major problems faced with regards to cybersecurity for the United States have less to do with capabilities and more to do with responsibilities. Large-scale cyberattacks such as Estonia 2007 or Georgia 2008 cross civil-military/private-public boundaries. Although policy-makers, think tanks, and academics have been working furiously to establish policy and write strategy documents, the fact remains that the United States remains woefully unable to respond to a significant cyberattack largely due to a failure to assign responsibilities and jurisdiction.

The ramifications associated with failure to assign responsibilities and jurisdictions are public knowledge and have been demonstrated in a wide variety of simulations. The Bipartisan Policy Center conducted a major cyber incident simulation in 2010 called Cyber Shockwave. Two of categories of findings in their follow up report dealt with significant problems associated with governmental organization and legal authorities and the third was international policy coordination. A 2011 report by DHS following Cyber Storm III, a simulation designed to test the effectiveness of the National Cyber Incident Response Plan, noted in one of its key findings: “Although public–private interaction around cyber response is continually evolving and improving, it can be complicated by the lack of timely and meaningful shared situational awareness; uncertainties regarding roles and responsibilities; and legal, customer, and/or security concerns.” As the United States and NATO pledge mutual defense, they are further expanding the problem of responsibilities and jurisdiction to an international institution with its own organizational and jurisdictional shortcomings.

The claim made by statesmen including NATO Secretary General Anders Rasmussen, that ambiguity of response facilitates deterrence is accurate, particularly when examining the use of nuclear weapons. However, that ambiguity falls back upon a rigid command and control system that enables a rapid response to hostile actions. If nuclear command and control functioned as it does for our cyber forces and nuclear warheads were headed across the Atlantic or Pacific towards major U.S. cities, our ability (or lack there of) to respond would make the concept of mutually assured destruction laughable. Our ability to adequately respond to an attack would be measured not in minutes or hours, but in days, weeks, and likely even months. At present, only long after the United States and her allies are left smoldering in the wake of a major cyberattack are we capable of even deciding who had the responsibility to respond.

Pledging mutual security in the face of an increasingly serious threat is admirable. Yet it is equally important to provide the structural aspects that underpin that security both at the national and international level for all NATO members. Currently the United States and her NATO allies lack a well-developed understanding of who has responsibility for what, when at the national and international level. And until those responsibilities and jurisdictional boundaries are formally defined the notion of ambiguity fostering cyber deterrence is largely an empty threat. It is imperative that Secretary General Jens Stoltenberg, who took office on October 1, 2014, facilitate policy discussions between NATO member states in the coming years that consider those aspects that facilitate meaningful deterrence in cyberspace.

#### Offensive buildup has to be accompanied by some level of underlying ambiguity for threats to be credible

Lupovici 11 – Amir Lupovici, lecturer in the Department of Political Science at Tel Aviv University, “Cyber Warfare and Deterrence: Trends and Challenges in Research,” *Military and Strategic Affairs*, Volume 3, Number 3, December 2011, pp. 49-62

Similarly, the concept of ambiguity should be studied. This concept may serve as a framework for practical thinking in confronting the dilemma inherent in the need for revealing capabilities on the one hand,40 balanced against the concern that the enemy will be able to exploit this exposure to increase its own strength and immunity to attack. Using insights developed in different contexts may provide an interesting foundation for developing ideas on cyberspace ambiguity, not only with regard to intention and willingness to make good on threats but generally with regard to the existence of capabilities. In this respect, it is possible, for example, to analyze the different efforts made by several nations in recent years in the field of cyber warfare. Not only are the means developed by nations likely to strengthen their strategy of deterrence against these threats, but the very prominence of these efforts may also serve as a deterrent tool. The same is true of the American establishment of a strategic command to manage cyber warfare:41 it has a range of objectives and functions, but its very reference and prominence allow not just improvements in capabilities but also demonstrate US willingness to invest resources in reducing threats and damage. It may be that stressing the desire to invest in measures of this sort and revealing the scope of the budgets, resources, and ~~manpower~~ dedicated to the subject – even absent a detailed breakdown of the measures acquired and their capabilities – can help increase the credibility of the deterrent message against threats in cyberspace, especially with regard to threats involving high levels of violence on the part of other nations. In other words, a partial revelation of capabilities while maintaining ambiguity about their essence allows for a reduction of the harmful effects described above but also transmits a forceful message. At the same time, one may expect that the low entry threshold for operating in cyberspace, especially in cases of asymmetrical confrontations, will continue to present a challenge to establishment of a strategy of deterrence seeking to prevent threats in this realm.

#### The status quo Article 5 doctrine is stabilizing, by making clear the costs of cyber operations – increasing OCOs can only enhance stability, not decrease it

Lewis 15 – James A. Lewis, senior vice president and director of the Technology Policy Program at the Center for Strategic and International Studies, “The Role of Offensive Cyber Operations in NATO’s Collective Defence,” 2015, https://ccdcoe.org/uploads/2018/10/TP\_08\_2015\_0.pdf

Dissimulation is an essential part of hybrid warfare, and Europe and the US face a propaganda barrage that is much more sophisticated than the clumsy Soviet efforts of the Cold War. Despite this clumsiness, a good portion of the Western public has found it persuasive. Similarly, those critical of NATO will find new complaints about aggression and militarisation credible. Russia has already complained that NATO’s defensive cyber doctrine is destabilising warmongering and part of a larger conspiracy to advance western hegemony.11 The Snowden revelations have lent a powerful impetus to Russian propaganda.

Behind the rhetoric lies both a desire to conceal their own use of cyber operations and a real fear that Russia’s decline leaves it vulnerable to new military technologies. The intent is to hamper and complicate any Western response to Russian efforts to regain control in Crimea and the “near abroad”. The Russian position is that NATO’s new cyber doctrine is destabilising as it threatens to use conventional or even nuclear responses (in the Russian description of the new policy towards low-level cyber attacks).

Any announcement by NATO relating to offensive cyber capabilities would be greeted with alarm and vitriol in Moscow. However, the effect on stability would likely be less pronounced. NATO-Russia relations are already in steep decline. It is possible that any NATO announcement would accelerate this, but it is also possible that Russia could recalculate the risk of further adventures if it were faced with a stronger defence. In terms of opponent attitudes, there is probably little effect. Russia, along with NATO’s other potential military opponents, is likely to overestimate both capabilities and coordination among NATO member states and underestimate NATO’s will to defend. This is an unhappy combination as it makes aggression against NATO seem less risky.

NATO’s decision on how cyber attacks could trigger Article 5, while greeted with complaints, had a stabilising effect. It made clear to potential opponents that cyber attacks are not risk-free. Similarly, a clear enunciation of how NATO would use offensive cyber capabilities as part of any defensive operation would also change opponents’ risk calculations in ways that would force them to consider how offensive actions, even if intended to be covert, are not free of risk or cost.

### Plan Secret---2AC

#### NATO MOUs interpret existing treaty obligations secretly within the alliance due to classification

Andrés B. Muñoz Mosquera 16, Legal Advisor, Director, at NATO Supreme Headquarters Allied Power, Europe - Allied Command Operations, October 2016, “Memorandum Of Understanding (MOU): A Philosophical and Empirical Approach (Part II),” NATO Legal Gazette, Issue #37, p. 34-38

In Part I3 of this article, we acknowledged that the increasing use of the MOU formula could trigger a quite stimulating debate among practitioners and academia. On the other hand, we also learned that international institutions, in the exercise of their legal personality, have fostered, by means of their implied powers, intra and inter-institutional practices that use MOUs as a protuberant instrument. These practices take place not only inter-States, but also intra and inter-institutions of international character – international organisations. In this vein, we have also seen in the previous Part, that MOUs have their place in international law and international relations, and that they are a clear contribution, inter alia, to international institutional law development.

On this note, the functionality of MOUs rest on the principle of good faith, which per definition creates legitimate expectations among participants. On the other hand, these legitimate expectations trigger a sort of duty that, if breached may consequently lead to potential legal effects, that are different from the legal obligations that emanate from the breach of treaty provisions. This is why even if MOUs are generally considered nonbinding instruments, the principle of good faith presents them as a conduit to interpret, inform, implement or supplement other - and superior - binding legal rules.

This provides the nucleus for MOUs’ characterisation, which permits seeing them – with certain flexibility – as normative standards among MOU participants. These participants, as members of a partner-specific community, could claim within that restricted community the legal effects of the agreed provisions.

Yet in the MOU realm, there is self-restriction to address the potential judicial consequences, if there are ever any, of breaching the provisions of an MOU and eventually the legitimate expectations created by the MOU. An MOU may not be the direct object of the dispute, however, courts will have little choice but to take a comprehensive approach towards the facts, and the agreements and arrangements among participants, in order to produce a judgment structured in space and time.

In the next sections we will discuss both the characterisation of MOUs and how national or international courts view them. Moreover, we will dedicate the last section to assist practitioners by developing a commented MOU structure.

MOUs Characterisation

The NATO Legal Deskbook briefly characterises MOUs as follows:

“The form of MOU is frequently used to record informal arrangements between States on matters which are inappropriate for inclusion in treaties or where the form is more convenient than a treaty (e.g. for confidentiality). They may be drawn up as a single document using non-treaty terms, signed on behalf of two or more governments, or consist of an exchange of notes or letters recording an understanding reached between two governments, or a government and an international organization. MOUs usually do not require ratification. However depending on the content and the agreement between the Parties on the nature of the document, MOUs can be subject of a certain level of domestic ratification…NATO, in general, concludes MOUs in numerous occasions. MOUs are a very flexible and adaptable instrument to record the will of entities with legal personality to achieve practical results that do not amount to treaty obligations.”4

How are MOUs practiced? There are several ‘schools’ of practice that nations and international organisations have developed, with different references to this practice in the British-law influential area5, continental European states and the United States.6 Aust highlights that in all of these areas, MOUs are considered ‘agreements without legally-binding force’ and refers to the European Commission document PESC/SEC 899 of 9 August 1996 to support his argument. Aust also admits that in certain circumstances nonbinding becomes binding.7 However, practice shows that states have different approaches depending on their political approach to the topic or topics addressed in specific MOUs.8

At this point, it is relevant to note the process for creating MOUs at NATO, a ‘classic’ international organisation practicing intergovernmentalism. At NATO, during the decision making process, members may reaffirm their sovereignty9, several times, by supporting or opposing the existence of an MOU in their collective realm. One wonders if in the process of creating MOU organisations or simple MOU initiatives there is any other international organisation in the world that gives its members so many opportunities to express their ‘super-will’10 with respect to scope and purpose, as well as to the provisions of MOUs, which are intended to implement the obligations under the foundational treaty. These treaty obligations are updated by an established practice that operates through the decisions taken, in general per the practice of consensus, by its highest decision making bodies. It is necessary to note that this consensual commitment does not only have a collective nature, as consensus reflects ineludibly the individual commitment of each of the NATO members on any specific decision taken by the Council for creating a concept supported by an MOU. In the Council’s decision, states do not particularly address the non-binding status of the MOUs. In fact, the non-binding status discussion rarely happens before the MOU text negotiations start and, normally, ends at national level exclusively mandated by political approaches or national legislation. This acts as almost pro-forma language applied dependent on a states’ individual practice and perspective, irrespective of the actual points negotiated in the MOU.

Consequently, are MOUs non-binding documents by default? How valid is the written commitment of the participants? Could the ‘bindingness’ 11 created in a non-binding environment lead to legal effects? This battery of ‘tricky’ questions, partially addressed ut supra, takes us outward to square one and convinces us that the law of parsimony fed by anterior facts and posterior behaviour surrounding the life of an MOU has to be taken into account seriously when determining its legal effects.

In this regard, MOUs are chosen for cross-border relations because there has been a previous political commitment or the basic principles of framework treaties have been implemented. The form of negotiations does not vary from that of a treaty, and in general, although there is a tendency to use lax or soft wording vis-à-vis treaties, the treaty negotiation strategies are clearly displayed. MOU texts, contrary to popular belief, have little flexibility for review once agreed upon. As such, MOU drafters incorporate predictable ‘mobile’ elements through annexes to MOUs, which negotiators assume can be opened by lower level managers, though it always requires a ‘political’ mandate either directly or indirectly.12 MOU practice shows that it is not common to incorporate reservations (statements of interpretation). However, these have recently found their way into MOUs carrying heavy and long-term financial commitments within their provisions.

Compared to treaties, MOUs have, in general, shorter internal coordination processes for approval, and few states pass them through parliament or their commissions. Moreover, since most MOUs have some financial clauses related to budget and taxes, many negotiators regularly announce that their parliaments or specialised commissions need to give their approval before the state in question can consider the text of the MOU agreed upon.

Another example of how MOUs trigger complicated internal coordination processes is seen in the Host Nation Support Arrangements13 negotiated with states not party to the North Atlantic Treaty and other NATO treaties. The fact of not counting on those treaties initiates a parallel process of negotiations for concluding treaties14 on status of forces and international military headquarters. These treaties commonly address an array of matters that range from entering and staying in foreign territory, taxes and customs, wearing uniforms, holding weapons, policing compounds, claim waivers, freedom of movement, concurrent jurisdiction, etc. In addition, another significant factor is that due to confidentiality, MOUs are published only at the level of for official use only, as most of them are classified.

#### Internal honesty exerts pressure on allies to fill capability gaps

Kulesa ’19 [Łukasz Kulesa is the deputy head of research at the Polish Institute of International Affairs (PISM). "The Future of Deterrence: Effectiveness and Limitations of Conventional and Nuclear Postures." https://carnegieeurope.eu/2019/11/28/future-of-deterrence-effectiveness-and-limitations-of-conventional-and-nuclear-postures-pub-80440]

THE WHO

On NATO’s Eastern flank, the focus is on Russia. Moscow seeks to achieve its strategic aims—a sphere of influence in the neighborhood and the prevention of NATO’s expansion—without a war but seems ready to engage in brinkmanship and is working on creating favorable conditions to prevail in a conflict. This makes it necessary for the allies to develop a credible deterrence strategy.

However, NATO also has to deter the threats from states and nonstate entities in the Middle East and North Africa. The effects of conflicts in the region are already being felt on NATO territory, and governments in the most affected member states are asking how they can prevent further spillover of existing and potential crises. The discussions have been light on specifics, though not for lack of options. The allies are already fielding missile defenses in Turkey to defend against missile attacks from Syria; deterring conventional attacks on NATO territory could be the next step, depending on developments in Syria itself. Other actors of concern include Iran, with its growing missile arsenal, and nonstate groups operating in Lebanon, Libya, and Syria.

Farther afield, given the U.S. and other allies’ engagement in the Asia Pacific and NATO’s close links with Australia, Japan, New Zealand, and South Korea, the alliance may have to consider the feasibility of deterring China and North Korea from threatening or harming member states. This would be a new task with significant resource implications and should not be undertaken lightly.

THE WHAT

Internally, NATO members need to be clear about specific actions they can reasonably expect the alliance to deter. Clearly, an armed attack—from whatever direction—is one course of action to be deterred, but other actions are not so simple.1

In the case of Russia (and other state actors), the focus is also on deterring coercion: the act of adversaries imposing their will on NATO allies through a combination of military threats and nonmilitary means. For now, the thinking at NATO has emphasized deterrence of a territorial grab or blockade in the Baltic region. However, the characteristics of the Russian approach to warfare mean that the alliance has to look beyond the Baltic Sea and beyond the physical domain, mainly to the cyber realm.2 More and more of the critical systems running hospitals, carrying electricity, or patrolling the skies are now connected to the internet and therefore vulnerable. NATO’s adversaries can, in theory, block allied governments from coming to each other’s aid by threatening devastating cyber attacks that will cause populations to panic and cripple economies.

NATO has already declared that a cyber attack could lead the alliance to invoke its Article 5 collective defense clause, a statement that aims to have a deterrent effect—though there is little evidence that it has stopped adversaries from trying.3 This is mainly because most cyber attacks are designed to stay below the level that would trigger a response of the whole alliance. The allies need a clearer policy on what to do if the line is crossed one day. That policy must also address the thorny issue of credible attribution and should be rehearsed rigorously.

THE HOW

NATO does not need to mirror the activities of its adversaries to deter effectively. The idea is to signal that the alliance will not be intimidated or coerced, but that can be done in multiple ways.

With regard to Russia and the threat of a land incursion, NATO has decided to rely on limited forward deployments along its Eastern flank and on the ability to reinforce quickly those small contingents in times of crisis. The shortcoming of this posture is that if Russia overwhelms the first line of defense, it may be able to use the strength of its conventional forces, as well as the threat of nuclear weapon use, to thwart allied reinforcement.

NATO, as a whole, is adapting its posture to respond, and the United States is strengthening its military presence in Europe to address these potential weak points. The mix of U.S. troops and stored equipment and supplies in Europe is being expanded, including in Poland. And NATO has taken steps to improve its ability to deploy units from North America and move them around Europe by creating a Joint Force Command for the Atlantic and a Joint Support and Enabling Command. Other means of strengthening deterrence include implicit or explicit threats of political or economic sanctions or threats of countermeasures in cyberspace.

Regarding the South, the exact form of deterrence has to match the threat that NATO chooses to deter. With regard to potential state adversaries, NATO’s existing deterrence tools and military capabilities can be utilized against threats from that direction. The creation of the Strategic Direction South Hub—a consultation and coordination body for allies and partners—at the NATO command in Naples, Italy, also contributes to the deterrence mission. However, these measures alone will not deter the main challenge in the South: terrorist groups, with the potential to strike in Europe, operate in lawless spaces.

RECOMMENDATIONS

NATO may be back to its traditional mission of deterrence, but deterrence itself has evolved. A new approach must be adapted to today’s environment, in which a number of deterrence challenges need to be tackled simultaneously and sophisticated nonconventional means can be used jointly with traditional military tools to test the alliance.

MAINTAIN ALLIANCE COHESION

While the allies’ initial response to deterrence challenges has been impressive, in the long run, deterrence fatigue may present problems. NATO needs to keep all allies committed to the deterrence mission and continue to secure sufficient contributions of committed forces, capabilities, and resources. The risk is that allies’ unity and cohesion—the indispensable foundations of NATO—will weaken as memories of the Islamic State’s caliphate and of Russia’s aggression against Ukraine fade. Adversaries will do their part to sow or exploit divisions or doubts about the strength of solidarity among alliance members.

To keep cohesion from fraying, NATO’s leadership should continuously engage every ally in dialogue about the rationale for the posture, the threat assessment, and members’ views on, and concerns over, the implementation of the deterrence mission. National governments have the same essential responsibility toward their parliaments and publics. NATO must also make sure that discussions do not focus only on one strategic direction but rather address both defense and crisis-management tasks.

Engagement with partners should include a dedicated dialogue on deterrence issues. In some cases, based on mutual consent, NATO should be ready to explore coordinated deterrence signaling or mutually reinforced deterrence activities, such as joint statements, deployments, or exercises.

Engagement with adversaries must be seen as an inseparable companion to deterrence. Dialogue and multiple contact channels remain crucial to convey and receive deterrence signals, avoid accidental or inadvertent escalation, and explore risk-reduction and arms control opportunities.

DETER RUSSIA’S ADVENTURISM

In the foreseeable future, specific challenges connected with deterring Russia will continue to dominate the practical agenda. As a priority, the allies should fully implement the 2018 decisions to adapt NATO’s command and force structure.4 The military credibility of the current deterrence posture depends, to a large extent, on the alliance’s ability to speedily augment its forward-deployed units with follow-on forces.

The allies should look for new ways of stimulating the development of necessary capabilities and interoperability. A more transparent discussion of the major gaps in allied capabilities could help exert pressure on members to make relevant investments. The NATO Military Committee should play a more active role in the alliance’s adaptation by more visibly highlighting the military requirements for credible deterrence to civilian authorities and—via individual military leaders—to NATO populations.

### AT: Leaks---2AC

#### NATO’s info security is air tight

Alasdair Roberts 3, University of Massachusetts Amherst - School of Public Policy, 5/15/3, “Entangling Alliances: NATO's Security Policy and the Entrenchment of State Secrecy,” https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=1307692

**SOI = security of information**

Concerns about the impact of NATO's security of information (SOI) requirements are justified. Although NATO's policy remains inaccessible, its broad outlines can be deduced. It is a conservative policy, largely crafted at a time when the western powers were faced with overwhelming military threats and non-state actors played a much smaller role in the process of governance. Archival records show that the original signatories went through a similar process of policy rationalization and articulated concerns comparable to those being expressed by critics today. In fact, NATO's SOI policy continues to play an important role in frustrating the work of transparency advocates in Western Europe and North America, some of who may be unaware of the role that is played by NATO and other similar SOI agreements.

European nations are caught in an increasingly dense web of multilateral commitments on the handling of information, based largely on the conservative policy crafted by the North Atlantic Treaty countries in the early years of the Cold War. There is good reason to think that the same may be said of countries in other parts of the globe. This may give us reason to be cautious in assuming that global integration is favorable to increased transparency. Advocates of transparency will also find that domestic policy on matters of state secrecy is increasingly constrained by this thickening web of agreements on security of information.

WHAT DOES NATO REQUIRE?

Governments throughout Central and Eastern Europe have said that their legislation is tailored to suit NATO requirements.11 However, observers have asked whether governments in the region are using the process of NATO expansion as a pretext for adopting unnecessarily broad laws, or whether NATO's SOI policy is itself unduly tilted against transparency. These are reasonable questions, but NATO has done little to provide answers. Its SOI policy is not publicly accessible. However, available evidence does suggest that the policy, crafted in the early years of the Cold War, is excessively tilted toward secrecy.

For most of NATO's history, its SOI policy was contained in a document known as CM( 55)15(Final), Security within the North Atlantic Treaty Organization. This document had three components. The first and oldest component was a Security Agreement adopted by parties to the North Atlantic Treaty at the third meeting of the North Atlantic Council in January 1950, as one of the basic components of NATO's "master Defense Plan."12 This became Enclosure "A" of C-M(55)15(Final). A second component, first adopted in 1950 but substantially revised over the next five years, outlined detailed security procedures for the protection of NATO classified information. This became Enclosure "C" of C-M(55)15(Final). A third component, adopted for the first time in 1955, had a broader reach. It outlined "basic principles and minimum standards" that were to govern the overall design of national security systems. This affected the handling of all sensitive information, whether produced by NATO or not. This became Enclosure "B" of CM( 55)15(Final) (See Table 2).

[TABLE 2 OMITTED]

A document which compiled these three components was approved by the North Atlantic Council in March 1955, and given the designation C-M(55)15(Final). The SOI policy was substantially revised in later years, although it retained this designation. Enclosure "D," providing guidance on information given to defense contractors, was added in 1958. A Confidential Supplement was added in 1961 that provided additional guidance on methods of personnel screening. Enclosure "E," which addressed anti-terrorism efforts, was added in the early 1980s, and apparently revised in early 2002.

The strictness of NATO's SOI policy may be illustrated by its treatment of the policy itself. The fact that NATO had adopted a SOI agreement was not acknowledged in the final communiqué of the January 1950 meeting of the Council.13 Although C-M(55)15(Final) was for many years an unclassified document, NATO refused for decades to make it publicly available.14 A narrow glimpse of NATO policy may have been provided in 1998, when a revised version of the Security Agreement (which apparently still constitutes Enclosure A of the policy) was made publicly available by some NATO member states.15 Versions of C-M(55)15(Final) adopted before 1964 have also been made available in the NATO Archives.

Nevertheless, the complete and current version of C-M(55)15(Final) always remained inaccessible. The policy reminded national governments that documents such as CM( 55)15(Final) are the property of NATO, and may not be given to any other individual or organization without NATO's consent. As a consequence, several governments recently refused requests made under national right to information laws for copies of the policy.16 NATO's Security Office, responding to one of these requests, explained in February 2002 that

NATO unclassified information . . . can only be used for official purposes. Only individuals, bodies or organizations that require it for official NATO purposes may have access to it . . . NATO information marked in this manner is subject to release via agreement from its originators and subject to recognized storage procedures for its protection.17

NATO began an overhaul of C-M(55)15(Final) in the late 1990s. The review, guided by an Ad-Hoc Working Group for the Fundamental Review for NATO Security Policy, was completed in early 2002. A revised SOI policy, now known as C-M(2002)49, was adopted by NATO on June 17, 2002. The Working Group completed its work in secrecy, and the new policy remains inaccessible to the public18, although its broad outlines may be reconstructed from other sources (Table 2).

NATO's reticence means that an assessment of its SOI policy must be largely speculative. Nevertheless it is possible to describe the policy in broad terms, drawing on NATO's archival documents19 and other sources, such as the language of the CEE's new state secrecy laws.

Another of these sources is the SOI policy of a related collective security pact, the Western European Union (WEU). Established by the Brussels Treaty of March 1948, the WEU actually served as the foundation for the broader alliance established by the North Atlantic Treaty in April 1949.20 There is good reason to believe that the two pacts maintained comparable security policies. Policymakers within NATO acknowledged that the first drafts of its security policy were based on the WEU's policy.21 All ten of the nations that are currently members of WEU are also members of NATO; in addition, there is a NATO-WEU SOI agreement, signed in 1992. An early version of NATO policy recognized that NATO and WEU materials might be "co-mingled" in the same administrative processes.22

Fortunately, the WEU's security policy is publicly accessible. The government of Sweden signed the WEU security agreement, and became responsible for complying with its security regulations, as a precondition for entering into cooperation on certain issues with the WEU in 1992. The Swedish government released the WEU security agreement and the 1996 version of the WEU security regulations in February 2002 in response to a request under Sweden's Freedom of the Press Act.23

Another view of NATO policy may be provided by bilateral agreements that are publicly accessible. The Council of the European Union recently released correspondence in 2001 between its Secretary General, Javier Solana, and NATO Secretary General Lord Robertson, which outlined an interim security agreement that serves as a foundation for closer cooperation between the two organizations.24 The Council of the European Union subsequently adopted security regulations that must be presumed to conform to NATO requirements.25

From all this, what can be said about NATO's SOI policy? That it has five basic features, each of which has been adopted with the aim of ensuring a high level of security for information. The cumulative effect of the rules is to put an extraordinary emphasis on control of information.

Breadth. The first of these elements might be called the principle of breadth, although this term is not used in NATO documents. It implies that the rules that a member state adopts regarding security of information should govern all kinds of sensitive information, in all parts of government. It eschews narrower approaches, perhaps limited to information received through NATO, or information held within military or intelligence institutions. Laws adopted by several CEE countries have this comprehensive quality. The principle is expressed in the 1964 edition of C-M(55)15(Final), which articulates standards for information security that apply to all sectors of government, on the grounds that member states must be assured that each country gives "a common standard of protection . . . to the secrets in which all have a common interest."26

Depth. The next principle underpinning NATO policy is that of depth of coverage, although again the rule is not expressed in this way in NATO documents. The policy errs on the side of caution when determining what information should be covered by an SOI policy. This is evident in the NATO classification policy, whose lowest category, RESTRICTED, applies to information whose relevance to security is negligible. Information may be classified at this level if its disclosure would be "undesirable to the interest of NATO."27 Several CEE countries have adopted equally broad classifications for the whole of government. Under Czech law, for example, information is classified as RESTRICTED if disclosure would be unfavorable to the Republic;28 in Slovenia, information is RESTRICTED if disclosure could harm the activity or performance of tasks of an agency.29

Centralization. A third principle of NATO policy is that of centralization. This has a national and intergovernmental aspect. At the national level, centralization of responsibility and strong coordination are regarded as "the foundations of sound national security."30 Member states are expected to establish a "national security organization" (NSO) that is responsible for the security of NATO information and screening of personnel; for "the collection and recording of intelligence regarding espionage, sabotage and subversion"; and for advice to government on threats to security and appropriate responses.31 Presumably the NSO is also responsible for leading the "high-level" system of inter-departmental coordination that is required to ensure tight integration of departmental policies and procedures.32 The NSO must also have the authority needed to conduct inspections of security arrangements for the protection of NATO information within other departments and agencies, and to investigate and respond to breaches of security.33

This structure is roughly replicated at the intergovernmental level. In 1955 the North Atlantic Council gave its Security Bureau the responsibility for "overall coordination" of security in NATO. The Bureau, now renamed as the NATO Office of Security, advises national authorities on the application of principles and standards, and carries out surveillance of national systems to ensure that NATO information is adequately protected.34 National authorities have an obligation to report possible breaches of security to the NATO office, which in turn must "coordinate with national authorities" in investigations.35

Controlled distribution. The NATO security policy invokes two rules that are intended to strictly control the distribution of information. The first of these is "the NEED TO KNOW principle": that individuals should have access to classified information only when they need the information for their work, and access should never be authorized "merely because a person occupies a particular position, however senior."36 This is regarded as a "fundamental principle" of security. Judgments about whether an individual has a "need to know" are made by the originator of the document, or by one of the addressees identified by the originator.37

The second rule that restricts the distribution of information might be called the principle of originator control. The principle acknowledges the right of member states, and NATO itself, to set firm limits on the distribution of information that is circulated among member states. The principle was central to the agreement signed by NATO members in January 1950, which stipulated that:

The parties to the North Atlantic Treaty . . . will make every effort to ensure that they will maintain the security classifications established by any party with respect to the information of that party's origin; will safeguard accordingly such information; . . . and will not disclose such information to another nation without the consent of the originator.38

The principle of originator control trumps the "need-to-know" principle, since originators may impose a high level of classification that restricts the number of individuals to whom the document might be referred by an addressee. Nor may a document be downgraded or declassified without the consent of its originator.39 The principle is even stricter with regard to distribution of documents outside the community of NATO governments. In this case, distribution is absolutely prohibited without consent, even if the information is graded as UNCLASSIFIED. In these circumstances, the information is regarded as "the property of the originator," which retains absolute control over its distribution.40

Personnel controls. The fifth and final element of the NATO security policy comprises strict rules regarding the selection of individuals who are entitled to view classified information. The precise requirements for personnel screening are not easy to discern. Some of the exact criteria adopted during the Cold War are probably no longer applicable; and some of the criteria used in NATO's early years were still withheld in late 2002.41

The policy relies on a system of "positive vetting," in which individuals who handle sensitive information are subjected to active background investigation before receiving clearance.42 NATO's early policy made clear that decisions could be based on assessments of character and lifestyle, and that the evidentiary threshold for denying clearances was low. Individuals were expected to demonstrate "unquestioned loyalty [and] such character, habits, associates and discretion as to cast no doubt upon their trustworthiness."43

Evidence that these rigorous standards are still applied can be found in CEE countries. Slovakia's new security agency recently stated that it will review political and religious affiliations, as well as lifestyles—including extramarital affairs—that are thought to create a danger of blackmail.44 The Associated Press reported that Romania intends to deny clearances to security staff with "anti-western attitudes."45 A constitutional challenge to Poland's Classified Information Act by Polish judges was also motivated by their concern about intrusive investigations to determine whether their lifestyles could make them "susceptible to . . . pressure."46

Other controls are imposed to control personnel after a clearance has been provided. The 1964 edition of C-M(55)15(Final) stipulated that supervisors had a duty "of recording and reporting any incidents, associations or habits likely to have a bearing on security." Evidence that created a "reasonable doubt" about loyalty or trustworthiness required the removal of a security clearance.47 Finally, there was an expectation that "disciplinary action" would be taken against individuals who are responsible for the unauthorized disclosure of information.48 Additionally, as demonstrated later in this article, there appeared to be an expectation that member states would establish clear criminal penalties for unauthorized disclosure.

### OCOs Solve---Cohesion---2AC

#### US lead over cybersecurity in NATO fosters alliance cohesion – bolsters mutual defense against an array of threats

Raimundas Karoblis ’19, Lithuania’s national defense minister, “Lithuania’s defense minister: Wavering US commitments? Think again.”, DefenseNews, 12/2/19, https://www.defensenews.com/outlook/2019/12/02/lithuanias-defense-minister-wavering-us-commitments-think-again/

Lately, **Europe has been positively spurred to action by the relentlessness of the U.S**. The continent is clearly on a positive trajectory as evidenced by the growing defense budgets and the sheer amount of newly launched defense initiatives. It is essential that this increased attention to security and defense in Europe maintains a clear focus on capability building and compatibility with NATO. Lithuania itself is making great strides in strengthening its defense. Thanks to the public support and determined political leadership, a historic sprint in defense spending to reach 2 percent of gross domestic product has been achieved, making a truly powerful impact on the ground. We are undergoing a major breakthrough in modernizing our Armed Forces and in rapidly enhancing military infrastructure. Less visibly but no less importantly, Lithuania is improving resilience of the society as well as developing cutting-edge cyber capabilities, which has already placed Lithuania among the top five in the world in the field of cybersecurity. **U.S. support and cooperation have been a critical ingredient in almost all of our recent successes**. Defense capability development is benefiting immensely from the synergy created by the U.S. security cooperation programs complementing Lithuania’s national efforts. Each dollar that the U.S. invests in supporting the Lithuanian military is matched several times over by Lithuania’s acquisitions of U.S. defense articles. Most recently, Lithuania has signed a long-term contract to purchase at least 200 Oshkosh Joint Light Tactical Vehicles, and commenced talks to acquire a fleet of Black Hawk helicopters that would replace our last remaining military platform from the Soviet era. **Bilateral cooperation with the United States has also led to the launch of the Regional Cyber Security Center. It will focus on research and development of next-generation cyber capabilities, training with partners and allies, as well as conducting analysis on cyberthreats.** Speaking of challenges ahead, air defense will remain a key vulnerability in the Baltic region for the foreseeable future. Our national investments in this area can only provide limited response to the potential threat stemming from Russia**. Solutions, therefore, will have to come through NATO and through bilateral cooperation with the United States**. Conceptual work has already started within the alliance, while recent U.S. exercises involving deployment of the Patriot missiles and F-35 aircraft indicate the way ahead to address this complex, yet highly important issue. We also noted that the U.S. Congress has proposed $400 million worth of support to boost air defense of the three Baltic states in its latest appropriations bill. If endorsed, it could signal a major step toward solving this conundrum and would help to patch a substantial hole in NATO’s capabilities. **All these important developments seem to tell one simple story: The trans-Atlantic bond, which held the alliance strong and secure for the past 70 years, is still very much alive, while the U.S. commitment to European defense** remains as strong as ever**.**

### OCOs Solve---Deterrence---2AC

#### Deterrence in cyberspace is possible and sufficient to avoid conflict, but NATO having offensive capabilities is necessary to prevent Russian malfeasance

Maldre 16 – Patrik Maldre, Adjunct Fellow at the Center for European Policy Analysis, “Moving Toward NATO Deterrence for the Cyber Domain,” May 2016, https://cepa.ecms.pl/files/?id\_plik=2446

Cyber deterrence clearly warrants more discussion among NATO members than ever, given the threats they now face—particularly from the East. Yet the Cyber Defence Committee doesn’t really cover it, nor will a full-fledged cyber deterrence concept be announced at the upcoming NATO summit in Warsaw. The main debate in Brussels and in national capitals centers on whether cyberspace should even be considered a domain of warfare, as many member states have already decide; the fuzzy concept of active cyber defense is only tentatively mentioned. However, senior NATO leaders have espoused deterrence as a potential future direction for the alliance. Importantly, several member states, including the United States, Britain and Estonia, are also publicly exploring such a strategy.20 The moment is not yet right for an alliance-wide declaration on this topic, but with concerted effort at all levels, NATO can and should continue to move toward deterrence for the cyber domain.

Deterrence aims to discourage an adversary from taking offensive action. Traditionally, its two pillars have been deterrence-by-denial and deterrence-by-punishment. The first refers to measures that reduce or eliminate the benefits of a certain aggressive move, while the second seeks to impose additional costs for performing it. NATO’s traditional mandate of defending its own systems fits comfortably into the deterrence-by-denial part of this framework. Deterrence-by-punishment, however, is far more controversial because of the problem of attribution—which refers to the difficulty of identifying the perpetrators of operations. Finally, both concepts also rely on intent, capability and credibility. As it stands, a palpable lack of trust among member states hinders collective action on both fronts. Progress in the denial category will be easier and more visible, but countermeasures should be considered as well.

NATO has come a long way in terms of working together to shore up technical defenses in cyberspace. The main barrier to further cooperation, however, is the difference in technical and administrative capacities as well as human and financial resources among member states. This, along with differing national views, remains the main barrier to further integration. The alliance is only as strong as its weakest member. When it comes to deterrence-by-denial, therefore, all member states must have the basics in place: computer security laws, national cyber strategies, a police focus on cybercrime, national CERTs, public-private partnerships and capable intelligence agencies. From there, members should enact effective, actionable information-sharing programs. After that, the next step is to develop joint situational awareness. Typically, adversary espionage campaigns target multiple NATO and memberstate organizations simultaneously. Early warning and shared situational awareness can prevent multiple entities in different countries from being breached by the same operation. The end goal for the denial part of the deterrence strategy is, of course, resilience. If NATO and its members can effectively work together to prevent, detect, respond and recover from cyber attacks, this would significantly decrease the benefits and increase the costs for an adversary. NATO collective action should continue in this direction, and joint efforts can help to promote trust and confidence—a key ingredient in further cooperation in deterrence-by-denial, but even more crucial when it comes to deterrence-by-punishment.

Preventing adversaries from benefitting from offensive actions, or at least limiting their gains, can help discourage them from conducting such attacks in the first place. Punishing them after the fact is another. While the term has an aggressive connotation, this part of the strategy is defensive and retaliatory in nature. It can refer to a broad spectrum of actions—from naming-and-shaming to nuclear strikes. In the cyber domain, the problem of attribution hinders the goal of effective deterrence. For this reason, NATO and its member states should invest heavily in the technological and analytical capabilities necessary to discern signs of a particular adversary, including in cooperation with the private sector.

As numerous cases of attribution to Russian cyber threat actors demonstrate, this is already taking place. Furthermore, member states should complement technical attribution with political and diplomatic attribution. Currently, months and even years pass before politicians and leaders feel comfortable about ascribing blame. For deterrence to work, however, governments must carry out both high-level and private attribution in conjunction with media and private companies as soon as they have conclusive evidence. Calling out threat actors and their state sponsors in diplomatic forums, public discussions and private meetings can motivate them to conduct less aggressive operations.

NATO and its member states should also adopt joint approaches to developing and employing offensive capabilities for collective defense purposes. Laudably, many individual allies have already declared that they possess such capabilities and the doctrines for using them. However, considerable mistrust persists among the allies, creating an atmosphere of uncertainty and doubt—which weakens deterrence as a whole. To overcome this hurdle, allies can begin by making political statements about potentially using these capabilities in case of attack, and in accordance with international law as part of a collective defense response. Ultimately, NATO should move toward sharing these capabilities, perhaps by using existing models based on nuclear doctrine. Transparency and straightforwardness in this arena could contribute substantively to deterring adversaries and reinforce collective defense among NATO members.

Intent and credibility will play into adversaries’ calculations for any type of countermeasure. For this reason, policy innovations and capability development need to be complemented by effective strategic communication. You cannot achieve deterrence if your adversary doubts that you’ll do what you say— and even less so if it doesn’t think you can do what you say. From this perspective, demonstrations such as the Aurora test in 2007 can be quite useful.21 Other, more subtle means include presentations by top officials at security conferences. Operations against third-party adversaries other than the intended target of deterrence can also deter attacks; few doubt that Russia paid close attention to the Stuxnet case, or that NATO drew conclusions from the Ukraine grid attack. In sum, effective strategic communication— both public and private—can be a key component or complement of a deterrence-by-punishment strategy.

#### The US is more than prepared to engage in long-term intel battles with OCOs – key to deterring large-scale cyberattacks and no risk of escalation

Joshua Rovner ’20, is associate professor in the School of International Service at American University, “The Intelligence Contest in Cyberspace”, Lawfare, 3/16/20, https://www.lawfareblog.com/intelligence-contest-cyberspace

Deterrence is different. It is difficult to deter states from activities below the line of armed conflict because retaliatory threats inherently lack credibility. No one is likely to believe that states will use violence to stop espionage, for instance, which probably explains why small states have spied on large ones for centuries. More importantly, **victims are surprisingly tolerant of cyber operations**. Research suggests that **individuals are less willing to retaliate against cyber blows than physical violence**. If this is correct, then strategies based on punishment are likely to fail. Deterrence by denial is also likely to disappoint, because the barriers to entry for espionage and harassment are relatively low. States will continue to conduct cyber intrusions even if previous efforts were unsuccessful. There are important exceptions to this rule. Deterring major attacks against critical infrastructure is possible, for instance, **because these attacks threaten significant harm to civilians**. **Deterring this kind of cyberspace operation makes sense because anyone considering such an attack would** risk a ferocious response. Executing large-scale attacks on infrastructure probably also requires a lot of time, money and organization. **Adversaries would surely think twice about that investment, especially if the United States issues clear deterrent threats**. But deterrence is mostly irrelevant in cyberspace, because most activities fall well short of threats to infrastructure. Understanding the present problem in terms of deterrence theory is not particularly helpful. At best, a well-fought intelligence contest can slowly convince adversaries that certain targets and methods are beyond the pale. During the Cold War, Soviet and U.S. intelligence professionals came to observe some rules of the game. Aggressive counterintelligence methods were expected, for example, but not against family members. Neither side could deter intelligence efforts, but they could structure the contest in order to reduce the risk. What does the future hold for the intelligence contest in cyberspace? **The good news is that the United States is exceptionally well positioned to compete**. It possesses extraordinary technical and human resources, in both the public and private sectors. **Its intelligence agencies are the largest and richest in the world**. It also benefits from decades of experience competing against capable rivals. This is not the first time the U.S. intelligence community has dealt with committed and occasionally ruthless intelligence foes.

### OCOs Solve---Deterrence---1AR

#### The best outcome is adversary perception of NATO willingness to use OCOs aggressively.

Smeets and Lin '18 [Max and Herb; 11/28/18; senior researcher at the Center for Security Studies at Stanford University, PhD in International Relations from the University of Oxford; senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution at Stanford University; "An Outcome-Based Analysis of U.S. Cyber Strategy of Persistence & Defend Forward," https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward]

From the U.S. standpoint, the optimal outcome is a United States that is more powerful in cyberspace along with a more stable cyberspace. Indeed, from the U.S. standpoint, the former will lead to the latter. A more stable cyberspace will involve norms of acceptable behavior, less conflict and so on.

One path towards this rosy outcome is that the strategy does what it is said to do: Creates significant friction and makes it hard for adversaries to operate effectively. Adversaries realize that the U.S. strategy of persistent engagement makes it more difficult to conduct various offensive cyber operations, and they have no strong incentives to escalate as it may trigger a U.S. response in the conventional domain. USCYBERCOM has the advantage from the beginning.

#### Offensive capabilities allow iterative training that increases coordination

Lewis 15 – James A. Lewis, senior vice president and director of the Technology Policy Program at the Center for Strategic and International Studies, “The Role of Offensive Cyber Operations in NATO’s Collective Defence,” 2015, https://ccdcoe.org/uploads/2018/10/TP\_08\_2015\_0.pdf

It could be argued, given NATO’s defensive orientation ( pace Russian fears of diabolic plots), that a purely defensive and technical focus for cyber operations is appropriate. The question, however, is whether NATO can field a credible military force without some public linkage to an offensive cyber capability.

Here again, the nuclear precedent offers some suggestions for a way forward. In the NATO phonetic alphabet, “whiskey” (“W”) and “romeo” (“R”) were used by NATO’s command structure in conflict to “warn” capitals that with a deteriorating situation on the ground it would be sending a request to release nuclear weapons for NATO use. Romeo was the actual request for release of nuclear weapons to NATO control. This terminology prepared nuclear capitals to make the decision on release.

Just as nuclear weapons remain under national control but senior NATO commanders can request their release, the US and UK could retain control of offensive cyber capabilities but be prepared to make them available to NATO commanders upon request. In practice, national teams could be assigned to support NATO commanders in theatre or could carry out some operations against targets selected by NATO commanders form their national duty station.

Such an arrangement needs more than ad hoc coordination. It requires an identified structure for request and release that is regularly practised. It demands offensive cyber operations used for defence purposes to be included in planning and exercises. It would also be beneficial for NATO’s defence mission if the exercise of systems for the use of offensive cyber capabilities in support of defensive operations was made public.

Cyber operations necessitate advance planning and practice, particularly for multinational operations that are already inherently complex in their coordination and de-confliction requirements. Offensive cyber operations create conflicts between goals and missions for the use of cyber techniques. The fundamental decision is whether to collect intelligence or to engage in military operations. This creates an immediate problem for NATO, because decisions on intelligence collection will be taken at the national level whereas military operations are in the purview of the NATO military command structure. This consideration would necessarily be part of the decision process in national capitals, which would likely be an iterative process to allow for additional input from the theatre of operations.

### OCOs Solve---Warfighting---2AC

#### Out-of-network OCOs are the foundation of US intel gathering

Joshua Rovner ’20, is associate professor in the School of International Service at American University, “The Intelligence Contest in Cyberspace”, Lawfare, 3/16/20, https://www.lawfareblog.com/intelligence-contest-cyberspace

The ongoing competition in cyberspace is largely an intelligence contest. Although the technology is different, the underlying contest exhibits all the characteristics of traditional spy-versus-spy battles. An intelligence contest is an effort to steal secrets and exploit them for relative advantage. Great powers today are using cyberspace with vigor, seeking to steal communications in transit and data at rest. China’s effort to steal intellectual property via cyberspace was famously described as the “most significant transfer of wealth in history.” China has attempted to exploit this effort to improve its military capabilities, with mixed results. Russia has also become more active in cyberspace espionage, targeting the United States and its partners abroad. Intelligence contests also include sabotage. All bureaucracies suffer from some amount of friction: the inevitable daily hiccups that slow down operations and make organizations less efficient. **Sabotage in cyberspace weaponizes friction to undermine rival capabilities and morale**. Offensive cyberspace operations are well suited for this task because they offer a range of tools for the saboteur. States can opt for cheap and easy harassment campaigns like denial of service attacks, or they can engineer sophisticated operations against specific facilities. In either case, the benefits to the saboteur are both practical and psychological. Practical results include harm to networks, data, and infrastructure, all of which forces the target to spend time and money on recovery. Psychological results are equally important. It may not be necessary to cause physical damage if personnel in target organizations fall victim to frustration and finger pointing. Finally, intelligence contests involve efforts to pre-position espionage assets that may be useful in war. Military organizations increasingly rely on cyberspace for organizing and directing conventional campaigns. Intelligence agencies have an obvious interest in monitoring their efforts. **Gaining access to adversary networks makes it possible to reduce the fog of war in the case of a conflict**. It also suggests the ability to confuse enemies by inhibiting their communications or flooding the zone with disinformation.

#### Sustained, preemptive offense against the initial cyber threat is necessary against armed attack and armed force.

Bigelow '19 [Brad; June 2019; Principal advisor to Assistant Chief of Staff for Communications, Information Services and Cyber Defence for planning, delivery and operation of CIS and CD capabilities throughout Allied Command Operations and NATO Crisis Response Operations, MS in Space Systems Engineering from the US Air Force Institute of Technology; "What are Military Cyberspace Operations Other Than War?” https://ccdcoe.org/uploads/2019/06/Art\_10\_What-Are-Military-Cyberspace-OperationsOther-Than-War.pdf]

In recent testimony before the U.S. Senate Armed Services Committee, Michael Sulmeyer proposed “two necessary conditions of posture” for U.S. military cyber mission forces to be better prepared to defend the U.S. against foreign attempts to interfere with elections. First, “Our cyber mission forces should be constantly conducting reconnaissance missions abroad to discover election-related threats to the United States and provide indicators and warnings to our forces and decision-makers.” Second, “Our cyber mission forces must be sufficiently ready to strike against targets abroad identified by reconnaissance as threats to our election” (Sulmeyer, 2018).

Although Sulmeyer’s proposal was in the specific context of reactions to Russian meddling in U.S. elections in 2016, at a more general level these two conditions apply to any application of military OCO capabilities: first, they are highly dependent upon sustained reconnaissance of potential adversaries and their systems; and second, they need to be maintained at a high level of readiness because there may be little or no warning before they need to be engaged. If a nation intends to use offensive cyberspace capabilities to precede or pre-empt kinetic operations, then operational preparation of the cyber battlefield must become “as routine as reconnaissance or surveillance of potential adversary activity” (Kehler, Lin & Sulmeyer, 2017). What does “operational preparation of the cyber battlefield” involve? Robert Chesney spells it out clearly in his analysis of the 2018 DOD Cyber Strategy: “Intrusions into the systems of potential adversaries in order to secure access of a kind that can be exploited for disruptive or destructive effect if and when the need later arises” (Chesney, 2018).

#### Offensive capabilities are necessary to adapt to changing adversary capabilities – the aff just establishes a cyber Maginot Line that is begging to be pushed back

Lewis 15 – James A. Lewis, senior vice president and director of the Technology Policy Program at the Center for Strategic and International Studies, “The Role of Offensive Cyber Operations in NATO’s Collective Defence,” 2015, https://ccdcoe.org/uploads/2018/10/TP\_08\_2015\_0.pdf

The nature of warfare is changing as opponents seek to circumvent Western military power by using a blend of political action, special forces, proxies and irregular units, unconventional tactics and cyber techniques to find a different way of applying force to gain their ends. What Russia sometimes call “hybrid warfare” will challenge NATO defence planning. A cyber defensive orientation is, however, the equivalent of a static defence, defending fixed positions rather than manoeuvring, and conceding initiative to opponents. The next public iteration of NATO cyber policy should describe how NATO members with offensive cyber capabilities would retain national control, but make these capabilities available to NATO in the event of aggression. NATO should be more explicit in how offensive cyber operations fit into its defensive and deterrent strategy. Finally, it needs to identify and describe a regular coordinating process to be established (similar to the Nuclear Planning Group) in NATO’s Cyber Defence Committee (CDC).

NATO would never refrain from using fighter aircraft because they can serve offensive purposes, and say it would rely solely on air defence missiles and damage control to deal with the threat of air attack. Nor would NATO renounce armoured vehicles and rely only on static defence. A defensive approach that forsakes the possibility of offensive action is essentially a cyber Maginot Line. This defensive orientation serves no one’s interest except that of our opponents. Offensive cyber operations are similarly a part of warfare that advanced militaries cannot ignore. The mechanisms for incorporating offensive cyber into NATO will be complicated by national sensitivities, and public presentation will need to be carefully crafted to reinforce a deterrent message; but the next step, however politically difficult, for NATO transformation is to publicly embrace offensive cyber capabilities in planning and exercises.

Warfare is evolving as technological and political developments change the requirements for effective operations. Military innovations create a new dynamic for calculating risk among potential adversaries. Forces and concepts that once seemed adequate for stability are called into question. It will be neither easy nor quick for NATO to discuss publicly the role of offensive cyber operations, but it is ultimately unavoidable.

### OCOs Solve---Warfighting---1AR

#### Less cyber offense is the worst possible outcome.

Scott '18 [Tennille; 5/25/18; MS in Information Technology from the University of Maryland, MA in Military Operations from the US Army School of Advanced Military Studies, Cyber Operations Officer for the US Army; "The Art of the Cyber Jab: Using Defensive Cyberspace Operations-Response Action at Corps and Below," https://apps.dtic.mil/sti/pdfs/AD1071483.pdf]

Russian aggression in the cyber domain over the past decade show that mere passive response to cyber attack is not sufficient to prevail against a well-rehearsed adversary that combines offensive cyberspace operations with combat operations. Fear of the unknown cannot be an excuse for idleness, and the US cannot afford to be “cyber punching bags” in combat.103 Inactivity is not an option. Lieutenant General Nakasone told senators in a confirmation hearing March 1, 2018 “As cyberspace develops, the longer that we have inactivity, the longer our adversaries are able to establish their own norms – and I think that is very, very important that we realize that.” 104 This sentiment resonates with Moltke in his statement that “omission and inactivity are worse than resorting to the wrong expedient.”105 While DCO-RA may not be a perfect solution, as its analogies in the physical domain demonstrate, perfection is not always necessary. Overcoming an adversary is the art of combining what is possible with what is necessary to achieve defense. At some point the US must stop being the world’s cyber punching bag and counter its adversaries with a few cyber jabs of its own. This research demonstrates that DCO-RA, when fully and properly enabled, is capable of doing just that.

#### The best cyber defense is day-to-day cyber offense.

Bigelow '19 [Brad; June 2019; Principal advisor to Assistant Chief of Staff for Communications, Information Services and Cyber Defence for planning, delivery and operation of CIS and CD capabilities throughout Allied Command Operations and NATO Crisis Response Operations, MS in Space Systems Engineering from the US Air Force Institute of Technology; "What are Military Cyberspace Operations Other Than War?” https://ccdcoe.org/uploads/2019/06/Art\_10\_What-Are-Military-Cyberspace-OperationsOther-Than-War.pdf]

Some have argued that military operations in cyberspace outside the context of armed conflict should be limited to the protection of military networks and information systems. Miriam Dunn Cavelty has flatly stated that “Militaries cannot defend the cyberspace of their country – it is no space where troops and tanks can be deployed because the logic of national boundaries does not apply” (Dunn Cavelty, 2012). Stephen J. Anderson agrees, writing that traditional concepts of national defense cannot be applied in cyberspace: “The US Navy defends the littoral territorial boundaries; air defenses, either through missile defense initiatives or alert aircraft, define airspace boundaries. Those lines are not readily identifiable in cyberspace” (Anderson, 2016). Some go even further, arguing that an active military role in peacetime cyber security undermines investment in alternative mechanisms. In a 2013 post for the Lowy Institute, Ian Wallace wrote that such efforts disincentivized “other longer-term and more sustainable efforts to address the new challenges that cyber brings to security systems” (Wallace, 2013).

Yet this debate has evolved significantly in recent years, in large part thanks to increasing evidence of state-sponsored attacks on civilian cyberspace infrastructure. In a recent paper entitled Rethinking Cyber Security, James Lewis has stated that “The primary source of risk in cybersecurity comes from conflict between states” (Lewis, 2018). This assessment is echoed by the Netherlands’ National Cyber Security Centrum, which concluded in its 2018 assessment that “The most significant threats are sabotage and disruption by nation-states” (National Cyber Security Centrum, 2018). As consensus on the state actor threat in cyberspace has grown, so have calls for the military to take a more active role in the defense of cyberspace.

In the 2017 U.S. Senate deliberations on increasing the Secretary of Defense’s authority to conduct clandestine military cyberspace operations, Senator John McCain asserted that the need for a strong military role in peacetime was self-explanatory: “It’s the Department of Defense’s job to defend this nation: that’s why it’s called the Department of Defense” (Pomerleau, 2017). This more active role— sometimes referred to as defending forward—is reflected in recent updates to military cyber strategies. The 2018 U.S. Defense Department Cyber Strategy, for example, states explicitly: “We are engaged in a long-term strategic competition with China and Russia” and declares that this requires (and justifies) “action in cyberspace during day-to-day competition to preserve U.S. military advantages and to defend U.S. interests” (U.S. Department of Defense, 2018). Similarly, the Netherlands’ Defence Cyber Strategy 2018, subtitled Investing in cyber striking power for the Netherlands, concludes that the current security environment demonstrates that “a more active contribution from Defence within the existing structures is required” (Netherlands Ministry of Defence, 2018). Jan Kallberg and Thomas S. Cook have gone even further, stating that nations should be prepared not only to use military cyberspace forces in peacetime but to actively foster these capabilities as an alternative to armed conflict: “Cyber is no longer a mere enabler of joint operations, but instead a viable strategic option for confronting adversarial societies” (Kallberg & Cook, 2017).

#### Balance of tech favors offensively disarming adversaries.

Davis '19 [Susan; 4/18/19; General Rapporteur to the NATO parliamentary Assembly Science and Technology Committee; "NATO in the Cyber Age: Strengthening Security & Defense, Stabilizing Deterrence," https://www.nato-pa.int/download-file?filename=sites/default/files/2019-04/087\_STC\_19\_E%20-%20NATO.pdf]

27. Although cyber security and defence capabilities continue to improve, most experts argue that the offence has the advantage in cyber space and that this is unlikely to change soon. Given sufficient time, skills, and resources, attackers could easily perpetrate a cyber attack, finding the targeted system’s vulnerabilities, gaining access, and delivering their payload. This is a key reason why the Alliance must complement dissuasion with strategies of deterrence by punishment. In other words, they must try “to prevent an attack by threatening unacceptable damage so that in the attacker’s cost-benefit calculations the best choice is not to attack” (Morgan, 2009; italicised in original). It should be noted some experts would argue that the offence is not as dominant. For example, the more sophisticated cyber weapons are, the more opportunities the defender has to stop an attacker and the more errors the attacker is likely to make. Additionally, continued organisational deficiencies could be a key reason why the attackers have had the advantage thus far (Slayton, 2017).

### AT: Defense Solves/Resilience---2AC

#### Playing pure defense undermines cybersecurity – only offensive operations ensure safety of networks

Michael Sulmeyer ’18, Former Director of the Cyber Security Project, “How the U.S. Can Play Cyber-Offense”, Harvard Kennedy School Belfer Center, 3/22/18, <https://www.belfercenter.org/publication/how-us-can-play-cyber-offense-0> \*edited for ableist language

The United States has been the victim of repeated cyberattacks by foreign powers, and it seems to have little power to stop them. During the 2016 U.S. presidential campaign, Russian hackers broke into the Democratic National Committee’s e-mail servers and made more general efforts to influence the election’s outcome, as detailed in Special Counsel Robert Mueller’s indictment of 13 Russians and three Russian entities. In February, U.S. intelligence and law enforcement officials warned that the Russian government would again try to use cyber-operations to interfere with midterm elections in November. That same month, the White House publicly blamed Russia for “the most destructive and costly cyberattack in history,” the 2017 NotPetya malware campaign, which ~~crippled~~ [undermined] the government of Ukraine before spreading to multinational corporations such as FedEx and Maersk, causing billions in damage. The Russians are not the only ones hacking at the United States’ expense. Chinese hacking groups have stolen U.S. intellectual property from industrial manufacturers and military contractors. In 2015, China weaponized its “Great Firewall” and conducted distributed denial of service attacks against U.S. websites, including GitHub, which Beijing wished to punish for hosting content that the Chinese leadership found undesirable. In 2014, North Korean hackers attacked the U.S. film studio Sony Pictures to block the release of a movie, The Interview, that depicted the attempted assassination of North Korean leader Kim Jong Un. The attack erased the content of thousands of computers, released embarrassing internal e-mails, and intimidated Sony into canceling the movie’s theatrical release. Iran too has lashed out in cyberspace, attacking U.S. financial institutions and a dam in New York. **These threats have led to renewed calls for cyber-deterrence measures that would impose greater costs on would-be hackers while denying them benefits**. The administration of President Donald Trump, for instance, has elevated U.S. Cyber Command to a unified combatant command, which it believes will signal greater capability and resolve. Deterrence is also likely behind the Trump administration’s broad declaratory policy in its Nuclear Posture Review, which contemplates the use of nuclear weapons to deter non-nuclear threats. Former President Barack Obama prioritized cyber-deterrence as well, including in his administration’s 2015 Department of Defense Cyber Strategy and in his Justice Department’s efforts to indict Chinese and Iranian hackers. **In cyberwarfare, Washington should recognize that the best defense is a good offense. This focus on cyber-deterrence is understandable but misplaced**. Deterrence aims to change the calculations of adversaries by persuading them that the risks of an attack outweigh the rewards or that they will be denied the benefits they seek. **But in seeking merely to deter enemies, the United States finds itself constantly on the back foot**. Instead, **the United States should be pursuing a more active cyberpolicy, one aimed not at deterring enemies but at disrupting their capabilities**. In cyberwarfare, Washington should recognize that the best defense is a good offense. THE PROBLEMS WITH DETERRENCE There are three main problems with U.S. efforts at cyber-deterrence. The first is that Washington is trying to use a cold war strategy to address a twenty-first-century problem. History teaches that deterrence kept the Cold War cold: the United States and the Soviet Union were each vulnerable to the other’s thousands of nuclear weapons. When it comes to cyberspace, however, the United States has more to lose than its adversaries because it has gone further in embracing innovation and connectivity without security. **But although the societies and infrastructure of Washington’s adversaries are less connected and vulnerable than those of the United States, their methods of hacking can still be disrupted**. Second, it is difficult to convince foreign leaders (and foreign hackers) that the costs of hacking really do outweigh the benefits. Deterrence is all about perception: does an actor believe that the threat of punishment is real enough to prevent him from acting? This is as much a question of psychology as one of national security strategy. Many U.S. adversaries are less vulnerable in cyberspace than the United States is, so meaningful punishment would require discerning their priorities (for instance, money or public reputation) and threatening concerted action against them. Yet gaining clarity about foreign leaders’ priorities—and credibly threatening them—is easier said than done: during the Cold War, Soviet leaders often misunderstood signals from their U.S. counterparts, as when they interpreted the NATO military exercise Able Archer 83 as a prelude to war. Not much has changed—National Security Agency Director Admiral Michael Rogers acknowledged during a recent hearing that the Russians “haven’t paid a price . . . that’s sufficient to get them to change their behavior.” Third, it is virtually impossible to know if deterrence is working. The goal is to prevent attacks. But if no attacks occur, it is hard to determine why—perhaps the would-be attacker was deterred by the threat of punishment; perhaps the attack failed for some other reason. Washington should not base its national cyberpolicy on a strategy whose success, almost by definition, cannot be evaluated, especially if there are good alternatives available. **Today’s fight in cyberspace occurs in the gray zone between war and peace. If the United States hopes to win, it should spend less time trying to persuade its competitors that it is not worth hacking and more time preempting them and degrading their ability to do so**. It is time to target capabilities, not calculations. HACK THE HACKER How could the United States begin degrading its opponents’ ability to hack? Washington’s actions need not always be aggressive or destructive. In countries where technology companies are willing to cooperate with the U.S. government (or with requests from their own government), a phone call to the right cloud provider or Internet service provider (ISP) could result in getting bad actors kicked off the Internet. **This is not a permanent solution, but it will force adversaries to rebuild, which often prompts unforced errors, making them more vulnerable to U.S. surveillance and disruption**. If subtle measures prove insufficient, the United States should be ready to take more offensive action. **In situations where the defense of the nation is on the line, U.S. hackers could pursue a campaign of erasing computers at scale, disabling accounts and credentials used by hackers to attack, and cutting off access to services so it is harder to compromise innocent systems to conduct their attacks**. Such a campaign would aim to make every aspect of hacking much harder: because hackers often reuse computers, accounts, and infrastructure, targeting these would sabotage their capabilities or render them otherwise useless. Such actions need not send a message that hacking the United States doesn’t pay. Instead, they should support a more limited but more achievable objective: stop adversaries from hacking the United States. Whether or not foreign leaders perceive that cyberattacks on the United States are worth conducting, Washington can prevent them from doing so in the first place. Offensive cyber-operations should not be undertaken lightly—the United States must bear in mind its commitments under international law and its relationships with its allies. But excessive caution cannot prevent Washington from defending itself: with the United States’ enemies already attacking it online, the country will need to be more proactive than it has been thus far. **The U.S. government has already undertaken a few asymmetric, or non-cyber, approaches to degrading its adversaries’ abilities to hack targets in the United States**. It has sanctioned foreign individuals and companies to limit their access to capital and resources. It has also indicted some hackers from China, Iran, and Russia in the hope that public exposure will make it more difficult for them to hack. These are efforts worth pursuing, but not because they deter. Rather, like offensive cyber-operations, they can degrade attackers’ capabilities, although only in indirect ways because they rely on the cooperation of foreign governments.

### AT: OCOs Bad---2AC

#### Allied OCOs are inevitable

Iftimie ’20 [Ion A.; May; PhD, Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business; NDC Policy Brief, “NATO's needed offensive cyber capabilities,” no. 10]

At the 2016 NATO Summit in Warsaw, cyberspace was recognized as an operational domain in which NATO military forces must be able to maneuver as effectively as they do on land, at sea and in the air. Since then, Allies have conducted several successful offensive cyber operations1 against non-state adversaries, such as Daesh. Due to technological transformations in recent years, cyber is no longer viewed by NATO and its member states only as a hybrid threat, but also as a weapon in its own right and as a force multiplier2 in current military operations. Over the next two decades, NATO will look for new ways to integrate cyber weapons (or offensive cyber capabilities) into its operations and missions.3

#### The only question is whether they’re unilateral or collectively integrated---unilateral OCOs cause cyber fratricide

Iftimie ’20 [Ion A.; May; PhD, Eisenhower PhD Candidate Fellow, NATO Defense College, and Senior Advisor, European Union Research Center, George Washington University School of Business; NDC Policy Brief, “NATO's needed offensive cyber capabilities,” no. 10]

The lack of integrated offensive cyber A2/AD capabilities undermines both the unity of the Alliance and its mandate of defence and deterrence. On the former, the lack of coordination between Allies during unilateral cyber operations could lead to friction when resulting effects infringe on Allied cyber-physical infrastructures. It could also lead to cyber fratricide, when failure to properly attribute Allied digital personas occurs during these military operations. On the latter, while most Allies are developing offensive cyber capabilities, some remain unable to face the growing number of cyber threats unilaterally.

#### US has already offered cyberweapons to allies

Baldor ’18 [Lolita; October 3; “US to offer cyberwar capabilities to NATO allies,” <https://apnews.com/article/north-america-russia-ap-top-news-international-news-asia-pacific-292c4d08912c4e3f8ae29973e0ecfbbc>]

“We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of a crisis or conflict,” the new strategy states, adding that the U.S. is prepared to use cyberwarfare along with other military weapons against its enemies when needed, including to counter malicious cyber activities targeting the country.

The document adds that the Pentagon will “work to strengthen the capacity” of allies and partners.

NATO has moved cautiously on offensive cyber capabilities. At the Warsaw Summit in 2016, allies recognized cyberspace as a warfighting domain. It has said that a computer-based attack on an ally would trigger NATO’s commitment to defend its members. And last year the alliance agreed to create a new cyber operations center. But the focus has always been on defending NATO networks and those of its members, not offensive cyberwar.

NATO Secretary-General Jens Stoltenberg said on Tuesday that the defense ministers will have a working session this week to address cyber and other risks, and how allies can cooperate to counter such threats. He did not provide details.

#### OCOs won’t escalate uncontrollably.

Sørensen ’19 [Heine; March; Senior Lecturer at the Institute for Strategy at the Royal Danish Defence College, and Dorthe Bach Nyemann, Senior Lecturer at the Institute for Strategy, Royal Danish Defence College, Represented Denmark in the Research Project Entitled “Countering Hybrid Warfare I-II” Within the Framework of the Multinational Capability Development Campaign (MCDC), US Joint Forces Command, “Deterrence by Punishment as a Way of Countering Hybrid Threats – Why We Need To Go ‘Beyond Resilience’ in the Gray Zone”, Multinational Capability Development Campaign, Mhttps://tinyurl.com/y6cko3at]

The Flipside of Deterrence by Punishment – the Fear of Escalation

One of the greatest reservations 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 an 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.

### AT: Escalation---1AR

#### US OCOs are restrained in nature – no risk of accidents

Joshua Rovner ’17, is Associate Professor in the School of International Service at American University, “ARE CYBER WEAPONS TOO DANGEROUS TO USE?”, War On the Rocks, 8/22/17, https://warontherocks.com/2017/08/are-cyber-weapons-too-dangerous-to-use/

Surprisingly, **we find that the effects of high-profile attacks have been quite limited**. In the aftermath of both Stuxnet and the Snowden revelations, users continued to log on in record numbers, and most do not seem to have taken additional steps to reduce their exposure. Although the data is still somewhat patchy — ours go from 2015 to 2016 — it appears that a small minority reduced the scope of their online activities and engaged in self-censorship. Meanwhile, the vast majority continued to communicate, share photos and videos, buy Christmas gifts, and so on. Firms acted similarly, even though business leaders were some of the fiercest critics of the National Security Agency’s actions. Their responses have not been uniform, but the general trend has been continued engagement online with increased investment in cyber defenses. Finally, **states have not noticeably reduced cooperation with the United States on cybersecurity**. This is true of states like India, which were third-party victims of Stuxnet, along with states like Brazil, whose leaders were allegedly targets of U.S. surveillance. The major exception is China, which suspended nascent cooperative efforts with the United States in 2014. But given the broader turmoil in U.S.-China relations, **it’s unclear whether this was a result of either Stuxnet or Snowden**. **The technical responses also suggest that the internet is resilient**. **The frequency, severity, and duration of attacks have not increased in the aftermath of the dual shock of Stuxnet and Snowden**. And the broader adoption of measures like encrypted web traffic suggests the internet’s infrastructure is becoming more robust. Some caveats are in order, because the data we use to assess the response to Stuxnet and Snowden is immature and incomplete. We will surely learn more, and it is possible that additional information will lead to a different assessment. It is also possible that new kinds of cyberattacks may lead to wider and longer-lasting destruction. Stuxnet, for instance, contained target verification checks to prevent collateral damage to machines it inadvertently affected. NotPetya notably did not, and caused real damage to third-party victims. One reason the attack propagated so quickly was that it used stolen credentials to pose as an administrator, allowing it to avoid detection. Moreover, NotPetya seems to have been designed to maximize confusion about its origin by raising the specter of states, criminals, and cyber-exploits run amok. If we learn that consumer, firm, or state behavior changes as a result of generalized fears stemming from NotPetya or its offspring, then we will have more doubts about internet resilience. So far, however, we do not have evidence that this is the case. The upshot is that it is possible for states to go on the offensive in cyberspace without undermining cybersecurity. Unlike ice-nine, **the tools the United States creates to fight in this realm do not appear, at least so far, to be uncontrollable**. There may be good reasons to eschew offensive cyber operations, and the United States already has a process to determine whether to act in any specific case, but officials need not be deterred by the fear of extensive and lasting collateral damage.

#### Low risk of escalation from OCOs

Brandon Valeriano ’20, is the Bren Chair of Military Innovation at the Marine Corps University and a Senior Advisor with the Cyberspace Solarium Commission, “Managing Escalation Under Layered Cyber Deterrence”, Lawfare, 4/1/20, https://www.lawfareblog.com/managing-escalation-under-layered-cyber-deterrence

A few patterns of escalation have been explored thus far. First, the cyber domain is not escalation dominant. **Most cyber operations exhibit no responses, let alone escalatory responses, that prevent future action**. Second, there are vastly different escalation patterns based on nationality or state. There is no uniform view of how escalation should work in cyberspace. We polled the public-at-large in Russia, the United States and Israel, and found that Americans prefer proportional responses, while Russians prefer escalatory or deescalatory response patterns. Assuming uniformity in responses across nationalities is folly. Third, there is a danger of escalation in cyberspace when a power with technological superiority attacks a state lacking technological capabilities. A feeling of inadequacy likely provokes an escalatory response to keep control of a situation. When escalatory options are used, they tend to appear in ongoing conflict situations, such as Israel’s kinetic attack on Hamas cyber operators in 2019. **Placed in the proper context, these cross-domain operations are not escalatory but, rather, are deescalatory when compared to other kinetic operations being run or considered at the same time**—such as a massive retaliatory bombing campaign or a ground operation to root out terrorist operators.

### OCOs Good---Election Interference---2AC

#### OCOs well in advance of threats secures elections.

Sulmeyer '18 [Michael; 2/13/18; Director of the Cyber Security Project at the Belfer Center for Science and International Affairs in the Harvard Kennedy School; "Testimony of Michael Sulmeyer," https://www.armed-services.senate.gov/imo/media/doc/Sulmeyer\_02-13-18.pdf]

In addition to improving defenses and becoming more resilient, we should also consider how best to counter threats abroad before they hit us at home. To that end, let me transition to how I see some potential roles for the military in protecting our elections. I will focus my remarks on roles that the military could play outside of the United States.

There are two necessary conditions of posture that I see as critical:

1. Reconnaissance Posture: Our cyber mission forces should be constantly conducting reconnaissance missions abroad to discover election-related threats to the United States and provide indicators and warnings to our forces and decision-makers. There will never be sufficient resources to prioritize all threats equally, so prioritizing threats to our elections and our democratic processes is crucial. If we do not prioritize collecting information abroad about election-related threats, than we cannot hope to disrupt them.

2. Force Posture: Our cyber mission forces must be sufficiently ready to strike against targets abroad identified by reconnaissance as threats to our election. Readiness is a critical issue for our armed forces today, and I would encourage the Senators on this committee to ensure they are asking tough questions about the readiness of our cyber mission forces just as they would about any other area of our military. Our forces must be ready to create different effects against a range of targets. Sometimes, they will not have much notice, so developing tactics that can be employed on the fly is important. If the military’s reconnaissance and forces are postured to focus on threats to our elections from abroad, there are four objectives that our forces should be prepared to pursue. It should go without saying that undertaking these actions would need to be consistent with international law and other relevant U.S. commitments.

1. Preventing Attacks from Materializing: Based on election-focused reconnaissance, U.S. cyber mission forces should develop options to disrupt the activities of those planning to meddle in our elections, and those who are in the early steps of doing so. Because these would be actions conducted by U.S. forces with a relatively long lead time, scenario-based plans should be developed and socialized with decision-makers so they are aware of the viability, risks, and benefits of different options.

2. Preempting Imminent Attacks: Reconnaissance abroad may provide indicators and warnings of an imminent cyber attack against election-related infrastructure, campaigns, and media and social media platforms. Our forces can prepare to neuter those attacks before they commence. Such actions would need to be undertaken rapidly as opportunities to strike may be fleeting, so developing options in advance to deliver effects promptly when so ordered is essential.

#### The success of election interference disintegrates the global liberal order.

Kagan et al. 19 [Frederick; 2019; PhD in Russian and Soviet military history @ Yale, Director of the Critical Threats Project at the American Enterprise Institute, Associate Professor of Military History at the U.S. Military Academy at West Point, “Confronting the Russian Challenge: A New Approach for The U.S.,” http://www.understandingwar.org/sites/default/files/ISW%20CTP%20Report%20-%20Confronting%20the%20Russian%20Challenge%20-%20June%202019.pdf]

The Ideals of the American Republic

The stakes in the Russo-American conflict are high. Russian leader Vladimir Putin seeks to undermine confidence in democratically elected institutions and the institution of democracy itself in the United States and the West.1 He is trying to interfere with the ability of American and European peoples to choose their leaders freely and is undermining the rules-based international order on which American prosperity and security rest. His actions in Ukraine and Syria have driven the world toward greater violence and disorder. The normalization of Putin’s illegal actions over time will likely prompt other states to emulate his behavior and cause further deterioration of the international system.

Moscow’s war on the very idea of truth has been perhaps the most damaging Russian undertaking in recent years. The most basic element of the Russian information strategy, which we will consider in more detail presently, is the creation of a sense of uncertainty around any important issue. Russia’s strategy does not require persuading Western audiences that its actions in Ukraine’s Crimean Peninsula or the Kerch Strait, which connects the Black Sea and the Sea of Azov, for example, were legal or justified.3 It is enough to create an environment in which many people say simply, “who knows?” The “who knows?” principle feeds powerfully into the phenomena of viral “fake news,” as well as other falsehoods and accusations of falsehoods which, if left unchecked, will ultimately make civil discourse impossible. The Kremlin’s propaganda does not necessarily need its target audiences to believe in lies; its primary goal is to make sure they do not believe in the truth.

This aspect of Putin’s approach is one of the greatest obstacles to forming an accurate assessment and making recommendations. It is also one of the most insidious threats the current Russian strategy poses to the survival of the American republic. The good news is that the war on the idea of truth does not involve military operations or violence, though it can lead to both. The bad news is that it is extraordinarily difficult to identify, let alone to counter. Yet we must counter it if we are to survive as a functioning polity.

### Norms Solve---2AC

#### Norms solves the DA

Aidan Simardone 18, junior research fellow at the NATO Association of Canada, “More than Security: NATO and the Rules-Based International Order in the Post-Cold War Era,” NATO Association of Canada, 5/23/18, http://natoassociation.ca/more-than-security-nato-and-the-rules-based-international-order-in-the-post-cold-war-era/

NATO’s increasing role in supporting the rules-based international order is tremendously valuable. Nevertheless, the Alliance’s record has not been perfect. Questions remain over the legality of its intervention in the Balkans, which did not receive approval from the U.N. Security Council, as airstrikes in Serbia and Libya contradicted international laws on excessive force. Double standards, such as the decision to intervene in Libya but not Syria, are numerous. While these cases may be exceptional, they can give the impression to other states that NATO only values the rules-based international order when it works in its interest. Were states to emulate this perceived self-interest, NATO actions would effectively help to undermine rather than protect the rules-based international order.

As NATO moves forward, it must be conscientious of past mistakes and ongoing challenges. Tradeoffs are sometimes unavoidable, such as intervening to stop genocide without U.N. Security Council approval. However, in other cases NATO can take actions that fall closer in line with international laws and norms. Doing so will bolster NATO’s role in supporting the rules-based international order—a role that is becoming more central to NATO and gives vitality to the Alliance.

## AT: Offcase

### AT: DOS/Security Assistance CP---2AC

#### Only the DOD can shape nato cyber policy---military expertise is key

Lonergan ’21 [Erica and Jacquelyn Schneider; December 17; assistant professor in the Army Cyber Institute and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University; Ph.D., Hoover Fellow at Stanford University and an affiliate at Stanford’s Center for International Security and Cooperation; War on the Rocks, “Cyber Challenges for the New National Defense Strategy,” https://warontherocks.com/2021/12/cyber-challenges-for-the-new-national-defense-strategy/]

Challenges (and Opportunities) of Alliances

Integrated deterrence goes beyond what is already a very difficult challenge of making cyberspace work better within the U.S. military. Alliances also seem to play a huge role in the Department of Defense’s new deterrence concept. As Undersecretary of Defense Colin Kahl explained, the new strategy requires that the Department of Defense be “integrated across our allies and partners, which are the real asymmetric advantage that the United States has over any other competitor or potential adversary.”

Cyberspace presents a unique challenge for alliances. For years, Washington’s traditional alliance relationships struggled to even agree on basic cyber terms and attempts to share information were complicated by cyber operations’ close relationship with the highly classified world of signals intelligence. Moreover, U.S. actions in cyberspace have, in some cases, strained alliance relationships. Two prominent examples include the backlash over the Edward Snowden leaks as well as concerns about the implications of persistent engagement and defend forward for allied-owned networks.

These were considerable challenges. However, as cyber incidents have escalated over the last few years, there has also been an increasing recognition across these relationships that cyberspace matters. This joint recognition spurred new information-sharing mechanisms and partner efforts to find and root out adversary infiltration attempts on allied networks. Most recently, joint attribution by NATO and E.U. partners called out China for the Microsoft Exchange Hack — a rare reaction from these organizations. This comes on the heels of public statements at the NATO summit in Geneva in June that reaffirmed the applicability of the mutual defense clause of the alliance agreement to cyberspace. Further, despite the aforementioned alliance tensions, the Defense Department has conducted 24 “hunt forward” operations in which U.S. cyber protection teams partnered with 14 countries to root out adversary activity on allied networks.

Building on this forward momentum, perhaps the greatest opportunity for the Biden administration’s national defense strategy is to use military alliances and partnerships to facilitate norm development. Norms are shared understandings about appropriate behavior. Some norms are written down and formalized in agreements, while others are more informal and emerge as a result of state practice over time. Moreover, norms are agnostic with respect to morality: there could be “good” norms that facilitate cooperation, but also “bad” norms that make the international system less stable.

In the past, particularly under the Obama administration, norms were considered the realm of the State Department while the Department of Defense focused on deterrence by punishment and denial. This changed under the Trump administration, when the State Department’s norms efforts took a back seat to Department of Defense efforts to defend forward. The initial foundational work done by the Obama administration on cyber norms, paired with four years of experimentation and more risk-acceptant cyber authorities under the Trump administration, have created a track record for cyber norms that is far more heterogeneous than policymakers have let on. While there are certainly many areas where states disagree, norms do exist in cyberspace. For instance, a diverse set of states — beyond just the United States and “like minded” nations — has come to formal agreements about “rules of the road” for cyberspace through various international institution-driven processes, most notably the United Nations Group of Governmental Experts and the Open-Ended Working Group. To the surprise of many observers, earlier this year both of these processes resulted in consensus reports where parties agreed to a set of cyber norms. And from a bilateral perspective, rivals such as Russia have been willing to engage the United States in discussions about cyber norms, even if the prospects for cooperation remain uncertain. And beyond formalized agreements, there is a range of unwritten, implied norms that shape mutual expectations of behavior in cyberspace. These include a firebreak between cyber and conventional operations, such that states to not respond to cyber attacks with the use of kinetic military force; the idea that cyber espionage is generally treated as other forms of espionage (with some exceptions); and a pattern of tit-for-tat responses in cyberspace that have led to a nascent sense of what counts as “proportional.”

The Defense Department plays a large role in this process — though in the past this hasn’t been a formal effort. Specifically, how the Department of Defense uses its own cyber capabilities or threatens to respond to cyber capabilities can play an outsized role in whether cyberspace norms proliferate. Some have argued that employing military cyber power can, through a tacit process, contribute to the development of cyber norms. However, the ambiguous signaling strategies that this line of argument generates are often overly complicated and obtuse. Strategic documents are some of the clearest articulations of norms that adversaries receive. Given that, the U.S. military should use the opportunity of a new national defense strategy to voice clearly what the U.S. believes are appropriate norms of behavior in cyberspace. In particular, it should consider making unambiguous statements about what the Pentagon won’t do in cyberspace — in effect, a declaratory policy of restraint. This may be as important to norm propagation as efforts by the State Department to codify international agreements.

#### The CP subordinates DOS to State---that wrecks developing interoperable cyber doctrine

Sadler ’21 [Brent; June 30; Senior Fellow for Naval Warfare and Advanced Technology; “Don’t Shift Security Cooperation to State Department,” https://www.heritage.org/defense/commentary/dont-shift-security-cooperation-state-department]

America spends billions each year on security cooperation and assistance programs, but the results do not match the investment. To help improve efficiencies, the Center for American Progress recently proposed consolidating all these programs within the State Department.

That would be a big mistake, because it would minimize the Pentagon’s role in shaping and directing security assistance and, ultimately, the program’s military objectives would be subordinated to State Department interests, such as judicial reform and humanitarian programs. Those are not the values by which such security assistance programs should be solely judged.

Security sector assistance programs deliver arms, military training, and other defense-related services to allies and partner nation governments via grants, loans, credit, cash sales, or leasing. By definition, these programs should prioritize national security. To this end, reforms should enhance joint State and Defense authorities so programs are evaluated in terms of America’s national strategic goals.

In the existing system, State consults with Defense on its security assistance designs. Defense then implements State programs, as well as its own security cooperation programs, such as multinational military exercises and military training and advising.

The departments differ in the scope to which they apply security assistance. Defense programs target narrower national security objectives, such as the Maritime Security Initiative, launched in 2015 to expand maritime domain awareness. State’s programs, such as the Central America Regional Security Initiative, emphasize broader regional stability and humanitarian goals.

Assistance programs can be better tailored to their objectives when State shares directive authority and decision-making power with the entity most relevant to each program’s purpose. For example, when the objective is military capacity-building, the Defense Department should be an equal partner; when the goal is justice system reform, the Department of Justice should be a full partner.

Consider how the Philippines used American-sourced coast guard cutters when responding to China’s intrusions at Whitsun Reef earlier this year. Given President Biden’s emphasis on strategic competition with China, strengthening partner nations to resist Beijing’s maritime coercion should be a no-brainer. In this context, State should ensure it ties the objectives of its weapons sales program to Defense Department priorities, such as improving maritime domain awareness, by enabling the Philippines and, perhaps other countries, to increase patrols of exclusive economic zones.

Another report published this month by the Center for a New American Security rightly suggests that security assistance in the Middle East should be guided by strategy and applied narrowly to military effects. However, the report’s recommendations are limited to counterterrorism activities and a strategy of deprioritizing the Middle East in favor of the Indo-Pacific. If limiting security assistance to military purposes would make programs more effective in a region of waning emphasis, it stands to reason that this should be the formative basis for all security assistance programs, especially when strategy calls for increased investment in the security capacities of partner nations.

Reforms to security assistance should push the agencies in this direction, encouraging—or compelling—State to design its programs in closer coordination with the Pentagon and in support of Defense Department’s operational needs, such as improving military forward presence, wartime resilience and interoperability.

Congress should recognize and re-evaluate its role in these decision as well, as legislative earmarks can limit State’s directive agility and responsiveness. But even the best-laid plans cannot succeed without follow-through.

The Global Security Contingency Fund (GSCF), for example, tried to catalyze cooperation between State and Defense, but it neglected assessment processes. As a result, it fell short. This pilot program required concurrence from each department on any GSCF project and offered more flexibility in program funding. But two years after the first seven projects were announced, none had materialized. State and Defense failed to clearly define timeframes and track GSCF projects against those benchmarks, only starting to implement these standards years into the program. By 2016, execution still lagged expectations, and a frustrated Congress stopped paying for the program.

Regular evaluation that prioritizes timely, tangible measures of success directly tied to U.S. strategic interests is crucial to ensuring that programs deliver on their objectives. But as the GSCF showed, implementing assessments only after problems arise is damage control, not effective program design.

In devising reforms to ensure that U.S. funds, arms, and training are directed to viable projects that serve our national strategy, it’s critical to keep the main thing the main thing. State Department priorities for security assistance should emphasize specific national security objectives that enable better Defense Department forward presence, resilience and interoperability with our security partners.

#### Allies have asked for security cooperation with the DOD for cybersecurity---they’re not compelled by the CP

Cronk ’21 [Terri Moon Cronk; June 25; reporter for DoD News, which provides news and feature articles for the U.S. Department of Defense website; “DOD Wants Partners to Up Their Cybersecurity Game, Official Says,” https://www.defense.gov/News/News-Stories/article/article/2672689/dod-wants-partners-to-up-their-cybersecurity-game-official-says/]

The Defense Department wants to help its partner contractors, large and small, become better at their own cybersecurity efforts, the deputy assistant of defense for cyber policy said yesterday.

"We definitely want to make sure that size is not an obstacle to working with the Defense Department," Mieke Eoyang said at the Defense One Tech Summit. "And we are trying to figure out how to make it easier for [contractors] to understand what kinds of better security practices are out there and what they can do to protect themselves."

Eoyang said U.S. adversaries are very much aware that DOD relies on innovation, but she added DOD doesn't just look at only large contractors when looking for a technological edge. It's also important for contractors to adopt best practices in cybersecurity — such as turning on multi-factor authentication, using cloud migration or working with cybersecurity companies — to enhance their own security, she said.

DOD participates in whole-of-government activities to target and disrupt ransomware, the deputy assistant secretary said, adding that the department is willing to work through its intelligence and law enforcement partners to provide insights to disrupt such threats.

It's vital for industry to think about this from the perspective of resilience, Eoyang said of protection in cybersecurity.

"Companies need to be prepared for the possibility that it could happen to them," Eoyang said. "They need to improve their security, make themselves harder targets, but also really think about continuity of operations, so if, or when, they get hit, they know how to keep moving and how to work around the problem. But I don't think that we want to be in a position where people are turning to the Department of Defense to try and stop every single criminal gang out there …. We have to be able to focus on those nation state adversaries, and we do focus on that. But in the meantime, people also need to focus on improving their own resilience, being harder targets."

DOD is resilient and mature in its cybersecurity practices, the deputy assistant secretary said. "I think it's very clear from the president on down … and other countries should make no mistake about the seriousness with which the United States treats this problem and our interest in being able to get after malicious actors."

DOD has been working through U.S. Cyber Command and other entities, she said, directly with industry to help contractors identify potential malicious activity on their networks. "And there are other things we can do to help people — [such as] when we identify malware, we can post it out there for the world to see — so that they can take that into consideration as part of their efforts to secure their own systems."

As DOD considers how to bolster its allies, security cooperation is a big factor, Eoyang said. "What I've seen so far is that one of the No. 1 requests to the combatant commanders for security cooperation assistance is in the area of cybersecurity. But we do not have the clarity of offerings that the private sector could provide under security cooperation funds to our partners and allies, so I would encourage industry to work with us so that we have a better understanding of what might be available, what they might be able to provide through security cooperation, to help shore up the cybersecurity of our partners and allies. And [our] door's always open to talk about that."

#### SC is whole-of-government---any exclusion ensures partner confusion

Arnold ’20 [Colonel Jason “Hap” Arnold, U.S. Air Force Reserve (Retired); Aug 6; Instructor at the Defense Institute of Security Cooperation and former Assistant Professor at National Defense University, Joint Forces Staff College; FAOA Journal of International Affairs, “Add Value to Security Cooperation through Joint Unification,” https://faoajournal.substack.com/p/add-value-to-security-cooperation?s=r]

Security Cooperation is inherently an interagency process, and requires a whole of government effort. Presidential Policy Directive 23 identified the Department of State (DoS) as the lead agency for United States Security Sector Assistance Policy, and all Security Assistance and Security Cooperation efforts require coordination and consent across agencies. The interagency process can be hampered by the diversity of processes and players that are presented by the separate Services’ SC organizations. It is not only our international partners that struggle with learning the different ways and means of the various implementing agencies, our own interagency partners can experience confusion as well in navigating the various systems, doctrine, and processes.

#### DOS fails---lack of training ensures they have little role in improving partner militaries

Karas ’20 [Mark; Oct 23; retired Colonel in the US Army, instructor at the Defense Institute of Security Cooperation Studies (DISCS), Wright Patterson Air Force Base, and graduate of the U.S. Army War College; FAOA Journal of International Affairs, “Reconciling Defense and State Department Cultures at Embassies: A FAO Survival Guide To Working On a U.S. Country Team,” <https://faoajournal.substack.com/p/reconciling-defense-and-state-department?s=r>]

In the area of DoD efforts in security cooperation with international partner military and security forces, DoD has certainly exploded with authorities and authorizations to conduct training and equipping efforts outside of the traditional security assistance programs enshrined under State Department Title 22 authority. After 9/11 and with the wars in Afghanistan and Iraq as well as GWOT efforts around the globe, DoD felt it needed these programs to address emergent requirements in partner capability development. In this environment, DoD deemed traditional programs like Foreign Military Financing Program (FMFP) and International Military Education and Training (IMET), State Department security assistance under its Title 22 authority, were no longer sufficient, if not wholly inappropriate. Established with the Foreign Assistance Act of 1961, these programs reflect the nature of traditional bilateral political relationships as opposed to an emergent security requirement. During the Bush Administration, building up indigenous security forces and coalition partners during operations in Iraq and Afghanistan became important requirements. Under President Obama, coalition development thinking evolved as the administration sought to address security challenges with “other people’s armies.” The Obama Administration sought to be preventative rather than reactive to security challenges, resolving such challenges before there was a need for another extended commitment of U.S. troops.

Civilian institutions of diplomacy and development express skepticism as to whether the U.S. military is suited for these tasks, pointing out that results are at best mixed and these efforts risk militarization of the problem set at the expense of social, economic, civil society, and governmental institutional development -- core issues of most security problems. Others counter that while the criticisms have merit, the U.S. military is the only institution with the personnel, resources, planning, and projection capability to reliably deliver security in relatively short order. As the DoS and some members of Congress have chafed at DoDs conduct of these sorts of activities, authorizations regularly mandate DoS coordination and concurrence on proposals. Many of these proposals, or “Building Partner Capacity” cases, funded with DoD Title 10 funds, require Country Team Assessments (CTA), ultimately expressing embassy agreement for a particular project. Now, the DoS is involved with these cases from the country team, through the geographic combatant command and the Pentagon, to congressional notification.

Writing in Foreign Policy, James Jeffery, former U.S. Ambassador to Turkey, Iraq, and Albania (and as of this writing serving as the U.S. Special Representative for Syria Engagement), agrees with Brooks’ argument of the outsized role of the DoD, noting that the “military’s effectiveness in such quasi-diplomatic business is limited.” He argues that the authorities and funding appropriations DoD has accumulated since 9/11 in training and equipping security forces should revert to DoS in its traditional role of managing and overseeing security assistance as foreign policy. However, he places a good bit of responsibility for State’s diminution in foreign policy on its own ever-expanding set of priorities at the expense of big-picture “traditional diplomacy.” He is critical of State Department’s direction over the years in emphasizing an unfocused grab bag of “soft power” social agendas in a bid to be a “deep transformer.” He notes that in the 2015 Quadrennial Diplomacy and Development Review (QDDR), issues like the South China Sea and Ukraine are dramatically less prominent than the stated priorities that consist of what he characterized as a “hodgepodge of social engineering” and climate change. He notes that now, “operationally, the State Department is seen as an alternative to -- rather than partner or exploiter of military and other hard power.”

FSOs, particularly more junior ones, do tend to view diplomatic and military actions almost as a binary choice. Instinctively, they have difficulty understanding what role the military plays in diplomacy. Accepting perhaps a very narrow role for the U.S. military to assist with host-nation defense reforms, or exercising with a friendly host-nation military, they tend to view the military as an entity to be called on in an emergency--“just break glass.” But in the meantime, it is best for the military to stay in the glass box. From their perspective, if DoS succeeds in its “deep transformation efforts,” there is little need for military involvement and the immense resources the military consumes. Today’s FSO’s view of diplomacy is broader than DoD’s view (which arguably trends more towards Ambassador Jeffrey’s more traditional model) and encompasses promoting American values through a host of agendas. They have seen that the military’s success has been limited and are naturally skeptical when an enthusiastic staff officer from a geographic combatant command pitches them on something he or she thinks is a grand new idea.

As Jeffrey and others have noted, DoS has accumulated a broad set of more narrow activities in what retired Ambassador Larry Butler has called a “proliferation of priorities.” The proliferation of priorities is perfectly understandable considering State’s culture of open discussion, respect for complexity, and resistance to risk. The result is numerous smaller “soft power” efforts of limited funds targeting big scope issues: child and gender issues, civil society development, LGBTQ issues, religious rights, micro-finance, anti-graffiti campaigns, media funding, civil society development, climate change intervention promotion, etc. This strategic diffusion results in many benign smaller programs that have a positive optic and may raise awareness but have questionable transformative effects, particularly at current funding levels. Jeffery argues that since World War II, “nowhere but Japan, Germany, and in Western Europe (via the Marshall Plan) have soft-power tools transformed strategic terrain to our advantage.” In many respects, the issue is not wholly of State Department’s diminution in foreign policy, but that institution’s diffusion of its efforts, which others have argued is the reason why many of State’s foreign policy development functions have migrated to an ever-growing National Security Council.

FAOs assigned to an embassy will often walk into a blizzard of DoS activities, outside of just defense and security. FSOs, in addition to their core task of cable writing, feverishly try to keep track of the myriad of issues, activities, and working groups. The DoS, particularly at the country team level, has difficulty in prioritizing its efforts and asking itself whether a particular initiative is necessary, sufficient, and truly transformational. Of course FSOs at embassies are quick to assess that the many things an embassy is doing at times need to be scaled back. Many well-intentioned country team meetings have sincerely tried to neck down priorities, but the open discussion format of problem sets often triggers the “it’s complicated” default and priority lists have ballooned again. Like any other bureaucracy in the U.S. Government, it’s hard for the DoS to drop product lines, even with its nuanced thinking and flexible approaches. In the end, the only solution agreed upon is the need for more people and more resources.

Much of this development work is done by the United States Agency for International Development (USAID), an agency that is separate from the DoS but which reports to the Secretary of State (somewhat analogous to the U.S. Marine Corps falling under the Department of the Navy), though the DoS also manages and implements specific programs in many sectors such as law enforcement and the media, and not every country has a USAID presence. USAID prefers to guard its independence from the DoS, and there are usually energetic and complex discussions at a country team between State and USAID on the direction of development as well. However, USAID does have a more deliberate planning and assessment process in the implementation of its programs that DoD is learning from to better enable security cooperation program assessments.

“So what’s a Combatant Command…?”

Given the ambassador’s authority over all U.S government representation at an embassy and State’s responsibility to coordinate “whole of government” approaches at the country team level, including DoD security cooperation, most rank-and-file FSOs typically know little of the U.S. military. It is true, however, that over the last several years a greater percentage of incoming FSO do have prior military experience, and there have been a significant number of FSOs that have served with the military as political advisors or on Provincial Reconstruction Teams (PRTs). Unfortunately, the DoS advancement systems don’t particularly value assignments that have FSOs working with the military. After their initial training at the Foreign Service Institute, FSOs have little professional development outside of on-the-job experience throughout their careers that can expand their aperture of the U.S. government.

Moreover, FSOs receive little development in leadership and management. There are often few opportunities for FSOs in the Political, Economic, and Public Diplomacy “cones” (State Department’s version of career tracks) to lead and manage and programs. There are FSOs that can go there entire careers without managing programs. For the interagency, this is unfortunate as DoS personnel at country teams are expected to coordinate and integrate multi-departmental efforts to support “whole of government” approaches. On a practical level, they chair working groups on such issues as economic development, investing in people, law enforcement, or countering violent extremism, which FSOs sometimes view as a distraction from their core tasks. These working groups tend not to be planning or strategy development affairs but have a more basic “clearing house” function. Interagency participants share activity information and present proposals, but too often the priority purpose of these fora is to ensure a particular department’s initiative first, does no harm.

In contrast to the State Department, the military sends service members to various professional military education (PME) courses throughout their careers. At the more senior courses, military members are at least exposed to the need for “whole of government" approaches and the primacy of the State Department in foreign affairs (though PME could do much better on presenting the functions and organization of State Department itself). Army officers training as FAOs, conducting their one-year in-region training, will intern at one if not several embassies under the direction and mentorship of an attaché or SCO. Even as FAOs prepare for attaché and SCO assignments by attending the Joint Military Attaché School (JMAS) and the Defense Institute of Security Cooperation Studies (DISCS) (SDO/DATTs attend both), they are exposed to concepts such as the interagency process and U.S. embassy roles and organization. At these courses, military personnel learn about the role of the DoS, the country team, and the authorities of DoS versus DoD in the conduct of security cooperation and security assistance. Military personnel report to a country team understanding that whatever DoD does requires consistency with, and support to, the ambassador’s Integrated Country Strategy (ICS). SCOs are briefed on their requirement to provide input to the embassy’s Mission Resource Request (MRR) by way of their FMF and IMET projections. As a result of this continuing education coupled with hard experience, military leaders regularly acknowledge the importance of DoS diplomacy, USAID’s important work in development, the insufficiency of a military-only approach, and the need for DoS leadership. Other than hard experience, there is nothing comparable for State Department FSOs to prepare them to work with interagency partners, including the military.

As professional development DoS sends few of its population to U.S. military professional military education institutions, and fails to make use of the experiences of those that do attend. Despite the strong demand signal sent out by senior military leaders, POLAD positions throughout the various U.S. military commands aren’t always filled with the most qualified candidates, and these positions aren’t thought to be particularly career enhancing within the DoS personnel advancement system. The political-military portfolio in a Political Section of an embassy isn’t considered particularly “attractive” and career enhancing, and these officers often feel the need to seek additional portfolios to make themselves more competitive. This is unfortunate as the Pol-Mil officer is an absolutely crucial position to integrate DoD-DoS efforts at the country team level. A good Pol-Mil officer is a “force and resource multiplier,” and are worth their weight in gold to DoD and DoS, and should be recognized and rewarded for their work.

As a result of unfamiliarity with the military and the lack of appeal of political-military issues, an FSO tends to be surprised at the role of the military at the country team and wonders why military officers show up to public affairs planning meetings, law enforcement working groups, and countering violent extremist meetings. Additionally, with the possible exception of FAOs, military personnel are not seen as having the requisite level of understanding of host-nation nuances to speak authoritatively on an issue, let alone suggest a remedy. This is particularly true of military members who come in from a command to propose an initiative or those who deploy to an embassy for temporary duty, often a source of consternation for FSOs. Having limited understanding of how DoD works, its capabilities, authorities, and resources, they can see themselves as holding the line against militarization. They generally do not understand DoD security cooperation programs and authorities. Many are even unaware that traditional security assistance programs such as Foreign Military Financing (FMF) and International Military Education and Training (IMET), are actually DoS Programs under Title 22 authority and only administered by DoD.

Military personnel can report to an embassy enthusiastically looking forward to jumping into “whole of government” efforts with a broad range of colleagues, only to be greeted at times with suspicion, dismissiveness, and curiosity as to the reason for the enthusiasm. The military person walks away disappointed their “whole of government” effort is unrequited, perhaps with the impression of the stereotypical arrogant FSO, an unfortunate take away for a future potential senior military leader. This can be particularly true of military members that deploy on short six-month rotations, who don’t have the time and opportunity to develop situational awareness and relationships of trust with FSOs. FAOs serving as Attaches and SCOs at embassies should work to build relations (face-to-face), trust, and inform foreign service personnel on the U.S. military, its organizational processes, its programs and capabilities, and resources -- and then let them lead. At embassy working groups, military members should work constructively with FSOs, suggesting potential options for organizing work, but make clear they are there to “complement and reinforce” embassy efforts, not to take over. And as hard as it may be for military, sometimes “dialing back” the energy and assertiveness is more appropriate for a country team setting. Attaches and SCOs should mentor short-term military deployers and help them navigate the idiosyncrasies of country teams. In turn, short-term deployers should work closely with DAOs and SCOs and not only coordinate with these offices, but seek out advice on how best to work within the culture of a given country team.

Conclusion

Considering the personnel and resources at the military’s disposal relative to DoS, it is easy to see how quickly a growing DoD presence and “Swiss army knife” of missions and authorities could soon overwhelm a country team. Aside from the traditional Defense Attaché Office and the Security Cooperation Office, civil affairs teams, MISTs, and special operations forces elements can increase the number of military members visible at an embassy. Obviously military individuals wearing civilian attire attract the eye and can stir consternation throughout the embassy sections. In the small bubble of an embassy community, the question, “what are they really doing here?” is asked in hushed whispers, as if witnessing some bad movie or television show. Some FSOs, concerned about the optic of a militarized embassy, would prefer short-term military personnel not come into the embassy at all.

### AT: Arms Control CP---2AC

#### Cyber arms control fails

Borghard ’18 [Erica and Shawn W. Lonergan; Jan 16; research fellows at the Army Cyber Institute at West Point; CFR, “Why Are There No Cyber Arms Control Agreements?,” https://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements]

During the Cold War, when nuclear-armed superpowers faced concerns regarding crisis instability and escalation, they entered into arms controls agreements. Arms control regimes can alter the military incentives for the use of offensive technologies; limit the damage to states in the event these technologies are used; and generally contribute to stable interstate relations, even between adversaries. With the emergence of a militarized cyber domain that creates the conditions for misperceptions that could lead to inadvertent conflict, why are there no cyber arms control regimes?

Traditional arms control regimes are inapplicable to cyberspace for four reasons: it is difficult to measure the relative strength of states in cyberspace; there is uncertainty regarding the military effects of cyber technology; the challenges of monitoring compliance; and difficulties with enforcement.

Arms control regimes require states to have a basic understating of each other’s relative strength so that an agreement can promote strategic stability. For conventional munitions, nuclear weapons, or even chemical ordinances, warheads or pounds of a virulent gas that a state possesses can be counted, allowing others to assess comparative strength. The same cannot be said for assessing relative strength in cyberspace for two reasons. First, how can a state possibly count virtual weapons that by definition cannot be destroyed and, in theory, could be continuously regenerated? Second, unlike nukes or tanks, some cyber weapons lack universal lethality—unique tools and accesses are often required to deliver effects against specific targeted systems.

In contrast, what may be more readily measurable in cyberspace is the technical skill of cyber threat actors—a qualitative, rather than quantitative measure of capability. However, using relative skill to drive arms control regimes may be impractical due to the difficulty of crafting or enforcing agreements that limit skill or access to technology, particularly when governments are not the sole proprietors.

Arms control regimes may also form if governments are able to make reasonable calculations regarding the likely military effect of technological changes. However, the rapid and unpredictable pace of technological innovation in the cyber domain complicates these assessments. At the tactical level, attack vectors and offensive capabilities are continuously evolving, in contrast to the nuclear arena where innovations had long development timelines and could often be observed. The lag time in nuclear innovation gave states breathing room to adjust arms control agreements or develop other means, such as tailored intelligence or their own complimentary programs, to mitigate the fears posed by technological advances. In cyberspace, the open-ended promise of innovation coupled with quickly changing tradecraft that can emerge with little to no warning challenges the creation of any agreement. A cyber arms control agreement runs the risk of being outdated or restrictive in some unanticipated way before the ink has even had time to dry.

Even if states are able to calculate relative capabilities and assess the military implications of a technological innovations, cyber arms control agreements are unlikely to form if governments cannot detect cheating. The verification problem contains two prongs: being able to ascertain the size of a state’s arsenal and monitoring it to ensure future compliance.

Ascertaining compliance in the cyber domain would require participants to agree to intrusive access to government networks. Malicious software can be developed just about anywhere, meaning that any verification mechanism would require a government to open up all of its networks to inspection. It would be unfathomable for one state to allow another, or any outside actor, to have unfettered access to its networks. Such access would provide an external party with critical information about vulnerabilities and potential exploits, and potentially violate the agreement it is attempting to enforce.

A less invasive means to assess compliance would be to have monitoring occur through national technical means of intelligence. During the Cold War, spies analyzed imagery collected from satellites that monitored the nuclear posture of another state. The equivalent in cyberspace would be to use cyber espionage to collect information about another state’s internal networks. However, while satellite collection is entirely passive, gaining access to and potentially absconding with data from sensitive government networks is not. If a state observes a third party penetrating its networks, it may be unable to distinguish between routine espionage activity for the purposes of monitoring compliance, other legitimate espionage purposes unrelated to compliance, or preparation for an offensive operation. This could prompt the targeted state to respond in an escalatory fashion. Therefore, the inability to perceive intent could, again, undermine the very stability the arms control agreements were meant to create.

Finally, even if the preceding obstacles could be overcome, enforcement of any arms control agreement would be difficult to implement due to two factors: problems associated with attribution and divining a proportionate punishment. First, in the event of a violation, states would have to attribute it with a level of confidence that would justify a reciprocal response. While attribution capabilities have unquestionably improved over time, not all states have the same attribution capabilities or enough confidence in them to justify action. This is particularly relevant given that a state that detects a violation would need to convince other parties to the same treaty that a violation occurred.

Second, enforcing an arms control agreement requires proportionate responses to observed derogation. This is problematic for several reasons. There may be a significant time lag between when a derogation occurs and when it is actually observed. Thus, the deterrent effect of a response is likely to be diluted by the simple passage of time. Furthermore, resource and access constraints may limit the capabilities a state has at a given moment to respond, which means that it may not necessarily be effective. A potential alternative could be to use non-cyber elements of national power to punish a derogation of a cyber arms control agreement. However, crafting an effective response that relies on physical elements of power may be difficult to formulate if the violation only caused virtual damage.

### AT: Early Warning CP---2AC

#### Its not credible

Whitney L. Cissell 20, MA thesis in Security Studies, Naval Postgraduate School, Army Major, Nuclear Nonproliferation Officer, March 2020, "DETERRENCE IN THE DANGER ZONE: HOW THE UNITED STATES CAN DETER RUSSIAN GRAY ZONE CONFLICT", https://calhoun.nps.edu/handle/10945/64844

2. Applying Deterrence in the Context of Russian Behavior

This section builds on the previous assessments and explores the application of deterrence theory at the sub-conventional level in the specific context of Russia as a state actor and its use of a gray zone strategy. It considers the value of tailoring a deterrent strategy against Russian gray zone conflict by supplementing conventional deterrence with “cumulative deterrence.” Recall that any deterrence strategy relies on sufficient capabilities, solid resolve, and strong communication of a threat, which in turn create credibility.225 Cumulative deterrence, elaborated in the following paragraphs, introduces the idea that credibility can be sustained across multiple encounters even if deterrence fails in certain instances, vis-à-vis classic zero-tolerance nuclear deterrence.

Regarding tailoring deterrence, Bunn writes, “If deterrence is about influencing the perceptions—and ultimately, the decisions and actions—of another party, it is logical that the requirements for deterrence will differ with each party that we might try to deter and may well differ in each circumstance or scenario.”226 Adapting deterrence to the subconventional level requires an understanding of the unique relationship between the states to identify the relative stability and instability that can inform deterrence strategy.

The stability–instability paradox applies to the nuclear and conventional level, and indeed, Russia’s effort to avoid conventional-level warfare with the United States strengthens stability between the states at the conventional level similar to the strategic nuclear level. While U.S.–Russian nuclear stability is based on parity, conventional stability in this relationship is more complex. As shown in Chapter II, Russia has a strong aversion to conflict with the United States and NATO at the conventional level. Russia would be outmatched in military superiority after two to three weeks of conflict and beyond its near abroad and, thus, prefers to operate at the sub-conventional level below the threshold of armed conflict.227 In effect, Russia’s strategy of avoiding any actions that might trigger conventional conflict aims to bolster a sort of “firewall” between conventional warfare and gray zone conflict. NATO, up to now, has effectively obliged this Russian strategy by not brandishing threats of conventional escalation in response to Russian gray zone aggression, let alone undertaking conventional responses. As much as Russia seeks to avoid escalation to conventional warfare it could not win, it is also learning how averse NATO is to threaten such escalation. This aversion is ironic insofar as Cold War–era extended deterrence relied on NATO’s threat of escalatory nuclear responses to conventional attacks.

These respective Russian and NATO postures enhance conventional stability, but at the cost of fueling instability at the gray zone level, reflecting a form of the stability– instability paradox familiar in nuclear strategies. This tailored application of the stability– instability paradox to the specific Russian context yields a tiered relationship of stability between the United States and Russia at each level of warfare, as depicted in Figure 1, and helps explain why the United States and Russia are the most unstable at the subconventional level, on which this research focuses.

Cumulative deterrence may be an option to address the issues created when adapting conventional deterrence to the sub-conventional level including the credibility and communication of the threat. Cumulative deterrence has not been a standard element of U.S. deterrence strategy in the past, and there is limited academic literature and strategic thought about its use in areas outside of cyber and terrorism. However, this new security environment characterized by great power competition at levels below open conflict requires a new way of looking at the deterrence landscape at the sub-conventional level. Subject matter experts for this research confirm that a zero-tolerance deterrence mindset will not work at the sub-conventional level and that the United States might have to choose what portions of the gray zone it wants to deter because it may be difficult to deter everything.229

There is a precedent for applying a cumulative model and mindset of deterrence to limit and shape the sub-conventional level of conflict, and this suggests it may also be applied to the current U.S. need to deter Russia’s gray zone conflict. According to Thomas Rid, cumulative deterrence “consists of a series of acts of force to create—and maintain— general norms of behavior for many political actors over an extended period. Using force, consequently, does not represent a principal failure of deterrence but its maintenance through swift, certain, but measured responses.”230 Cumulative deterrence has been a key part of Israel’s strategy for decades and was developed in the conventional and subconventional level focusing on limiting and shaping ongoing conflicts against both state and non-state actors at the conventional and sub-conventional level.231 In addition, cumulative deterrence has recently been considered for use in deterring terrorism and cyberattacks, as it is designed for long-term sustained conflict, such as competition in the gray zone.232

Doron Almong describes cumulative deterrence as functioning on two levels: the macro, which creates an image of overwhelming military superiority, and the micro, which relies on responses to adversarial actions.233 Almong also explains that cumulative deterrence has three key features.

First, its effectiveness is measured in terms of the number of victories accumulated over the duration of the conflict, which might be envisioned as “assets in a victory bank.” Second, over time, these victories produce increasingly moderate behavior on the part of the adversary and a shift in its strategic, operational, and tactical goals until there is a near-absence of direct conflict. Third, this moderation may eventually result in political negotiations and perhaps even a peace agreement.234 Almong is describing cumulative deterrence as applied to the conventional level of warfare; however, in the context of Russia, the construct can be transposed to the subconventional level. At the sub-conventional level, U.S. responses over time to Russian gray zone aggression could moderate Russian behavior, causing a shift in Russia’s decision calculus and strategic goals, thereby diminishing the conflict.

The advantage of layering a strong conventional deterrence strategy with cumulative deterrence is that it allows the restoration of deterrence over time if conventional threats fail to deter at the sub-conventional level. Over time, cumulative deterrence responses to gray zone actions bolster the credibility of the United States and alter Russia’s decision calculus at the sub-conventional level, therefore strengthening deterrence overall. Successful deterrence at the sub-conventional level requires a reorientation in how the U.S. views deterrence, moving from a zero-tolerance strategy to the long-term attrition of gray zone conflict. This renewed mindset allows for tailored punitive strategies that over time limit the bounds of the gray zone through the reiteration of unacceptable behavior through punishment. Regardless of the level at which a state wishes to conduct warfare, all deterrence strategies rely on three aspects that must work in concert: sufficient capabilities, solid credibility, and strong communication of a threat.235 As Rid explains, confrontations should be “seen as necessary evils that should be kept on as low a level as possible, but that could not be pushed down to zero.”236 This argument assumes escalation control, which is to say that the United States can control escalation at the sub-conventional level on its own terms.

Many authors challenge the notion of escalation control, claiming that it is risky and nearly impossible. Scholars claim that avoiding escalation requires deterring the action and that a policy to deter one action could in fact risk escalation to another. Additionally, scholars claim, “Escalation control or management is an inherently imperfect business. It can be done well or poorly, but it is extremely rare for any set of policies to eliminate the risk of significant escalation altogether.”237 These same scholars agree that the risk of inadvertent escalation can be reduced, but they are concerned that policy makers are incorrectly assuming it can be eliminated altogether.238 The concerns over escalation control are valid; however, it is possible to control escalation and use the threat of escalation to bolster deterrence. Mazarr explains that the gray zone puts the defender in the position to escalate, which is part of the challenge of deterrence.239 Both escalation control and deterrence fundamentally rely on communication and a thorough understanding of the adversary. Proper communication of the capability and the resolve to use the capability to deny or punish an action are just as crucial to escalation control as they are to deterrence. The same scholars who express concerns over escalation control also admit there is a way to control the risk: “Escalation depends heavily on an astute understanding of how the adversary will perceive and interpret events that have not yet occurred—not only in a general sense, but also under the specific and often difficult-to-predict conditions that will shape the opponent’s perceptions and responses when a particular event occurs.”240 The United States can both mitigate escalation and contribute to deterrence by adding an element of ambiguity to its deterrence threats that leave something to chance but also allow a response that limits or controls the escalatory response of the adversary.

When the United States responds with an instrument of state power in any DIME category, such as the expulsion of 60 Russian diplomats in response to the Russian nerve agent attack on a British citizen in 2018, it can strengthen cumulative deterrence credibility. Some of the literature on cumulative deterrence suggests that deterrence works by banking “wins” by responding to events with military power. However, when adapted to the gray zone, it seems critical that all elements of state power must be utilized, not just the military. The military is sometimes—not always—an appropriate response to an action in the gray zone, so threatening military retaliation for every tactic in the gray zone is not credible; however, a state must still have the ability to impose costs on an adversary for an action to make cumulative deterrence successful.

### AT: Inducements CP---2AC

#### Inducements can’t solve interoperability

Kunertova ’20 [Dominika; April 24; postdoctoral research fellow at the Center for War Studies in Denmark, with a Ph.D. in Political Science from Université de Montréal, she researches trans-Atlantic security and defense cooperation, NATO-EU relations, and military technology; War on the Rocks, “CAN THE NEW ‘MAGI’ SAVE NATO?,” https://warontherocks.com/2020/04/can-the-new-magi-save-nato]

You Can’t Buy Interoperability

In contrast to statistical engineering that aims to adjust numbers to fit the desired “fair share,” true burden-sharing would put emphasis on defense capabilities and operational readiness. Shifting the emphasis away from abstract macroeconomic numbers to practical cooperation based on strategic needs should inform the content (which capabilities to buy), not only the form (defense spending levels), of burden-sharing debates. This highlights the problem that allies cannot just buy interoperability, as it requires enhanced cooperation and coordination. Although interoperability is considered the alliance’s core business, it has not been systematically treated in the burden-sharing debate. In addition, burden-sharing that includes the mutual-aid dimension would further refine the cash, capabilities, contributions — or “three C’s” — framework regularly mentioned by the current NATO secretary-general.

The current defense spending narrative is thus a symptom of empty formalism in NATO that reflects a lack of clarity about the alliance’s purpose, and favors statistical deceptions over effectively implementing the mutual commitment to defend each other. A February 2020 poll by the Pew Research Center revealed a worrying trend: While NATO is generally seen in a positive light across publics within the alliance (a median of 53 percent view NATO positively, though with double-digit percentage point declines in Germany and France over the past 10 years), many in 16 surveyed NATO countries seem reluctant to fulfill Article V collective defense obligations. A median of 50 percent across 16 NATO member countries is against their country defending an ally, while only 38 percent express willingness to come to help a fellow ally.

Future Defense Spending in Peril right, especially in the context of the short- and long-term consequences of the ongoing COVID-19 pandemic. While the scope of the economic impact is still unclear, it is likely to reshuffle financial priorities in NATO countries. Defense ministries will find it more difficult to reach the 2 percent spending level by 2024 or even to maintain the current defense expenditures programs. Moreover, with economies put to halt and eventual drops in national GDP, even if countries fulfill the 2 percent pledge, they could end up spending less in real terms. If NATO members continue to frame fairness in terms of the 2 percent defense spending target, it will further aggravate the burden-sharing problem, seriously test NATO solidarity, and ultimately endanger the alliance’s ability to adapt to the increasingly unpredictable security environment and the changing nature of security threats.

Improving NATO’s cohesion and its political role will not happen overnight or through high-level political declarations. If there are any lessons to be learned from the Three Wise Men’s effort back in 1956, it is that perseverance, personal relationships and reputation, pragmatism, and humility matter a great deal.

to describe cyber “attack,” “information operations,” and attribution findings with different implicit assumptions or implications.

### AT: Process/Conditions CP---2AC

#### Cumbersome approval processes bad---wreck effective cyber policy

Schneider ’22 [Jacquelyn; April 25; assistant professor and affiliate faculty at the Center for Cyber Conflict Studies at the U.S. Naval War College; Wall Street Journal; “The Biden White House's Cyberwarfare Power Grab,” Factiva]

To most onlookers, the U.S. appears to be in the midst of a successful cyber defense campaign against Russia. As Gen. Paul Nakasone, commander of U.S. Cyber Command, recently testified before Congress, the U.S. military is deploying military members to the region to sit "side by side with our partners." Cyber Command has also "crafted options for national decision makers" and is "conducting operations as directed." Yet at a pivotal time in Ukrainian cyber defense, the Biden administration is reportedly considering a proposal to take away Defense Department authorities to conduct offensive cyber operations and reinstate a centralized approval process from the White House. This would be a mistake.

All departments and agencies within the federal government operate under different authorities, delegated from the president through executive policies and from Congress through law. These define what an organization can and can't do and when it needs to ask for permission. In a conflict or military campaign, the president (and sometimes Congress) delegates authorities to the Defense Department to conduct operations.

Offensive cyber operations didn't quite fit under existing military authorities, so the Obama administration created Presidential Policy Directive 20 in 2012. This directive created a centralized interagency review process to approve offensive cyber operations and gave other government organizations a veto over military cyber operations. The review process was slow, deliberative and prone to internecine fights: The intelligence community didn't want to cede control over cyber operations; the diplomatic community worried over implications for international partnerships; the Pentagon was eager to come off the cyber sidelines. Not surprisingly, few if any offensive cyber operations made it through the review process, despite significant cyber incidents such as North Korea's hack of Sony in 2014 and Russia's cyber-enabled election interference in 2016. When Sen. Mike Rounds (R., S.D.) asked Gen. Nakasone in April about military offensive cyber operations under PPD-20, he replied, "I know of no effects operations ever conducted prior to 2018."

For the Obama administration, military cyber restraint was an acceptable hedge against the risk of escalation. Faced with uncertainty about responses to cyberattacks, the administration chose to err on the side of inaction.

That perception of cyber risk changed during the Trump administration—and so did the military's cyber authorities. While National Security Presidential Memorandum 13 remains classified, U.S. officials' public statements suggest the policy delegates authorities to the Defense Department to conduct "time-sensitive" offensive cyber operations without a cumbersome interagency approval process. Concurrently, Congress delegated authorities to the Pentagon in the 2019 National Defense Authorization Act to conduct "military activity and operations in cyberspace," including "active defense" against China, Russia, North Korea and Iran. The act went on to define this as traditional military activity not subject to a presidential finding, which is required for covert action.

In the decade since the Obama administration began defining U.S. offensive cyber policy, cyberspace has become less uncertain. Academic research and the emerging lessons from Russia's invasion of Ukraine suggest that cyber operations don't escalate to violence. Case studies, data analyses, experiments and war games all show the Obama administration's fears about cyber escalation were misplaced.

Cyberspace isn't the "Wild West." Norms are being developed—both tacitly as actors operate and explicitly as states agree on formal cyber rules. The lack of violent responses to cyber operations, for example, suggests that states view cyberspace differently than conventional uses of force. And a United Nations Group of General Experts on cyberspace (which includes the U.S., China and Russia) agreed in 2021 that cyberattacks against critical infrastructure before violent conflict is inappropriate.

We know more about when and how cyber operations are most effective. They are best for espionage, perception shaping, or creating fog, friction and uncertainty, all of which are most effective at the early stages of conflict. Gaining access to networks and exploiting their weaknesses requires large investments, which is why highly centralized operations with tight control struggle to keep pace as network configurations change, patches are implemented, or other new controls are adopted. Ukraine has proved that bottom-up adaptation and experimentation are key to success, especially in cyberspace.

Critics argue that current cyber authorities gave the Pentagon free rein to conduct whatever offensive cyber operations it deems useful. But given how little evidence we've seen of U.S. offensive cyber operations in the general public, this is likely an exaggeration. Instead of taking away these authorities, the White House should clearly communicate what the Defense Department can do in cyberspace before a declared war or conflict and, as important, what it will not do. Finally, we should be wary of turning cyber authorities into a partisan debate.

### AT: Security K---2AC

#### Hybrid warfare disrupts NATO’s ontological security---reproduces the narrative of the “other” and turns the K---strengthening collective identity solves

Bahar Rumelili 15, Professor and Jean Monnet Chair at the Department of International Relations, Koc University, Istanbul, “Identity and desecuritisation: the pitfalls of conflating ontological and physical security,” Journal of International Relations and Development volume 18, pages52–74 (2015), https://link.springer.com/article/10.1057/jird.2013.22

With regard to ontological security, the distinction between security and insecurity is the more critical one. In a state of ontological insecurity, the Self experiences instability and uncertainty of being. Ontological insecurity refers to a state of disruption where the Self has lost its anchor for the definition of its identity and, consequently, its ability to sustain a narrative and answer questions about doing, acting, and being (Kinnvall 2004). It may arise from deep uncertainty (Mitzen 2006a) and/or from the failure to have its sense of Self affirmed by others (Zarakol 2010). Conversely, in a state of ontological security, the Self experiences a stable, certain, and consistent social existence, where it remains in control about its identity and capacity for action. While I do not rule out the possibility of a state of ontological asecurity, where the Self is simply not concerned with the stability and certainty of its identity, I do not explore this possibility and how it varies across different states of physical security in this article.

Having identified different states of physical and ontological security, I make the further assumption that since ontological and physical security are distinct, states of security do not vary uniformly across the ontological and physical layers of security. One can be at a state of physical insecurity while being at a state of ontological security, and vice versa. Consequently, Table 1 charts out the four possible states of security based on the conception of security as both ontological and physical.

The state of ontological insecurity/physical (in)security is one where the Self experiences concern about physical harm and the instability and uncertainty of its being. Ontological insecurity tempts actors to engage in practices that mark Others as not only different, but also as morally inferior and threatening (Campbell 1992). Ontological insecurity and physical (in)security reproduce one another. As actors seek ontological security through constructing Others as threats to their security-as-survival, they mobilise their physical defences in the pursuit of physical security through representing the sources of threat as different and morally inferior.

Similarly, in a state of ontological security/physical (in)security, actors experience stability and certainty of being in a relationship where the Other is constructed as threat to their security-as-survival. Consequently, they remain locked into conflict-producing routines to maintain their certainty of being (Mitzen 2006a). In protracted conflicts such as in Cyprus and Israel/Palestine, this state of security sustains a stable Self/Other relationship based on enemy roles. When in such a state of security, minority and majority groups, migrants and host societies perceive and represent each other’s identities as radically different and inherently incompatible, and reproduce these perceptions and representations through acts of securitisation in order to ensure their ontological security. The states of ontological insecurity/physical (in)security and ontological security/physical (in)security are both securitised states; however, whereas the former compels actors to construct new narratives of difference and threat and engage in the securitisation of new issues to regain their certainty and stability of being, the latter compels actors to reproduce the existing narratives and continue the securitisation of existing differences and conflicts to maintain it.

The state of ontological security/physical asecurity is certainly the most attractive state of security from a normative point of view. Security communities in international relations, and in particular, the European non-war community (Wæver 1998) and the Nordic community (Browning and Joenniemi 2012) constitute the best examples of such a state of security in international relations. A collective identity discourse makes it possible for states in security communities to maintain the us/them distinctions, which are necessary for the certainty and stability of being, while remaining in a state of physical asecurity vis-à-vis one another (Mitzen 2006b; Browning and Joenniemi 2012). In this state of security, conflicts are sustainably resolved; issues that have propelled conflict in the past are either settled or have shed their physical security-ness, and are negotiated in normal political channels. Yet, identity differences maintain their ontological security-ness as groups reproduce their distinct identities through various social and cultural practices.

### AT: Turf Wars DA---2AC

#### Squo causes turf wars---NSA and Cyber Command compete for priority, and NSA’s veto power over OCO’s both distracts from effective NSA law enforcement and rapid, effective cyber operations

Schoka ’19 [Andrew; April 3; active duty Army cyber operations officer assigned to U.S. Cyber Comman and Distinguished Military Graduate of Virginia Tech with a bachelor’s degree in systems engineering; War on the Rocks, “CYBER COMMAND, THE NSA, AND OPERATING IN CYBERSPACE: TIME TO END THE DUAL HAT,” https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/]

However, though Cyber Command and NSA share technical similarities in their operations, they operate under distinct legal authorities for different purposes. NSA, with authority from Title 50 of the U.S. Code, is responsible for conducting signals intelligence collection, which involves accessing computer networks for the purpose of secretly gathering information from them. Conversely, Cyber Command primarily derives its authority from Title 10 and is responsible for conducting military computer network operations, which involves accessing computer networks for the purpose of creating noticeable effects on them. These effects, which are intended to support a specific military objective, are typically one of the “5 Ds”: deny, degrade, disrupt, deceive, or destroy. This subtle, yet important, distinction between the two organizations’ authorities and missions is critical to understanding the sometimes contentious relationship between Cyber Command and NSA. Cyber Command, in its earliest days, was essentially an organizational arm of NSA established to provide legality for conducting operations that NSA possessed the technical capability to execute, but not the legal authority. While some of Cyber Command’s recent operational successes against adversaries have made headlines, NSA’s operations have not — and that’s exactly how it ought to be.

The dual hat arrangement was never intended to be permanent. The guidance that President Barack Obama issued after signing the 2017 National Defense and Authorization Act clearly stated the commander in chief’s desire to see the two organizations separated. That NDAA established a specific set of criteria to terminate the dual hat relationship. A number of these criteria are easily quantifiable and have already been met, such as Cyber Command’s mission forces achieving full operational capability. Others, however, are more difficult to objectively assess, such as ensuring that “robust command and control systems and processes have been established for planning, deconflicting, and executing military cyber operations.” These are systems and capabilities that continue to be developed out by Cyber Command with significant influence and assistance from NSA.

Cyber Command’s current approach to conducting computer network operations focuses heavily on the review and approval process. In addition to ensuring legal compliance with the myriad authorities and orders pertaining to cyberspace operations, review processes focus on risk management. Strategic-level operations conducted by Cyber Command undergo exhaustive review and approval processes meant to minimize risk to tradecraft, capabilities, and security. Operational security is of critical importance to cyberspace operations, where the efficacy of a weapon system hinges upon its ability to operate secretly. In 2016, a hacking group known as the Shadow Brokers published cyber tools and capabilities that allegedly belonged to NSA, causing profound damage to the agency’s ability to conduct operations.

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

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

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

The review process for a Cyber Command operation also requires an equities review by a multitude of government, intelligence, and military stakeholders. The idea is that all relevant parties have an opportunity to address potential concerns with a proposed offensive cyberspace operation. While one of the principal original concerns with the dual hat arrangement was the potential for unfair prioritization of Cyber Command support requests to the NSA, the equities review process has instead created the opposite problem. Because Cyber Command depends so heavily on NSA logistical and operational support, it has essentially lent the agency de facto veto authority on offensive cyberspace operations: Cyber Command risks losing NSA-facilitated training, NSA-provided office space, and access to NSA’s signals intelligence data by bickering with NSA over who get a shot at a given targets. The responsibility of balancing the prioritization of the distinct missions of two different organizations should not be delegated to a single individual. Doing so inevitably privileges one mission at the other’s expense, and ultimately impedes overall progress for both.

The self-defeating nature of the dual hat also runs contrary to America’s increasingly risk-tolerant approach to countering adversary competition in cyberspace. Analysts have repeatedly advocated that the United States take a more proactive approach to cyberspace operations. The summary of the 2018 Department of Defense Cyber Strategy shifts toward a focus on “defending forward,” establishing a more aggressive stance in cyber operations through a policy of embracing constant forward contact. The strategy explicitly replaces the previous focus on risk mitigation and escalation control with a risk-acceptant commitment to “assertively defend our interests.” The strategy indicates that the Department of Defense will “accept and manage operational and programmatic risk in a deliberate manner that moves from a ‘zero defect’ culture to one that fosters agility and innovation.” The document acknowledges the risk inherent to the conduct of cyberspace operations, but ultimately accepts the possibility of operational failure as a necessary consequence of deterring adversary competition in cyberspace. Shifting to a more proactive stance with military cyberspace operations is not a provocative overreaction to malicious activity, nor does it reasonably stand to elicit an escalatory response from adversaries. Rather, shifting Cyber Command away from a risk-averse mindset is a recognition of an increasingly contested information environment in which the command is at serious risk of being outpaced and outplayed in its current state.

The missions of NSA and Cyber Command will continue to compete for priority and advocacy under the dual hat. The shaping effect of this relationship has diminished Cyber Command’s appetite for risk, and slowed the approval process for military cyberspace operations to a sluggish crawl. What takes adversaries mere minutes to do takes Cyber Command weeks, or even months. In the cyberspace domain, where windows of opportunity for an operation can be vanishingly small, Cyber Command’s review and approval processes need a paradigm shift. NSA has been instrumental to the development of Cyber Command, and the existence of the command, as well as its operational successes, are a credit to NSA’s diligent work to establish and support a military presence in cyberspace. However, as has been echoed by previous presidential administrations, the time has come to allow Cyber Command to stand on its own, and free NSA from the responsibility of nurturing a full-fledged combatant command in addition to pursuing its own mission.

#### 2018 DoD Cyber Strategy thumps---and ensures effective relationships that solve turf wars

Herr ’18 [Trey and Jacquelyn Schneider; Oct 10; visiting fellow at the Hoover Institution; assistant professor and affiliate faculty at the Center for Cyber Conflict Studies at the U.S. Naval War College; “Sharing is Caring: The United States’ New Cyber Commitment for NATO,” https://www.cfr.org/blog/sharing-caring-united-states-new-cyber-commitment-nato]

Given the recent blockbuster headlines about alleged Chinese snooping on server hardware sold to major technology companies and the latest joint-denunciation of Russian cyber operations, you could be forgiven for having missed an important NATO-related development. The Associated Press reports that the U.S. Defense Department will announce a new commitment to use offensive and defensive cybersecurity capabilities on behalf of NATO allies.

The new commitment is notable given how cybersecurity has long been treated as an exceptional domain of operations, and cyber capabilities reserved as strategic national assets to be shared with only the closest of allies. With this announcement, the Pentagon is suggesting that cyber capabilities might be used alongside conventional weapons with allies and indeed, equal weight appears to be given to offensive and defensive operations. Perhaps most significantly, the announcement moves NATO partners closer to what has been a tight coterie of U.S.-favored signals intelligence partners such as the United Kingdom, New Zealand, Australia, and Canada.

The DoD announcement is a sign of the continued, if nascent, normalization of cybersecurity under the current administration and in Europe. Even where offensive cyber operations may not rise to the level of war, they provide decision-makers with options to influence the geopolitical environment. This aligns with recent trends in the U.S. military to integrate cyber capabilities into maneuver units and large exercises, and reflects the shift towards more risk acceptant and offensive measures to counter cyberattacks found in the 2018 DoD Cyber Strategy.

Moving cyber capabilities into the same strategic frame as conventional weapons, especially with NATO, reflects a shift in institutional cyber arrangements within the United States and the growing power of the military relative to the intelligence community. For the United States, cyber capabilities have always had a complicated relationship with the intelligence community, in particular the National Security Agency (NSA). When Cyber Command stood up in 2010 as a sub-unified combatant command within the Department of Defense, it moved into the NSA’s headquarters, staffed its management ranks with longtime NSA employees, borrowed networks and technical capabilities, and to this day shares a dual-hatted commander. In the immediate years after the command was created, it was logical that the structure of partnerships with allies looked more like the special signals intelligence relationships formed around the NSA rather than traditional alliance networks in NATO and Asia. The recent announcement aligns cyber operations more closely with Department of Defense missions, which are more likely to posture capabilities for deterrent effects, than intelligence missions, which view capabilities as assets to be carefully husbanded.

Treating cybersecurity capabilities more like conventional arms and less like national assets also helps drive the integration of cyber operations into the planning and execution of a broader array of conventional military missions. Early cyber operations were largely conventional espionage and surveillance activities supercharged by the spread of computing and the internet. In the United States, this led to the creation of large and complex software tools, carefully guarded by the intelligence community as national assets (sometimes unsuccessfully). The DoD’s announcement indicates a move towards treating at least some of these capabilities, along with their supporting infrastructure, more like conventional armaments and making them available for broader use; a model closer to Central or Special Operations Command and less like the National Security Agency.

The Pentagon’s new commitment also reflects changes in how Europe talks about cybersecurity and characterizes the Russian threat. The last two years have seen a trend toward more open discussion of offensive cyber operations and the possibility of the alliance adopting more assertive postures to counter cyber operations against its members. After years of devastating ransomware attacks and cyber-enabled information attacks, NATO members are more willing to explore cyber triggers to Article 5. They have also been more willing to articulate the cyber threat against the alliance. In addition to last week’s denunciation by Dutch, UK, and U.S. authorities, Russian state actors are widely suggested to be responsible for an increasingly brazen series of operations, including targeting German government ministries, French and British TV stations, and more.

Sharing offensive cyber capabilities raises the question of whether cyber operations can extend effective deterrence to NATO partners. There seems to be little focus on using these operations to deter conventional or nuclear attacks on NATO countries, but this may evolve. The United States seems to want NATO to use cyber operations to deter other cyber operations, particularly those falling under the threshold of armed conflict. Cyber operations have all sorts of problems for deterrence: signaling is difficult, they can be perceived as a cheap threat, and their effects are largely uncertain. By contrast, moving new military forces in Eastern Europe or conducting ground exercises are credible signals of extended deterrence, but are costly and time consuming. Cyber capabilities aren’t free, nor are they necessarily cheap, but the promise to use them can add new credibility to a deterrent threat without the same investment and delay as conventional alternatives. Sharing cyber capabilities may be a cheaper way to signal alliance commitment than other options and might signal a further maturation, and acceptance, of cybersecurity into geopolitics.

#### CYBERCOM is already trampling on NSA authority

DeGeurin ’18 [Mack; September 11; Education Fellow at INSIDER, Writer for New York Magazine, BA from New York University; New York Magazine, “U.S. Silently Enters New Age of Cyberwarfare,” https://nymag.com/intelligencer/2018/09/us-rescinds-ppd-20-cyber-command-enters-new-age-of-cyberwar.html

This past month, buried beneath an ant mound of political scandal and news cacophony, President Trump set in motion a plan to gut Presidential Policy Directive 20, an Obama-era policy limiting the use of destructive offensive cyberweapons like Stuxnet. What exactly will replace PPD-20 remains clouded in uncertainty, but one thing seems clear: The military’s gloves are off. Without PPD-20, the U.S. military can now use hacking weapons with far less oversight from the State Department, Commerce Department, and intelligence agencies. A paper released earlier this year by U.S. Cyber Command, the hacking arm of the U.S. military, outlines a proposed policy of increased military intervention, and paints a landscape of nations under constant cyberassault. It’s not a stretch to say the removal of PPD-20 may fundamentally restructure the way America conducts war in cyberspace. Whether or not that is a good thing depends on whom you ask.

“What this is all about is streamlining the process and giving the military permission to use cyberweapons under certain circumstances without having to go through a cumbersome process of coordination with all the different agencies,” former Navy Captain Gail Harris says. In conversation, Harris, who was involved in cyberdefense for the Department of Defense, echoed the arguments laid forth by Cyber Command in its paper. In that document, Cyber Command describes cyberspace as an “active and contested operational space in which superiority is always at risk.” Whether you like it or not, Cyber Command argues, we are currently engaged in a persistent war of code with adversaries continuously attacking and entrenching themselves deep in American networks. The brisk nine-page document details a world under constant subversion. These “persistent threats,” Cyber Command argues, require swift and aggressive military responses in kind. Be they Russian and Iranian state hackers, terrorists, or hacktivists, the document blames bureaucratic red tape and political hand-holding for much of America’s recent cyber woes.

“We cede our freedom of action with lengthy approval processes that delay US responses or set a very high threshold for responding to malicious cyber activity,” the vision statement reads.

If Cyber Command has its way, it will also be able to transition its fundamental role from defense to potentially more offensive campaigns. Cyber Command says it wants to “expand the military options available to national leaders,” and “defend forward as close as possible to the origin of adversary activity.” The move follows a recent trend by officials geared toward strengthening Cyber Command and granting it far more offensive capability.

While anyone losing hair over election hacking, foreign manipulation, and electrical grid vulnerabilities may take some solace in sharpening the military’s cyber teeth, the prospect of a perpetual online war could come with serious, sometimes unforeseen, consequences.

The Plunge Into Perpetual War

“We’ve slipped into permanent warfare,” Columbia research scholar and cybersecurity expert Jason Healey told Select All. “There is no winning this war, it is happening online.” Healey, who wrote the first history of cyberconflict and previously worked on network defense for the Pentagon, said he worried traditional military solutions may simply not work to address cyberconflict. “The military is asking politicians to give them this authority and then get out of the way forever. Once we have done this, we are not going to be able to go back to the way it was before.”

#### NSA lawyering will meet the letter of the plan but they’ll still find loopholes

Schlanger ’15 [Margo, Professor of Law at the University of Michigan Law School, and the founder and director of the Civil Rights Litigation Clearinghouse., Intelligence Legalism and the National Security Agency’s Civil Liberties Gap]

One key question about all this legal advice is whether it is ever constraining—whether the lawyers ever tell their clients no. NSA’s lawyers do sometimes advise their clients/colleagues not to do specific things. One released training document, for example, advises analysts not to use certain search techniques, cautioning: “Do Not: Wildcard domains. Wildcard user names. Wildcard across domains.”149 One would expect agency counsel to say no with relative ease where the rules are clear and when those rules govern how and not whether a particular activity can occur. It is crucial to remember, however, that agency lawyer advice-giving is not adjudication and agency lawyers are not judges. The judicial ideal of even-handedness is not, even theoretically, applicable. Rather, the goal of legal advice for lawyers within the Intelligence Community, as with any organization’s lawyers, is to assist the client. To quote the same senior IC lawyer, “you’re hoping to get done what your client wants to get done, so there’s a tendency to try to find the most room to get that done.”150 Or, in the less careful words of a former NSA chief analyst, “Look, NSA has platoons of lawyers and their entire job is figuring out how to stay within the law and maximize collection by exploiting every loophole.” 151 Unsurprisingly, then, some training slides that say no also include work-arounds—methods for achieving various searching or analytic goals that are not covered by the stricter FISA rules.152

#### No OCrime impact

Stewart Patrick 17, James H. Binger Senior Fellow in Global Governance and Director of the International Institutions and Global Governance Program at the Council on Foreign Relations, Fall, “Civil Wars & Transnational Threats: Mapping the Terrain, Assessing the Links,” Daedalus, 146.4, 45-58

Here again, though, nuance is warranted. Much of the organized crime in wartorn states is localized, and the connections between state failure and transnational crime vary depending on the type of criminal activity.37 Most countries experiencing civil war, for instance, are not heavily implicated in illegal cross-border ventures like human trafficking, money laundering, drug trafficking, or environmental crime (to say nothing of intellectual property theft, cybercrime, and manufacturing of counterfeit merchandise). As with terrorism, it is not state failure that criminals find advantageous, but a more modest level of state weakness: collapsed and wartorn states are generally less attractive than superficially functional states that maintain a baseline level of political order and easy access to the infrastructure of global commerce, but also where corruption is rife, the rule of law absent or imperfectly applied, and gaps in public services and shortages in licit economic opportunities provide openings for illicit actors. To sell illegal commodities and launder the proceeds, criminals need secure access to financial services and modern telecom- munications, banking, and transportation. Such requirements are often (though not always) lacking in war-torn states. In their thirst for profits, criminals may be drawn to a convenient geographical base and proximity to the global marketplace, even if it presents other risks. Such factors help explain why Mexico and South Africa –neither of which is a war-torn or even fragile state–have emerged as hotbeds of criminal activity and violence.38

#### DOS solves organized crime.

Keller ’16 (Andrew; Deputy Assistant Secretary in the Bureau of Economic and Business Affairs at the U.S. Department of State, former Deputy Legal Adviser at the State Department; 6/9/16; “Statement of Deputy Assistant Secretary Andrew Keller U.S. Department of State Bureau for Economic and Business Affairs before the United States House of Representatives Committee on Foreign Affairs Subcommittee on Terrorism, Nonproliferation, and Trade”; <http://docs.house.gov/meetings/FA/FA18/20160609/105045/HHRG-114-FA18-Wstate-KellerA-20160609.pdf>)

The Department of State works closely with the Department of Treasury on diplomatic engagement efforts to counter the financing of terrorism with countries and international organizations. We also provide assistance to build the capacity of partner countries around the world to help strengthen their legal frameworks to prevent money laundering and terrorist financing, prosecute criminals and terrorist financiers, strengthen financial regulatory institutions and improve information sharing, and track suspicious transactions that could support criminal or terrorist activity. These activities require constant interagency collaboration, as well as adaptation and coordination with our foreign partners. Terrorist financing is a complex and dynamic threat, and one that requires the U.S. Government to utilize the full range of its tools. I sit in the Bureau of Economic and Business Affairs (EB) at the Department of State. We help coordinate Department of State policy on terrorist finance among a number of regional and functional bureaus and liaise with our interagency partners, including the Department of Treasury and Department of Defense, to shape the counter ISIL finance campaign at the strategic level. My team in EB also coordinates counter terrorist finance sanctions for the Department of State and works closely with other bureaus in the Department of State and with the Department of Treasury to ensure our sanctions target individuals and groups effectively and in a way that promotes broader U.S. foreign policy interests. The fight against the Islamic State in Iraq and the Levant (ISIL) is one of our highest priorities, and it is my principal counter-terrorist finance focus. Our efforts to diminish ISIL’s finances illustrate the Department of State’s many tools to disrupt terrorist groups’ financial networks, and our work with the interagency demonstrates how effectively we can leverage the full spectrum of U.S. authorities and capabilities in pursuit of this important goal. We have worked very closely with our interagency colleagues, including those represented here today, since 2014 to disrupt ISIL’s finances, and we can point to the real impact our efforts and those of our coalition partners have had on ISIL’s finances. ISIL’s revenues in 2014 and 2015 made it by far the richest terrorist group in the world, and the sources of its revenues make it an unusual counter-terrorist financing challenge. In 2015 ISIL earned at least $1 billion, mostly through the production and sale of energy resources and through extortion of the population in ISIL-controlled areas of Iraq and Syria. ISIL likely made around $500 million in 2015 from oil and gas sales and about $350 million from extortion. In addition to those two large revenue streams, ISIL made at least several million from foreign donations in 2014 and in 2015, between $20 and $45 million from kidnapping for ransom in 2014 but less in 2015, and less than $10 million from trafficking in antiquities. In 2014 and early 2015, when ISIL seized cities throughout northern Iraq, it captured between $500 million and $1 billion dollars in Iraqi currency from local bank vaults – a one-time windfall and not a recurring source of revenue. Other terrorist groups, including Al-Qaida, have traditionally raised funds primarily by soliciting donations. ISIL, on the other hand, makes the majority of its money from the territory it controls. This relative financial self-reliance has hindered our ability to use our traditional counter-terrorist finance tools and obliged us to develop creative approaches to address each aspect of the problem. U.S. and coalition partner countries have adapted and pursued new strategies to squeeze ISIL’s ability to fund its operations. Efforts to Disrupt ISIL’s Finances As the interagency co-lead of the counter-ISIL finance effort alongside the Department of Treasury’s Office of Terrorist Financing and Financial Crimes, we coordinate the Department of State’s counter-ISIL finance activities and leverage our diplomatic authorities and resources to disrupt ISIL’s finances. We work closely with our interagency partners in the Departments of Treasury, Defense, Justice, Homeland Security, and the Intelligence Community to coordinate this unique and challenging mission. As a result of the efforts detailed below, we have seen a significant impact on ISIL’s operations in Iraq and Syria. ISIL has cut salary payments to its fighters in Raqqa and Mosul by fifty percent, leading many ISIL fighters to defect and leave the battlefield. ISIL has struggled to fulfill its various governance obligations such as basic services to Iraqi and Syrian citizens in ISIL-controlled territory due to stretched finances. ISIL has also increasingly resorted to the theft of property and arbitrary “tax” increases to make up the funding gap. Finally, we have seen increasingly frequent incidents of corruption within ISIL’s ranks as funds have diminished. While encouraged by these indications of financial stress, there is still much work to do both in Iraq and Syria and around the world against ISIL’s affiliates and supporters.

### AT: Turkey DA---2AC

#### Russian hybrid tactics threatens the unity and credibility of the alliance

Ivana Stradner and Max Frost 2o, Jeane Kirkpatrick fellow at the American Enterprise Institute, senior research associate at the American Enterprise Institute, NATO Has a New Weak Link for Russia to Exploit, https://foreignpolicy.com/2020/04/22/north-macedonia-nato-russia/

In 1938, British Prime Minister Neville Chamberlain made it possible for Adolf Hitler to march into Czechoslovakia despite the overwhelming military superiority of Prague’s Western allies because Chamberlain had decided the issue was “a quarrel in a faraway country, between people of whom we know nothing.” Today, it is similarly difficult to believe that NATO would go to war over its far-flung commitments in Eastern Europe. Nevertheless, on March 27, the Western alliance admitted North Macedonia as its newest—and weakest—member. In so doing, it has given Russian President Vladimir Putin a terrific opportunity to expand his influence, further erode NATO’s unity, and test the bloc’s commitment to defend a member of the alliance.

North Macedonia is the definition of a weak link and easy pickings for an adversary. A landlocked country of 2 million inhabitants, it has weak political institutions and only a short history of independence. As of 2018, it spent only 1 percent of its GDP on defense—short of the 2 percent NATO guideline—and had just 8,000 active-duty soldiers. There is simmering communal tension between a Slavic Orthodox majority and a sizable ethnic Albanian, mainly Muslim minority, making it vulnerable to interference. Within NATO, only neighboring Albania has a lower per capita GDP and a higher level of corruption. The Economist Intelligence Unit’s Democracy Index ranks North Macedonia as having Europe’s least developed political culture.Russia has held massive war games that were only thinly disguised simulations of attacks on NATO members such as Poland and the Baltic States.

Moscow has viewed NATO’s expansion in Eastern Europe with suspicion since the 1990s. Yet it wasn’t until the 2000s, after Russia’s military and economy rebounded from the chaos of the post-Soviet era, that Putin declared NATO’s eastward expansion a “direct threat” and openly confronted the alliance. Russia’s invasion of Georgia in 2008—not coincidentally, the year that NATO declared an interest in Georgia’s eventual accession to the alliance—stopped the bloc’s expansion into former Soviet-controlled areas in its tracks. Putin’s 2014 invasion of Ukraine and subsequent annexation of Crimea, while not a direct assault on a NATO member, further demonstrated Western impotence in the face of Russian aggression. Further north, Russia has held massive war games that military experts say were thinly disguised simulations of attacks on NATO members such as Poland and the Baltic States.

Now that North Macedonia has joined NATO, Putin appears to be relishing his first chance to prove that the alliance is little more than a paper tiger. In 2018, Russia’s ambassador to North Macedonia declared the country a “legitimate target” if tensions between NATO and Russia were to increase. But there was no “if” about it: Even before North Macedonia became a member, Russia had already been working assiduously to ratchet up tensions in the region. Moscow has shipped S-400 anti-aircraft missiles to neighboring Serbia for joint Russian-Serbian military drills, facilitated an attempted coup in Montenegro, and tried to destabilize Bosnia and Herzegovina by stoking sectarian tensions. And in North Macedonia itself, Russia has funded troll factories that, among other things, were used to target the 2016 U.S. presidential campaign with disinformation. Moscow also tried to influence North Macedonia’s September 2018 referendum on NATO membership, is using its embassy and consulates there as bases for intelligence-gathering operations, and has spread propaganda detailing alleged Western plots to break up the country.

That Russia would threaten NATO’s members in Eastern Europe is nothing new, of course. Russia has long attempted to undermine the Baltic countries—Lithuania, Latvia, and Estonia—which joined NATO and the European Union after gaining their independence from the Soviet Union. But today, the Baltic States are well integrated into alliance structures and the European economy and are home to thousands of NATO troops. Whereas the Baltics have become part of NATO’s well-armored front, the Balkans are its soft underbelly.

Whereas the Baltics have become part of NATO’s well-armored front, the Balkans are its soft underbelly.

 NATO’s posture in North Macedonia and its neighborhood is very limited. The Balkan countries are also poorer, more ethnically divided, and less economically integrated with Europe. Their potential instability and the much lower likelihood of a robust response by the West make North Macedonia and its neighbors ripe and easy targets for Russian meddling.

Taking a page from history’s playbook, Putin rightly assumes that most decision-makers in NATO capitals would consider North Macedonia a “faraway country” of “people of whom we know nothing.” U.S. President Donald Trump, whose relationship with Putin continues to attract attention, confirmed a similar suspicion with regard to neighboring Montenegro when he appeared to question NATO’s commitment to defend the Balkan nation during an interview aired on Fox News. And while some may have taken offense at Trump’s statement, the truth is he speaks for many.

According to a February poll by the Pew Research Center, less than half the populations of France, Spain, Turkey, and Greece hold a favorable view of NATO. Pandering to the alliance’s critics, French President Emmanuel Macron last year declared that NATO had “brain death.” The citizens of only three European countries—Britain, the Netherlands, and Lithuania—say their country should respond with military force if Russia were to attack a NATO member in Eastern Europe.

No surprise then that NATO’s posture toward its newest member remains unclear. Though NATO broadened the definition of its joint defense commitment—Article 5 of the alliance’s charter—to include cyberattacks in 2014, it has failed to clarify just what that means. When asked what level of cyberattack on one of its members would trigger a response, NATO Secretary-General Jens Stoltenberg said only, “We will see.” The 2018 Brussels Declaration reaffirmed NATO’s intent to defend member states from nonconventional attacks—but only meekly asserted that in “cases of hybrid warfare, the Council could decide to invoke Article 5.” These Western weasel words will have been duly noted in the Kremlin.

These Western weasel words will have been duly noted in the Kremlin.

The type of meddling Russia has specialized in includes election interference, inflaming ethnic tensions, and provoking violent conflict. These three real possibilities could trigger a NATO response under Article 5. The most pressing issue is securing North Macedonia’s upcoming elections, now postponed until further notice due to the COVID-19 pandemic. Polls last showed VMRO-DPMNE, a pro-Russian nationalist party, in a dead heat with the pro-Western Social Democrats. Russian interference in the election process or outcome not only threatens Macedonian sovereignty but, if successful, could result in a government that tilts North Macedonia toward Moscow.

Russia may also seek to pressure and destabilize North Macedonia in other ways, including through Moscow’s regional client, Serbia. Russian propaganda aimed at North Macedonia includes conspiracy theories about the country’s sizable Albanian minority supposedly colluding with NATO and Albania to fold North Macedonia into a “greater Albania” amid great bloodshed. As any student of Balkan history knows, such rhetoric has led to ethnic violence in the region before. Alternatively, Russia may stoke simmering conflicts in Serbia, whose unstable Presevo region directly borders North Macedonia, or the unresolved Kosovo dispute. Either conflict could easily spill into North Macedonia.

NATO’s next steps to secure its new member could include adapting the successful tactics used when Montenegro joined the alliance in 2017. A NATO-sponsored cyberteam provided the Montenegrin government with technical support to learn to identify and counter hybrid warfare. NATO raised awareness of the benefits of NATO membership by working with officials, civil society, local governments, and media organizations. It also worked to improve governance in Montenegro’s defense sector. Similarly, the European Union, which has just opened accession talks with North Macedonia, could move quickly to signal to the world that the Balkan nations are an integral part of Europe.

More broadly, however, NATO needs a mechanism to respond to Russian aggression in the event that the alliance’s members can’t unanimously agree to do so. Article 5 requires unanimity before invoking collective defense, but NATO’s members differ in their attitudes to Russia.

Article 5 requires unanimity before invoking collective defense, but NATO’s members differ in their attitudes to Russia.

 One solution would be to form, as a backstop in case it is needed, a coalition of the willing comprising NATO members with credible defense capabilities that are willing to confront Russia and prepare a collective response to any attack.

Despite NATO’s overall military superiority, it has a weak hand in the Balkans, and Russia continues to outmaneuver it there. NATO must quickly signal that it remains steadfast and, having decided to admit it, that North Macedonia is an integral member of the alliance. If NATO fails in its support of new members like North Macedonia, the chances have just risen that it will be met with Russian aggression—hybrid or conventional—that may just mean the end of NATO as a credible alliance.

#### Hybrid war uniquely threatens Turkey – they require better NATO planning

Oktay Bingöl 17, Professor of International relations at Istanbul Arel University, December 2017, Hybrid War and Its Strategic Implications to Turkey, Gazi Akademik Bakış, 11(21):123-125

In addition to the dependencies, the foreign relations pose serious risks to Turkey’s political and military capability to deter hybrid adversaries and fight them when necessary. First area is the fact that Turkey has been encircled by troubled neighbors. Turkey is at hybrid war with the regime, ISIL, PYD and others in Syria, Iran, Iraq, RF and Armenia. The foreign relations with Greece, Southern Cyprus, Egypt, Israel, the EU an even with the US are fragile. Turkey’s isolated position particularly in the Middle East does not provide her with acceptable opportunities to establish alliances and balance potential adversaries. This is a significant weakness in emerging hybrid strategic environment. When Turkey approaches Sunni Monarchies of the Gulf to overcome such a weakness, fragile domestic fault lines activate. Turkey has been in a hybrid conflict context for long years, intensifying in the last decade, especially after a Russian aircraft was shot down by Turkish Armed Forces (TAF) at Syrian border on 24 November 2015.78 On this event, Russia had initiated temporally coordinated attacks against Turkey in physical, moral, economic and cognitive domains to exploit Turkey’s vulnerabilities.

The battle in the cognitive and moral domains was especially intense. Russian Federation soughted to gain regional and international legitimacy in its struggle against Turkey and targeted Turkish public will. Russian hybrid war became effective and created strategic implications as a result of interaction of several internal, regional and international dynamics influencing Turkey. Russian hybrid strategies against Turkey perfectly fit some of the strategies and tactics discussed above. The RF has implemented several economic sanctions on Turkey including ban on tourism, agricultural product, suitcase trading, international contracts, and direct investments.79 The RF endangered Turkish foreign policy in Syria by targeting Turkey supported rebels and Syrian Turks (Turkomans), and by supporting Esad regime and PYD/ YPG which is accepted as a terrorist organization by Turkey. The deployments of Russian S-300/400 missile systems to Syria had established a no-fly zone for Turkey.80 Thus Russia closed Syrian airspace to Turkey which could not fly its aircrafts to target PYD/YPG and ISIL even if it was attacked by them. After the shot down of Russian aircraft, PKK terrorist activities inside Turkey dramatically increased. PKK used Russian made manportable air-defense system MANPADS which is a big threat to Turkish aircrafts and particularly helicopters although the weapon used by PKK to hit Turkish helicopter on 14 May 201681 does not prove Russian direct involvement.82 While Russian direct military support to PKK is questionable, diplomatic and moral support to PKK, PYD/YPG and affiliated political organizations is clear.83 Moreover, Russian hybrid concept had focused on indicating Turkey’s supports to ISIL.84 Overall, Russia foughted in cognitive and moral domains and aimed to shape perceptions of Turkish public opinion, regional and international community. In Lieu of Conclusions: Recommendations for Turkish Decision Makers Defeating hybrid threats and winning a hybrid war requires, first of all, to understand what is hybrid war and make preparation in terms of civil military relations, suitable theory and adjusted policies, strategies, concepts and doctrines, structures, education of civilian and military leaders, equipment, training and readiness of forces. The most important measure is clearly building a resilience society. This means that Turkish society should be freed from further polarization and marginalization of various sub groups. Identities should not be exploited by politicians to consolidate their electoral bases. However, this requires a radical change in mentality, not only of the ruling party and ruling elites but also opposition parties and the media, to develop a more positive approach. Turkish strategic paradigm must reorient to give more emphasis to the cognitive and moral domains, just as potential enemies’ paradigms have changed. It may be time to learn and adapt to the enemy’s way of war with an increase in the effective use of the cognitive and moral domains. The use of the media in hybrid war is a force multiplier to complement hybrid war asymmetric advantages. Turkey’s response to hybrid war will require a whole of government approach that is very difficult for Turkey to coordinate, plan, and de-conflict. This actually requires inter- agency planning and implementation mechanism which Turkey is clearly lacking. The western states and organizations have long endeavored to formulate suitable policies to deter hybrid threats. The EU and NATO efforts led to the emergence of a comprehensive approach blending all actors and available instruments: military forces, diplomacy, humanitarian aid, political processes, economic development, and technology. While NATO has developed Comprehensive Approach in 200885 the EU’s own comprehensive approach was adopted in December 2013.86 In these approaches, government-led actions have increasingly been complemented by whole-of-society strategies aimed at managing risks and building resilient societies by believing that the focus on resilience helps to mitigate risks that might lead to hybrid conflicts in the future and improves associated resource-management practices. The western governments have recently taken concrete steps to increase and modernize their civilian and military capabilities. The EU is aware of the fact that some of the present legal concepts and frameworks are anachronistic and do not always address hybrid threats adequately. It initiated new legal measures to overcome the weaknesses. Lastly many countries have adjusted to hybrid threats by expanding the missions of existing institutions or creating new organizations.87 Turkey obviously needs such a comprehensive approach which requires a cooperative and constructive internal and external atmosphere, and a transformed security sector. Yet it is unfortunate that Turkey, being trapped to polarization and conflict, does have many difficulties to overcome.

## AT: Dedev

### AT: Dedev---Top-Level---2AC

#### Growth key to space colonization---extinction.

Kovic '19 [Marko; March 2019; co-founder president of the Zurich Institute of Public Affairs Research; "The future of energy," https://osf.io/preprints/socarxiv/aswz9/download]

Ideally, the mitigation of climate risks will coincide with and contribute to the development of improved or even entirely novel sources of energy that will increase the long-term chances of humankind’s survival by means of space colonization. This is not an unrealistic expectation, given that the mitigation of climate risks consists, to a large degree, of replacing fossil fuels with other, less harmful sources of energy. However, some climate change mitigation strategies might actually harm the long-term prospects of humankind.

First, it is possible that dominant climate change mitigation strategies will actively exclude any form of nuclear energy from the repertoire of climate-friendly energy sources. Existing and experimental (molten salt) fission reactors could play a significant role in replacing carbon-heavy energy sources, but pro-environmental attitudes often overlap with anti-nuclear sentiments [65]. As a result, and in combination with other problems such as large-scale market failures of existing fission reactors (one of the reasons being that generating electricity from fossil fuels is cheaper) [66], nuclear fission does not currently have significant standing as a “cleantech” contribution to climate change mitigation. From a long-term perspective, an unfavorable view of nuclear energy in the context of climate change might mean that technological progress in the areas of nuclear fission and fusion might come to a halt (for example, due to explicit bans or implicit disincentives). If such a scenario came to be, our attempts at colonizing space would almost certainly fail: There are currently no alternatives to fission and fusion, and it is highly improbable that Solar power alone could suffice for sustaining extraterrestrial habitats.

Second, there is some probability that climate change mitigation strategies will change the social order towards a degrowth philosophy. Degrowth is a vague socio-economic concept and social movement that, in general, calls for a contraction of the global and national economies by means of lower production and consumption rates, and, to some degree, to more profound changes to the “capitalist” system of economic production [67]. Degrowth or degrowth-like approaches are being actively considered as climate risk mitigation strategies [68, 69], and degrowth would almost certainly be a highly effective measure for mitigating climate change. After all, if we were to drastically reduce or even completely eliminate the (industrial) sources of greenhouse gases, the amount of greenhouse gases that are being emitted would accordingly drastically sink. From the long-term perspective of humankind’s survival, degrowth is problematic in at least two ways. First, there is a risk that the general contraction of economic activity would also slow or eliminate progress in the domain of energy, which would, in turn, reduce the probability of successful space colonization due to an absence of suitable energy sources. Second, and more fundamental: If degrowth were to become a dominant societal paradigm, it is uncertain whether the long-term survival of humankind by means of space colonization would be regarded a desirable goal. In a literal sense, establishing extraterrestrial colonies would mean growth; the size of the total human population would grow, and the area of space-time that humans occupy would grow.

In a more philosophical sense, degrowth might even be antithetical to space colonization. Even though both degrowth and space colonization have a similar moral goal – increasing wellbeing – , the ends to that goal are very different. Within degrowth philosophy, the goal is, metaphorically speaking, not to “live beyond our means”: We should strive for “ecological balance”, and such a state should increase the average wellbeing. But the frame of reference is the status quo; Earth and humankind as we know it today. Space colonization, on the other hand, operates with a much larger frame of reference: All the future generations of humans (and other sentient beings) who could enjoy wellbeing if we succeed in colonizing space – and who will categorically be denied that wellbeing if we fail to colonize space [70]. The goal of space colonization as a moral project is not to live beyond our means, but to actively redefine and expand what our means are through scientific and technological progress.

#### Growth outruns recurrent blackball risks and shifts public preference to optimal existential risk mitigation---unlocks infinite future value.

Aschenbrenner ’20 [Leopold; September 6; Research Fellow in Economics at the Forethought Foundation and Global Priorities Institute at the University of Oxford, B.A. from Columbia University; Global Priorities Institute, “Existential risk and growth,” no. 6]

Secondly, note that this existential risk Kuznets curve appears in the transition dynamics of the optimal allocation. Considering that existential risk mitigation is a global public good, it is unlikely resources are allocated to safety optimally in the real world. As such, this should not be taken to be a prediction of what a particular country with a particular set of institutions will do with regard to existential risk.

Nevertheless, there are a number of reasons why we might still be interested in the transition dynamics under the (impatient) optimal allocation. For one, since there are very long timescales involved here, it is very hard to know (and thus model) what government and societal institutions will evolve to deal with existential risk. However, the ideal these institutions will likely aim at is the optimal allocation. The optimal allocation might thus be a rough proxy for the real-world allocation.

Moreover, the (impatient) optimal allocation represents what I would call the “democratic possibilities frontier” or the “impatient public possibilities frontier.” Those who are principally concerned about the long-run future of humanity and advocate for a zero rate of pure time preference might want us to spend as much as possible on safety in order to avoid existential catastrophe and enable human flourishing millions of years into the future. Indeed, even in the Hamiltonian of the optimal allocation, the relative value of life ˜vt is a discounted term; the lower your discount rate ρ, the more you would want to spend on safety. However, the broader public is not so patient. As the empirical evidence cited earlier shows, people tend to have a (relatively large) positive rate of pure time preference; the public is impatient. Even perfectly designed institutions that take into account existential risk externalities will ultimately be constrained by the degree to which society actually cares about the future—they will be constrained by an impatient public. The existential risk Kuznets curve illustrates the implications of this impatience. On the one hand, this impatience results in a period of initially rising levels of risk. For example, this might mean that the arguably rising level of existential risk of the past century is not necessarily a market failure, but may well be part of the optimal path given positive pure time preference. On the other hand, rising standards of living lead even the most impatient public to start caring more about safety and averting an existential catastrophe. This leads workers and scientists to be shifted to the safety sector, eventually causing the hazard rate δ to exponentially decline. Even if people are impatient, if you make them well off enough, they will start caring about existential risk.

Seeing the arguably rising levels of existential risk in the past century, some might call for an end to economic growth. Yet this existential risk Kuznets curve indicates that stopping economic growth would be deleterious: it would simply freeze the hazard rate at a high level, leading to a fatal catastrophe sooner or later. Economic growth enables even an impatient public with a high rate of pure time preference to start caring about life, thus ultimately reducing risk and even leading to positive M ∞.

Some prominent thinkers have previously posited that humanity is passing through a unique period with an elevated risk of technological catastrophe. Sagan (1994) calls this the “time of perils.” Parfit (2011, p. 616), concurs:

We live during the hinge of history. Given the scientific and technological discoveries of the last two centuries, the world has never changed as fast. We shall soon have even greater powers to transform, not only our surroundings, but ourselves and our successors. If we act wisely in the next few centuries, humanity will survive its most dangerous and decisive period. Our descendants could, if necessary, go elsewhere, spreading through this galaxy.

This existential risk Kuznets curve provides theoretical evidence that grounds the intuition that we are living in a “time of perils.” We may be economically advanced enough to have created the means for our permanent destruction, but not economically advanced enough to care enough about decreasing this existential risk.

This “time of perils” has profound implications. For instance, those alive today who care about preserving the long-term future of humanity may have extraordinary altruistic leverage. By working to reduce existential risk now (increasing the resources dedicated to safety), they can reduce the area under the “hump” of the hazard rate δ. This in turn increases M∞, unlocking tremendous value. Moreover, since so few resources are dedicated to safety at the moment, there are likely very high marginal value opportunities available to work on safety. This is a unique situation. Suppose existential risk did not decline to zero exponentially: then M∞ = 0 regardless—the existential risk curve would never bend—so reducing risk now would not change the probability of a long and flourishing future of humanity. And if existential risk did not initially increase, it would never be such a substantial challenge and there wouldn’t be such high marginal value opportunities to work on reducing it.

#### Dedev fails and causes transition wars.

Smith '19 [Noah; 4/5/19; Bloomberg Opinion columnist, former assistant professor of finance at Stony Brook University; "Dumping Capitalism Won’t Save the Planet," https://www.bloomberg.com/opinion/articles/2019-04-05/capitalism-is-more-likely-to-limit-climate-change-than-socialism]

It has become fashionable on social media and in certain publications to argue that capitalism is killing the planet. Even renowned investor Jeremy Grantham, hardly a radical, made that assertion last year. The basic idea is that the profit motive drives the private sector to spew carbon into the air with reckless abandon. Though many economists and some climate activists believe that the problem is best addressed by modifying market incentives with a carbon tax, many activists believe that the problem can’t be addressed without rebuilding the economy along centrally planned lines.

The climate threat is certainly dire, and carbon taxes are unlikely to be enough to solve the problem. But eco-socialism is probably not going to be an effective method of addressing that threat. Dismantling an entire economic system is never easy, and probably would touch off armed conflict and major asdasd upheaval. In the scramble to win those battles, even the socialists would almost certainly abandon their limitation on fossil-fuel use — either to support military efforts, or to keep the population from turning against them. The precedent here is the Soviet Union, whose multidecade effort to reshape its economy by force amid confrontation with the West led to profound environmental degradation. The world's climate does not have several decades to spare.

Even without international conflict, there’s little guarantee that moving away from capitalism would mitigate our impact on the environment. Since socialist leader Evo Morales took power in Bolivia, living standards have improved substantially for the average Bolivian, which is great. But this has come at the cost of higher emissions. Meanwhile, the capitalist U.S managed to decrease its per capita emissions a bit during this same period (though since the U.S. is a rich country, its absolute level of emissions is much higher).

In other words, in terms of economic growth and carbon emissions, Bolivia looks similar to more capitalist developing countries. That suggests that faced with a choice of enriching their people or helping to save the climate, even socialist leaders will often choose the former. And that same political calculus will probably hold in China and the U.S., the world’s top carbon emitters — leaders who demand draconian cuts in living standards in pursuit of environmental goals will have trouble staying in power.

The best hope for the climate therefore lies in reducing the tradeoff between material prosperity and carbon emissions. That requires technology — solar, wind and nuclear power, energy storage, electric cars and other vehicles, carbon-free cement production and so on. The best climate policy plans all involve technological improvement as a key feature.

#### Transition impossible---requires reversing centuries of notions of everyday life

Timms 20 [Aaron; 1/27/20; writer for the New Republic, articles have appeared in The Guardian, The Outline, The Daily Beast, and The Los Angeles Review of Books; "Beyond the Growth Gospel," https://newrepublic.com/article/156024/degrowth-movement-cerbere-can-decreix-commune]/

We all know that our time to stabilize the climate is short. But in the supposed battle between the Green New Deal left and degrowthers, there’s only one side that seeks, in any meaningful sense, to stabilize the climate with anything like the required urgency. In its critique of economism and rejection of technocratic business as usual, in the exhortation of its proponents to think critically about what we as a species really want, degrowth contains much that I find theoretically compelling. But the movement has surprisingly little to say on renewable energy, the result of a latent hostility to techno-scientific innovation, and the idea that billions, within the next decade, will voluntarily embrace degrowth at a sufficient scale to arrest global heating is unrealistic. Even its most ardent defenders concede that genuine degrowth—which means real, Can Decreix-grade upheaval to daily life, not just fewer steaks or car trips every year—will not materialize under present economic and social conditions. Latouche is typically forthright on this question: “Degrowth society cannot emerge from the iron corset of scarcity, needs, economic calculation, and homo æconomicus.” His meaning is what the experience of Can Decreix makes plain: that a life of pure degrowth is logically impossible in this world, indeed that the preconditions for degrowth society do not yet exist. Any attempts to institute degrowth from above will be seen as an intolerable offense to human dignity and well-being, so long as the rest of civilization is hitched to the train of economic expansion—whether capitalist, socialist, or otherwise.

Not even François can avoid compromising himself through contact with the world as it is. The degrowth he practices at Can Decreix is necessarily a diluted form of the ideal, dependent as it is on the structures and economies of the very system degrowth hopes to supersede. There’s an additional irony here, which is that virtually no degrowther wants to put down roots in the home of degrowth, though François’s partner, Alexandra Guerri, lives with him in the austere precincts of Can Decreix. Other degrowth sympathizers have joined François at the encampment in the eight years since its foundation, but they have not stayed; today he continues alone. De Decker returns to Barcelona shortly after his business at the Belvédère is concluded; other summer school speakers appear in Can Decreix for a day or two and then scuttle back to the city. If the defining property of utopia is that it’s nowhere (the word’s meaning in Greek), it’s perhaps appropriate that this utopia has attracted no one. “I feel isolated with this practice here,” François tells me on my first night at Can Decreix. “It’s a struggle to convince people about this way of life. The idea was to do something collective, but now it’s just me. Few people are willing to try something else with flowing and a new way of living.” This is no surprise. Even a hair shirt worn voluntarily is uncomfortable. Le Guin once described the anarchist lunar colony she puts at the center of The Dispossessed, the fiction that everyone here is reading, as an “ambiguous utopia.” A similar description seems apt for the home of degrowth.

A group of rowdy Irish cycling tourists stops by the Dorade, cleats clacking, and they ask for douze bières merci while the owner replies in English. I finish my coffee, then continue on my path back to Can Decreix. In the town square, I pass some of the summer school attendees. It’s been only two hours since breakfast up on the deck at Can Decreix—porridge, plums, nuts—but one of them is seated at a bench, noise-canceling headphones on, bopping to the beat, and oblivious to the world as he tears into a whole wheel of Camembert with rye crisps and a family-size packet of Bolognese sauce-flavored chips by his side. The man is salt-deprived and hungry. I feel a great surge of sympathy.

Since degrowth can’t form the basis of a realistic electoral politics, its proponents are left clinging to the lifeboat of “institutional and cultural change” as they attempt to plot a course to our collective degrowing, or they retreat into didacticism. (The working class “must master” its wants, Kallis has written, “not insist that they should be satisfied.”) What the degrowthers seek, in their priestliest utterings, is not only a new society but also a complete reset of the psychological habitus of everyday life. For degrowth to “work,” its ideal-type citizen must be radically different from you or me, or almost anyone else living under industrial modernity today. This homo post-æconomicus will operate according to as yet undiscovered automatisms, affects, and instincts, conjuring in the process a more sustainable model of human endeavor onto the stage of our desperately overheated globe.

This could indeed be a great thing. After all, a society built on reciprocity, sharing, self-limitation, and care sounds far preferable to the plutocratic catastrophe of present-day financialized capitalism. But such a society cannot arise if we continue to view material limitations as privations. It will only work if the longing for less comes naturally, is authentically aspirational—if we want to live the life unseasoned. This is the journey from the Belvédère to Can Decreix: a journey from We Want Everything to Actually, We Want Very Little. Climate stabilization needs to happen now. Degrowth cannot happen now. This is why degrowth is not a plan for combating climate change, not in any immediate or direct sense at least. Instead, it is something much more ambitious, with a much hazier time horizon: a project to build a new person.

My contributions to the many energy-sapping tasks required to keep Can Decreix in order throughout the summer school—lugging wood, creating shade for discussion groups using bamboo mats and wooden rods, repairing stone walls, building rocket stoves, coming to grips with human compost—have been every bit as half-assed as you’d expect from a weak, unresourceful knowledge worker in the dog days of capitalism with panna cotta-soft hands and no interest in camping. I am, on anyone’s reading, a hopeless volunteer, the least useful of the useful muzhiks. The one activity at which I’ve shown any kind of skill is the chabrot, a postprandial ritual François has adapted from regional custom. There are two types of wine made in-house at Can Decreix: a sweet grenache and rancio, a dry oxidized wine similar to sherry. To perform the chabrot, each diner pools wine into their plate at the end of the meal, agitates the wine with a fork to degrease the plate, then drinks the wine. (Blessedly the house prohibition on addictive substances does not extend to alcohol.) The point of this ritual is to “go easy on the pipes” when washing the dishes, François tells us. I’ve developed a technique of mopping food scraps off the wine-flooded plate with my fingers, drinking the wine, licking my fingers, then licking the plate clean, such that it does not need to be washed at all and is immediately ready for reuse. For days, I survive off a single, self-cleaned plate, earning François’s trust as the summer school’s “official zealot of the chabrot.” The revulsion others feel at this practice is obvious; despite eager propagandizing on my part, no one performs the chabrot with anything like my level of ideological rigor.

There was once a time in the West when licking your fingers at the table, along with a host of other behaviors now considered beyond the pale of respectable society, such as blowing your nose into your hand, were deemed acceptable. The “civilizing process,” as Norbert Elias called it—the gradual recalibration of daily social mores by which Europeans cast off these habits—took centuries, and required the mass internalization of a completely new model of individuality. This was not planned, but was rather the result of myriad colliding stochastic evolutions: state formation and the state’s monopoly over violence, urbanization, the growing differentiation of occupations in increasingly complex economies. A similar process on a similar time line seems necessary for degrowth. Society’s collective degrowing will only make sense once individuals want in a way we don’t want, feel as we don’t feel. Whether a future this different can be engineered is debatable. But that does not mean there remains, in the interim, no virtue to thinking carefully about our course, or even slowing down. On the train of progress, sometimes it’s wise to pull the emergency brake.

### Growth Good---War---2AC

#### Growth solves war

Gat, 19—professor of national security and international politics at the University of Tel Aviv (Azar, “Is War Declining: Why and Where?,” Anali 16 (1) 201-208 (2019), dml)

Most people are very surprised by the claim that we live in the most peaceful period in history. Are we not flooded with media reports and images of conflicts around the world today, some of them very active and bloody, and others seemingly waiting to happen? Have the United States and its allies not been involved in a series of messy wars over the past few decades? Scholars, for their part, ask themselves, if there has indeed been a decline in belligerency, when exactly did it begin: with the end of the Cold War, in 1945, or perhaps earlier? And what exactly caused it?1

Again, most people are surprised to learn that the occurrence of war and overall mortality rate in war sharply decreased from as early as 1815 onward, especially in the developed world. The so-called Long Peace among the great powers after 1945 is more recognized, and is widely attributed to the nuclear factor, a decisive factor to be sure, which concentrated the minds of all the protagonists wonderfully, as they say about the hanging rope. The (inter-)democratic peace has been equally recognized. However, the decrease in war had been very marked even before the nuclear era, and has encompassed nondemocracies as well as democracies. In the century after 1815, wars among industrializing countries declined in their frequency to about a third of what they had been in the previous centuries, an unprecedented change. Compared to their record during the eighteenth century, Austria and Prussia, for example – neither of them a democracy – fought about a third to a quarter as much during the century after 1815.

Indeed, the Long Peace after 1945, more than 70 years to date and counting, was preceded by the second longest peace ever among the modern great powers, between 1871 and 1914, 43 years in all; and by the third longest peace, between 1815 and 1854, 39 years. Thus, the three longest periods of peace by far in the modern great powers system have all occurred after 1815, with the first two taking place before the nuclear age. This striking phenomenon cannot be accidental. A decline in belligerency began from 1815, not 1945 or 1989. Clearly, one needs to explain the entire period of reduced belligerency since 1815, while also accounting for the glaring divergence from the trend: the two world wars.

There is a tendency to assume that wars have declined in frequency during the past two centuries because they have become too lethal, destructive and expensive – fewer but more ruinous wars. This hypothesis barely holds, however, because relative to population and wealth wars have not become more lethal and costly than earlier in history. The wars of the nineteenth century, from 1815 to 1914 – the most peaceful century in European history – were in fact particularly light, in comparative terms. Prussia won the German Wars of Unification in short and decisive campaigns and at a remarkably low price, and yet Germany did not fight again for 43 years. True, the world wars, especially World War II, were certainly on the upper scale of the range in terms of casualties. Yet, contrary to widespread assumptions, they were far from being exceptional in history. We need to look at relative casualties, general mortality rates in wars, rather than at the aggregate created by the fact that many states participated in the world wars.

For example, in the Peloponnesian War (431-403 BC) Athens is estimated to have lost between a quarter and a third of its population, more than Germany in the two world wars combined. In the first three years of the Second Punic War (218-216 BC), Rome lost some 50,000 male citizens of the ages of 17-46, out of a total of about 200,000 in these ages. This was roughly 25 percent of the military age cohorts in only three years, the same range as the Russian military casualties and higher than the German rates in World War II. Similarly, in the thirteen century the Mongol conquests inflicted on the societies of China and Russia casualties and destruction that were among the highest ever suffered during historical times. Even by the lowest estimates casualties were at least as high as, and in China almost definitely far higher than, the Soviet Union's horrific rate in World War II of about 15 percent of its population. A final example: during the Thirty Years War (1618- 1648) population loss in Germany is estimated at between a fifth and a third – either way again higher than the German casualties in the First and Second World Wars combined.

People often assume that more developed military technology during modernity must mean greater lethality and destructiveness, but in fact it also means greater protective power, as with mechanized armour, mechanized speed and agility, and defensive electronic measures. Offensive and defensive advances generally rise in tandem and tend to offset each other. In addition, it is all too often forgotten that the vast majority of the many millions of non-combatants killed by Germany during World War II – Jews, Soviet prisoners of war, Soviet civilians – fell victim to intentional starvation, exposure to the elements, and mass executions rather than to any sophisticated military technology. Instances of genocide in general during the twentieth century, much as earlier in history, were carried out with the simplest of technologies, as the Rwanda genocide horrifically reminded us.

Nor is it true that wars during the past two centuries have become economically more costly than they were earlier in history, again relative to overall wealth. War always involved massive economic exertion and was the single most expensive item of state spending. Both sixteenth and seventeenth centuries Spain and eighteenth century France, for example, were economically ruined by war and staggering war debts, which in the French case brought about the Revolution. Furthermore, death by starvation in premodern wars was widespread.

Another strand of interpretation of the perceived decrease in warfare during recent times has posited voluntary and ideaic factors, has attributed the decline of warfare during recent times to a social 'attitude change'. Why this attitude change should have occurred at this point in history rather than any time earlier is not explained. After all, most powerful moral doctrines such as Buddhism and Christianity decried war for millennia without this having any noticeable effect.

It is suggested that people have suddenly become aware that war is senseless if not crazy, devoid of any rationale. Such a view of war is widespread in today's modern and affluent world. In the discipline of international relations so-called realists, especially ‘defensive realists’, even claim with a straight face that countries have never gained from war because of the balancing effect that contain rising powers. Try this strange idea on Rome, the Aztecs or Inca, the Ottomans, the Mughals or eighteenth century Britain, to name but a few out of many examples. Or on Chinggis Khan, whose descendants constitute, according to genetic studies, 8 percent of all males in Eastern and Central Asia, evidence of staggering sexual opportunities enjoyed by his sons and grandsons whose houses ruled over that part of the world for centuries.

And you should not think that only autocrats and military aristocracies profited from war, while the people were its unwilling victims. This idea was advanced during the Enlightenment and is very popular today. However, it ought to be remembered that the two most successful war-making states of classical antiquity were democratic Athens and republican Rome. And they were so successful precisely because the people of these polities benefited from war and imperial expansion, championed them, and enlisted in their cause. Half of the Athenian budget at the time of Pericles came from the tribute of the Empire which was used to build the Acropolis and pay for the huge navy, in both of which the demos was employed.

We said before that in pursuit of their aims people may resort to cooperation, peaceful competition, or violent conflict. Each of these behavioral strategies is a well-designed tool interchangeably employed, depending on the particular circumstances and prospects of success. Thus, to understand the gravitation of human choices – and norms – from violent conflict towards the non-violent options of cooperation and peaceful competition one needs to understand the changing circumstances and calculus of cost-effectiveness during the past two centuries and in recent decades.

So if modern war has not become more lethal and expensive, why the decline? Two main theories dominate the scene: the democratic peace and the capitalist/trade peace. But, in and of themselves they cannot be the complete answer because of the following, contradicting historical evidence: premodern democracies and republics actually did fight each other; nondemocratic great powers also shared in the general reduction in belligerency during modern times, from 1815 on, including communist powers that largely opted out of the global trade system; until the nineteenth century states tried to monopolize trade by force and bar all others out rather than share with them – think ancient Athens, medieval Venice, early modern Holland, France and Britain, and many others.

What then is the cause of the decline in belligerency? Even before the middle of the nineteenth century, thinkers such as Saint-Simon, Auguste Comte, and John Stuart Mill, who were quick to note the change, realized that it was caused by the advent of the industrial-commercial revolution, the most profound transformation of human society since the Neolithic adoption of agriculture. In the first place, given explosive growth in per capita wealth, about 30 to 50-fold from the onset of the revolution to the present, the Malthusian trap has been broken. Wealth no longer constitutes a fundamentally finite quantity, when the only question is how it is divided, so wealth acquisition progressively shifted away from a zero-sum game.

Secondly, the significance of trade in the economy has ballooned to entirely new dimensions precisely because of the new process of industrial growth. Greater freedom of trade has become all the more attractive in the industrial age for the simple reason that the overwhelming share of fast-growing and diversifying production has now been intended for sale in the marketplace rather than for direct consumption by the family producers themselves. During industrialization, advanced powers' foreign trade increased twice as quickly as their fast growing GDPs, so that by the beginning of the twentieth century, exports plus imports grew to around half of GDP in Britain and France, more than onethird in Germany, and around one-third in Italy and Japan. Consequently, economies are no longer overwhelmingly autarkic, having become increasingly interconnected by specialization, scale and exchange. Foreign devastation potentially depresses the entire system and is detrimental to a state's own wellbeing. What Mill discerned in the abstract in the 1840s, was repeated by Norman Angel during the first global age before World War I, and formed the cornerstone of John Maynard Keynes' criticism of the harsh reparations imposed on Germany after that war.

Greater economic openness has decreased the likelihood of war also by disassociating economic access from the confines of political borders and sovereignty. It is no longer necessary to politically possess a territory in order to benefit from it. Of all these factors, commercial interdependence has attracted most of the attention in the scholarly literature. But both the escape from Malthus with rapid industrial growth and open access have been no less significant aspects of what I call the Modernization Peace.

Thus, the greater the yield of competitive economic cooperation, the more counterproductive and less attractive conflict becomes. Rather than war becoming more costly, as is widely believed, it is in fact peace that has been growing more profitable.

If so, why have wars continued to occur during the past two centuries, albeit at a much lower frequency? In the first place, ethnic and nationalist tensions often overrode the logic of the new economic realities, accounting for most wars in Europe between 1815 and 1945. They continue to do so today, especially in the less developed parts of the globe. Moreover, the logic of the new economic realities receded during the late nineteenth and early twentieth centuries, as the great powers resumed protectionist policies and expanded them to the undeveloped parts of the world with the New Imperialism. This development signalled that the emergent global economy might become partitioned rather than open, with each imperial domain becoming closed to everybody else, as, indeed, they eventually did in the 1930s, with the Great Depression. A snowball effect ensued, generating a runaway grab for imperial territories. For the territorially confined Germany and Japan the need to break away into imperial Lebensraum or 'co-prosperity sphere' seemed particularly pressing. Here lay the seeds of the two world wars. Furthermore, the retreat from economic liberalism in the first decades of the twentieth century spurred, and was spurred by, the rise to power of anti-liberal and anti-democratic political ideologies and regimes, incorporating a creed of violence: communism and fascism.

Since 1945 the decline of major war has deepened further. Nuclear weapons have been a crucial factor in this process, but no less significant have been the institutionalization of free trade and the closely related process of rapid and sustained economic growth. The spread of liberal democracy has been equally potent. Indeed, although nonliberal and nondemocratic states also became much less belligerent during the industrial age, it is the liberal democracies that have been the most attuned to its pacifying aspects.

Relying on arbitrary coercive force at home, nondemocratic countries have found it more natural to use force abroad. By contrast, liberal democratic societies are socialized to peaceful, law-mediated relations at home, and their citizens have grown to expect that the same norms be applied internationally. Living in increasingly tolerant societies, they have grown more receptive to the Other's point of view. Promoting freedom, legal equality, and political participation domestically, liberal democratic powers – though initially in possession of vast empires – have found it increasingly difficult to justify ruling over foreign peoples without their consent. And sanctifying life, liberty and human rights, they have proven to be failures in forceful repression. Furthermore, with the individual’s life and pursuit of happiness elevated above group values, sacrifice of life in war has increasingly lost legitimacy in liberal democratic societies. War retains legitimacy only under narrow and narrowing formal and practical conditions, and is generally viewed as extremely abhorrent and undesirable.

Thus, modernization, most notably its liberal path, has sharply reduced the prevalence of war, as the violent option for fulfilling human desires has become much less rewarding than the peaceful option of competitive cooperation. For instance, with the much increased sexual opportunity within society, young men now are more reluctant to leave behind the pleasures of life for the rigors and chastity of the field. 'Make love, not war' was the slogan of the powerful anti-war youth campaign of the 1960s, which not accidentally coincided with a far-reaching liberalization of sexual norms. Furthermore, is societies of plenty people naturally become risk-averse. Ingelhart’s World Values Survey reflects this, as does, only a bit less seriously, Thomas Friedman’s concept of a Macdonald Peace. All these are interrelated aspects of the Modernization Peace.

The fruits of these deepening trends and sensibilities have been nothing short of miraculous. The probability of war between affluent democracies has declined to a vanishing point, where they no longer even see the need to prepare for the possibility of a militarized dispute with one another. The security dilemma between neighbours – that seemingly intrinsic feature of international anarchy – no longer exists among them. This is most conspicuously the case in North America and Western Europe, the world's most modernized and liberal-democratic regions.

Realists in international relations theory have never been able to explain why Holland and Belgium no longer fear in the slightest a German (or French) invasion, a historically unprecedented situation. Similarly, Canada is not at all concerned about the prospect of conquest by the United States, though people find it difficult to explain why exactly this is so. In East Asia, the most developed countries, such as Japan, South Korea, and Taiwan, do not fear war among themselves or with any of the other developed countries, though they are deeply apprehensive of being attacked by less developed neighbors, such as China or North Korea.

With the collapse of the Soviet Empire and rapid economic growth coupled with democratization in Eastern Europe, East and South Asia and Latin America, the prospect of a major war within the developed world seems to have become very remote. Thus, war's geopolitical centre of gravity has shifted radically. The modernized, economically developed parts of the world have become a 'zone of peace'. War now appears to be confined to the less developed parts of the globe, the world's 'zone of war', where countries that have lagged behind in modernization and its pacifying spin-off effects occasionally still fight among themselves, as well as with developed countries.

### AT: Warming---2AC

#### Growth and innovation solves warming.

Ogutonye, 21—Policy Lead, Science & Innovation Unit, Tony Blair Institute for Global Change (Olamide, “Should Tech Make Us Optimistic About Climate Change?,” <https://institute.global/policy/should-tech-make-us-optimistic-about-climate-change>, dml)

In the middle of a climate emergency, it is challenging to stay upbeat. Yet the good news is that investment in climate technology has continued to grow since the early 2010s. US-listed companies involved with providing technology solutions that support global decarbonisation have consistently outperformed the average since 2019 (Figure 7). Venture capital (VC) investment in the sector grew tenfold between 2013 and 2018, representing five times the growth rate of the overall VC market. By comparison, the growth rate of VC investment in Artificial Intelligence was a third of climate tech between 2013 and 2018 although AI is renowned for its uptick within the same timeframe. Beyond VC, public investment in climate technology research has continued to grow too. In 2019, government research and development funding for energy technologies alone stood at $30 billion, with around 80 per cent of it aimed at low-carbon solutions.

In addition to the positive role of technology, political leaders are increasingly showing a willingness to make ambitious commitments on climate. The Paris Agreement is a case in point. The international treaty was adopted in 2015 and ratified internationally within a year – a much quicker pace than its predecessor, the Kyoto Protocol, which took eight years. The Paris deal grew into a political snowball, galvanising further commitment from most of the world’s leading emitters and arguably becoming the most symbolic climate event of the 21st century. The US withdrawal from the Paris Agreement in 2019 dealt a political blow to the global pact although the decision, since reversed by President Biden, did not resonate or last long enough to have any major impact.

The Biden-Harris administration has already indicated that it will not sit on the fence but will instead revive the country’s leadership on climate action. In the UK and elsewhere, similar efforts can be observed as more countries commit to some form of net zero target. More than 100 countries have pledged a commitment towards net zero, with estimates suggesting that over 70 per cent of global GDP and 55 per cent of CO2 emissions are now covered by a similar target. A Climate Action Tracker Report indicates that the cumulative effect of countries’ pledges to the Paris Agreement – if kept and fully achieved – could keep global temperature rise below 2.1°C by 2100, putting the stated goal of 1.5°C within striking distance.

As explored in our recent Institute paper, there are also important insights for politicians in terms of applying lessons from the Covid-19 pandemic to the climate emergency. Although the pandemic is different in scale, complexity and timeline, it offers an immediate window into how policy leaders can adapt and make decisions in order to better support climate innovation. Countries can also apply the “recovering better together” principles outlined by the UN, which calls for a commitment to climate-related actions as economies recover from the Covid-19 slowdown. More than 60 countries, including high emitters, are already making an explicit promise to link their nationally determined contributions (NDC) to Covid-19 recovery, supported by the United Nations Development Programme’s Climate Promise programme. Countries in the Global South are equally aligning their climate mission with international support for various NDC support programmes. A green recovery can cut the level of 2030 emissions to 25 per cent lower than projections based on pre-Covid commitments and put the world close to a 2°C pathway. The pandemic has also highlighted the significance of tech innovation, not least in record-breaking vaccine delivery but also in the suite of digital solutions developed for contact tracing, compliance monitoring and management of health-care records.

The global financial landscape is evolving to become more responsive to climate innovation. Since they were first issued in 2007, green bonds have grown into what is now estimated to become a $1 trillion market. Analysts expect as much as $500 billion of green bonds this year as the EU raises capital for its Covid recovery fund. From target-linked to transition bonds, innovations in this green market are being used to bring projects in energy, transport, buildings and other economic sectors to life. Investor-led initiatives such as Climate Action 100+, whose members control over $50 trillion of assets, are actively using funds to ensure the world’s largest corporate greenhouse gas emitters commit to climate action. Other investor networks are pursuing a similar agenda, including Europe’s Institutional Investors Group on Climate Change (IIGCC) and Australia and New Zealand’s Investor Group on Climate Change (IGCC). Humanity’s competence in technology and innovation will be central to the race in mitigating and tackling climate change.

#### The overall environment is resilient---‘existential’ threats are false

Ronald Bailey 20, Science Correspondent at Reason, Member of the Society of Environmental Journalists and the American Society for Bioethics and Humanities, “The Global Environmental Apocalypse Has Been Canceled”, Reason Magazine, 8/1/2020, <https://reason.com/2020/08/01/the-global-environmental-apocalypse-has-been-canceled/> [grammar edit]

According to these activists and politicians, humanity is beset on all sides by catastrophes that could kill off civilization, and maybe even our species. Are they right?

Absolutely not, answers the longtime environmental activist Michael Shellenberger in an engaging new book, Apocalypse Never: Why Environmental Alarmism Hurts Us All. "Much of what people are being told about the environment, including the climate, is wrong, and we desperately need to get it right," he writes. "I decided to write Apocalypse Never after getting fed up with the exaggeration, alarmism, and extremism that are the enemy of positive, humanistic, and rational environmentalism." While fully acknowledging that significant global environmental problems exist, Shellenberger argues that they do not constitute inexorable existential threats. Economic growth and technological progress, he says, can ameliorate them.

Shellenberger's analysis relies on largely uncontroversial mainstream science, including reports from the Intergovernmental Panel on Climate Change (IPCC) and the Food and Agriculture Organization. And as a longstanding activist, Shellenberger is in a good position to parse the motives behind the purveyors of doom.

Shellenberger's activism is the real deal. To raise a donation to the Rainforest Action Network, he charged his friends $5 to attend his 16th birthday party. At 17 he went to Nicaragua to experience the Sandinista revolution. In the 1990s he worked with the Landless Workers' Movement in Brazil.

In 2003, Shellenberger and allies launched the New Apollo Project to jumpstart a no-carbon energy revolution over the next 10 years. In 2008, Time named him "A Hero of the Environment." He co-founded the ecomodernist Breakthrough Institute, which advocates the use of advanced technologies such as nuclear power and agricultural biotechnology to decouple the economy from the ecology, allowing both humanity and the natural world to flourish. More recently, he founded Environmental Progress, which campaigns for, among other things, the deployment of clean modern nuclear power. He is an invited expert reviewer of the Intergovernmental Panel on Climate Change's next assessment report.

Ohio Passes Controversial Conscience Clause for Doctors

So what does he say about climate change? "On behalf of environmentalists everywhere, I would like to formally apologize for the climate scare we created over the last 30 years," he wrote in an essay to promote his new book. "Climate change is happening. It's just not the end of the world. It's not even our most serious environmental problem." Needless to say, there are environmentalists everywhere who do not believe they have anything to apologize for. A group of six researchers assembled by the widely respected Climate Feedback fact-checking consortium rated his article as having low scientific credibility.

Shellenberger doesn't devote much of Apocalypse Never to the science behind man-made climate change. He basically accepts the consensus that it's a significant problem and instead focuses on various claims about the harms it is supposedly already causing. In that promotional essay, he argues that (1) human[s] being are not causing a "sixth mass extinction," (2) the Amazon rainforests are not the "lungs of the world," (3) climate change is not making natural disasters worse, and (4) fires have declined 25 percent around the world since 2003.

Shellenberger isn't denying the reality of man-made climate change. He's arguing that humanity is already adapting to the ways climate change has been making weather patterns evolve, and that we will continue to adapt successfully in the future. His book is ultimately a sustained argument that poverty is world's most important environmental problem, and that rising prosperity and increasing technological prowess will ameliorate or reverse most deleterious environmental trends.

### AT: AI---2AC

#### AI won’t cause extinction

Shermer ’17 [Michael; April; Publisher of Skeptic magazine, a monthly columnist for Scientific American, and a Presidential Fellow at Chapman University; “Why Artificial Intelligence Is Not an Existential Threat,” Skeptic, vol. 22, no. 2, pp. 29–35]

Why AI is not an Existential Threat First, most AI doomsday prophecies are grounded in the false analogy between human nature and computer nature, or natural intelligence and artificial intelligence. We are thinking machines, but natural selection also designed into us emotions to shortcut the thinking process because natural intelligences are limited in speed and capacity by the number of neurons that can be crammed into a skull that has to pass through a pelvic opening at birth, whereas artificial intelligence need not be so restricted. We don't need to compute the caloric value of foods, for example, we just feel hungry. We don't need to calculate the waist-to-hip ratio of women or the shoulder-to-waist ratio of men in our quest for genetically healthy potential mates; we just feel attracted to someone and mate with them. We don't need to work out the genetic cost of raising someone else's offspring if our mate is unfaithful; we just feel jealous. We don't need to figure the damage of an unfair or non-reciprocal exchange with someone else; we just feel injustice and desire revenge. Emotions are proxies for getting us to act in ways that lead to an increase in reproductive success, particularly in response to threats faced by our Paleolithic ancestors. Anger leads us to strike out, fight back, and defend ourselves against danger. Fear causes us to pull back, retreat, and escape from risks. Disgust directs us to push out, eject, and expel that which is bad for us. Computing the odds of danger in any given situation takes too long. We need to react instantly. Emotions shortcut the information processing power needed by brains that would otherwise become bogged down with all the computations necessary for survival. Their purpose, in an ultimate causal sense, is to drive behaviors toward goals selected by evolution to enhance survival and reproduction. AIs -- even AGIs and ASIs -- will have no need of such emotions and so there would be no reason to program them in unless, say, terrorists chose to do so for their own evil purposes. But that's a human nature problem, not a computer nature issue. To believe that an ASI would be "evil" in any emotional sense is to assume a computer cognition that includes such psychological traits as acquisitiveness, competitiveness, vengeance, and bellicosity, which seem to be projections coming from the mostly male writers who concoct such dystopias, not features any programmer would bother including, assuming that it could even be done. What would it mean to program an emotion into a computer? When IBM's Deep Blue defeated chess master Garry Kasparov in 1997, did it feel triumphant, vengeful, or bellicose? Of course not. It wasn't even "aware" -- in the human sense of self-conscious knowledge -- that it was playing chess, much less feeling nervous about possibly losing to the reigning world champion (which it did in the first tournament played in 1996). In fact, toward the end of the first game of the second tournament, on the 44th move, Deep Blue made a legal but incomprehensible move of pushing its rook all the way to the last row of the opposition side. It accomplished nothing offensively or defensively, leading Kasparov to puzzle over it out of concern that he was missing something in the computer's strategy. It turned out to be an error in Deep Blue's programming that led to this fail-safe default move. It was a bug that Kasparov mistook as a feature, and as a result some chess experts contend it led him to be less confident in his strategizing and to second-guess his responses in the subsequent games. It even led him to suspect foul play and human intervention behind Deep Blue, and this paranoia ultimately cost him the tournamentt.[ 13] Computers don't get paranoid, the HAL 9000 computer in 2001 notwithstanding. Or consider Watson, the IBM computer built by David Ferrucci and his team of IBM research scientists tasked with designing an AI that could rival human champions at the game of Jeopardy! This was a far more formidable challenge than Deep Blue faced because of the prerequisite to understand language and the often multiple meanings of words, not to mention needing an encyclopedic knowledge of trivia (Watson had access to Wikipedia for this). After beating the all-time greatest Jeopardy! champions Ken Jennings and Brad Rutter in 2011, did Watson feel flushed with pride after its victory? Did Watson even know that it won Jeopardy!? I put the question to none other than Ferrucci himself at a dinner party in New York in conjunction with the 2011 Singularity Summit. His answer surprised me: "Yes, Watson knows it won Jeopardy!" I was skeptical. How could that be, since such self-awareness is not yet possible in computers? "Because I told it that it won," he replied with a wry smile. Sure, and you could even program Watson or Deep Blue to vocalize a Howard Dean-like victory scream when it wins, but that is still a far cry from a computer feeling triumphant. This brings to mind the "hard problem" of consciousness -- if we don't understand how this happens in humans, how could we program it into computers? As Steven Pinker elucidated in his answer to the 2015 Edge Question on what to think about machines that think, "AI dystopias project a parochial alpha-male psychology onto the concept of intelligence. They assume that superhumanly intelligent robots would develop goals like deposing their masters or taking over the world." It is equally possible, Pinker suggests, that "artificial intelligence will naturally develop along female lines: fully capable of solving problems, but with no desire to annihilate innocents or dominate the civilization."[ 14] So the fear that computers will become emotionally evil are unfounded, because without the suite of these evolved emotions it will never occur to AIs to take such actions against us. What about an ASI inadvertently causing our extinction by turning us into paperclips, or tiling the entire Earth's surface with solar panels? Such scenarios imply yet another emotion -- the feeling of valuing or wanting something. As the science writer Michael Chorost adroitly notes, when humans resist an AI from undertaking any form of global tiling, it "will have to be able to imagine counteractions and want to carry them out." Yet, "until an AI has feelings, it's going to be unable to want to do anything at all, let alone act counter to humanity's interests and fight off human resistance." Further, Chorost notes, "the minute an A.I. wants anything, it will live in a universe with rewards and punishments -- including punishments from us for behaving badly. In order to survive in a world dominated by humans, a nascent A.I. will have to develop a humanlike moral sense that certain things are right and others are wrong. By the time it's in a position to imagine tiling the Earth with solar panels, it'll know that it would be morally wrong to do so."[ 15] From here Chorost builds on an argument made by Peter Singer in The Expanding Circle (and Steven Pinker in The Better Angels of Our Nature[ 16] that I also developed in The Moral Arc[ 17] and Robert Wright explored in Nonzero[ 18]), and that is the propensity for natural intelligence to evolve moral emotions that include reciprocity, cooperativeness, and even altruism. Natural intelligences such as ours also includes the capacity to reason, and once you are on Singer's metaphor of the "escalator of reason" it can carry you upward to genuine morality and concerns about harming others. "Reasoning is inherently expansionist. It seeks universal application," Singer notes.[ 19] Chorost draws the implication: "AIs will have to step on the escalator of reason just like humans have, because they will need to bargain for goods in a human-dominated economy and they will face human resistance to bad behavior."[ 20] Finally, for an AI to get around this problem it would need to evolve emotions on its own, but the only way for this to happen in a world dominated by the natural intelligence called humans would be for us to allow it to happen, which we wouldn't because there's time enough to see it coming. Bostrom's "treacherous turn" will come with road signs ahead warning us that there's a sharp bend in the highway with enough time for us to grab the wheel. Incremental progress is what we see in most technologies, including and especially AI, which will continue to serve us in the manner we desire and need. Instead of Great Leap Forward or Giant Fall Backward, think Small Steps Upward. As I proposed in The Moral Arc, instead of Utopia or dystopia, think protopia, a term coined by the futurist Kevin Kelly, who described it in an Edge conversation this way: "I call myself a protopian, not a Utopian. I believe in progress in an incremental way where every year it's better than the year before but not by very much -- just a micro amount."[ 21] Almost all progress in science and technology, including computers and AI, is of a protopian nature. Rarely, if ever, do technologies lead to either Utopian or dystopian societies. Pinker agrees that there is plenty of time to plan for all conceivable contingencies and build safeguards into our AI systems. "They would not need any ponderous 'rules of robotics' or some newfangled moral philosophy to do this, just the same common sense that went into the design of food processors, table saws, space heaters, and automobiles." Sure, an ASI would be many orders of magnitude smarter than these machines, but Pinker reminds us of the AI hyperbole we've been fed for decades: "The worry that an AI system would be so clever at attaining one of the goals programmed into it (like commandeering energy) that it would run roughshod over the others (like human safety) assumes that AI will descend upon us faster than we can design fail-safe precautions. The reality is that progress in AI is hype-defyingly slow, and there will be plenty of time for feedback from incremental implementations, with humans wielding the screwdriver at every stage."[ 22] Former Google CEO Eric Schmidt agrees, responding to the fears expressed by Hawking and Musk this way: "Don't you think the humans would notice this, and start turning off the computers?" He also noted the irony in the fact that Musk has invested $1 billion into a company called OpenAI that is "promoting precisely AI of the kind we are describing."[ 23] Google's own DeepMind has developed the concept of an AI off-switch, playfully described as a "big red button" to be pushed in the event of an attempted AI takeover. "We have proposed a framework to allow a human operator to repeatedly safely interrupt a reinforcement learning agent while making sure the agent will not learn to prevent or induce these interruptions," write the authors Laurent Orseau from DeepMind and Stuart Armstrong from the Future of Humanity Institute, in a paper titled "Safely Interruptible Agents." They even suggest a precautionary scheduled shutdown every night at 2 AM for an hour so that both humans and AI are accustomed to the idea. "Safe interruptibility can be useful to take control of a robot that is misbehaving and may lead to irreversible consequences, or to take it out of a delicate situation, or even to temporarily use it to achieve a task it did not learn to perform or would not normally receive rewards for this."[ 24] As well, it is good to keep in mind that artificial intelligence is not the same as artificial consciousness. Thinking machines may not be sentient machines. Finally, Andrew Ng of Baidu responded to Elon Musk's ASI concerns by noting (in a jab at the entrepreneur's ambitions for colonizing the red planet) it would be "like worrying about overpopulation on Mars when we have not even set foot on the planet yet."[ 25] Both Utopian and dystopian visions of AI are based on a projection of the future quite unlike anything history has given us. Yet, even Ray Kurzweil's "law of accelerating returns," as remarkable as it has been has nevertheless advanced at a pace that has allowed for considerable ethical deliberation with appropriate checks and balances applied to various technologies along the way. With time, even if an unforeseen motive somehow began to emerge in an AI we would have the time to reprogram it before it got out of control. That is also the judgment of Alan Winfield, an engineering professor and co-author of the Principles of Robotics, a list of rules for regulating robots in the real world that goes far beyond Isaac Asimov's famous three laws of robotics (which were, in any case, designed to fail as plot devices for science fictional narratives).26 Winfield points out that all of these doomsday scenarios depend on a long sequence of big ifs to unroll sequentially: "If we succeed in building human equivalent AI and if that AI acquires a full understanding of how it works, and if it then succeeds in improving itself to produce super-intelligent AI, and if that super-AI, accidentally or maliciously, starts to consume resources, and if we fail to pull the plug, then, yes, we may well have a problem. The risk, while not impossible, is improbable."[ 27

### AT: AI---1AR

#### No catastrophic AI impacts – their ev is flawed scholarship

Edward Moore Geist 15, MacArthur Nuclear Security Fellow at Stanford University's Center for International Security and Cooperation, 8/9/15, “Is artificial intelligence really an existential threat to humanity?,” <http://thebulletin.org/artificial-intelligence-really-existential-threat-humanity8577>

Superintelligence: Paths, Dangers, Strategies is an astonishing book with an alarming thesis: Intelligent machines are “quite possibly the most important and most daunting challenge humanity has ever faced.” In it, Oxford University philosopher Nick **Bostrom**, who has built his reputation on the study of “existential risk,” argues forcefully that **a**rtificial **i**ntelligence might be the most apocalyptic technology of all. With intellectual powers beyond human comprehension, he prognosticates, self-improving **a**rtificial **i**ntelligences could effortlessly enslave or destroy Homo sapiens if they so wished. While he expresses skepticism that such machines can be controlled, Bostrom claims that if we program the right “human-friendly” values into them, they will continue to uphold these virtues, no matter how powerful the machines become.

These views have found an eager audience. In August 2014, PayPal cofounder and electric car magnate Elon Musk tweeted “Worth reading Superintelligence by **Bostrom**. We need to be super careful with AI. Potentially more dangerous than nukes.” Bill Gates declared, “I agree with Elon Musk and some others on this and don’t understand why some people are not concerned.” More ominously, legendary astrophysicist Stephen Hawking concurred: “I think the development of full artificial intelligence could spell the end of the human race.” Proving his concern went beyond mere rhetoric, Musk donated $10 million to the Future of Life Institute “to support research aimed at keeping AI beneficial for humanity.”

Superintelligence is propounding a **solution that will not work** to a **problem that** probably **does not exist**, but Bostrom and Musk are right that now is the time to take the ethical and policy implications of artificial intelligence seriously. The extraordinary claim that machines can become so intelligent as to gain demonic powers requires **extraordinary evidence**, particularly since artificial intelligence (AI) researchers have struggled to create machines that show much evidence of intelligence at all. While these investigators’ ultimate goals have varied since the emergence of the discipline in the mid-1950s, the fundamental aim of AI has always been to create machines that demonstrate intelligent behavior, whether to better understand human cognition or to solve practical problems. Some AI researchers even tried to create the self-improving reasoning machines Bostrom fears. Through decades of bitter experience, however, they learned not only that creating intelligence is more difficult than they initially expected, but also that it grows increasingly harder the smarter one tries to become. Bostrom’s concept of “superintelligence,” which he defines as “any intellect that greatly exceeds the cognitive performance of humans in virtually all domains of interest,” builds upon similar **discredited assumptions about the nature of thought** that the pioneers of AI held decades ago. A summary of Bostrom’s arguments, contextualized in the history of artificial intelligence, demonstrates how this is so.

In the 1950s, the founders of the field of artificial intelligence assumed that the discovery of a few fundamental insights would make machines smarter than people within a few decades. By the 1980s, however, they discovered fundamental limitations that show that there will always be diminishing returns to additional processing power and data. Although these technical hurdles pose no barrier to the creation of human-level AI, they will likely **forestall the sudden emergence of an unstoppable “superintelligence**.”

#### It’s far off and won’t cause extinction

Brooks et al 15 -- Panasonic Professor of Robotics (Emeritus), Computer Science and Artificial Intelligence Lab, Massachusetts Institute of Technology; Founder, Chairman, and Chief Technology Officer, Rethink Robotics; Abhinav Gupta -- Assistant Research Professor, Robotics Institute, Carnegie Mellon University; Andrew McAfee -- Principal Research Scientist and Cofounder, Initiative on the Digital Economy, Sloan School of Management, Massachusetts Institute of Technology (Rodney, 2/27/2015, "Artificial Intelligence and the Future of Humans and Robots in the Economy," Malcolm and Carolyn Wiener Annual Lecture on Science and Technology: Artificial Intelligence and the Rise of Robots, http://www.cfr.org/technology-and-science/artificial-intelligence-future-humans-robots-economy/p36205)

BROOKS: People always want us to fight, but we don't really. I think, although I agree with the general themes that Andy talks about, I think it's very easy for people who are not deep in the technology itself to make generalizations, which may be a little dangerous. And we've certainly seen that recently with Elon Musk, Bill Gates, Stephen Hawking, all saying AI is just taking off and it's going to take over the world very quickly. And the thing that they share is none of them work in this technological field. So let me explain why—and they're all smart people, but I think they're making a fundamental error and it gets to NEIL, actually. THOMPSON: After taking down Bill Gates, Elon Musk and Stephen Hawking, he's going to take down the Dalai Lama. Please continue, Rodney. BROOKS: So let's go back to an example from the '90s, when IBM's Deep Blue beat Kasparov, beat the world chess champion. And Kasparov got up and said, well, at least it didn't enjoy beating me. That was his—holding on to his humanity. And now, today, you can get programs that run on—and that was on a supercomputer and now you can get programs that run on laptops. There's about twelve of them that have a better chess rating than any human being has ever had. So people see that -- MCAFEE: It's so bad now—let me underscore what Rod is saying. It's so bad now that they asked human grand master a couple years ago how he would prepare for a match against a computer and he said, I'd bring a hammer. BROOKS: So they can play chess really, really well. And I think people generalize that in the way that if a person can do some task really, really well, they can do adjacent tasks quite well. But none of those chess programs can play tic-tac-toe. Imagine a chess grand master who couldn't play tic-tac-toe. It doesn't make sense. None of those chess programs can give advice to an aspiring human on how to play better. All they can be is a sparring partner. MCAFEE: That program couldn't play tic-tac-toe without being substantially redirected, right? BROOKS: Right. So people, I think, are seeing some of the image labeling that's going on, for instance. Google came out with image labeling, which is a great commercial problem for them. They want to be able to label images. And one of the examples was, that Jeff Hinton shows, one of the chief scientists, is, it's a picture and it says there's a baby holding a teddy bear or doll in there. You look at it, it's a baby holding a teddy—a doll. But then if you ask the program, where is the baby? All it can say is, well, this pixel has 10 percent probability of being a baby, this pixel has 80 percent. And people have done experiments. You have a mashup of, you know, a grotesque mashup of baby parts and it says it's a baby. It's a baby. It's got all the parts. But a person says, no, that's a grotesque mashup of baby parts in the image. THOMPSON: But Abhinav, you've solved this, right? GUPTA: No, no, no. BROOKS: Well, he's working towards-- GUPTA: So, can I-- BROOKS: He's working towards it because it's such a hard problem. GUPTA: Yeah, OK. Thank you. So since we are talking about images, I think I should chime in a little bit and tell you that—so what Andrew is talking about, that we have made big advances, again, they're very, very specific tasks. Given an image, tell me what label can you put on that image? We have gotten really good at this task. Some people claim even better than humans. I don't buy that, but let's assume that even better than humans. But that doesn't mean we can do anything else apart from that exact task. And that's what Rodney was talking about. They have no idea that—what does baby mean? What does having a baby mean in those images? No idea. You, as a human, would know, OK, if I'm saying there's a baby, it has a lot of meaning inside. You get a lot of meaning out of that thing. So while we have made significant advances in the last two years, I want to boil it down a little bit and say we still are a long, long way to go but Elon Musk or Bill Gates, everyone is talking about, we still have a long way to go. But there's hope, and that's what I think we have to see here. Two years ago, if you asked me can computers take an image and solve this problem, I would say I have invested seven years of my life but if you give me a random image, it will not work. And now, given a random image, it will work. So all it -- MCAFEE: This was the guy who was doing this for a living and if you asked him two years ago would this happen, he would say, no. This progress is weirdly fast and is surprising insiders in the field. GUPTA: Yeah. I agree. And I'm an insider in the field and I'm very surprised, I have to say. Now, at this point of time, I am like living in an awe of myself, in some sense, that—but it was like Rodney told—Rodney told us that in thirty-five years he never thought he'd do this all. I also thought some of it, like that, for thirty-five years, I will not solve—see this kind of classification performance. But as I'm saying this, still a long, long way to go and much harder way to go. What—where all the kind of gains have come from is the data. And I think—so technology, this like deep-learning technology has been there from '70s and '80s. Don't misunderstand that this technology came two years ago and everything's changed. This has been there for thirty years. It's just that for the first time in our technological advances we have data for this deep-learning technology to learn. MCAFEE: Let me jump on this because I think the three of us are really agreeing, instead of disagreeing. I chose my adjective pretty carefully. I said these advances are going to be economically significant. I completely agree with Rod that they're not going to be existentially significant on any timeframe that we really need to worry about, for exactly the reasons that you're bringing up. One way to think about this, the way I try to get my mind around it, is there are, from what I've been able to take in, there are something like between ten and twenty really fundamental challenges that these guys and their discipline have been working on. Common sense is a really great example of that. As I've looked around, these breakthroughs that we're seeing seem to be—kind of indicate that we're making real progress on one of those challenges, the challenges of learning in a pretty unstructured environment. That's a big deal. There are lots of other fundamental challenges in the discipline where the progress has not been as fast, and these are the ones that you're working on.

#### Empirically true.

Allenby 15 (Brad, Lincoln Professor of Engineering and Ethics; President’s Professor of Civil, Environmental, and Sustainable Engineering, and of Law; and founding chair of the Consortium for Emerging Technologies, Military Operations and National Security at Arizona State University, “Emerging technologies and the future of humanity,” Bulletin of the Atomic Scientists, November/December 2015, Vol. 71, No. 6, p. 29-38, Accessed Online through Emory Libraries)//cmr

Although it was not clear at the time, Bill Joy’s article warning of the dangers of emerging technologies was to spawn a veritable “dystopia industry.” More recent contributions have tended to focus on artificial intelligence, or AI; electric car and space technology entrepreneur Elon Musk has warned that AI is “summoning the demon” (Mack, 2015), while physicist Stephen Hawking has argued that “the development of full artificial intelligence could spell the end of the human race” (Cellan-Jones, 2014). The Future of Life Institute (2015) recently released an open letter signed by many scientific and research notables urging a ban on “offensive autonomous weapons beyond meaningful human control.” Meanwhile, the UN holds conferences and European activists mount campaigns against what they characterize as “killer robots” (see, e.g., Human Rights Watch, 2012). Headlines reinforce a sense of existential crisis; in the military and security domain, cyber conflict runs rampant, with hackers accessing millions of US personnel records, including sensitive security clearance documents. Technologies such as uncrewed aerial vehicles, commonly referred to as “drones,” are highly contentious in both civil and conflict environments, for many different reasons. A recent US Army Research Laboratory report foresees genetically and technologically enhanced soldiers networked with their battlespace robotic partners and remarks that “the presence of super humans on the battlefield in the 2050 timeframe is highly likely because the various components needed to enable this development already exist and are undergoing rapid evolution” (Kott et al., 2015: 19). How is one to think about this outpouring of analysis, hypothesis, events, and existential angst? A useful first step is to realize that there are three levels to such discussions of technology.2 Level I is the instrumental level: a gun shoots a bullet and kills someone; a watch is used to tell time; a vaccine is used to prime an individual’s immune system to protect against a disease. Level II is the systems level: an uncrewed aerial vehicle conducting surveillance is part of a battlefield intelligence system; watches function in a globally standardized time system that was only institutionalized in the United States by an act of Congress in 1918; vaccinations are part of a public health system. Level III, the effect of a technology on individual psychology, society and culture, economic patterns, geopolitical status, and other Earth systems, is unpredictable and uncertain. One of the major drivers for standardized time, for example, was railroad technology, which was certainly not foreseen by those who first began developing steam locomotives. It is important to remember, however, that even if the specifics of Level III impacts cannot be predicted a priori, they will occur. Level I effects are usually not difficult to figure out: They are the reasons that a technology is commercialized. For example, the Level I effect of a bomb-dismantling robot is clear: It helps save the lives of soldiers who would otherwise have to be doing that job. Level II effects can be more complex and may point in different directions than first-order effects. A robotic hummingbird surveillance device may have entirely beneficial effects if used in counterinsurgency, because it can improve targeting and thus reduce collateral damage (Level I effect). But if the same technology becomes widely available to political parties and divorce lawyers, it could have very negative effects on privacy and public discourse (a Level II effect). And, hypothetically, robotic bugs and hummingbirds, combined with data-mining software and massive databases, could become important tools of techno-totalitarian elites, a possible, but hypothetical, Level III effect. This distinction among Level I, Level II, and Level III is useful because much of the confusion regarding emerging technologies comes from conflating relatively predictable Level I aspects of an emerging technology with highly unpredictable Level III hypotheticals, and treating them as equally valid insights into future technological trajectories. Not so. A concern about the use of drones to attack human targets in countries that are not participants in a conflict is qualitatively different than polemics against “killer robots,” and while conflating the two for purposes of argumentation may be effective, it is profoundly misleading. We have historical and operational data that enable us to evaluate the former; we don’t even know what a “killer robot” really is, except as an evocative term, and virtually no idea what would happen if such technologies became widespread in the real world. An analogous analytical mistake occurs when a particular use of a technology is treated as if it were separable from the technology itself. A medical advance in computer-brain interfaces in prosthetics, for example, is the same technology that might be used in the near future to directly connect a soldier to a remote weapons system. Any effort to ban “military AI” will fail because “military AI” is not a relevant technology category; rather, it is the advance of the underlying technology as a whole that ensures at some point that AI will be integrated into military devices. (Notably and presumably unintentionally, the proselytizing against “military AI” fails to admit that such a policy implicitly favors powers, such as Russia and ISIS, that are operating under doctrines of asymmetric warfare that privilege non-traditional tactics, technologies, and conflict.) It is precisely this confusion that one notes in the language used in many of the comments on and critiques of emerging technologies, including some of the examples given above. It is not so much a question of whether these popular dystopian visions are accurate predictions: They almost certainly are not, because the ability to predict the future paths and implications of complex and powerful technology systems is simply nonexistent. Level I assertions of knowledge are being extended to inherently unpredictable Level III systems without understanding that an important conceptual shark has been jumped. But it is useful to explore the assumptions underneath the current rage for dystopian visions of emerging technologies, which are not as implausible as some have suggested. To reduce such confusion, let me be clear from the beginning. Because much recent commentary regarding emerging technologies is generic and apocalyptic, that is what this essay will focus on. In other words, I will not concern myself with whether a particular weapon system, or smart phone app, or cyber worm, or AI tool is good or bad or competitively successful, a Level I question. Nor will I address the foreseeable Level II effects, an analysis which, as in the case of Level I, would focus on particular technological artifacts or applications and their systemic effects. Rather, since apocalyptic tends to be Level III stuff, that’s where we’ll go. Emerging technologies as an Earth system The first question to ask about emerging technologies is deceptively simple: Is today really that different? Is there something about today’s emerging technologies—which for purposes of this analysis include nanotechnology, biotechnology, information and communication technology (ICT), robotics, applied cognitive science, humtech (design and engineering of the human as a foundational emerging technology), and their various combinations and permutations—that is qualitatively different from those that characterized other eras of technological change? If there isn’t, much of today’s dramatic language can be understood as simply a reflection of the emphasis that all humans give to the particular era and landscape and culture within which they exist. Each generation tends to overemphasize the degree of change that it experiences, partly because of the immediacy of the stresses to which it is exposed, and partly because it is easy to underestimate how difficult and unpredictable life was in the past**,** since when one looks back at history it seems to flow logically and necessarily. Indeed, apocalyptic fears have been common when many major technology systems first emerged because of this immediacy, even as subsequent generations grew to view the technology as banal, even boring. In the early days of railroads, for example, there was a widespread belief that traveling at the heretofore unimaginable speed of 25 miles per hour would kill the passengers, in part because such technology was against the obvious will of God. As an Ohio school board put it, If God had designed that His intelligent creatures should travel at the frightful speed of 15 miles an hour by steam, He would have foretold it through His holy prophets. It is a device of Satan to lead immortal souls down to Hell. (Nye, 1994: 57)3 In this case, however, a strong argument can be made that emerging technologies today are different not just in degree, but in kind, from those of the past. To begin with, the scope, scale, and speed of technological change are unprecedented. Where previous waves of technological change have involved a few core technologies, such as railroads or electrification, today technological evolution is occurring across the entire technological frontier. Partially as a result of such technologies rippling across a population of seven billion people, we now live on a terraformed planet, the first world we know of anywhere that has been shaped by the deliberate activities of a single species. That is not a discontinuous process, but it is qualitatively new. Moreover, as the discussion of the engineered warrior of 2050 suggests, the human itself has become a design space. It is certainly true that people have always changed themselves in many ways, from consuming intoxicants of all kinds, to medicine, to education, but there is little question that the direct interventions that are now possible, combined with accelerating advances in fields such as neuroscience, genetics and molecular biology, and prosthetics, make virtually all aspects of the human, including cognitive and psychological domains, potentially subject to design. That the designer is not just engineering external systems, but him- or herself, adds a degree of reflexivity, nonlinearity, and complexity that makes simple predictions about particular technologies tangential and irrelevant at best. It is worth emphasizing in passing that the argument that humans are at risk from emerging technologies is in an important sense circular. Humans are increasingly both designer and designed; they are, in other words, increasingly an emerging technology in their own right. People are many things, but they are now, and certainly will be in the future, a design project. Thus, in a meaningful way the argument that people are at risk from emerging technologies becomes the argument that emerging technologies are at risk from emerging technologies, which makes little sense, and isn’t very helpful analytically, or in guiding policy or practice. Additionally, technological evolution is accelerating, which has significant implications. Past rates of technological change were slow enough that psychological, social, and institutional adjustments were possible, but today technology changes so rapidly that technology systems decouple from governance mechanisms of all kinds. All these factors, operating together, synergistically increase the impact, speed, and depth of change. Any technology potent enough to be interesting will inevitably destabilize existing institutions, power relationships, social structures, reigning economic and technological systems, and cultural assumptions. Previous waves of technological change—from steam and coal, to electricity, to rail and automotive technologies—have destabilized and restructured human and natural systems at all scales, interacting unpredictably with contemporary natural, human, and built systems. Railroads, for example, opened up continental interiors, creating the underlying transportation infrastructure necessary to support industrialized agriculture, which, coupled to advances in production of artificial fertilizers and innovation in farm machinery, created the potential for dramatic increases in global human population. It also dramatically changed ecologies and landscapes; the American Midwest is an agricultural breadbasket, not a large swamp, because railroads provided the link between that farming region and the demand of the East Coast and, via steamship, Europe. The Earth’s atmosphere has been in part restructured by development of internal combustion engine technology coupled to a psychologically potent automotive technology, which is in turn based on a massive fossil fuel infrastructure. Proposals to address climate change through so-called “geoengineering technologies,” from designing the atmosphere to reflect incoming sunlight to deploying devices that capture carbon dioxide in the atmosphere, are explicitly intended to engineer major natural systems and cycles. In short, major new technologies are not just about artifacts; rather, they represent an unpredictable, sometimes apparently discontinuous, shift in the structure of integrated Earth systems. Moreover, these shifts are not predictable a priori; railroads, for example, required new systems of time, of communication, and, more subtly, of finance and of corporate management. Development of a mass consumption economy, with washing machines from new merchandising giants and cars from Detroit, required innovation in the development of consumer credit, and massive coupled innovation in everything from road systems to supply-chain management. Widespread consumer credit, in turn, generated an ability to consume, and a concomitant quality of life, that was beyond imagining for those generations of humans that lived prior to the 20th century. It is thus highly likely that the first implicit assumption of the dystopian perspective is correct: Things are indeed different today, and the difference is fundamental and qualitative, not simply one of degree. Emerging technologies are making everything from individual molecules, to the human, to the planet itself, design spaces. Moreover, it is also likely that technological evolution, and all the concomitant changes in coupled institutional, social, economic, and cultural systems, will be more challenging and complex than anything humans have yet experienced. The remaining two issues, then, are: First, what can we do about it; and second, is this the end of humanity? What can we do about it? Precisely because new technologies are disruptive, they inevitably call forth opposition, both by conservative social forces and by threatened economic interests. Historical examples abound. With railroad technology, for example, conservative states such as the Austro-Hungarian Empire and Russia resisted rapid deployment, in part because it was feared that railroads might create social unrest in the still somewhat feudal and highly stratified cultures that characterized such countries; the French held back because of concerns it would destroy rural culture. The predictable result was that modernizing states that realized the commercial and military potential of railroad technology, such as Prussia, rapidly overtook the laggards in building rail infrastructure, with an eventual shift in geopolitical stature. In the United States, railroads were bitterly opposed by river transportation interests; in fact, Abraham Lincoln, when still a practicing lawyer, argued and won the seminal case for the Rock Island Railroad.4 (River shippers at the time were arguing that any railroad bridge over a river was an unlawful obstruction of commerce; had they been successful, railroads would have been limited to operating between rivers and streams, but not crossing them.) A more recent example is provided by the thousands of people sued by the Recording Industry Association of America in its vain effort to defend a technologically obsolete business model for the distribution of music. There are plenty of reasons, in other words, why emerging technologies might be regarded as dangerous and disruptive, and thus worth stifling. History, however, indicates that while local opposition can be successful, it will not halt the evolution of technology. Consider, for example, the Japanese attempt to limit gunpowder technology to preserve traditional Samurai culture; successful in the short term, it left Japan open to subjugation by Western naval forces with gunpowder technology. Similarly, environmentalists and governments in Europe have aggressively opposed genetic engineering (GMOs, or “genetically modified organisms”) in agriculture. Outside Europe, however, GMO technology has been one of the most rapidly adopted agricultural technologies in history. Efforts to regulate the proliferation of nuclear weapon technology have been somewhat successful, but it appears unrealistic to assume that the technology can be uninvented. Especially given today’s globalized culture, and the strategic and military advantages that emerging technologies can provide, it is highly unlikely that meaningful constraints on technological evolution, whether derived from cultural, competitive, or religious foundations, will be successful. That is particularly true as all players in the global Great Game understand that leadership in science and technology domains is a necessary, if not sufficient, prerequisite for dominance. Moreover, given the complexity of many emerging technology systems, especially as they co-evolve with other natural, built, and human systems, it is unfortunately also likely that projecting their effects and evolutionary paths before they are actually adopted and become embedded in their social and cultural context is not just hard, but for all practical purposes impossible. One can, and should, generate scenarios. But exhortations that purport to elevate hypotheticals to predictions and implications of certainty about future states are misplaced. In short, there is no certainty, and the genie is well and truly out of the bottle. However, that doesn’t necessarily imply that we can’t modulate future technological evolution, but that the way we think about it today may be too simple, and our institutions too slow and maladaptive, to be up to the task. Beyond simplistic dystopianism This analysis suggests that, as dystopians might argue, emerging technologies are indeed potent, and that, especially as the human is becoming an active design space, if AI doesn’t destroy humanity, something will. But this is a grossly incomplete perspective. Humanity, as it appears at any particular time, is always doomed. Foragers and hunter-gatherers were doomed, as were the serfs of medieval Europe with their small plots and lives lived within a radius of a few miles of where they were born. And so, in our turn, are we. Doom is, in other words, evolution, and it is unlikely that we will stop it—or, really, that we should want to. In fact, the images that we cling to, personally and institutionally and culturally, are already obsolete. The ethics and values that we insist we will impose on the future are not only historically and culturally contingent, but already obsolete as well. We want the physical and cultural landscape we live in now to propagate into tomorrow, because we all unconsciously privilege the present, but that is not how complex systems work. They evolve, and indeed our world is evolving at a remarkable and accelerating clip. The fallacy of the dystopians, then, is not in their analysis of the power of technology, or the accelerating and destabilizing rates of change. The fallacy is in equating evolution with dystopia, and, without admitting it, privileging the present over the promise and inevitability of the future. What is at risk is the limited mental model of “human” that all of us carry with us, not “humans” as an ongoing process. This is actually a common category mistake in modern discourse: Sustainability advocates and environmental activists often claim that “the planet is at risk,” but of course it is not. The planet is a large mass of rock and a film of various carbon compounds, and that is not at risk at all. What is at risk is a particular mental model of what the world should look like, a constructed snapshot. That does not mean that there aren’t many environmental issues that require attention; of course there are. But, as in the case of the emerging technology discourse, it does mean that existential catastrophe language is not only invalid, but can actually prevent seeking constructive adaptations to accelerating change. Our only recourse is neither technological fatalism nor ethical relativism. It is true that we have not yet appreciated, much less begun to respond to, the challenge of a future that will indeed be more complex and difficult than anything we have experienced as a species. Nonetheless, we can already identify several important principles. For example, we need to stop thinking of “problems” with “solutions,” and think more in terms of “conditions” that will require long-term, adaptive management. Challenges such as ISIS and climate change will not be solved, but they can and must be managed in light of other relevant goals. In this, the experience with nuclear weapons is instructive: They are not a problem that can be unmade, but they are a condition that can be, and has so far been, relatively successfully managed. We also need to focus on creating option spaces—portfolios of social, institutional, and technological choices that can be adaptively and flexibly deployed in complex environments. Similarly, we need to play with scenarios: If dystopian pronouncements are instead taken as scenarios—“What would you do if…?”—they are far more useful and informative than suggestions of doom. Socially and institutionally, we need to become more agile and adaptive. This is uncomfortable for many, because it implies a degree of contingency and uncertainty, but that is precisely why such skills are necessary. The rate of technological change is unforgiving and has already decoupled to a large extent from traditional governance mechanisms. So we need to develop new ones. Individually, we need to become far more humble about our ability to visualize and prognosticate on a complex and dynamic future. Cautionary scenarios and hypotheticals are welcome exercises in practicing to adjust to the unknowable that lies in front of us, but they are not appropriate foundations for policy or legal action in the present. Nightmares are seldom reality, and when bad things do happen they are seldom the ones we thought about. Fear and anger in the face of change are popular responses—witness the rise of far right and far left factions, and fundamentalisms of all stripes, around the world—but they are maladaptive, and those in responsible positions at least cannot afford such luxuries.

### AT: Phosphorous---1AR

#### No peak phosphorous

**Cho, 13** – staff blogger for the Earth Institute and a freelance environmental writer who has written for www.insideclimatenews.com, E Magazine and On Earth. Previously, Renee was Communications Coordinator for Riverkeeper, the Hudson River environmental organization. She received the Executive Education Certificate in Conservation and Sustainability from the Earth Institute Center for Environmental Sustainability (Renee, 4/1. “Phosphorus: Essential to Life—Are We Running Out?” http://blogs.ei.columbia.edu/2013/04/01/phosphorus-essential-to-life-are-we-running-out/)

In fact, phosphorus is a renewable resource and there is plenty of it left on earth. Animals and humans excrete almost 100 percent of the phosphorus they consume in food. In the past, as part of a natural cycle, the phosphorus in manure and waste was returned to the soil to aid in crop production. Today phosphorus is an essential component of commercial fertilizer. Because industrial agriculture moves food around the world for processing and consumption, disrupting the natural cycle that returned phosphorus to the soil via the decomposition of plants, in many areas fertilizer must now be continually applied to enrich the soil’s nutrients.

Most of the phosphorus used in fertilizer comes from phosphate rock, a finite resource formed over millions of years in the earth’s crust. Ninety percent of the world’s mined phosphate rock is used in agriculture and food production, mostly as fertilizer, less as animal feed and food additives. When experts debate peak phosphorus, what they are usually debating is how long the phosphate rock reserves, i.e. the resources that can economically be extracted, will hold out.

Pedro Sanchez, director of the Agriculture and Food Security Center at the Earth Institute, does not believe there is a shortage of phosphorus. “In my long 50-year career, “ he said. “Once every decade, people say we are going to run out of phosphorus. Each time this is disproven. All the most reliable estimates show that we have enough phosphate rock resources to last between 300 and 400 more years.”

In 2010, the International Fertilizer Development Center determined that phosphate rock reserves would last for several centuries. In 2011, the U.S. Geological Survey revised its estimates of phosphate rock reserves from the previous 17.63 billion tons to 71.65 billion tons in accordance with IFDC’s estimates. And, according to Sanchez, new research shows that the amount of phosphorus coming to the surface by tectonic uplift is in the same range as the amounts of phosphate rock we are extracting now.

### AT: Chemicals---1AR

#### No impact

**Kareiva and Carranza 18**—Institute of the Environment and Sustainability, University of California, Los Angeles (Peter and Valerie, “Existential risk due to ecosystem collapse: Nature strikes back,” Futures, available online January 5, 2018, ScienceDirect, dml)

Another hypothesized planetary boundary entails the conversion of natural habitats to agricultural land. The mechanism by which too much agricultural land could cause a crisis is unclear—unless it is because land conversion causes so much biodiversity loss that species extinctions are the proximate cause of an ecocatastrophe. Excessive chemical pollution and excessive atmospheric aerosol loading have each been suggested as planetary boundaries as well. In the case of these pollution boundaries, there are well-documented mechanisms by which surpassing some concentration of a pollutant inflicts severe human health hazards. There is abundant evidence linking chemical and aerosol pollution to higher mortality and lower reproductive success in humans, which in turn could cause a major die-off. It is perhaps appropriate then that when Hollywood envisions an unlivable world, it often invokes a story of humans poisoning themselves. That said, it is doubtful that we will poison ourselves towards extinction. Data show that as nations develop and increase their wealth, they tend to clean up their air and water and reduce environmental pollution (Flörke et al., 2013; Hao & Wang, 2005). In addition, as economies become more circular (see Mathews & Tan, 2016), environmental damage due to waste products is likely to decline. The key point is that the pollutants associated with the planetary boundaries are so widely recognized, and the consequences of local toxic events are so immediate, that it is reasonable to expect national governments to act before we suffer a planetary ecocatastrophe.

### Growth Sustainable---1AR

#### Innovation is desirable and norms are malleable---reject pessimism.

Zenghelis '21 [Dimitri; 5/19/21; Visiting Fellow at the London School of Economics, founder of the Wealth Economy Project at the Bennett Institute, University of Cambridge; "Sustainability Is Not Only Compatible With Growth, It Requires It – But Only With Targeted Innovation," Sustainability Is Not Only Compatible With Growth, It Requires It – But Only With Targeted Innovation/]

Innovation is therefore necessary and we will have to change our material consumption. Yet tastes, preferences and social norms are not fixed. As we get richer, we value personal services such as performance art, care services and socialising over material goods. The ‘degrowthers’ are right: prosperity does not rely on ever-increasing material consumption (despite its many flaws, real GDP is a chain weighted value concept, so it will pick up our changing preferences for dematerialised existence, albeit slowly and imperfectly).

In short, what matters is decarbonisation and dematerialisation, not ‘degrowth’. The primary route to dematerialisation is through innovation. And this requires strong, clear and credible policy intervention. There is no reason why the future cannot be cleaner, quieter and more secure as well as more efficient, productive and innovative. We just need to design it that way. Our species developed effective vaccines for COVID-19 in record time. For all our failings as stewards of the planet, innovation is one thing humans excel at. We need more of it and of the right kind.

#### No overaccumulation---dematerialization is globally true!

Lokshin, 21—Lead Economist with the Office of the Chief Economist for Europe and Central Asia, World Bank (Michael, “Dematerialization, degrowth, and climate change agenda,” <https://blogs.worldbank.org/developmenttalk/dematerialization-degrowth-and-climate-change-agenda>, dml)

These are not isolated examples of the intensity of modern agriculture. The total crop tonnage in the United States tripled since the 1970s, but the cropland area shrunk from about 472 million to 390 million hectares by the 2010s, saving an area three times larger than the United States’ total urban area. Productivity gains in animal agriculture dramatically reduced the environmental footprint of livestock production in the US. Similar reductions in farmland accompanied by large increases in output are seen in countries of Europe, Latin America, and East Asia. The global footprint of agriculture has “started decreasing in size during the past two decades.”

US agriculture, having a positive trade balance, consumes 25 percent less fertilizer than it did in 1999, and the volume of water used for irrigation has decreased by 22 percent since then. Raising the average world farm productivity to the levels seen among US farmers would allow enough food to be grown to feed 10 billion people an American-type diet on half the land currently used for farming. The land released would exceed the area of Amazonia (7 million square kilometers).

Most developed countries are now in the stage of “forest transition,” when a country gains forest area. Europe is greener now than it was 100 years ago; the size of US forest resources remained constant over the 20th century and increased over the last decade. China is adding almost 2 million hectares (about 1 percent) of forests a year. And rates of global forest loss have been slowing since 1980.

At the same time, forestry has become more productive. Shifting wood harvest from the north to the southeast, where the forests are twice as productive, decreased the United States’ logged area by 3.1 million hectares. Forest plantations are much more productive than unmanaged forests: Brazilian eucalyptus plantations provide at least 10 times more timber per hectare per year than northern forests do. The consumption of wood is also declining. Ships and railroads are no longer built of wood. Globally, the use of wood for fuel and construction dropped sharply since the 1960s; the global demand for paper has been stagnant, decreasing across the developed countries over the last two decades. The footprint of the developed world on the planet, as an area occupied by human activities, is shrinking.

There has also been a marked decline in US consumption of the most economically important minerals. According to the US Geological Survey (USGS), since the end of the 20th century, US consumption of metals has fallen by 15 percent for steel, 30 percent for aluminum, and 40 percent for copper. The decline reflects increased efficiency. Aluminum soda cans are six times lighter than they were in the early 1960s, and cars weigh 30 percent less than they did. The introduction of high-strength steel framing, reinforced concrete, and stronger and lighter glass have reduced consumption of cement, stone, sand, and gravel in construction. US energy use has plateaued for more than a decade. Similar trends are observed in the UK, which began to reduce its consumption of physical resources between 2001 and 2003. Even individual caloric intake is falling in the UK, mainly because of the decline in most environmentally damaging meat consumption.

Off-shoring could affect the local consumption of national resources. Country statistics, which rely on a territorial perspective of material use, might fail to account for the global patterns of material consumption. What looks like “green growth” might be just an artifact of globalization. For example, some intermediate metal consumption might be hidden in imported finished merchandise like cars or trucks. While these are valid concerns, the reduction of materials used in agriculture, forestry, and construction appears to be largely isolated from such measurement issues. Actual consumption of these materials in developed countries is dropping; whether the material is imported or not is irrelevant.

The concept of dematerialization refers to an absolute or relative reduction in the quantity of materials required to serve economic functions in society. Unlike the traditional `end-of-pipe’ measures, dematerialization is an input-oriented strategy intended to reduce environmental damage at the source. The production and consumption of products, the so-called “industrial” and “social metabolisms,” could harm the environment. Reducing the volume of material and energy used to produce goods and services diminishes the environmental impact. But in contrast with the degrowth movement, which is based on the premise that environmental damage rises with population and economic growth, the proponents of dematerialization argue that societal metabolism might exhibit an inverted U-shaped relationship with economic growth. A country’s environmental impact rises as its national income grows but then declines after a (very) high level of GDP is reached. Similar argument is made by the recent literature on growth and pollution conversions.

If we believe these trends, the reduction (both relative and absolute) of material consumption observed in developed countries might have important policy implications. Growth in developed countries might not necessarily cause environmental distress and natural resource depletion. Advanced economies may be able to decouple economic growth and growing volumes of resource use. The new technologies are making the economic growth in developing countries greener and less material-intensive compared to the growth the now rich countries experienced at comparable income levels decades ago.

Several factors drive dematerialization. Technological progress improves efficiency and reduces the consumption of resources in manufacturing. The digital economy “swaps bits for atoms,” replacing physical goods and services with their digital versions; 3D printing shifts technologies toward custom-designed components with little or no waste. Competition encourages companies to cut costs and use less materials. Citizens and governments are increasingly putting premiums on the environment, embracing policies to reduce social metabolism.

### AT: Agriculture---1AR

#### Industrial ag is better.

Ted Nordhaus 21, Founder and Executive Director of the Breakthrough Institute and Co-Author of An Ecomodernist Manifesto, and Dan Blaustein-Rejto, Director of Food and Agriculture at the Breakthrough Institute, Conducted Research with the Environmental Defense Fund, International Center for Tropical Agriculture, and Farmers Market Coalition, “Big Agriculture Is Best”, Foreign Policy, 4/18/2021, https://foreignpolicy.com/2021/04/18/big-agriculture-is-best/

Moreover, organic farms, large and small, don’t actually outperform large conventional farms by many important environmental measures. Scale, technology, and productivity make good environmental sense and economic sense. Because organic farming requires more land for every calorie or pound produced, a large-scale shift to organic farming would entail converting more forest and other land to farming, resulting in greater habitat loss and more greenhouse gas emissions. And while organic farming doesn’t use synthetic pesticides or fertilizers, it often results in greater nitrogen pollution because manure is a highly inefficient way to deliver nutrients to crops.

Another benefit of large-scale U.S. farms is that because they are so efficient, economically and environmentally, they are also able to produce vastly more food than Americans can consume, making the country the world’s largest agricultural exporter as well.

That benefits the U.S. economy, of course, but it also comes with an environmental benefit for the world. In the contemporary environmental imagination, highly productive, globally traded agriculture is a bad thing—poisoning the land at home and undermining food sovereignty abroad. But in reality, a pound of grain or beef exported from the United States almost always displaces a pound that would have been produced with more land and greenhouse gas emissions somewhere else.

### AT: Financialization---1AR

#### No market complexity or financialization.

Hung Tran 19, nonresident senior fellow with the Atlantic Council and a former executive managing director of the Institute of International Finance, with; Jaime Caruana, former general manager at Bank for International Settlements, is a member of the board of directors at BBVA, 4/9/19, “Diversity builds financial resilience,” https://www.atlanticcouncil.org/blogs/new-atlanticist/diversity-builds-financial-resilience/

The diversity of financial institutions, with their differences in business models, liability structures, time horizons, and investment motivations could contribute greatly to financial resilience. Since the 2008 crisis, financial institutional diversity has helped sustain market liquidity while banks have curtailed their market-making activity [a readiness to buy and sell securities to accommodate their clients] due to regulatory changes and business strategies. Improving resiliency and liquidity in financial markets is critical to better finance the real economy, allocate risks properly, and support financial stability.

Many financial institutions and practices, together with regulatory and accounting requirements, however, tend to exacerbate cyclical fluctuations in the economy by buying assets or extending credit in good times and cutting back in bad times. It is important, therefore, to promote financial diversity and foster counter-cyclical behaviors among institutions capable of doing so. This helps reduce the risk of market imbalances leading to liquidity crises and offset self-reinforcing dynamics in times of financial stress. This risk has become important to guard against as the International Monetary Fund’s just-released World Economic Outlook finds the global economy entering a synchronized slowing phase.

The idea is to exploit the natural differences in the balance sheet structures of financial institutions like banks and investment funds on the one hand, and insurance companies and pension funds on the other, and develop regulatory and accounting regimes that encourage diversity of behaviors.

Banks and investment funds have a positive duration gap in their balance sheets—meaning the average duration of their assets tends to be longer than that of their liabilities. Consequently, banks and investment funds tend to act in a pro-cyclical manner. When asset quality deteriorates, prices fall, and interest rates rise, the value of banks’ assets declines by more than that of their liabilities. Regulatory capital and liquidity requirements increase under those circumstances, pressuring banks to liquidate falling assets.

Investment funds can sell into falling markets to meet redemption demand, according to research by the Bank for International Settlements. Funds can also buy and sell at the same time if they use similar investment strategies, sharing economic and market views.

The pro-cyclical practices described above can be ameliorated to some extent by regulations requiring higher capital and liquidity ratios for banks as well as heightened liquidity risk management. Better capitalized banks with sufficient liquidity can arguably contribute less, but more reliable, market liquidity—compared with the very liquid pre-crisis market conditions driven by high leverage, which turned out to be illusionary. Funds can also maintain adequate cash positions to meet possible redemption demand. In any event, pro-cyclicality remains a natural tendency for those institutions and needs to be managed.

By contrast, insurance companies and pension funds have a negative duration gap in their balance sheets and, under some circumstances, could play a stabilizing role in mitigating selling pressure. As their average asset duration is much shorter than that of their liabilities, when rates rise, the value of their assets fall by less than that of their liabilities. This strengthens their solvency, allowing them to acquire assets having fallen in prices. They thus can act in a counter-cyclical manner. However, some research indicates that this counter-cyclical behavior may need to be further supported. The International Monetary Fund’s Global Financial Stability Report observed that life insurance companies—but not property and casualty insurers—and pension funds act counter-cyclically in liquidity crises, but pro-cyclically in solvency crises.

More recent empirical research, using recently available granular data on security-by-security holdings by EU institutional investors, shows that their behavior is more nuanced. Overall, insurers and pension funds behaved in a counter-cyclical manner, but the intensity of such effect has weakened since the pre-crisis period. Other preliminary research notes that the counter-cyclical behavior of insurers and pension funds can be observed for safe assets whose value can be discounted by the same risk-free rate used for liabilities. However, these institutions tend to pro-cyclically reduce holding of risk assets, including equities and corporate bonds, as their values tend to fall by more than liabilities in a market correction.

Regulators should encourage insurers and pension funds to make more use of the counter-cyclical measures provided in the EU insurance regulatory regime Solvency II—as highlighted by the European Insurance and Occupational Pension Authority. While interventions by government authorities are necessary to stabilize severe financial turmoil, more counter-cyclical behaviors by insurers and pension funds, many of which likely stay resilient in a crisis, can help reduce the frequency and severity of financial crises. Remember: during the Great Depression in the United States and its aftermath, some 7,000 banks failed but most of the insurers remained financially healthy.

### AT: CCS Bad---1AR

#### ONLY CCS solves irreversible climate change---BUT market incentives and trading is key to overcome financial barriers.

Deanna D'Alessandro 21, Deanna Michelle D'Alessandro is an Australian chemist who is a Professor and Australian Research Council Future Fellow at the University of Sydney. “Engineers have built machines to scrub carbon dioxide from the air. Will it halt climate change?,” Phys.org, 1-21-2021, https://phys.org/news/2021-01-built-machines-carbon-dioxide-air.html

On Wednesday this week, the concentration of carbon dioxide in the atmosphere was measured at 415 parts per million (ppm). The level is the highest in human history, and is growing each year.

Amid all the focus on emissions reduction, the Intergovernmental Panel on Climate Change (IPCC) says [emissions reductions] will not be enough to avoid dangerous levels of global warming. The world must actively remove historical CO2 already in the atmosphere—a process often described as "negative emissions."

CO2 removal can be done in two ways. The first is by enhancing carbon storage in natural ecosystems, such as planting more forests or storing more carbon in soil. The second is by using direct air capture (DAC) technology that strips CO2 from the ambient air, then either stores it underground or turns it into products.

US research published last week suggested global warming could be slowed with an emergency deployment of a fleet of "CO2 scrubbers" using DAC technology. However a wartime level of funding from government and business would be needed. So is direct air capture worth the time and money?

What's DAC all about?

Direct air capture refers to any mechanical system capturing CO2 from the atmosphere. Plants operating today use a liquid solvent or solid sorbent to separate CO2 from other gases.

Swiss company Climeworks operates 15 direct air capture machines across Europe, comprising the world's first commercial DAC system. The operation is powered by renewable geothermal energy or energy produced by burning waste.

The machines use a fan to draw air into a "collector," inside which a selective filter captures CO2. Once the filter is full, the collector is closed and the CO2 is sequestered underground.

Direct air capture of CO2 will be needed to address climate change.

Canadian company Carbon Engineering uses giant fans to pull air into a tower-like structure. The air passes over a potassium hydroxide solution which chemically binds to the CO2 molecules, and removes them from the air. The CO2 is then concentrated, purified and compressed.

Captured CO2 can be injected into the ground to extract oil, in some cases helping to counteract the emissions produced by burning the oil.

The proponents of the Climeworks and Carbon Engineering technology say their projects are set for large-scale investment and deployment in coming years. Globally, the potential market value of DAC technology could reach US$100bn by 2030, on some estimates.

Big challenges ahead

Direct air capture faces many hurdles and challenges before it can make a real dent in climate change.

DAC technology is currently expensive, relative to many alternative ways of capturing CO2, but is expected to become cheaper as the technology scales up. The economic feasibility will be helped by the recent emergence of new carbon markets where negative emissions can be traded.

DAC machines process an enormous volume of air, and as such are very energy-intensive. In fact, research has suggested direct air capture machines could use a quarter of global energy in 2100. However new DAC methods being developed could cut the technology's energy use.

While the challenges to direct air capture are great, the technology uses less land and water than other negative emissions technologies such as planting forests or storing CO2 in soils or oceans.

DAC technology is also increasingly gaining the backing of big business. Microsoft, for example, last year included the technology in its carbon negative plan.

Artist impression of a DAC facility to be built in the US state of Texas. If built, it would be the largest of its kind in the world. Credit: Carbon Engineering

Opportunities for Australia

Australia is uniquely positioned to be a world leader in direct air capture. It boasts large areas of land not suitable for growing crops. It has ample sunlight, meaning there is great potential to host DAC facilities powered by solar energy. Australia also has some of the world's best sites in which to "sequester" or store carbon in underground reservoirs.

Direct air capture is a relatively new concept in Australia. Australian company Southern Green Gas, as well as the CSIRO, are developing solar-powered DAC technologies. The SGG project, with which I am involved, involves modular units potentially deployed in large numbers, including close to sites where captured CO2 can be used in oil recovery or permanently stored.

If DAC technology can overcome its hurdles, the benefits will extend beyond tackling climate change. It would create a new manufacturing sector and potentially re-employ workers displaced by the decline of fossil fuels.

Looking ahead

The urgency of removing CO2 from the atmosphere seems like an enormous challenge. But not acting will bring far greater challenges: more climate and weather extremes, irreversible damage to biodiversity and ecosystems, species extinction and threats to health, food, water and economic growth.

DAC technology undoubtedly faces stiff headwinds. But with the right policy incentives and market drivers, [DAC] may be one of a suite of measures that start reversing climate change.

### No Mindset Shift---1AR

#### Economic incentives and elites push for return to normal

Small '20 [Mike; 4/8/20; contributor to Enough, editor of Bella Caledonia magazine; "Degrowth and Our Post-COVID Future," https://enough.scot/2020/04/08/degrowth-and-our-post-covid-future/]

The demand to “return to normal” and decimate all of the ecological social and cultural gains will be overwhelming.

We will be complicit in this “return” unless we can articulate a response.

The dark tragedy is this:

We have been catapulted to the future we demanded and are presented with vast opportunity to create a radically different and ecologically viable economy. But all of the forces in society that benefited from the pre-covid world are working for a fast return to radical unsustainability and uncertainty.

Elite forces want us to return as soon as possible to a world hurtling to climate disaster, extreme inequality and hierarchy, pointless and useless work and endless growth. Capital wants us to return as quick as possible to constant consumption and mindless economic activity. We must resist this will all the force we can manage and with all of the enlightenment we have glimpsed at in our experience of lockdown.

#### No mindset shift – material consumption is hardwired and won’t be overcome by external slowdown – COVID proves

Bhar '20 [Soumyajit; 4/21/20; PhD scholar from the Ashoka Trust for Research in Ecology and the Environment, research fellow at LEAD at Krea University; "Degrowth and COVID-19: Are we drawing a simplistic connection?" https://india.mongabay.com/2020/04/commentary-degrowth-and-covid-19-are-we-drawing-a-simplistic-connection/]

COVID-19 economic pause: Can we equate with degrowth?

Many scholars are comparing the current state of the economy with the state of degrowth. However, I argue this comparison is not only conceptually incorrect but also simplistic. At first, we need to acknowledge that the pandemic is an external, independent factor that is inducing such a drastic downshift in the economy. There is no change happening at the systemic level to ensure the sustainability of such a shift.

Such a pandemic is denoted as an upshot of climate crisis and disruption in the ecological balance. In the coming future, with resorting to business as usual, such external events are likely to be frequent and intense. However, once we manage to find our way around such an external factor, even if temporarily, the economy is waiting to bounce back to its normal. Moreover, as observed in the post-world war II economic boom, the economy is likely to reach a higher throughput than the initial after the lockdown.

To sustain the drastic downshift of the economy that resembles degrowth, consumers have a major role to play in the realisation of such a massive economic shift as the current capitalist economy is entirely fueled by consumer desires. In our lives, we consciously or at times unconsciously uphold a notion of a good life. This amicable notion guides us continuously in making decisions, be it life-changing ones or concerning everyday affairs.

My research, as well as several anthropological studies, show how the prevailing notions of the good life have slowly turned into being materialistic. It means now we use material goods to earn status, construct identities, and mark success and value them over intangible things like relationships.

Our life stories are now stitched around material possessions that we carefully choose. These notions are socio-culturally constructed. One’s social upbringing and conditioning enable the seeping of certain notions of good life over others. These socio-culturally construed notions are influenced by the economic climate to give rise to insatiable desires or false needs among consumers.

Upshots of COVID-19- a welcome push towards practising degrowth

To achieve a sustained state of degrowth, we as consumers need to realize the intricate interconnection between our constructed notions of a good life and our consumption decision. A realisation of how we as consumers are turned into this driving force, that is running the entire economic juggernaut by discounting ecological balance and a consequent conscious decision to move away from it, would be the first step to degrowth.

As the second step, we need to ensure that the wealth produced in degrowth or controlled growth of the economy should entirely be diverted to ensuring a good life for the socio-economically underprivileged ones, which requires a certain amount of sacrifice from the privileged sections of the society. However, this would not appear as a sacrifice if we can adopt alternative notions of a good life that value the current state of the environment and social justice over a world obsessed with material possessions and growth.

A sustained change in the economic system can only come if the main internal driving force of the system – consumers – starts valuing things that the current system cannot simply offer. It is going to be a slow socio-cultural shift, but that seems to be the only way to realise a sustained change.

### Space Col---1AR

#### Colonization solves inevitable extinction.

Kovic '19 [Marko; March 2019; co-founder president of the Zurich Institute of Public Affairs Research; "The future of energy," https://osf.io/preprints/socarxiv/aswz9/download]

Existential risks are risks that might lead to the extinction of humankind [1]. Natural existential risks (such as asteroids that might crash into Earth) are basically constant. The risks of a giant asteroid crashing into Earth today is the same as it was 500 years ago. Anthropogenic, man-made existential risks, on the other hand, are growing in number and severity. They are a side-effect of technological progress: The more we develop technologically, the greater man-made existential risks become. Nuclear weapons, to name only one example, are a direct consequence of scientific and technological progress.

There are different approaches to existential risk mitigation. One approach is to develop targeted strategies for specific existential risks. If we want to reduce the existential risk posed by nuclear weapons, then we can and should develop specific strategies for that risk.

Another approach is to develop and pursue what can be called meta-strategies that target all existential risks at once. One of most effective meta-strategies for tackling existential risks in general is space colonization: If we manage to establish permanent and self-sustainable human habitats beyond Earth, then our proverbial existential eggs are not all in one basket anymore. For example, if disaster strikes on Earth, but there are billions of humans living on Venus and Mars, humankind would continue to exist even with Earth-humans gone.

Because of existential risks, a long-term future in which humankind still exists almost certainly has to be a future in which humankind has succeeded in colonizing space. Today, even though we regularly venture into space, we do not yet have space colonization capabilities. There are a number of technological challenges that we need to overcome in order to become capable of space colonization. One of those challenges is energy. There are several reasons why.

#### Disease doesn’t cause extinction.

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

However, there are some reasons to think that naturally occurring pathogens are unlikely to cause human extinction. Firstly, Homo sapiens have been around for 200,000 years and the Homo genus for around six million years without being exterminated by an infectious disease, which is evidence that the base rate of extinction-risk natural pathogens is low.82 Indeed, past disease outbreaks have not come close to rendering humans extinct. Although bodies were piled high in the streets across Europe during the Black Death,83 human extinction was never a serious possibility, and some economists even argue that it was a boon for the European economy.84 Secondly, infectious disease has only contributed to the extinction of a small minority of animal species.85 The only confirmed case of a mammalian species extinction being caused by an infectious disease is a type of rat native only to Christmas Island. Having said that, the context may be importantly different for modern day humans, so it is unclear whether the risk is increasing or decreasing. On the one hand, due to globalisation, the world is more interconnected making it easier for pathogens to spread. On the other hand, interconnectedness could also increase immunity by increasing exposure to lower virulence strains between subpopulations.87 Moreover, advancements in medicine and sanitation limit the potential damage an outbreak might do.

### AT: Spacecol Fails---1AR

#### Fourth wave of science solves

**Kaku 18** [Michio, an American theoretical physicist, futurist, and popularizer of science. He is a professor of theoretical physics in the City College of New York and CUNY Graduate Center. “There's Only One Way For Humanity to Survive. Go To Mars.,” <https://news.nationalgeographic.com/2018/02/there-s-only-one-way-for-humanity-to-survive--go-to-mars-/>]

You use the phrase “the fourth wave of science.” Explain what this means and how it could one day make it possible to terraform Mars. We’ve had three waves of scientific innovation. The first wave, the Industrial Revolution, gave us the steam engine, the locomotive, and factories. The second wave was electricity and magnetism, whereby we had TV, internal combustion cars, a beginning of the space program. The third revolution is high tech: computers, lasers, the Internet. Now we have the fourth wave of innovation: artificial intelligence, biotech, and nanotech. That’s going to change the way we view Mars. Many people say Mars is cold and desolate, and there’s nothing to grow there. We can genetically modify plants and algae to thrive in the Martian atmosphere. But who’s going to do the heavy lifting? We all would like to see futuristic cities on Mars, but robots are going to become much more adapted to working in these harsh environments by the end of this century, so we expect to see robotic construction workers building the fantastic domed cities you see in science fiction novels.

### AT: Spacecol Bad---1AR

#### Inter-planetary conflict is science fiction

**Ćirković 19** [Milan, Corresponding author at: Future of Humanity Institute, Faculty of Philosophy, University of Oxford, “Space colonization remains the only long-term option for humanity: A reply to Torres,” [https://www.sciencedirect.com/science/article/pii/S0016328718302222#](https://www.sciencedirect.com/science/article/pii/S0016328718302222)!]

4. Interstellar warfare: fantasy and real fantasy Even if we accept – in spirit, if not in words – Clarke’s Third Law (“any sufficiently advanced technology is indistinguishable from magic”; Clarke, 1999), the inverse does not hold: there are infinitely many conceivable “magical” effects which could not be realized with any advanced technology under the known laws of physics. As stated above, it is doubtful, to say at least, that there ever will be a “galaxy destroying weapon”, irrespectively of how much time and effort is expended. The influence of science fictional discourse, while in general beneficial for futures studies, becomes at this point perhaps too strong (especially in a rather naïve, Star Wars- or Starship Troopers-like manner). The discussion might be finished here, since it seems unreasonable to engage in such extreme speculation; so, a few comments in the rest of this section should be taken with reservations. Although there have not been serious strategic studies of the topic, there are many indications that the “interstellar warfare” is an oxymoron. Insofar as there are no topological shortcuts in forms of traversable wormholes (and even if there are some, but with fixed points of entrance and egress), there is a large delay and logistic nightmare in sending any military expeditions across interstellar distances. Except in the case of huge technological imbalance – which is possible in contact between (post)human and some extraterrestrial civilization, but highly unlikely if not impossible between any two (post)human factions – the defense of planetary systems would have overwhelming advantage, measured by orders of magnitude in both reconnaissance, logistics, and capacity for tactical concentration of forces. Above all, the defenders could easily destroy any non-stellar resources in the defended system if their situation becomes desperate enough, so that “piracy and plunder” would simply not be viable options in the interstellar case. And, if the desired resources consist of uplifted stellar matter, there would always be billions of undefended stars in the Galaxy. (This would be valid even if the efficiency of colonization is 99%. In the unlikely scenario that all stars in the Galaxy are colonized and defended, which is perhaps in itself incompatible with the Torres’s argument, since the constant destructive warfare will likely impede or arrest the colonization efforts, the required timescale is so long that it will perhaps make more economic and strategic sense to go after undefended resources in other Local Group galaxies.) In brief, plunder is hardly viable as a motivation for interstellar warfare. A reasonable conclusion that interstellar travel will always be expensive and difficult, coupled with the defensive advantages and the total abundance of undefended cosmic resources elsewhere, makes this motivation of “Machiavellian actors” largely irrelevant. “Tuckerian actors” have been dealt with in the Section 2 above. Finally, there remains the option of warfare for the sake of spreading particular “bad memes” (Zubrin, 1999). If this kind of motivation requires the same expenditure of time and resources required for the interstellar travel (not to mention intergalactic travel, which is an entirely different order of magnitude problem, with additional difficulties, like the impossibility of gathering any fuel or resources en route), it is reasonable to conclude that such instances would be rare. Of course, it is impossible to eliminate the possibility that particularly virulent political or religious movements will emerge in the distant future, leading to an overwhelming motivation for spreading The Word by fire and sword even in the face of unfavorable strategic odds. This seems improbable, however, for at least two reasons. (i) The relevant “bad memes” will certainly be easier to spread by other means, notably modulated radiation and inscribed matter packages, in forms of self-reproducing software or other virulent forms, which might be violent in a generalized sense, but still would not entail any of the drastic scenarios of destruction invoked by Torres. Insofar human history is any guide, while religions are stronger in the contemporary world than they have been for the last couple of centuries, this is manifested by televangelists rather than crusades.7 (ii) The immunization against such bad memes is quite likely to improve by many orders of magnitude, just as new computer viruses always provoke stronger and more efficient immunization response. In this sense, the conclusions of Pinker (2011) seem fully vindicated; and they are certainly more appropriate for the interstellar case.

#### We’re alone --- studies prove

---esp true given no alien observation and uncertainty in Drake parameters.

Sandberg et al 18 [Andres Sandberg, Future of Humanity Institute researcher, PhD in computational neuroscience from Stockholm University.] “Dissolving the Fermi Paradox” 6 June 2018 (<https://arxiv.org/abs/1806.02404>) – MZhu

Our argument so far is related to a recent argument sketched by Max Tegmark [34]. Like us, he suggests that we should have great uncertainty about f\_l and f\_i, making us very uncertain about the probability of intelligent life arising around a given star. He thus models our uncertainty over the average distance between two independently arising intelligent civilizations as log-uniform. That is, we should be no more surprised if this average distance were at one order of magnitude rather than another. Thus, when we gain some evidence that there is no other civilization within our galaxy, we update this prior by greatly lowering our credence in the average distance being less than this (≈10^21 m). Since there are only six orders of magnitude from the radius of our galaxy to the radius of the observable universe (≈10^27 m) and infinitely many beyond that, he reaches a conclusion that it is unlikely for two civilizations to arise within the same observable universe. Brian Lacki has suggested an improvement to Tegmark’s model, in which the log-uniform prior is replaced with a bounded log-log-uniform prior [35].

Our argument shares the same broad outline. But rather than starting with a very abstract prior representing initial radical uncertainty over more than 10^100 orders of magnitude, we used two different methods to provide a prior that captured the existing scientific uncertainties of tens or hundreds of orders of magnitude. We have seen how this is more than enough make an empty observable universe plausible ex ante (dissolving the Fermi paradox), and quite likely once we account for the Fermi observation.

5 Updating the factors

So far we have looked at how the Fermi observation affects our credence in N. We can go further than this and examine how it affects our credence in each of the Drake parameters. Updating on the Fermi observation reduces the expectation of all the parameters. However, parameters with broad distributions (those with the most uncertainty) tend to have their expectation reduced far more than parameters with tight distributions (see Supplement IV).

All the observations we consider have a strong effect on our estimates for f\_l , a substantially weaker effect on our estimates for L, and almost no effect on our estimates of the more certain astrophysical factors. As we can see in Table 2, the observations reduce the median for fl by between a factor of 7 and factor of 10^37, while the median for L is only reduced by a factor between 1 and 2.

Given the state of scientific uncertainty about the Drake parameters and the Fermi observation, the default guess should hence be that the low-probability term is likely in the past (fl) rather than the future (fc, L). The Fermi observation thus provides only very weak evidence about whether we will soon go extinct or whether interstellar communication or travel is impossible. Instead, the observation mainly just increases our credence that life is rare.

This conclusion is quite robust to changing the log-uncertainties of the factors (it remains as long as most uncertainty is in the past factors) or their distribution shape (using log-normals instead of log-uniform distribution has no effect). The conclusion can be changed if we reduce the uncertainty of past terms to less than just 7 orders of magnitude, or if the f\_c factor turns out to be radically uncertain.

6 Conclusion

We have seen that a Fermi paradox arises if we combine a high and extremely confident prior for the number of civilizations in our galaxy with the absence of evidence for their existence. The high confidence that causes this clash typically results from applying a Drake-like model using point estimates for the parameters. These estimates, however, make implicit knowledge claims about processes (especially those connected with the origin of life) which are untenable given the current state of scientific knowledge.

When we take account of realistic uncertainty, replacing point estimates by probability distributions that reflect current scientific understanding, we find no reason to be highly confident that the galaxy (or observable universe) contains other civilizations, and thus no longer find our observations in conflict with our prior probabilities. We found qualitatively similar results through two different methods: using the authors’ assessments of current scientific knowledge bearing on key parameters, and using the divergent estimates of these parameters in the astrobiology literature as a proxy for current scientific uncertainty.

When we update this prior in light of the Fermi observation, we find a substantial probability that we are alone in our galaxy, and perhaps even in our observable universe (53%–99.6% and 39%–85% respectively). ’Where are they?’ — probably extremely far away, and quite possibly beyond the cosmological horizon and forever unreachable.

#### No interstellar travel means no aliens

Wright and Oman-Reagan 18 [Jason Wright, Department of Astronomy & Astrophysics and Center for Exoplanets and Habitable Worlds. Michael Oman-Reagan, Department of Anthropology, Memorial University.] “Visions of Human Futures in Space and SETI” International Journal of Astrobiology, vol. 17, no. 02, pp. 177–188 (<https://doi.org/10.1017/S1473550417000222>) – MZhu

To illustrate this another way, a foundational concept in SETI, the Drake Equation, contains a final term, “L”, representing the length of time a civilization may be transmitting signals, or the “lifetime” of a civilization (Drake, 1980; Shostak, 2011). A civilization that is destroyed (whether by self-destruction or some external cataclysm) will probably not be actively communicating, and so the opportunities for detecting alien civilizations are extremely sensitive to this term. But spaceflight enables a civilization to spread beyond its birthplace, inoculating it against many forms of annihilation and multiplying the number of potential transmission sites (e.g. Wright et al., 2014). The success of SETI is thus strongly dependent on the prior success of interstellar spaceflight and settlement by alien species. Indeed, interstellar spacecraft themselves may be a signal detectable via SETI (Yurtsever and Wilkinson, 2015; Lingam and Loeb, 2017).

### Nuclear War Causes Extinction---2AC/1AR

#### Even a small nuclear war causes extinction and destroys the ozone

Starr 14 [Steven Starr, the Senior Scientist for Physicians for Social Responsibility and Director of the Clinical Laboratory Science Program at the University of Missouri. Starr has published in the Bulletin of the Atomic Scientists and the Strategic Arms Reduction (STAR) website of the Moscow Institute of Physics and Technology, June 11, 2014, “There Can be No Winners in a Nuclear War”, Truth Out, [https://truthout.org/articles/there-can-be-no-winners-in-a-nuclear-war](https://truthout.org/articles/there-can-be-no-winners-in-a-nuclear-war/)]

Nuclear war has no winner. Beginning in 2006, several of the world’s leading climatologists (at Rutgers, UCLA, John Hopkins University, and the University of Colorado-Boulder) published a series of studies that evaluated the long-term environmental consequences of a nuclear war, including baseline scenarios fought with merely 1% of the explosive power in the US and/or Russian launch-ready nuclear arsenals. They concluded that the consequences of even a “small” nuclear war would include catastrophic disruptions of global climate and massive destruction of Earth’s protective ozone layer. These and more recent studies predict that global agriculture would be so negatively affected by such a war, a global famine would result, which would cause up to 2 billion people to starve to death. These peer-reviewed studies – which were analyzed by the best scientists in the world and found to be without error – also predict that a war fought with less than half of US or Russian strategic nuclear weapons would destroy the human race. In other words, a US-Russian nuclear war would create such extreme long-term damage to the global environment that it would leave the Earth uninhabitable for humans and most animal forms of life. A recent article in the Bulletin of the Atomic Scientists, “Self-assured destruction: The climate impacts of nuclear war,” begins by stating: “A nuclear war between Russia and the United States, even after the arsenal reductions planned under New START, could produce a nuclear winter. Hence, an attack by either side could be suicidal, resulting in self-assured destruction.” In 2009, I wrote “Catastrophic Climatic Consequences of Nuclear Conflicts” for the International Commission on Nuclear Non-proliferation and Disarmament. The article summarizes the findings of these studies. It explains that nuclear firestorms would produce millions of tons of smoke, which would rise above cloud level and form a global stratospheric smoke layer that would rapidly encircle the Earth. The smoke layer would remain for at least a decade, and it would act to destroy the protective ozone layer (vastly increasing the UV-B reaching Earth) as well as block warming sunlight, thus creating Ice Age weather conditions that would last 10 years or longer. Following a US-Russian nuclear war, temperatures in the central US and Eurasia would fall below freezing every day for one to three years; the intense cold would completely eliminate growing seasons for a decade or longer. No crops could be grown, leading to a famine that would kill most humans and large animal populations. Electromagnetic pulse from high-altitude nuclear detonations would destroy the integrated circuits in all modern electronic devices, including those in commercial nuclear power plants. Every nuclear reactor would almost instantly meltdown; every nuclear spent fuel pool (which contain many times more radioactivity than found in the reactors) would boil off, releasing vast amounts of long-lived radioactivity. The fallout would make most of the US and Europe uninhabitable. Of course, the survivors of the nuclear war would be starving to death anyway. Once nuclear weapons were introduced into a US-Russian conflict, there would be little chance that a nuclear holocaust could be avoided. Theories of “limited nuclear war” and “nuclear de-escalation” are unrealistic. In 2002 the Bush administration modified US strategic doctrine from a retaliatory role to permit preemptive nuclear attack; in 2010, the Obama administration made only incremental and miniscule changes to this doctrine, leaving it essentially unchanged. Furthermore, Counterforce doctrine – used by both the US and Russian military – emphasizes the need for preemptive strikes once nuclear war begins. Both sides would be under immense pressure to launch a preemptive nuclear first-strike once military hostilities had commenced, especially if nuclear weapons had already been used on the battlefield. Both the US and Russia each have 400 to 500 launch-ready ballistic missiles armed with a total of at least 1800 strategic nuclear warheads, which can be launched with only a few minutes warning. Both the US and Russian Presidents are accompanied 24/7 by military officers carrying a “nuclear briefcase,” which allows them to transmit the permission order to launch in a matter of seconds. Yet top political leaders and policymakers of both the US and Russia seem to be unaware that their launch-ready nuclear weapons represent a self-destruct mechanism for the human race. For example, in 2010, I was able to publicly question the chief negotiators of the New START treaty, Russian Ambassador Anatoly Antonov and (then) US Assistant Secretary of State Rose Gottemoeller, during their joint briefing at the UN (during the Non-Proliferation Treaty Review Conference). I asked them if they were familiar with the recent peer-reviewed studies that predicted the detonation of less than 1% of the explosive power contained in the operational and deployed US and Russian nuclear forces would cause catastrophic changes in the global climate, and that a nuclear war fought with their strategic nuclear weapons would kill most people on Earth. They both answered “no.” More recently, on April 20, 2014, I asked the same question and received the same answer from the US officials sent to brief representatives of the NGOS at the Non-Proliferation Treaty Preparatory Committee meeting at the UN. None of the US officials at the briefing were aware of the studies. Those present included top officials of the National Security Council. It is frightening that President Obama and his administration appear unaware that the world’s leading scientists have for years predicted that a nuclear war fought with the US and/or Russian strategic nuclear arsenal means the end of human history. Do they not know of the existential threat these arsenals pose to the human race . . . or do they choose to remain silent because this fact doesn’t fit into their official narratives? We hear only about terrorist threats that could destroy a city with an atomic bomb, while the threat of human extinction from nuclear war is never mentioned – even when the US and Russia are each running huge nuclear war games in preparation for a US-Russian war. Even more frightening is the fact that the neocons running US foreign policy believe that the US has “nuclear primacy” over Russia; that is, the US could successfully launch a nuclear sneak attack against Russian (and Chinese) nuclear forces and completely destroy them. This theory was articulated in 2006 in “The Rise of U.S. Nuclear Primacy,” which was published in Foreign Affairs by the Council on Foreign Relations. By concluding that the Russians and Chinese would be unable to retaliate, or if some small part of their forces remained, would not risk a second US attack by retaliating, the article invites nuclear war. Colonel Valery Yarynich (who was in charge of security of the Soviet/Russian nuclear command and control systems for 7 years) asked me to help him write a rebuttal, which was titled “Nuclear Primacy is a Fallacy.” Colonel Yarynich, who was on the Soviet General Staff and did war planning for the USSR, concluded that the “Primacy” article used faulty methodology and erroneous assumptions, thus invalidating its conclusions. My contribution lay in my knowledge of the recently published (in 2006) studies, which predicted even a “successful” nuclear first-strike, which destroyed 100% of the opposing side’s nuclear weapons, would cause the citizens of the side that “won” the nuclear war to perish from nuclear famine, just as would the rest of humanity.

#### Ozone independently causes extinction

**Greenpeace 95** – Environmental Organization (“Full of Holes: Montreal Protocol and the Continuing Destruction of the Ozone Layer -- A Greenpeace Report with contributions from Ozone Action, http://archive.greenpeace.org/ozone/holes/holebg.html)

When chemists Sherwood Rowland and Mario Molina first postulated a link between chlorofluorocarbons and ozone layer depletion in 1974, the news was greeted with scepticism, but taken seriously nonetheless. The vast majority of credible scientists have since confirmed this hypothesis. The ozone layer around the Earth shields us all from harmful ultraviolet radiation from the sun. Without the ozone layer, life on earth would not exist. Exposure to increased levels of ultraviolet radiation can cause cataracts, skin cancer, and immune system suppression in humans as well as innumerable effects on other living systems. This is why Rowland's and Molina's theory was taken so seriously, so quickly - the stakes are literally the continuation of life on earth.

#### Err aff---nuclear war is under-researched and secondary effects ensure extinction

Seth Baum 15, Executive Director of the Global Catastrophic Risk Institute (gcrinstitute.org), a nonprofit think tank that he co-founded in 2011. His research focuses on risk, ethics, and policy questions for major risks to human civilization including nuclear war, global warming, and emerging technologies. Dr. Baum received a Ph.D. in geography from Pennsylvania State University with a dissertation on climate change policy. He then completed a post-doctoral fellowship with the Columbia University Center for Research on Environmental Decisions. His research has appeared in many journals including Ecological Economics, Science and Engineering Ethics, Science and Global Security, and Sustainability. He is currently co-editor of a special issue of the journal Futures titled “Confronting future catastrophic threats to humanity.”, “The Risk of Nuclear Winter”, FAS, May 29 2015, <https://fas.org/pir-pubs/risk-nuclear-winter/>

Since the early 1980s, the world has known that a large nuclear war could cause severe global environmental effects, including dramatic cooling of surface temperatures, declines in precipitation, and increased ultraviolet radiation. The term nuclear winter was coined specifically to refer to cooling that result in winter-like temperatures occurring year-round. Regardless of whether such temperatures are reached, there would be severe consequences for humanity. But how severe would those consequences be? And what should the world be doing about it? To the first question, the short answer is nobody knows. The total human impacts of nuclear winter are both uncertain and under-studied. In light of the uncertainty, a risk perspective is warranted that considers the breadth of possible impacts, weighted by their probability. More research on the impacts would be very helpful, but we can meanwhile make some general conclusions. That is enough to start answering the second question, what we should do. In regards to what we should do, nuclear winter has some interesting and important policy implications. Today, nuclear winter is not a hot topic but this was not always the case: it was international headline news in the 1980s. There were conferences, Congressional hearings, voluminous scientific research, television specials, and more. The story is expertly captured by Lawrence Badash in his book A Nuclear Winter’s Tale.1)Much of the 1980s attention to nuclear winter was driven by the enthusiastic efforts of Carl Sagan, then at the height of his popularity. But underlying it all was the fear of nuclear war, stoked by some of the tensest moments of the Cold War. When the Cold War ended, so too did attention to nuclear winter. That started to change in 2007, with a new line of nuclear winter research2) that uses advanced climate models developed for the study of global warming. Relative to the 1980s research, the new research found that the smoke from nuclear firestorms would travel higher up in the atmosphere, causing nuclear winter to last longer. This research also found dangerous effects from smaller nuclear wars, such as an India-Pakistan nuclear war detonating “only” 100 total nuclear weapons. Two groups—one in the United States3) and one in Switzerland4)—have found similar results using different climate models, lending further support to the validity of the research. Some new research has also examined the human impacts of nuclear winter. Researchers simulated agricultural crop growth in the aftermath of a 100-weapon India-Pakistan nuclear war.5)The results are startling- the scenario could cause agriculture productivity to decline by around 10 to 40 percent for several years after the war. The studies looked at major staple crops in China and the United States, two of the largest food producers. Other countries and other crops would likely face similar declines. Following such crop declines, severe global famine could ensue. One study estimated the total extent of the famine by comparing crop declines to global malnourishment data.6) When food becomes scarce, the poor and malnourished are typically hit the hardest. This study estimated two billion people at risk of starvation. And this is from the 100-weapon India-Pakistan nuclear war scenario. Larger nuclear wars would have more severe impacts. This is where the recent research stops. To the best of my knowledge there are no recent studies examining the secondary effects of famines, such as disease outbreaks and violent conflicts. There are no recent studies examining the human impacts of ultraviolet radiation. That would include an increased medical burden in skin cancer and other diseases. It would also include further loss of agriculture ecosystem services as the ultraviolet radiation harms plants and animals. At this time, we can only make educated guesses about what these impacts would be, informed in part by what research was published 30 years ago. When analyzing the risk of nuclear winter, one question is of paramount importance: Would there be permanent harm to human civilization? Humanity could have a very bright future ahead; to dim that future is the worst thing nuclear winter could do. It is vastly worse than a few billion deaths from starvation. Not that a few billion deaths is trivial—obviously it isn’t—but it is tiny compared to the loss of future generations. Carl Sagan was one of the first people to recognize this point in a commentary he wrote on nuclear winter for Foreign Affairs.7) Sagan believed nuclear winter could cause human extinction, in which case all members of future generations would be lost. He argued that this made nuclear winter vastly more important than the direct effects of nuclear war, which could, in his words, “kill ‘only’ hundreds of millions of people.” Sagan was however, right that human extinction would cause permanent harm to human civilization. It is debatable whether nuclear winter could cause human extinction. Alan Robock, a leader of the recent nuclear winter research, believes it is unlikely. He writes: “Especially in Australia and New Zealand, humans would have a better chance to survive.”8) This is hardly a cheerful statement, and it leaves open the chance of human extinction. I think that’s the best way of looking at it. Given all the uncertainty and the limited available research, it is impossible to rule out the possibility of human extinction. I don’t have a good answer for how likely it is. But the possibility should not be dismissed. Even if some humans survive, there could still be permanent harm to human civilization. Small patches of survivors would be extremely vulnerable to subsequent disasters. They also could not keep up the massively complex civilization we enjoy today. It would be a long and uncertain rebuilding process and survivors might never get civilization back to where it is now. More importantly, they might never get civilization to where we now stand poised to take it in the future. Our potentially bright future could be forever dimmed.9) Nuclear winter is a very large and serious risk. But that on its own doesn’t mean much—just another thing to worry about. What’s really important are the implications of nuclear winter for public policy and private action.

war between India and Pakistan would pose an existential threat to both countries. A larger nuclear war would threaten humanity itself. These realities make bolt-from-blue strikes much less likely and in turn, reduce the imperative for pre-emptive strikes.