**Aff**

**AT – NATO Tradeoff [G]**

**2AC – N/I/L – No Tradeoff**

**Not zero sum – NATO will just increase total resources invested because cyber defense is a priority.**

**DOD, '18** (U.S. Department of Defense; "News Conference by Secretary Mattis at NATO Headquarters, Brussels, Belgium"; ; https://www.defense.gov/News/Transcripts/Transcript/Article/1654419/news-conference-by-secretary-mattis-at-nato-headquarters-brussels-belgium/; 10-4-2018, Accessed 6-24-2022)//ILake-NoC

**Amid** many **competing priorities**, American lawmakers **did not reduce funding** for the European Deterrence Initiative **by a single cent**, instead maintaining the highest levels of commitment since the 1989 fall of the Berlin Wall. We have maintained the number of U.S. troops currently assigned to Europe while adding additional capability.

We **quickly staffed** with -- the Hub of the South at the request of our allies in Southern Europe, for we are keenly aware the dangers close to your home.

In that regard, I commend France for taking **targeted financial measures** against those responsible for the attempted terrorist attack on Paris earlier this summer and the support from Belgium and Germany for the investigation into Iran's continued malign activity.

Regarding cyber, as the secretary general just noted, cyber attacks are more frequent, they're more complex and they're more destructive. And, of course, he just got late breaking word in that regard. But this is why the United States, like the United Kingdom, Denmark, the Netherlands, Estonia, will provide national cyber contributions to help NATO fight in this important domain, **consistent with NATO's defense mandate** and as agreed by our leaders at the July summit.

This demonstrates and **enduring** American **bipartisan commitment** in Washington to keeping the fabric of our trans-Atlantic alliance strong and a clear recognition that NATO is central to American national security interests, a theme echoed across Europe and Canada.

As was abundantly clear from our detailed and extensive conversations here, NATO is also taking action, moving out on directives from our leaders summit, to include supporting our Georgian partners as they chart their own diplomatic, economic and security destiny; reforming NATO's command structure to keep this alliance fit for its time; initiating our Four 30s readiness program: 30 air squadrons, 30 ships and 30 battalions ready to be employed in under 30 days.

**2AC – I/L – AT: Baltics – Deterrence Fails**

**Conventional causes Russia Baltics escalation**

**Kühn, 18** – nonresident scholar at the Carnegie Endowment for International Peace, and the head of the arms control and emerging technologies program at the Institute for Peace Research and Security Policy at the University of Hamburg. (Ulrich Kühn, “NATO’s Options – Preventing Escalation in the Baltics,” 3-28-2018, Accessed 06-28-2022, https://carnegieendowment.org/2018/03/28/nato-s-options-pub-75883)//ILake-NoC

DETERRENCE BY DENIAL

If NATO wants to deny Russia the ability to successfully attack one or more Baltic states, it has little choice but to deploy forces on a much larger scale than it currently does. Such forces could be deployed gradually to avoid giving Russia a casus belli and to make such deployments more palatable to skeptical NATO members. The 2017 RAND study proposed deployments of around 35,000 personnel, with an additional reinforcement capability of up to about 70,000 personnel;1 this would certainly prevent a Russian military fait accompli and force Moscow to fight a bloody and drawn-out conventional war, should it attack. These deployments would also, perhaps, eliminate most of the difficulties—and some of the resulting escalation pathways—that stem from the alliance’s current need to reinforce troops rapidly and on a large scale in a crisis. In addition, these troop deployments would raise the costs to Moscow of deliberately forcing a military crisis with NATO.

While such measures might mitigate the short-term risk of deliberate Russian escalation, they would create a number of severe political trade-offs. First, a deterrence-by-denial approach would risk overstretching the delicate political consensus among NATO members about conventional deterrence and assurance. A number of member states, perhaps led by Germany and France, would not support such a policy and would seek to block it. Even more importantly, perhaps, not even the Baltic states are supportive of such a maximalist approach. While many Baltic officials and experts would like to see greater U.S. military engagement in the region, some of them are highly skeptical of the assumptions underlying the RAND war games and think that they are too pessimistic about Baltic defenses. While they would like to see a strong, unified allied response to the growing threat from Russia, they also recognize the need to avoid unnecessarily escalating general tensions with Russia.2 Also, against the background of often contentious debates within NATO about financial and military burden sharing, it would not be clear at all who would provide the necessary funds and forces for such a large military footprint. Neither the United States nor most other allies currently seem to be both willing and capable.

Second, instead of preventing deliberate Russian escalation this deterrence-by-denial approach could, in fact, reinforce Russian perceptions of insecurity. Russia would be loath to accept a NATO force that size so close to its borders. Moscow might seek to prevent NATO force deployments through various means, including, not inconceivably, by considering the preventive use of force (that is, Russia might wage a war because it could only see its position deteriorating in the future). This risk might become more acute in the early stages of a crisis when Russia could misinterpret the large-scale movement of sizable forces, such as the 70,000 personnel reinforcement the RAND study suggested, as NATO preparations for a preemptive attack on Russia. Third, large-scale conventional deployments could help further solidify Russian reliance on its nuclear deterrent and could even serve to lower Russia’s threshold for nuclear use, making the early employment of nuclear weapons more likely.

**2AC – !! – AT: Climate**

**Warming won’t be catastrophic**

Dr. Benjamin **Zycher 21**, Senior Fellow at the American Enterprise Institute, Doctorate in Economics from UCLA, Master in Public Policy from the University of California, Berkeley, and Bachelor of Arts in Political Science from UCLA, Former Senior Economist at the RAND Corporation, Former Adjunct Professor of Economics at the University of California, Los Angeles (UCLA) and at the California State University Channel Islands, and Former Senior Economist at the Jet Propulsion Laboratory, California Institute of Technology, “The Case for Climate Change Realism”, 6/21/2021, https://www.aei.org/articles/the-case-for-climate-change-realism/

CLIMATE TRENDS

Beyond exhibiting **extreme overconfidence** in a **cherry-picked analysis** of climate-change causes, politicians and activists frequently ground their **alarmism** in **frightening predictions** about consequences that are likewise **far from certain**. This is not only true within the very new (and still quite unreliable) field of predictive climate science; it is true even in the context of ongoing climate phenomena. Indeed, politicians and journalists frequently characterize dramatic or unusual climate phenomena as the product of anthropogenic climate change, yet there is **little ev**idence to support those claims.

For one thing, there is no observable upward trend in the number of “hot” days between 1895 and 2017; 11 of the 12 years with the highest number of such days occurred before 1960. Since 2005, NOAA has maintained the U.S. Climate Reference Network, comprising 114 meticulously maintained temperature stations spaced more or less uniformly across the lower 48 states, along with 21 stations in Alaska and two stations in Hawaii. They are placed to avoid heat-island effects and other such distortions as much as possible. The **reported data** show **no increase** in average temperatures over the available 2005-2020 period. In addition, a recent reconstruction of global **temp**erature**s** over the past **1 million years** — created using data from ice-sheet formations — shows that there is **nothing unusual** about the current warm period.

Rising sea levels are another frequently cited example of impending climate crisis. And yet sea levels have been rising since at least the **mid-19th century**. This rise is tied closely with the end of the Little Ice Age that occurred not long before, which led to a rise in global temperatures, some melting of sea ice, and a thermal expansion of sea water. There is some evidence showing an acceleration in sea-level rise beginning in the early 1990s: Satellite measurements of sea levels began in 1992 and show a sea-level rise of about 3.2 millimeters per year between 1993 and 2010. Before 1992, when sea levels were measured with tidal gauges, the data showed an increase of about 1.7 millimeters per year on average from 1901 to 1990.

But because the datasets are from two different sources — satellite measurements versus tidal gauges — they are not directly comparable, and therefore they cannot be interpreted as showing an acceleration in sea-level rises. Moreover, the period beginning in 19**93** is short in terms of global climate phenomena. Since sea levels have risen at a constant rate, remained constant, or even fallen during similar relatively short periods, inferences drawn from them are **problematic**. It is of course possible there has been an acceleration in sea-level rise, but even still, it would not be clear whether such a development stemmed primarily from anthropogenic or natural causes; clearly, both processes are relevant.

A study of changes in Arctic and Antarctic sea ice yields **very different** inferences. Since 1979, Arctic sea ice has declined relative to the 30-year average (again, the degree to which this is the result of anthropogenic factors is not known). Meanwhile, Antarctic sea ice has been **growing** relative to the 30-year average, and the global sea-ice total has **remained** roughly **constant** since 1979.

Extreme weather occurrences are likewise used as evidence of an ongoing climate crisis, but again, a **study** of the **available data** undercuts that assessment. U.S. tornado activity shows either no increase or a downward trend since 1954. Data on tropical storms, hurricanes, and accumulated cyclone energy (a wind-speed index measuring the overall strength of a given hurricane season) reveal little change since satellite measurements of the phenomena began in the early 19**70s**. The number of wildfires in the United States shows no upward trend since 1985, and global acreage burned has **declined** over past decades. The Palmer Drought Severity Index shows no trend since 1895. And the IPCC’s Fifth Assessment Report, published in 2014, displays substantial divergence between its discussion of the historical evidence on droughts and the projections on future droughts yielded by its climate models. Simply put, the available data do not support the ubiquitous assertions about the causal link between greenhouse-gas accumulation, temperature change, and extreme weather events and conditions.

Unable to demonstrate that observed climate trends are due to anthropogenic climate change — or even that these events are particularly unusual or concerning — climate catastrophists will often turn to **dire predictions** about prospective climate phenomena. The problem with such predictions is that they are almost always generated by climate models driven by **highly complex sets of assumptions** about which there is **significant dispute**. Worse, these models are **notorious** for **failing** to accurately predict already documented changes in climate. As climatologist Patrick Michaels of the Competitive Enterprise Institute notes:

During **all periods** from 10 years (2006-2015) to 65 (1951-2015) years in length, the observed **temp**erature trend lies in the **lower half** of the collection of climate model simulations, and for several periods it lies very close (or even below) the **2.5th percentile** of all the model runs. Over shorter periods, such as the last two decades, a plethora of mechanisms have been put forth to explain the observed/modeled divergence, but none do so completely and many of the explanations are inconsistent with each other.

Similarly, climatologist John Christy of the University of Alabama in Huntsville observes that almost all of the 102 climate models incorporated into the Coupled Model Intercomparison Project (CMIP) — a tracking effort conducted by the Lawrence Livermore National Laboratory — **overstate** past and current temperature trends by a **factor of two to three**, and at times **even more**. It seems axiomatic to say **we should not rely on climate models** that are unable to predict the past or the present to make predictions about the distant future.

The overall temperature trend is not the only parameter the models predict poorly. As an example, every CMIP climate model predicts that increases in atmospheric concentrations of greenhouse gas should create an enhanced heating effect in the mid-troposphere over the tropics — that is, at an altitude over the tropics of about 30,000-40,000 feet. The underlying climatology is simple: Most of the tropics is ocean, and as increases in greenhouse-gas concentrations warm the Earth slightly, there should be an increase in the evaporation of ocean water in this region. When the water vapor rises into the mid-troposphere, it condenses, releasing heat. And yet the satellites cannot find this heating effect — a reality suggesting that our understanding of climate and atmospheric phenomena is **not as robust** as many seem to assume.

The **poor predictive record** of mainstream climate models is **exacerbated** by the tendency of the IPCC and U.S. government agencies to assume **highly unrealistic future increases** in greenhouse-gas concentrations. The IPCC’s 2014 Fifth Assessment Report, for example, uses four alternative “representative concentration pathways” to outline scenarios of increased greenhouse-gas concentrations yielding anthropogenic warming. These scenarios are known as RCP2.6, RCP4.5, RCP6, and RCP8.5. Since 1950, the average annual increase in greenhouse-gas concentrations has been about 1.6 parts per million. The average annual increase from 1985 to 2019 was about 1.9 parts per million, and from 2000 to 2019, it was about 2.2 parts per million. The largest increase that occurred was about 3.4 parts per million in 2016. But the assumed average annual increases in greenhouse-gas concentrations through 2100 under the four RCPs are 1.1, 3.0, 5.5, and an astounding 11.9 parts per million, respectively.

The studies generating the most alarmist predictions are the IPCC’s Special Report on Global Warming of 1.5°C and the U.S. government’s Fourth National Climate Assessment, both of which were published in 2018. Both assume RCP8.5 as the scenario most relevant for policy planning. The average annual **g**reen**h**ouse-**g**as increase under RCP8.5 is over five times the annual average for 2000-2019 and almost four times the single biggest increase on record. Climatologist Judith Curry, formerly of the Georgia Institute of Technology, describes such a scenario as **“borderline impossible.”**

RCP6 is certainly more realistic. It predicts a temperature increase of 3 degrees Celsius by 2100 in the average of the CMIP models. But on average, those CMIP models overstate the documented temperature record by a factor of at least two. Ultimately, models with a **poor record** of successfully accounting for past data and **highly unrealistic** future greenhouse-gas concentrations should **not be considered a reasonable basis** for future policy formulation.

**No climate impact---bad studies and adaption.**

Nils P. **Gleditsch 21**, Research Professor at the Peace Research Institute Oslo, “This time is different! Or is it? NeoMalthusians and environmental optimists in the age of climate change,” Journal of Peace Research, pg. 5-6, 2021, SAGE. clarification denoted with brackets.

The most extreme contrarian position is, of course, to deny one or both key conclusions of the IPCC: the reality of global warming or the human contribution to it. However, most environmental **optimists** accept these two key conclusions but raise other problems with the panel’s discussion of the social **effects of climate** **change** and even more so with **popular interpretations** of the panel reports. For instance, Hausfather & Peters (2020), by no means ‘climate deniers’, decry the **common** use of choosing the **high-risk** **[scenario]** RCP8.59 to illustrate **‘business as usual’** as **misleading**.

The causal chains from climate change to the **proposed** effects on human beings are **long** and **complex**, and the **uncertainty increases every step** of the way. In the literature on the social effects of climate change, including the **IPCC reports**, **statements** abound that something **‘may’ lead** to something else, or that a variable **‘is sensitive to’ another**, without any guidelines for how to **translate** this into **probabilities** (Gleditsch & Nordås, 2014: 87f). Uncritical use of the **precautionary principle**, where **a**ny **remotely** possible calamity unwittingly becomes a probable event, **is not helpful**.

Gleditsch & Nordås (2014: 85) note that while AR5 (IPCC, 2014) did **no**t find **strong evidence** for a **direct** link between climate change and conflict, it **argue**d that climate change is likely to impact known **conflict-inducing factors** like poverty and inconsistent political institutions and therefore might have an indirect effect on conflict. But this assumes that correlations are **transitive**, which is not generally the case. If **A correlates with B** and **B with C**, we know nothing about how **A relates to C** unless **both** correlations are **extremely high**. The strongest case for the climate–conflict link is the effect of interaction between climate change and factors like poverty, state failure, or ethnic polarization. It may be more cost-effective to try to deal with these other risk factors than with global warming itself if the goal is to reduce the ‘risk multiplier’ effect of climate change on armed conflict.

The articles in this special issue do not generally see scarcity by itself as necessarily resulting in strongly negative outcomes. Factors like development, state failure, and previous overload on ecosystems continue to play an important role in that they interact with climate change to produce conflict and other social outcomes. For instance, Ide, Kristensen & Bartusevicˆius (2021) conclude that the impact of floods on political conflict are contingent on other factors such as population size and regime type. Moreover, most of the articles do not assume that scarcities are likely to arise at the global level. They may be regional (mostly in Africa), national, or local. Urban and rural areas may be affected by different scarcities. Climate change may also affect particularly strongly groups that are already at an economic or political disadvantage. The effects can be alleviated and adaptations constructed at these levels.

The argument about how climate change may indirectly impact **conflict** leans heavily on the **negative economic consequences** of climate change, but with little or **no reference** to the research that explicitly deals with this topic. In fact, the relevant chapter in AR5 concluded that for most sectors of the economy, the impact of climate change was likely to be dwarfed by other factors. Tol (2018) finds that the long-term global economic effects are likely to be negative, but that a century of climate change will have about the **same impact** on the economy as the **loss of one year** of economic growth. Other economists are more cautious, but the dean of climate change economics, William Nordhaus (2018: 345, 359), estimates that ‘damages are 2.1 percent of global income at 3C warming and 8.5 percent of income at 6C’, while also warning that the longer the delay in taking decisive action, the harsher the necessary countermeasures. Stern (2006) is more pessimistic, based mainly on a lower discount rate (the interest rate used to calculate the present value of future cash flows) as are Wagner & Weitzman (2015). Heal (2017) argues that the Integrated Assessment Models generally used in the **assessment** of the economics of climate change are **not accurate enough** to provide **quantitative insights** and should not be taken as **serious** forecasts. Yet, all these economists take the basically optimistic view that climate change is manageable with appropriate policies for raising the price on the emission of greenhouse gases. With a chapter heading from Wagner & Weitzman (2015: 17): ‘We can do this’.

This more optimistic assessment of climate change does not assume that the challenge will go away by itself or can be left to the market. A plausible approach, favored by most economists,10 is the imposition of a robust and increasing price on carbon emissions (whether as a carbon tax or through a cap and trade scheme) high enough to reduce the use of fossil fuels and encourage the search for their replacement. More than 25 countries had such taxes by early 2018 (Metcalf, 2019), but generally not at a level seen as necessary for limiting global warming to, say, 2C. This approach relies on the use of the market mechanism, but with targets fixed by public policy. Income from a carbon tax can be channeled back to the citizens to avoid increasing overall taxation. To speed up the transition, funds can also be allocated to the research and development of cheaper and more efficient production of various forms of fossil-free energy, including nuclear power (Goldstein & Qvist, 2019).

The response of the environmental optimists continues to emphasize the role of **innovations**; technological innovations, such as **improvements in battery technology**, the key element in the 2019 Nobel Prize in chemistry,11 but also social innovations, as exemplified by the **experimental** **approach** to the alleviation of **poverty**, rewarded in the same year by the Nobel Prize in economics.12

While the most important countermeasures will be directed at the mitigation of climate change, there is also a strong case for **adaptation**. If sea-level rise cannot be totally prevented, dikes and flood barriers will be **cost-effective** and **necessary**, at least in high-value urban areas. If parts of Africa suffer from drought, there will be increased use for **new crops** that are **more suitable** for a **dry** climate, possibly developed in part by **GMO technology**. **Industrialization** in Africa can decrease the **one-sided reliance** on rain-fed agriculture, as it has in other parts of the world, which have moved human resources from the primary sector to industry (and then to services). Continuing urbanization will move millions out of the **most vulnerable communities** (Collier, 2010). While structural change failed to produce economic growth in Latin America and Africa after 1990, Africa has experienced a turnaround in the new millennium (McMillan & Rodrik, 2014) and there are also potentials for increasing **productivity** by **structural** **change** within agriculture in Africa (McCullough, 2017).

**No warming impact and emissions are inevitable**

a) Huge uncertainties---climate sensitivity models range from barely any warming to catastrophic with no gauge of certainty

b) Can’t be existential---the worst-case models assume impossible emissions levels with no mitigation or adaptation

c) Timeframe---impacts are slow which allows time to adapt and manage the consequence

d) Renewables worse---fast transition locks in natural gas as a bridge fuel which makes zero emissions impossible OR causes energy shortages because storage tech isn’t ready---that’s Curry.

Judith **Curry 19**, President of Climate Forecast Applications Network (CFAN), Professor Emerita of Earth and Atmospheric Sciences at the Georgia Institute of Technology, Ph.D. in atmospheric science from the University of Chicago, 2/9/19, “Statement to the Committee on Natural Resources of the United States House of Representatives,” https://curryja.files.wordpress.com/2019/02/curry-testimony-house-natural-resources.pdf

The urgency (?) of CO2 emissions reductions

In the decades since the 1992 UNFCCC Treaty, global CO2 emissions have continued to increase, especially in developing countries. In 2010, the world’s governments agreed that emissions need to be reduced so that global temperature increases are limited to below 2 degrees Celsius.17 The target of 2oC (and increasingly 1.5oC)18 remains the focal point of international climate agreements and negotiations.

The original rationale for the 2oC target is the idea that ‘**tipping points**’ − abrupt or nonlinear transition to a different climate state − become likely to occur once this threshold has been crossed, with consequences that are largely uncontrollable and beyond our management. The IPCC AR5 considered a number of potential tipping points, including ice sheet collapse, collapse of the Atlantic overturning circulation, and permafrost carbon release. Every single catastrophic scenario considered by the IPCC AR5 (WGII, Table 12.4) has a rating of **very unlikely** or **exceptionally unlikely** and/or has **low confidence**. The only tipping point that the IPCC considers likely in the 21st century is disappearance of Arctic **summer** sea ice (which is fairly **reversible**, since **sea ice freezes every winter**).

In the **absence of tipping points** on the timescale of the 21st century, the 2oC limit iss more usefully considered by analogy to a highway speed limit:19 driving at 10 mph under the speed limit is not automatically safe, and exceeding the limit by 10 mph is not automatically dangerous, although the faster one travels the greater the danger from an accident. Analogously, the 2oC (or 1.5oC) limit should **not be taken literally as a real danger threshold**. An analogy for considering the urgency of emissions reductions is your 401K account: if you begin making contributions early, it will be easier to meet your retirement goals.

Nevertheless, the 2oC and 1.5oC limits are used to motivate the urgency of action to reduce CO2 emissions. At a recent UN Climate Summit, (former) Secretary-General Ban Ki-moon warned that: “Without significant cuts in emissions by all countries, and in key sectors, the window of opportunity to stay within less than 2 degrees [of warming] will soon close forever.”20 Actually, this window of opportunity may remain open for quite some time. The implications of the **lower values of climate sensitivity** found by Lewis and Curry21 and other recent studies is that human caused warming is not expected to exceed the 2oC ‘danger’ level in the 21st century. Further, there is growing evidence that the RCP8.5 scenario for future greenhouse gas concentrations, which drives the largest amount of warming in climate model simulations, is **impossibly high**, requiring a combination of numerous borderline **impossible socioeconomic scenarios**.22 A **slower rate of warming** means there is **less urgency** to phase out greenhouse gas emissions now, and **more time** to find ways to **decarbonize the economy affordably** and with a minimum of **unintended consequences**. It also allows for the **flexibility to revise our policies** as further information becomes available.

Is it possible that something truly dangerous and unforeseen could happen to Earth’s climate during the 21st century? Yes it is possible, but **natural climate variability** (including geologic processes) may be a more likely source of possible undesirable change than manmade warming. In any event, attempting to avoid such a dangerous and unforeseen climate by reducing fossil fuel emissions will be **futile** if natural climate and geologic processes are dominant factors. Geologic processes are an important factor in the potential instability of the West Antarctic ice sheet that could contribute to substantial sea level rise in the 21st century.23

Under the Paris Agreement, individual countries have submitted to the UNFCCC their Nationally Determined Contributions (NDCs). Under the Obama Administration, the U.S. NDC had a goal of reducing emissions by 28% below 2005 levels by 2025. Apart from considerations of feasibility and cost, it has been estimated24 using the EPA MAGICC model that this commitment will prevent 0.03oC in warming by 2100. When combined with current commitments from other nations, **only a small fraction of the projected future warming will be ameliorated by these commitments**. If climate models are indeed running too hot,25 then the amount of warming prevented would be even smaller. Even if emissions immediately went to zero and the projections of climate models are to be believed, the impact on the climate would **not be noticeable** until the 2nd half of the 21st century. Most of the expected benefits to the climate from the UNFCCC emissions reductions policy will be realized in the 22nd century and beyond.

Attempting to use carbon dioxide as a control knob to regulate climate on decadal to century timescales is arguably **futile**. The UNFCCC emissions reductions policies have brought us to a point between a rock and a hard place, whereby the emissions reduction policy with its **extensive costs** and questions of feasibility are **inadequate for making a meaningful dent** in slowing down the expected warming in the 21st century. And the **real societal consequences** of climate change and extreme weather events (whether caused by manmade climate change or natural variability) **remain largely unaddressed**.

This is not to say that a transition away from burning fossil fuels doesn’t make sense over the course of the 21st century. People prefer ‘clean’ over ‘dirty’ energy – provided that all other things are equal, such as reliability, security, and economy. However, assuming that current wind and solar technologies are adequate for providing the required amount and density of electric power for an advanced economy is misguided.26

The recent record-breaking cold outbreak in the Midwest is a stark reminder of the challenges of providing a reliable power supply in the face of extreme weather events, where an inadequate power supply not only harms the economy, but jeopardizes lives and public safety. Last week, central Minnesota experienced a natural gas ‘brownout,’ as Xcel Energy advised customers to turn thermostats down to 60 degrees and avoid using hot water.27 Why? Because the wind wasn’t blowing during an exceptionally cold period. Utilities pair natural gas plants with wind farms, where the gas plants can be ramped up and down quickly when the wind isn’t blowing. With bitter cold temperatures and no wind, there wasn’t enough natural gas.

A transition to an electric power system driven solely by wind and solar would require a **massive amount of energy storage**. While energy storage technologies are advancing, massive deployment of **cost-effective energy storage** technologies is well beyond current capabilities.28 An unintended consequence of rapid deployment of wind and solar energy farms may be that **natural gas power plants become increasingly entrenched** in the power supply system.

Apart from energy policy, there are a number of land use practices related to croplands, grazing lands, forests and wetlands that could increase the **natural sequestration** of carbon and have ancillary economic and ecosystem benefits.29 These co-benefits include **improved biodiversity**, **soil quality**, **agricultural productivity** and wildfire behavior modification.

In evaluating the urgency of CO2 emissions reductions, we need to be realistic about what reducing emissions will actually accomplish. Drastic reductions of emissions in the U.S. will not reduce global CO2 concentrations if emissions in the **developing world**, particularly **China** and **India**, continue to increase. If we believe the climate model simulations, we would not expect to see any changes in extreme weather/climate events until late in the 21st century. The greatest impacts will be felt in the 22nd century and beyond, in terms of reducing sea level rise and ocean acidification.

Resilience, anti-fragility and thrivability

Given that emissions reductions policies are very costly, politically contentious and are not expected to change the climate in a meaningful way in the 21st century, **adaptation strategies** are receiving **increasing attention** in formulating responses to climate change.

The extreme damages from recent hurricanes plus the recent billion dollar disasters from floods, droughts and wildfires, emphasize that the U.S. is highly vulnerable to current weather and climate disasters. Even worse disasters were encountered in the U.S. during the 1930’s and 1950’s. Possible scenarios of incremental worsening of weather and climate extremes over the course of the 21st century don’t change the fundamental storyline that many regions of the U.S. are not well adapted to the current weather and climate variability, let alone the range that has been experienced over the past two centuries.

As a practical matter, adaptation has been driven by local crises associated with extreme weather and climate events, emphasizing the role of ‘surprises’ in shaping responses. Advocates of adaptation to climate change are not arguing for simply responding to events and changes after they occur; they are arguing for **anticipatory adaptation**. However, in adapting to climate change, we need to acknowledge that we cannot know how the climate will evolve in the 21st century, we are certain to be surprised and we will make mistakes along the way.

‘Resilience’ is the ability to ‘bounce back’ in the face of unexpected events. Resilience carries a connotation of returning to the original state as quickly as possible. The difference in impact and recovery from Hurricane Sandy striking New York City in 2012 versus the impact of Tropical Cyclone Nargis striking Myanmar in 200830 reflects very different vulnerabilities and capacities for bouncing back.

To increase our resilience to extreme weather and climate events, we can ‘bounce forward’ to reduce future vulnerability by evolving our infrastructures, institutions and practices. Nicholas Taleb’s concept of antifragility31 focuses on learning from adversity, and developing approaches that enable us to thrive from high levels of volatility, particularly unexpected extreme events. Anti-fragility goes beyond ‘bouncing back’ to becoming even better as a result of encountering and overcoming challenges. Anti-fragile systems are dynamic rather than static, thriving and growing in new directions rather than simply maintaining the status quo.

Strategies to increase antifragility include: economic development, reducing the downside from volatility, developing a range of options, tinkering with small experiments, and developing and testing transformative ideas. Antifragility is consistent with decentralized models of policy innovation that create flexibility and redundance in the face of volatility. This ‘innovation dividend’ is analogous to biodiversity in the natural world, enhancing resilience in the face of future shocks.32

Similar to anti-fragility, the concept of ‘thrivability’ has been articulated by Jean Russell:33 “It isn’t enough to repair the damage our progress has brought. It is also not enough to manage our risks and be more shock-resistant. Now is not only the time to course correct and be more resilient. It is a time to imagine what we can generate for the world. Not only can we work to minimize our footprint but we can also create positive handprints. It is time to strive for a world that thrives.”

A focus on policies that support resilience, anti-fragility and thrivability avoids the hubris of thinking we can predict the future climate. The relevant questions then become:

• How can we best promote the development of transformative ideas and technologies?

• How much resilience can we afford?

The threats from climate change (whether natural or human caused) are fundamentally regional, associated not only with regional changes to the weather/climate, but with local vulnerabilities and cultural values and perceptions. In the least developed countries, energy poverty and survivability is of overwhelming concern, where there are severe challenges to meeting basic needs and their idea of clean energy is something other than burning dung inside their dwelling for cooking and heating. In many less developed countries, particularly in South Asia, an overwhelming concern is vulnerability to extreme weather events such as floods and hurricanes that can set back the local economies for a generation. In the developed world, countries are relatively less vulnerable to climate change and extreme weather events and have the luxury of experimenting with new ideas: entrepreneurs not only want to make money, but also to strive for greatness and transform the infrastructure for society.

Extreme weather/climate events such as landfalling major hurricanes, floods, extreme heat waves and droughts become catastrophes through a combination of large populations, large and exposed infrastructure in vulnerable locations, and human modification of natural systems that can provide a natural safety barrier (e.g. deforestation, draining wetlands). Addressing current adaptive deficits and planning for climate compatible development will **increase societal resilience** to future extreme events that may possibly be more frequent or severe in the future.

Ways forward

Climate scientists have made a forceful argument for a future threat from manmade climate change. Based upon our current assessment of the science, **the threat does not seem to be an existential one** on the time scale of the 21st century, even in its most alarming incarnation. However, the perception of manmade climate change as a near-term apocalypse and alignment with range of other social objectives has **narrowed the policy options that we’re willing to consider**.

**No impact to warming.**

--CO2 levels are historically low

--CO2 is not correlated with higher temperatures

--Humans and fossil fuels are the primary cause of carbon concentrations

Jay **Lehr 19**, Ph.D. in Groundwater Hydrology from the University of Arizona, and Tom Harris, Executive Director of the International Climate Science Coalition, “Global Warming Myth Debunked: Humans Have Minimal Impact on Atmosphere’s Carbon Dioxide and Climate”, Western Journal, 2-14, <https://www.westernjournal.com/global-warming-myth-debunked-humans-minimal-impact-atmospheres-carbon-dioxide-climate/> [language modified]

Global warming activists argue carbon-dioxide emissions are destroying the planet, but the climate impacts of carbon dioxide are **minimal, at worst**. Activists would also have you believe fossil-fuel emissions have driven carbon-dioxide concentrations to their highest levels in history. The Obama-era Environmental Protection Agency went so far as to classify carbon dioxide as a toxic pollutant, and it established a radical goal of closing all of America’s coal-fired power plants.

Claims of unprecedented carbon-dioxide levels ignore most of Earth’s 4.6-billion-year history. Relative to Earth’s entire record, carbon-dioxide levels are at **historically low** levels; they only appear high when compared to the dangerously low levels of carbon dioxide that occurred in Earth’s very recent history. The geologic record reveals carbon dioxide has **almost always** been in Earths’ atmosphere in much greater concentrations than it is today. For example, 600 million years ago, when history’s greatest birth of new animal species occurred, atmospheric carbon-dioxide concentrations exceeded 6,500 parts per million (ppm) — an amount that’s **17 times** greater than it is today.

Atmospheric carbon dioxide is currently only 410 parts per million. That means only 0.04 percent of our atmosphere is carbon dioxide (compared to 0.03 percent one century ago). Only one molecule in 2,500 is carbon dioxide. Such levels certainly do not pose a health risk, as carbon-dioxide levels in our naval submarines, which stay submerged for months at a time, contain an average carbon-dioxide concentration of 5,000 ppm.

The geologic record is important because it reveals relationships between carbon-dioxide levels, climate, and life on Earth. Over billions of years, the geologic record shows there is **no long-term correlation** between atmospheric carbon-dioxide levels and Earth’s climate. There are periods in Earth’s history when carbon dioxide concentrations were **many times** higher than they are today, yet temperatures were identical to, or **even colder** than, modern times. The claim that fossil-fuel emissions control atmospheric carbon-dioxide concentrations is also **invalid**, as atmospheric concentrations have gone up and down in the geological record, **even without** human influence.

The absurdity of climate alarmism claims gets even stranger when you consider there are 7.5 billion people on our planet who, together, exhale 2.7 billion tons of carbon dioxide each year, which is almost 10 percent of total fossil-fuel emissions every year. However, we are but a single species. Combined, people and all domesticated animals contribute 10 billion tons.

Further, 9 percent of carbon-dioxide emissions from all living things arise not from animals, but from anaerobic bacteria and fungi. These organisms metabolize dead plant and animal matter in soil via decay processes that recycle carbon dioxide back into the atmosphere. The grand total produced by all living things is estimated to be 440 billion tons per year, or 13 times the amount of carbon dioxide currently being produced by fossil-fuel emissions. Fossil-fuel emissions are **less than 10 percent** of biological emissions. Are you laughing yet?

Every apocalyptic pronouncement you hear or read is **[totally wrong]** ~~nothing short of insanity~~. Their primary goal is not to save plants, humans, or animals, but rather to use climate “dangers” as a justification for centralizing power in the hands of a select few.

**Even extreme warming won’t cause extinction**

Dr. Toby **Ord 20**, Senior Research Fellow in Philosophy at Oxford University, DPhil in Philosophy from the University of Oxford, The Precipice: Existential Risk and the Future of Humanity, Hachette Books, Kindle Edition, p. 110-112

But the purpose of this chapter is finding and assessing threats that pose a direct existential risk to humanity. Even at such **extreme levels** of warming, it is difficult to see exactly how climate change could do so. Major effects of climate change include reduced **ag**ricultural yields, sea level rises, water scarcity, increased tropical diseases, ocean acidification and the collapse of the Gulf Stream. While extremely important when assessing the overall risks of climate change, **none** of these **threaten extinction** or irrevocable collapse.

Crops are very sensitive to reductions in temperature (due to frosts), but less sensitive to increases. By all appearances we would **still have food** to support civilization.85 Even if sea levels rose **hundreds of meters** (over centuries), **most** of the Earth’s land area would remain. Similarly, while some areas might conceivably become uninhabitable due to water scarcity, other areas will have increased rainfall. More areas may become susceptible to tropical diseases, but we need only look to the tropics to see civilization **flourish** despite this. The main effect of a collapse of the system of Atlantic Ocean currents that includes the Gulf Stream is a 2°C cooling of Europe—something that poses no permanent threat to global civilization.

From an existential risk perspective, a more serious concern is that the high temperatures (and the rapidity of their change) might cause a large loss of biodiversity and subsequent ecosystem collapse. While the pathway is not entirely clear, a large enough collapse of ecosystems across the globe could perhaps threaten human extinction. The idea that climate change could cause widespread extinctions has some good theoretical support.86 Yet the evidence is **mixed**. For when we look at many of the **past cases** of extremely high global **temp**erature**s** or extremely rapid warming we **don’t see** a corresponding loss of **biod**iversity.87

[FOOTNOTE]

We don’t see such biodiversity loss in the **12°C warmer climate** of the **early Eocene**, nor the rapid global change of the **PETM**, nor in rapid **regional** changes of climate. Willis et al. (2010) state: “We argue that although the underlying mechanisms responsible for these past changes in climate were very different (i.e. natural processes rather than anthropogenic), the rates and magnitude of climate change are similar to those predicted for the future and therefore potentially **relevant** to understanding future biotic response. What emerges from these past records is evidence for **rapid community turnover**, **migrations**, **development** of novel ecosystems and thresholds from one stable ecosystem state to another, but there is **very little evidence** for **broad-scale extinctions** due to a warming world.” There are similar conclusions in **Botkin** et al. (2007), **Dawson** et al. (2011), **Hof** et al. (2011) and **Willis & MacDonald** (2011). The best evidence of warming causing extinction may be from the end-Permian mass extinction, which may have been associated with large-scale warming (see note 91 to this chapter).

[END FOOTNOTE]

So the most important known effect of climate change from the perspective of direct existential risk is probably the most obvious: **heat stress**. We need an environment cooler than our body temperature to be able to rid ourselves of waste heat and stay alive. More precisely, we need to be able to lose heat by sweating, which depends on the humidity as well as the temperature.

A landmark paper by Steven Sherwood and Matthew Huber showed that with sufficient warming there would be parts of the world whose temperature and humidity combine to exceed the level where humans could survive without air conditioning.88 With 12°C of warming, a very large land area—where more than half of all people currently live and where much of our food is grown—would exceed this level at some point during a typical year. Sherwood and Huber suggest that such areas would be uninhabitable. This may not quite be true (particularly if air conditioning is possible during the hottest months), but their habitability is at least in question.

However, **substantial regions** would also **remain below** this threshold. **Even with an extreme 20°C of warming** there would be **many** coastal areas (and some **elevated regions**) that would have no days above the temperature/humidity threshold.89 So there would remain **large areas** in which humanity and **civ**ilization could **continue**. A world with 20°C of warming would be an unparalleled human and environmental tragedy, forcing mass migration and perhaps starvation too. This is reason enough to do our utmost to prevent anything like that from ever happening. However, our present task is identifying existential risks to humanity and it is hard to see how any realistic level of heat stress could pose such a risk. So the runaway and moist greenhouse effects remain the only known mechanisms through which climate change could directly cause our extinction or irrevocable collapse.

This doesn’t rule out unknown mechanisms. We are considering large changes to the Earth that may even be unprecedented in size or speed. It wouldn’t be astonishing if that directly led to our permanent ruin. The best argument against such unknown mechanisms is probably that the PETM did not lead to a mass extinction, despite temperatures rapidly rising about 5°C, to reach a level 14°C above pre-industrial temperatures.90 But this is tempered by the imprecision of paleoclimate data, the sparsity of the fossil record, the smaller size of mammals at the time (making them more heat-tolerant), and a reluctance to rely on a single example. Most importantly, anthropogenic warming could be over a hundred times faster than warming during the PETM, and rapid warming has been suggested as a contributing factor in the end-Permian mass extinction, in which 96 percent of species went extinct.91 In the end, we can say little more than that direct existential risk from climate change appears **very small**, but cannot yet be ruled out.

**2AC – !! – AT: Libicki**

**Flows aff**

**Libicki, '14** – American scholar and Professor at the Frederick S. Pardee RAND Graduate School in Santa Monica, California (Martin Libicki; "Is Cyberwar Good for Peace? [par Martin Libicki]"; FIC; https://incyber.org/en/is-cyberwar-good-for-peace-par-martin-libicki/; 01-2014, Accessed 6-27-2022)//ILake-NoC

Rogue Actors

The calculus of cyberwar should also take the possibility of rogue actors into account.

For many forms of warfare, worries about rogue actors – individuals or groups that make war without authorization – are theoretical threats, suitable for Hollywood (e.g., Dr. Strangelove), but of little practical moment. War is a dangerous business, the risk of being caught is nontrivial, and isolated units (e.g., an unsupported fighter squadron) are generally ineffective against states.

Militias may be an exception, particularly those that prey on unarmed populations. The dangers are low, the risk of getting caught is modest, and they can be militarily effective operating in guerilla mode. The possibility of militias is a constant worry in states where policing is corrupt or ineffective; they can start fights and make it very difficult to conclude them.

Cyberspace may have considerable scope for militias. The direct risks of combat to combatants are zero (in the usual case that physical proximity is not necessary). The risks of getting caught are small if such groups and their systems practice operational security. Finally, cyberattacks can do damage against countries that have not fully secured their own systems. In contrast to militias, they can have global effects, and, if the hackers are particularly skillful or lucky (e.g., by finding an exploitable vulnerability in a critical system) they can have serious ones. Although states continue to have advantages over nonstate actors in employing hackers (and states with ample resources can usually outdo states without resources), it does not take a particularly large team to generate effects, as long as the members of this team are sufficiently talented. Because the work of cyberwar is closely aligned to nations’ intelligence communities (the vast majority of system penetrations by governments are to collect information not bring such systems down), they arise from a culture that prizes and usually practices secrecy. Intelligence agencies that pursue courses (seemingly) antithetical to declared state policies do occur: Pakistan’s ISI is a case in point.[7]

Attacks by rogue operators create a path to conflict that carry a far lower risk to itself than would be the case if the only option were kinetic warfare. Indeed, there are good reasons to believe that if, say, Russia wanted to convey its ire at one or another U.S. action, then it could convince itself that the risks to its own well-being were low if it simply empowered its mafiya to carry out such attacks on the state’s behalf, perhaps in return for winking at other mafiya activities taking place within Russia itself. The relationship between the state and hackers in China is still unclear even after the Mandiant report. Similar ambiguity exists with Iran. Perhaps attackers would believe that risks are low because attribution is difficult. The argument that Russia will be forced to assist the United States in catching the actual attackers vies with the observation Russia denied Estonia’s request for assistance after the 2007 attack (or the previous attempt by the United States to trace the origins of the 1998 intrusion into DoD computers subsequently labeled Moonlight Maze[8]). Conversely, a target country’s attempts to trace responsibility for a cyberattack consequential enough to risk escalation to the kinetic level may be harder to turn aside. Faced with the decision of admitting that one of its own carried out the attack outside official command-and-control, or brazening through a crisis, the attacking country may well double down, setting the stage for a confrontation.

Crisis

Military capabilities may also affect crisis dynamics in ways that predispose countries to slide into or away from warfare. Even those disinclined to believe that cyberwars alone are likely to be consequential must admit that kinetic conflict can be consequential and that cyberattack capabilities might affect the latter’s onset or course. Of note is that cyberwar capabilities may increase the likelihood of a full-fledged kinetic conflict (as distinguished from a kinetic attack discussed above) either by presenting opportunities for attackers or by making defenders think that their opponents are creating such opportunities.

Cyberattacks might be used to cripple conventional capabilities at the outset of conflict giving the attacker a decisive, albeit fleeting, opportunity to carry out a successful kinetic attack while its foe has been blinded (by attacks on its ISR capabilities), confused (by attacks on its command-and-control), or immobilized (by attacks on its logistics and deployment system). The last may be the least consequential (if forces are pre-equipped with a week’s worth of supplies), but may also be most accessible. If the U.S. military is a model, logistics systems are much more likely to be connected to the Internet while the command and control of military units is more likely to sit on air-gapped networks; ISR systems as befits their intelligence origin, are even more isolated.

The difficulty of attributing cyberattacks, and the near-impossibility of seeing a well-executed cyberattack coming, coupled with the short duration of their immediate effects make a bolt-from-the-blue in cyberspace prefatory to kinetic war more insidious. First, attackers may convince themselves that a bolt-from-the-blue is relatively riskless. If such attacks shift the correlation of forces enough, the shooting starts because the prospects of victory by the country that carries out the cyberattack are that much brighter. If such attacks fail to do enough to change the odds of victory, the attacker holds off on shooting, and the target may not necessarily respond as if war had started – or so the cyber attacker may reason. Such reasoning is much less plausible if the bolt from the blue were a kinetic attack whose provenance was much harder to deny. Second, the well-founded presumption that the effects of a cyberattack are likely to last only until such systems are restored to where they are usable (hours to weeks?), means that the decision to exploit the opening has to be made more quickly than if the damage were permanent (as it might be if the bolt from the blue, for instance, disabled satellites in orbit). Strong confirmation biases (thinking fast[9]) may induce countries to capitalize on what they hope was success, even when they might have held back given more time to consider (thinking slow) what a rush to war might produce.

Instability may also arise from the defender’s reaction to a possible bolt from the blue. Granted, if the defender noticed that its military systems had been crippled by a cyberattack, then responding with alacrity is appropriate. But the possibility of a bolt-from-the-blue suggests that in a crisis (as the victim of the cyberattack sees it) any cyberattack may have to be treated as prefatory to a kinetic attack. The target country may then turn up its warnings-and-indications sensors to catch the minute ripplings of its foes on the match. Unfortunately, the higher the gain, the greater the likelihood of reading artifacts as though they were indicators – and so off to war.[10]

Unfortunately, this scenario understates the problem. Both acts of cyberwar and cyber-espionage canonically start with the penetration of the target to insert malware. This malware then calls out for instructions, which variously can instruct the infected machine to do something damaging (cyberwar) or to send back information of a particular type (cyber-espionage). Discovering the penetration, particularly if it can be attributed to a potential adversary, may convince the target country that it will soon face attack. It may then turn up its indicator-and-warning sensors with the same violent result.

Either way, the possibility of a cyber bolt-from-the-blue coupled with the difficulty of ascertaining who carried it out or even whether what looks like preparations for one are, in fact, such preparations or just apparitions adds the possibility of instability to crisis.

In all fairness, the wars that such cyberattacks might predispose would have to be those where the outcome of the first few days fighting is particularly decisive: a quick high-intensity conflict is ideal for such treatment. The prospect for success in long wars or low-intensity conflicts is scarcely affected by opening-day hijinks; logically therefore the possibility of cyberwar should have little effect on starting such conflicts.

Escalation

The assumption that cyberwar is a cool war also rests on the presumption that what starts in cyberspace will stay in cyberspace; there will be no escalation into kinetic conflict. Clearly the chance of escalation that crosses domains is greater than zero, but for cyber war to lose its cool status requires that the risks of escalation into kinetic conflict for a cyberattack be substantially less than similar risks associated with a comparable kinetic attack.

The thin history we have of cyberattacks does not suggest that a cyberattack will necessarily be followed by much of anything at all. The Russian[11] 2007 attacks on Estonia which crippled public and major private web sites was followed by Estonia’s complaints and NATO’s unwillingness to deem this an Article V attack (triggering collective self-defense measures) but it led to nothing violent or even close.[12] If Georgia had reacted kinetically to the cyberattacks on it in 2008, it would have been difficult to distinguish such actions from the war Georgia was forced to fight following its invasion by Russian forces. The 2007 Israeli air strike on a purported nuclear facility in Syria may have been facilitated by an opening cyberattack on Syrian air defenses but Syria did not respond at all to the cyberattack or the raid itself. Iran did not react kinetically to Stuxnet, even if it created cyberwar cadres that may have been implicated in carrying out denial-of-service attacks on banks[13] in the United States (from whence, supposedly, Stuxnet), but also attacks which trashed computers in Saudi Arabia (specifically, Aramco[14]) and Qatar (specifically, RasGas[15]), neither of which could be plausibly accused of complicity in creating Stuxnet. Similarly, the United States carried out no kinetic attack in response to the aforementioned denial-of-service attacks on banks that its intelligence community ascribed to Iran.

To be fair, cyberattacks unaccompanied by the outbreak of war are easier to liken to a raid than a war. In a raid, forces cross borders, wreak their mischief, and go home. In a war, they intend to stay permanently or turn what they have taken (be it territory or the entire country) over to those they deem their allies. It is very difficult of conceive of a cyberattack that can change the head of state and even harder to conceive of one that can conquer all or even part of another country. In worst-case scenarios, a cyberattack can disrupt life and maybe even break some machines. But they do not persist unless the cost of eradicating them – for instance, by doing a system reboot, or replacing infected machines with uninfected machines – exceeds the cost of tolerating their presence. It is worth remembering that there is no forced entry in cyberspace. Almost all wars tend to be two-side engagements because the attacked side has no option but to fight or surrender. In a raid, there is a third option to offer, at most, some resistance but not pursue the attacker for fear of worse. Thus, not all raids lead to counter-raids. The aforementioned 2007 Israeli raid on Syria did not. The many U.S. drone strikes have not, so far. China invaded Vietnam in 1979, wreaked damage, caused casualties, and departed having, in its mind, taught Vietnam a lesson. Vietnam did not return the favor by invading China. Neither did India in 1962 under similar circumstances. Granted, some nations do respond. Arabs and Israelis traded raids in the decade or so after Israel declared independence (1948); Palestinians and Israelis traded attacks over the last three decades, as well. Both Koreas sent raiding parties across the 38th parallel in the years prior to North Korea’s 1950 invasion. The history of raids escalating into open conflict (as distinguished from raids preceding open conflict as was the Korean case) is also thin.

Two other difficulties associated with attribution and the difficulties of disarming the attacker are likely to reduce the pressure to retaliate, much less, escalate in response to a cyberattack. Difficulties of attribution are likely to have two related effects. The first is that the target may not be so certain about who did it – or at least not be certain of its ability to convince third parties such as other countries who did it – to validate a response. The second is that if it takes too much time to analyze the attack to the point where it can determine (and make the case about) who did it with the requisite confidence, the political pressure for vengeance may have cooled and the politico-military situation that warranted retaliation may have changed (e.g., yesterday’s foe might be today’s partner).

The impetus to respond can also be reduced if the public has little idea about the identity of the attacker and even the fact of the attack (e.g., the failure to function is not obvious to the outside). Until the New York Times reported on Stuxnet, the public did not know that Iran had been attacked (it is not clear whether anyone in Iran actually understood that they were being attacked before it was reported). If no one knows that two parties are trading blows in the dark, there is much less requirement to appear strong as a way of establishing third-party deterrence.

The difficulty of disarming the other side’s cyberwar capabilities removes another reason for responding to a cyberattack. A kinetic response to a kinetic attack can be justified, not only as a way to reinforce deterrence, but also as a way to reduce the attacker’s ability to carry out further attacks; it does so by killing opposing forces and destroying military equipment, ancillary supplies and infrastructure, especially staging areas. A cyber response can only be justified in terms of deterrence because it is very difficult for a cyberattack to permanently or even temporarily damage the other side’s ability to carry out cyberattacks, which require little more than hackers, information, computing equipment, software, and network connections.[16] Granted, the target country may conclude that it may win some relief from cyberattack by carrying out a kinetic attack on the attacker’s cyberwar corps. Such actions cannot be ruled out[17] — but suffice it to say that at least the tools of a cyberattack cannot be identified from afar in the same way that the tools of a kinetic attack can be. Alternatively, the target can convince itself that the only way to rid itself of the cyberattack menace is to change the regime that governs the attacking country. If the sole aim of such logic is to minimize the likelihood of future damage to the target country, it can be convincing only by substantially underestimating the cost and risk of war or substantially overestimating the inconvenience associated with adopting other measures to improve cyber-security.

Finally, and in lieu of regime change, the escalation path from a cyberattack into a kinetic response also crosses a threshold that does not come up when the original provocation and the response were both kinetic. It is unclear whether this threshold is more like a speed bump or a yawning abyss, but it is clearly present. It should therefore seem obvious that a cyberattack is less likely to result in a kinetic response than an equivalent kinetic attack would have. However, this raises the question of what constitutes equivalence. Assessing kinetic damage when it is damage to you is a straightforward exercise. Assessing the damage from a cyberattack that leads to the widespread corruption of information systems requires knowing what systems have, in fact, been corrupted (something that, ironically, the attacker may have a better handle on). A target country that has been spooked by a cyberattack into imagining that the real damage is a multiple of the visible damage may well overreact (at least initially until it realizes over time which of its systems is or is not behaving as if they had been corrupted).

In sum, although the risks of violent escalation following a cyberattack are nonzero, the odds are against it, in isolation and particularly in comparison to a kinetic attack of similar magnitude.

Conclusions

New ways of carrying out conflict would, intuitively, seem to increase the likelihood of conflict. They create new ways to fight without necessarily lessening existing ways. We can easily imagine two countries carrying out cyberattacks on one another, when they would have had no such option were cyberwar not a possibility. To the extent that the reverberations of such a conflict escape beyond cyberspace they would seem to increase the likelihood of violence. But that rule does not always apply. Nuclear weapons, for instance, were not only not used during the Cold War, they are credited with having reduced the odds of conventional conflict in Europe. And cyberattacks, if they can substitute for kinetic attacks, may also reduce the odds of violence.

Do they? Although it is too soon to tell for sure; logic suggests otherwise. First, there are more ways in which countries, possessed of cyberattack capabilities, would use them or use cyberattack-enhanced conventional operations than there are ways in which cyberattacks would substitute for kinetic attacks. Second, cyberattacks may be used by rogue elements operating against distant countries in ways harder to imagine with conventional warfare capabilities. Third, cyberattack capabilities may exacerbate crises by creating the possibility of a disabling strike, or because the preparations for such a strike are hard to distinguish from cyber espionage. The saving grace is that the escalation potential, particularly a kinetic response, following a cyberattack, while nonzero, is suppressed by many factors.

**Case**

**2NC – Cyber Doesn’t Escalate**

**2NC – Allied Mistrust**

**Either allies won’t integrate OCOs due to political, cultural, and legal constraints OR they’ll feel pressured to which causes premature, faulty system development.**

**Black & Lynch, 20** – Research Leader Defence, Security and Infrastructure RAND Europe J=(James Black & Alice Lynch; "Cyber Threats to NATO from a Multi-Domain Perspective"; RAND; https://ccdcoe.org/uploads/2020/12/7-Cyber\_Threats\_NATO\_Multidomain\_Perspective\_ebook.pdf; 07-2020, Accessed 6-28-2022)//ILake-NoC

B. Policy Tensions

Policy differences exacerbate conceptual ones. Allies differ in their **policy and legal constraints**, strategic **cultures**, **threat perception,** **resources**, planning and budgetary cycles and forces (Sondhaus, 2006). While solidarity ultimately remains NATO’s strongest asset, these differences create seams that adversaries can exploit. This is **especially** so **with cyberspace**, where there is more sensitivity and less commonality to emerging national approaches than in more established domains, and to MDO, which is inherently predicated on integration and interoperability (Sharpy, 2020).

**Info**rmation **sharing is especially problematic** for the cyber dimension of MDO, with **Allies reticent to share details** of their capabilities across NATO given security concerns and political sensitivities. The issue of permissions is also a ‘significant challenge in the development of cyber capabilities’, especially where reconnaissance on Allied soil and networks is required to detect hostile cyber activity (Watling & Roper, 2019). Nations also have differing policy, legal and ethical stances on key technologies on which MDO relies. This **includes** **the use of offensive cyber capabilities** or basing of hypersonic missiles or longrange penetrating fires in Europe, which some fear could be destabilising and escalatory (Quintin & Vanholme, 2020). NATO similarly lacks a common approach to governance and use of AI, autonomy and automation, all envisaged as essential enablers for JADC2 (Williams, 2020). This affects the levels of autonomy (with the human in, on or out of the loop) used for sensor data fusion and decision-making, or to deliver effects using uncrewed platforms, automated cyber systems and human-machine teaming (Scharre, 2018). 138 In considering cooperation and burden-sharing, Allies face several dilemmas depending on their ambitions and resources for both cyberspace and MDO. The US must overcome domestic inter-service rivalries and decide how to integrate partners, including whether it can accept a multinational vision of MDO that is not imposed on smaller allies—or excludes them entirely, at NATO’s expense—but rather is genuinely collaborative (Watling & Roper, 2019). Larger European nations face the dilemma of whether to buy into a US-led architecture and system-of-systems with **implications for freedom of action**, data-sharing and procurement choices, or shoulder the costs of sovereign or multinational alternatives.11 They also face choices over how best to contribute to multinational MDO: whether to aspire to full-spectrum capabilities to allow sovereign action and offer redundancy to Allies’ capabilities or to specialise in certain domains (e.g. cyber) to offer niche capability and buy leverage with the US and NATO by making themselves indispensable. Smaller nations must decide how to influence larger Allies and NATO, and what to do if they lack cyber capabilities (or others deemed central to MDO, e.g. long-range fires) or their forces are too small to operate or gain MDO experience at echelons above brigade (Watling & Roper, 2019).

The economic fallout of COVID-19 also raises **renewed questions about affordability** and the extent to which Allies are willing and able to invest in new cyber capabilities—though some may see these as cost-efficient alternatives to land, air or maritime forces—and how they time investments in ambitious transformation programmes such as MDO (Clark, 2020). Timing presents both threats and opportunities from a cyber perspective. **Rapid**, hasty **transformation** risks **undermining NATO cohesion** **and interoperability** or creating vulnerabilities in JADC2 systems with immature cyber defences (Donaldson & Sciarini, 2019b). Conversely, overly cautious change risks ceding ground to adversaries such as Russia and China which are investing heavily in asymmetric means, including offensive cyber capabilities, to gain an information advantage over NATO (Kilcullen, 2020).

**No intra-NATO info-sharing – allies are reluctant to disclose info; they value autonomy and fear weaker countries cannot protect their info.**

**University of Exeter** **20** – public research university in Exeter, Devon, South West England, United Kingdom. Its predecessor institutions, St Luke's College “Should NATO Adopt a Joint Offensive Cyber Capability?” 09-2020, Accessed 06-28-2022, <https://socialsciences.exeter.ac.uk/media/universityofexeter/strategyandsecurityinstitute/pdfs/mstrat/James_Prideaux.pdf>. //ILake-NoC

Nevertheless, the largest barrier to a joint cyber capability is national intelligence agencies’ tendency to keep their activities in cyberspace highly classified.182 As Chapter 2 discussed, effective cyberattacks are utterly dependent on excellent intelligence.183 Members have significantly stepped up intelligence-sharing over the last two decades. They established the NATO Intelligence Fusion Centre in 2006, the Joint Intelligence, Surveillance and Reconnaissance initiative in 2012 and the Joint Intelligence and Security Division (JISD) in 2017. The JISD’s first Assistant Secretary General, Arndt Freytag von Loringhoven, says it has fostered a new culture of intelligence cooperation, increased efficiency and has helped avoid the duplication 37 of effort.184 Notably, he claims this new fusion of intelligence has ‘positioned the JISD to contend effectively with the… cyber… threats increasingly confronting NATO’.185

However, von Loringhoven’s optimism glosses over the **great difficulty of intra-Alliance intelligence sharing**. Divulging secret information is a trade-off between trusting a partner enough to share information that **could endanger one’s own** **source** against the benefits of doing so.186 Therefore, national agencies are **reluctant to share** it with international organisations, instead **preferring** **bilateral cooperation** on a case-by-case basis.187 It is shared between states with closely aligned interests, mutual trust and good diplomatic relations, as seen in the Anglo-American UKUSA Agreement.188 The exclusive ‘Five Eyes’ Alliance this evolved into is a rare example of multilateral intelligence sharing, involving NATO members America, Canada and the UK. These agreements tend to be more concerned with the security of the intelligence shared rather than its content, due to concerns over how other states will circulate the information. 189 Accordingly, wider intelligence cooperation within NATO would be much harder to achieve, primarily because many states **do not share strong levels of trust**, common interests and diplomatic relations with each other. For instance, France remains unsympathetic to intelligence integration in any multilateral environment, preferring strategic autonomy.190 This is compounded by an uneasy relationship with the Alliance, with President Emmanuel Macron calling it ‘brain dead’ in 2019.191 Furthermore, some allies fear that if countries with lower resilience are infiltrated, they could possibly compromise sensitive information shared between members.192 Consequently, **apprehension about Italy’s weak cyber systems** hinders allies’ propensity to share with Rome, since the **potential for leaks undermines their trust**.193

These concerns have resulted in a **division between** those **member states** that possess more advanced intelligence assets and those that do not. The former have been resisting serious intelligence integration, while the latter – including Belgium and The Netherlands – have even pressed for a CIA-style European agency.194 So far, NATO’s more powerful members have successfully **repelled** such **initiatives**. Following the 2015 Paris terror attacks, Belgian Prime Minister Charles Michel proclaimed the need for a ‘European CIA’.195 Nonetheless, German Interior Minister Thomas de Maizière shot this proposal down, claiming that ‘I cannot imagine we will be willing to **give up our national sovereignty’**.196

Unsurprisingly, NATO’s own collaborative efforts to date have also been **heavily limited by national agencies’ desire for secrecy** and autonomy. Pushback against greater transparency is especially strong on the part of the US, which owns a large share of NATO’s intelligence capabilities.197 not have access to all US intelligence, but NATO releasable information only.198 Such secrecy is a big practical obstacle to a joint offensive cyber capability. Although it is justified, elevating America’s role in Alliance cyber policy without increasing transparency would likely limit the tactical and strategic effectiveness of a combined offensive cyber capability.199 NATO’s intelligence fusion efforts have suffered from other, less important problems too. Different languages, cultures and infrastructures have proved to be **structural constraints**, while battlefield commanders have criticised the intelligence provided for lacking the strategic dimension.200 For instance, Lieutenant-General Mark Hertling judged NATO’s information on Islamic State too narrow and target-oriented, thus missing the bigger picture.201

Overall, the establishment of a joint capability would face some serious practical problems, both when confronting NATO’s internal politics and national intelligence agencies’ clandestine modus operandi. There would be significant legal hurdles to overcome too, which Chapter 4 discusses in more detail.

**Black & Lynch, 20** – Research Leader Defence, Security and Infrastructure RAND Europe J=(James Black & Alice Lynch; "Cyber Threats to NATO from a Multi-Domain Perspective"; RAND; https://ccdcoe.org/uploads/2020/12/7-Cyber\_Threats\_NATO\_Multidomain\_Perspective\_ebook.pdf; 07-2020, Accessed 6-28-2022)//ILake-NoC

Assuming NATO can overcome conceptual and policy hurdles, significant effort will still be required to develop the necessary forces and capabilities across all domains, but perhaps especially for cyberspace.

Operationalising MDO demands a ‘calibrated force posture’ with multi-domain formations strategically positioned, held at readiness and able to deploy over large distances, trained and equipped to operate across multiple contested domains (Grispen-Gelens, 2020). The vision is for different sensors and shooters to share and fuse data, build a common operating picture, inform rapid decision-making and deliver effects at a time and place of the commander’s choosing and to do so agnostic of domains, nation, service or platform (Niewood, Grant & Lewis, 2019). Forces must operate at pace and against an adversary contesting all domains. This tempo necessitates moving beyond NATO’s past focus on synchronisation of pre-planned effects in individual domains towards more agile targeting and more resilience against hostile attempts at ‘disorganisation’ or ‘systems attack’ (Thomas, 2019; Engstrom, 2018).

Linking all this together demands novel approaches to C4ISR, as reflected in investments in JADC2 (Harrigian, 2020). This US initiative leverages advances in information and communication technologies such as mesh networks, cloud and edge computing, open architectures, data analytics, AI and machine learning, autonomy and automation, software-defined systems, robotics, satellite communications and sophisticated cyber and EMS capabilities (Hitchens, 2019). Future JADC2 networks must be secure, robust, resilient, agile and more decentralised, with enough bandwidth to share data in a timely and secure manner despite cyber attacks, jamming, spoofing or physical destruction of communication nodes (Goldfein, 2017). Trust is also essential, handling data from different sources and at multiple security levels without making controls so arduous that users and devices cannot access the network (Donaldson & Sciarini, 2019a).

Reliance on connectivity makes cyberspace, space and the EMS the ‘centre of gravity’ for MDO (Hess et al., 2019). JADC2 introduces obvious challenges from a cyber threat perspective, both in terms of the attack surface for different threat vectors and the cascading effects from hostile cyber activity—though, of course, existing centralised C2 hubs also have their own vulnerabilities to cyber or physical attack (Hess et al., 2019). Improved cyber capabilities are not only needed to secure and enable operations in other domains (Reilly, 2020). Investments by Russia and China to contest cyberspace and the EMS may also limit the ability of NATO commanders to employ offensive cyber capabilities at a time and place that will ‘converge’ with effects through other domains. Securing networks against disruption is critical at the operational and strategic levels given requirements for reach-back to headquarters, especially constraining organisations responsible for delivering offensive cyber effects, since these are likely to be physically located in the homeland (Watling & Roper, 2019; Nettis, 2020).

D. Challenges for Command and Control

Any shift towards MDO also raises difficult questions about C2. NATO is arguably already challenged by seams when executing joint warfare, let alone a more ambitious vision of future JADC2 (Perkins & Olivieri, 2018; Zadalis, 2018). In broad terms, this could adopt a more hierarchical or de-centralised model, each with associated benefits, costs and risks (DCDC, 2015). The 140 NATO C2COE has launched an MDO C2 demonstrator to explore these issues, including how new technology might enable accelerated decision-making, reduced reliance on siloed physical command centres and a re-imagining of mission command for future MDO (NATO C2COE, 2020a).

Problematically, authorities associated with using cyber capabilities are typically held at the strategic and national level; how tactical or operational commanders might call upon cyber means as part of future MDO remains unclear (Nettis, 2020). Responsibilities for cyberspace also often fall at least partly to civilian agencies, adding the complexity of cross-government cooperation. The private sector’s role developing and applying technologies in the cyber domain (and, increasingly, space) also necessitates that NATO work more closely with industry, academia and others than for land, maritime or air operations (Ablon et al., 2019). This presents operational, policy and legal difficulties for C2, and cybersecurity challenges associated with reliance on industry-owned networks, though Allies continue to evolve novel mechanisms for partnering with industry to address cyber threats (Carr, 2016). There is also the question of tempo: how to synchronise operations in cyberspace with the delivery of effects in other domains (Reilly, 2020). Though cyber attacks might initiate in a moment, the underlying tools and exploits may take years to develop and the lead times and scale of their eventual effect may be difficult to predict or measure given the difficulties with battle damage assessment in cyberspace or the EMS (Patrikarakos, 2017; US Joint Staff, 2019). Similarly, commanders may lack awareness or understanding of available cyber instruments and their limitations and effects compared to more familiar weapons in the physical domains, limiting inclusion in joint planning and decision-making (Carbonell, 2017).

**SDFSDF**

**University of Exeter** **20** – public research university in Exeter, Devon, South West England, United Kingdom. Its predecessor institutions, St Luke's College “Should NATO Adopt a Joint Offensive Cyber Capability?” 09-2020, Accessed 06-28-2022, <https://socialsciences.exeter.ac.uk/media/universityofexeter/strategyandsecurityinstitute/pdfs/mstrat/James_Prideaux.pdf>. //AN

Nonetheless, significant challenges remain with regard to jus in bello and cyberweapons. First, distinguishing between military and civilian targets is sometimes hard, because so many military functions and systems rely on civilian technology.225 Although Chapter 2 gave the example of air defence networks, which have little crossover with civilian networks, many other targets are more complicated. Large amounts of military communications are still sent across civilian networks, while civilian websites can be used to coordinate military operations.226 For instance, Kurdish militias in Syria used Google Earth to coordinate American airstrikes on Islamic State positions.227 Although civilian technologies used for military purposes unquestionably qualify as military objectives in times of war, they may still not qualify as legitimate targets if there is a risk of excessive collateral damage.228 Thus, cyberwarfare exacerbates the long-standing debate over the definitions of military and civilian targets.229

Second, it can be very difficult to launch a proportional cyber response, for several reasons. If Russia launched a cyberattack on a member state’s banks, as it did against Estonia, IHL would prevent NATO from launching commensurate attacks on Russian banks, because they are clearly civilian targets.230 Attacking a different target to achieve similar effects would be very hard to perform. Additionally, before launching a retaliatory cyberattack, it is difficult to anticipate whether its likely collateral damage will be excessive in relation to the anticipated military advantage gained.231 As Stuxnet demonstrated, even exceptionally well-executed cyberattacks can spread in unpredictable ways.232 If a retaliatory strike did unintentionally contravene the principles of proportionality or distinction, it would be extremely difficult to hold NATO to account. If NATO breaches IHL, its constituent members are held accountable in international courts and tribunals.233 However, it is very hard for victims to determine exactly which state is responsible because they lack mission- specific knowledge, while NATO’s documents are mostly classified.234 The highly secretive nature of cyber operations would likely aggravate this.

Finally, it would likely be very challenging to pool members’ sovereign capabilities in the first place, because they currently abide by different legal codes in cyberspace. This is even posing a problem at the CyOC. According to Eneken Tikk of the Cyber Policy Institute in Finland, the legal ‘elephant in the room’ at Mons is bringing national realities and strategic ambitions together.235 The starkest example of this problem is different member’s legal conceptions of sovereignty in cyberspace. Although France perceives any penetration of its networks as a violation of sovereignty, the UK has instigated a lively legal debate by stating that it does not recognise sovereignty in cyberspace at all.236 Moreover, the UK actually accepts that it cannot entirely conform to the laws of armed conflict when using offensive cyber in a deterrence capacity.237 It seems it would be very hard for NATO to follow international law if its own members admit they cannot. Meanwhile, with regard to jus in bello, the US labels war-sustaining objects, such as munitions factories, as military objectives susceptible to lawful attack.238 However, most other states do not adopt the US approach, most likely because attacking these targets risks infringing on the principles of proportionality and distinction.239 Overall, NATO would face three very tough legal challenges if it were to form a joint offensive cyber capability. It would have to navigate the uncertainties of jus ad bellum, before selecting targets judiciously in accordance with jus in bello. Plus, to even establish the capability, it would have to iron out some of its members’ key legal disagreements. This would not be easy and it would be unrealistic to hope to establish a joint capability in the short-term. However, it could be possible long-term, as Chapter 5 elaborates.