**DA – NATO Tradeoff**

**DA – NATO Tradeoff [Collective Defense]**

**Notes**

**At: Ukraine/thumpers**

Ukraine did not require shift priorities, just shifting where existing budget is spent

Plan requires rewriting military strategy

**Do not read climate & collective together**

**L- INFO**

Clearinghouse – NATO orgnaizationa focused on logistics (set of requirements for what we need to communicatE) 🡪 bureaucratized, takes time, incentivzes ppl to ofocus on how much they r compling w/ those rules.

Bilateral info solves – much more flexible,

Competition – aff must do it through NATO process

Disrupts NATO’s rpiroities as an instituionT

**NOTES**

Low-level cyber ops (spreading disinfo, getting data, etc.)

OCOs are credible deterrent b/c they are proportionate

Credibly threaten to impose costs/

Deterrence by punishment

SANCTIONS similar – not credible & Russia invaded ukraine anyway, sanctions very costly – deterrnec by punishment, signaling

Alternative is do nothing or overreact

Current OCOs sufficient to deter Russia

No follow on

AF===

Conventional military responses to what Russia does in Baltics not credible b/c Russia believes they would be disprorpotinate or bluff

Small towns in eastern slice of Baltic country – Russia could get to Estonia in a couple of hours, invading nato member

If they take town and stop, what do we do? Do we just let thme keep it, lahout w/ military? – OCOs = FINE GRAIN

CP that imposes other credible deterrence

Deterrence by denial vs punishment – make it extremely difficult for thme to do the thing vs. threat of imposing costs – IRL deterrence is both

Conventional = NOT NUCLEAR and physical exchange of fire.

US beefing up forward presence throughout eastern europe

If Russia push further, have to go thru US, creates tripwire, much more likely to make them think twice

DA not great at deterring low level cyber

* have internal link and impact defense to Russia low level cyber

1. Russia sufficiently deterred now

2. conventional stuff matters more – and cyber stuff doesn’t –

- limitations of cyber what are the limits of what we can accomplish through OCOs – plan prevents exposing each other 🡪 more effectively do OCOs, but can’t make OCOs more capable of more than they can do. Maybe we can trun off power grid for a couple days, but is that really enough of a cost to not do something that threatens NATO – no

- conventional warfare key “forces postured” in Estonia – need to beat Russia

VERY intrinsic physical forces = tripwire

TURN OFF POWER GRID RELIES ON THEM THINKING THAT’S SOMETHING THEY CARE ABOUT

3. even insofar as cyber are able to deter, current cyber sufficient to do that already

-- AT: takeout I/L – current OCOs do as much as they could. Conventional operations/focus on NATO force posture key –

READ on case – u r wrong that there is fratricide, doesn’t actually disrupt operations 🡪 why did they happen to conclude that current OCOs are fine. b/c they were wrong

Blockade black sea – care about continued flow of foods and goods etc.

If current OCOs are working well, 2NR can just say we need combo of all of these things, aff is wrong that they make other thing that much better, but they do sacrifice the other key piece of the puzzle that is in place – ONLY cyber stuff ONLY slightly better – neg = enough cyber stuff + other things we need to.

CP about force posture – do not go for w/ tradeoff

* sanctions, posturing forces, position long-range strike capabilities far forward, destroy individual tanks – PROPORTIONAL
* goes with OCOs bad

focusing NATO’s attention around sharing info to cyber stuff

1. do not fiat set of stuff that impact is about

2.

**1NC – DA [Russia]**

**NATO will double down on collective defense against Russia now**.

**Kochis & Spoehr, 6/23** – senior policy analyst in European affairs in the Margaret Thatcher Center for Freedom (Daniel Kochis and Thomas W. Spoehr; "NATO Summit Madrid: Reinforcing Deterrence at This Crucial Time Is in the U.S. National Interest"; The Heritage Foundation; https://www.heritage.org/sites/default/files/2022-06/IB5276\_0.pdf; 06-23-2022, Accessed 6-25-2022)//ILake-NoC

The North Atlantic Treaty Organization’s (NATO’s) summit in Madrid on June 29 and 30 comes at a consequential moment for the Alliance. Russia’s unprovoked second invasion of Ukraine, the ensuing war that has resulted in the deaths of at least 4,000 Ukrainian civilians,1 and the displacement of over 14 million people is very likely a fulcrum in history. The transatlantic community will not return to the pre-invasion relations with Russia and must plan accordingly. As the shock of Russia’s invasion on February 24 has evolved into the realization that the war is likely to grind on, the transatlantic community must steel itself for the long haul.

For NATO, the Madrid Summit is an opportunity to expand upon the initiatives announced at the Brussels Summit in April, fulfilling the immediate **need for further deterrence measures** in Eastern Europe with a clear-eyed resolve, while putting in place plans to ensure that NATO has the capabilities to continue tackling challenges over the long term. While the summit provides a **historic opportunity**, the danger is that the summit will merely repackage half measures—which Russia would see as a sign of weakness, inviting further aggression. The U.S. must ensure that the Madrid Summit fulfills its potential. For the United States, a stable, secure Europe is firmly in U.S. national interest, and a stable and secure Europe begins and ends with a vigorous NATO capable of deterring Russian aggression against its member states.

The past few months have underscored the reality that, while many European nations have stepped up, there is no substitute for U.S. leadership within NATO. As such, the U.S. should ensure that NATO implements measures that bolster deterrence immediately while laying the groundwork for retaining strength in the long term through robust defense investment. The U.S. should propel its allies toward a wholesale recommitment to collective defense and all that entails: robust, lasting commitments to defense spending, moving beyond tripwire forces in Eastern European member states toward a force posture of deterrence with broad participation across the Alliance; swift consideration of Finland and Sweden in NATO; and support for member states that are aiding Ukrainian forces.

In the U.S. National Interest: A Robust NATO

For economic, political, and security reasons, the U.S. maintains a central interest in the peace and security of the European continent. While Russia’s second invasion of Ukraine has proven profoundly destabilizing, the core mission of NATO, to deter aggression against member states, remains intact, and Russia has thus far shied away from any direct military action against a NATO member state. To avoid further miscalculations and lessen the chance that Vladimir Putin strikes a NATO member, the Alliance must bolster its deterrence posture, **starting with fleshing out the promises** of the Brussel Summit to put in place new forces to deter Russian aggression and, if necessary, defeat an invasion of a NATO country.

In response to Russia’s first invasion of Ukraine in 2014, NATO created an Enhanced Forward Presence (EFP) of four multinational battalions in each of the Baltic states and Poland. While the force size in each battalion, typically 1,000 to 1,500 troops, is small, the idea was to deploy a multintional force as a signal of resolve as well as a so-called tripwire to ensure that, should Russia invade, the battalion would not only slow down any advance but also provide critical political insurance that member states contributing troops would literally have skin (or, more accurately, lives) in the game to galvanize their sustained involvement in the conflict. This spring in Brussels, the Alliance announced the creation of four additional battalions, one each stationed in Bulgaria, Hungary, Romania, and Slovakia. While the Alliance’s decision to create additional battalions is helpful, it is clear that a small tripwire force does not provide the deterrence effect that a larger force, **complete with enablers, such as air defenses**, could. Recently, German Chancellor Olaf Scholz backed the calls of Lithuanian officials (where Germany leads the EFP battalion) to create a brigade-size presence (usually 3,000 to 5,000 troops).2

**The aff overcommits NATO to broad info-sharing responsibilities, which trades off with a focus on collective defense.**

**Moller, '20** – Assistant Professor at the School of Diplomacy and International Relations (Sara Bjerg Moller; "It Will Take More Than a Biden Victory to Solve NATO’s Strategic Malaise"; War on the Rocks; https://warontherocks.com/2020/09/it-will-take-more-than-a-biden-victory-to-solve-natos-strategic-malaise/; 9-25-2020, Accessed 6-24-2022)//ILake-NoC

If and when the Biden team embarks on its grand European tour, it seems virtually certain that, beyond the expressions of gratitude for America’s “return” that will surely follow them wherever they go, the delegation can expect to be met with a lengthy list of items requiring their immediate attention. Moreover, appeals for Washington’s assistance are likely to differ from capital to capital, with each NATO ally arguing that their particular issue or concern represents the most pressing challenge and therefore requires the most attention and resources. In Warsaw and the capitals of the Baltic states, the U.S. delegation will hear that, despite a new U.S. rotational troop deployment, a revanchist Russia necessitates additional NATO (but especially U.S.) military commitments along the Eastern flank of the alliance. In Rome, Athens, and Madrid, U.S. policymakers will learn that the Mediterranean countries represent the “soft underbelly” of NATO and that the alliance must do more to project stability along its southern arc of instability. In Ankara, the message will be one of anger directed at what the Erdogan government perceives as NATO’s collective failure to support Turkish actions in Syria and elsewhere. In Paris, the message for the U.S. delegation will be that the alliance must strengthen its counter-terrorism efforts in the Middle East and North Africa, while in Berlin the focus will be on reforming NATO’s nuclear posture and salvaging expiring arms-control agreements. Meanwhile, securing the Arctic and halting the effects of climate change will be at the top of the agenda in Copenhagen and Oslo.

In short, wherever the Biden presidential delegation goes, it will be met with requests that Washington — and with it, the NATO alliance — **prioritize** **everything**, thereby fulfilling the old adage that, “**When everything is a priority, nothing is a priority**.” Given the precarious state of international relations today, the temptation to do more is understandably strong. It is easy to understand why, in the present climate of global instability, calls for the transatlantic alliance to reinforce and strengthen its existing commitments while simultaneously adding new mandates, missions, and programs are popular. Rather than adding more items to its **already crowded agenda**, however, the time has come for not just the United States but also NATO to consider **doing less but** doing it **better**.

When More Is Less, and Less Is More

For an alliance that has long prided itself on its commonality of purpose and interests, the truth is that NATO is in danger of losing both. On paper and in public, the members still agree the core purpose of the 71-year-old alliance is deterrence and defense of the North Atlantic region. When internal disagreements are aired publicly, other allies are quick to dispel reports of rifts by pointing out that differences of opinion are nothing new. But unlike during the Cold War, when a single adversary occupied all of the alliance’s attention, today’s security environment — as the allies routinely remind each other — is multifaceted and complex. In an effort to address members’ often disparate security requirements, NATO has taken on additional tasks over the past three decades almost as quickly as it has taken on additional members. The NATO-ization of every security challenge has meant that issues once considered the purview of individual nations or other international organizations — such as migration, terrorism, and foreign security force assistance — are now lumped onto NATO’s agenda under the guise of fulfilling its ambitious (and potentially limitless) post-Cold War mandate of “projecting stability.”

For far too long now, alliance leaders have tasked the NATO military infrastructure with a seemingly impossible undertaking: weighing down the military organization with new responsibilities like peacekeeping and counter-terrorism while simultaneously allowing members to **shirk on contributing** the **resources** required to fulfill old and new alliance missions. To date, much of the criticism surrounding NATO’s current strategic deadlock has focused on the **resource** **issue** and the **strains** caused by uneven burden-sharing within the alliance. Far less attention has been paid to the first part of the “ends-means-ways” formulation of strategy, namely NATO’s original purpose. While addressing “means” and “ways” are crucial elements in any strategic enterprise, it is past time the Allies got around to focusing on NATO’s strategic ends once more.

Confronting NATO’s present strategic dilemma will require looking beyond existing strategic documents like the 1949 North Atlantic Treaty, which proclaimed the signatories’ commitment to the “preservation of peace and security” in the North Atlantic area. As the past three decades of NATO transformation have shown, there is not much that does not fit under the rubric of fostering “peace and security” and consequently cannot be tacked onto the alliance’s agenda. True strategy requires setting (and adhering to) actual **goals and priorities**, as well as developing plans to achieve them. Although the alliance’s past strategic documents have often sought to define NATO’s evolving strategic purpose with more precision than the founding treaty, the alliance has not adopted a new strategic concept since 2010 for fear that embarking on such an exercise would only further inflame the deep rifts within the alliance that such strategic endeavors are meant to help address.

Officially, NATO members still assert collective defense is the alliance’s primary task, despite the inclusion of two other core tasks — projecting stability and cooperative security/crisis management — in all three of its post-Cold War Strategic Concepts (1991, 1999, 2010). The addition of these latter two core tasks — coupled with members’ differing threat perceptions about what rises to the level of an existential security threat — has **clouded the organization’s focus**. After **three decades** of continual adaptation, the danger that the alliance’s original raison d’étre of collective defense gets further downgraded to the point where it risks becoming primus inter pares among NATO’s many other responsibilities is real. As with previous critical junctures in transatlantic relations, it will take American leadership to change NATO’s future course. Come January 2021, a Biden administration should move swiftly to announce its intention to commission a new NATO strategic concept by 2022. Should Trump win, all bets are off.

Defenders of NATO’s post-Cold War emphasis on projecting stability and collective security argue that NATO has a proven track record of crisis management and capacity-building beyond its borders in places like Bosnia and Herzegovina, Kosovo, Afghanistan, and Iraq. The alliance’s cooperative security track record, however, is hardly stellar. This past June, the NATO-led international peacekeeping force in Kosovo entered its 22nd year of operation. Almost 17 years after the alliance’s Integrated Military Command first assumed responsibilities in Afghanistan, the NATO flag continues to fly in Kabul, where some 15,000 allied troops remain as part of NATO’s Resolute Support mission. Nor can the alliance’s intervention in Libya in 2011 be considered a resounding success, judging by the state of affairs there today. That NATO remains engaged in some of these places decades afterward is not an impeachment of the men and women who served in these operations and performed the tasks demanded of them. It is, howevwer, evidence of NATO’s failure to give sufficient consideration to its core strategic purpose.

While one can debate the wisdom of NATO having accumulated such an expansionist security agenda in an era marked by American unipolarity, an all-encompassing approach to security is harder to justify in a time of waning American power. Just as the diminishing threat of great-power competition in the 1990s and early 2000s freed NATO to take on additional security tasks beyond its traditional mission of collective defense, its return should prompt a reexamination to determine whether NATO is still the appropriate entity for handling such tasks.

Another center of excellence, special representative, or office will not fix what ails NATO. As the authors of a recent Heritage Foundation report on “NATO in the 21st Century” put it, it is time for NATO to get “back to the basics.” There are limits to what an international institution — even one as successful as NATO — can accomplish: “When policymakers expect or want NATO to do what it was never designed to do, that is when the Alliance risks failure.”

The launch of NATO Secretary Gen. Jens Stoltenberg’s #NATO2030 reflection process earlier this year to address political reforms within the alliance presented just such an opportunity to tackle these and other big-picture questions. It is still unclear to what extent the pandemic has delayed the work of the group of experts begun last March. The Biden team will have to move quickly if it hopes to help shape the working group’s deliberations, as Stoltenberg is slated to brief members on the path forward for the alliance at the April 2021 Leaders’ Summit.

Back to the Future: Narrowing (Not Broadening) NATO’s Remit

Looking ahead, alliance leaders should consider ways to **streamline current NATO missions** and tasks so that responsibilities that fall below the threshold of existential challenges can be **unloaded onto other multilateral institutions** or **global partnerships**. In addition to bringing an end to the Resolute Support Mission in Afghanistan, alliance leaders should consider getting NATO out of the security assistance and stabilization business altogether. Calls for NATO to look for opportunities to do more in the MENA region should also be rebuffed. Few would dispute that this region poses real security challenges to European states or that these challenges are particularly acute for the southernmost members of the alliance, some of whom might even view migration and refugee flows as rising to the level of **existential threats**. But while the 21st century challenges to the “stability and well-being” of member states may be numerous and growing, there is only one NATO. A single organization cannot tackle every national security challenge its members face. To remain useful, the alliance must **choose which threats to prioritize**.

Doing so requires recognizing that **not every security issue** rises to the level of an existential threat to the alliance. Terrorist attacks were a common occurrence in many West European nations in the 1970s and 1980s, yet NATO did not fundamentally transform its agenda back then because members recognized that the threat posed by the Soviet Union was greater. While neither Russia nor China as yet represents a threat on par with the Soviet Union, NATO should prepare for the possibility that the latter (either alone or in combination with **Moscow**) **could pose an existential challenge** to the Atlantic community in the coming decades.

Nor is it evident that NATO was ever the appropriate venue for tackling threats like terrorism in the first place. Effective counter-terrorism requires intelligence-sharing; local policing and counter-radicalization programs; and financial instruments that agencies like Europol, Interpol, the Global Counterterrorism Forum, and others are better equipped to lead than an overstretched military alliance. The same is true when it comes to other activities the transatlantic alliance has added to its roster since 1991, like stabilization missions and security sector reform. In fact, organizations such as the United Nations, the Organization for Security and Co-operation in Europe, and the European Union provide more appropriate venues for tackling many of the collective security duties the alliance has assumed since the 1990s. As a regional defensive military alliance, NATO’s comparative advantage lies in providing territorial defense against other states or groups of states. This is a comparative advantage that should be preserved, not diluted by the addition of other security tasks. True comparative advantage arises from specialization. Continuing to add more and more security responsibilities to NATO’s already-full plate risks **transforming** the **military alliance into** a **glorified clearinghouse** or administrative apparatus whose sole task is the **facilitation of information-sharing** rather than the provision of **collective defense.**

Yes, NATO is better equipped to handle the myriad security problems its members face than any other multilateral security organization in existence today. But the proposition that because NATO has the resources and coordinating mechanisms it should automatically take on the latest mission du jour is what has led to a strategically deadlocked alliance.

Much like the 1990s, the coming decade will be one of transition for NATO. Back then, proponents of alliance reform argued that the only way forward was to enlarge the alliance and take on new responsibilities. Without such reforms, they claimed, NATO would disappear. The choice facing NATO members today is different: not a world without NATO, but a world in which NATO fails to fulfill its intended purpose. Preparing NATO for China’s rise does not mean sending alliance-flagged vessels to the South China Sea. But the reality is, as Stoltenberg put it last December, China is already “coming closer to us.”

Ultimately, NATO possesses few capabilities of its own. Individual allies — and not the alliance itself — retain ownership and control over the military material and personnel assigned to NATO operations and missions. The alliance’s **real strength**, however**, lies in its integrated military command structure**. Preserving and protecting the integrated command structure’s organizational bandwidth should be the primary focus in the coming years. Unloading the alliance’s collective security responsibilities onto other international actors would allow alliance military officials to focus on the challenges emanating from China (and, to a far lesser degree, **Russia**) free of the need to also tackle a host of lower-threshold security concerns, all of which require office space, funding, and personnel billets. Bifurcating collective security tasks from collective defense would also force European leaders once and for all to decide exactly what price they are willing to pay for their own national defense.

The Way Forward

Instead of seeking to **tackle every** new security **challenge** of the 21st century, NATO leaders should work to preserve NATO’s **core assets and capabilities** for the task that it is uniquely suited for: **deterring state-based adversaries** and defending the territorial integrity of its members. The time when NATO could be **both** a **collective defense** and a **collective security** organization has passed. Amid the reemergence of great-power rivalries, it no longer makes sense to assign NATO’s limited resources to naval operations in support of the refugee crisis as the organization did back in 2016. Or for the alliance to continue to try its hand at stabilizing war-torn nations.

NATO has survived this long by adapting. But unlike in the past, where NATO adaptation has always meant taking on more responsibilities, the reforms needed today are those that involve **shedding commitments** rather than taking on additional ones. In seeking to reestablish NATO once again as an alliance focused **solely on collective defense**, and not a collective security organization, the Biden team will need to resist the urge to pick up the phone and call NATO Headquarters whenever a new security challenge emerges, like previous U.S. presidents have done since the end of the Cold War.

Jettisoning the collective security responsibilities the NATO alliance has assumed over the past three decades won’t be easy. Nor does freeing NATO from responsibility for tackling issues like counter-terrorism and instability in the near abroad mean that such threats are not deserving of international cooperative efforts by states. It simply means that going forward, countries committed to these kinds of activities will have to look to organizations and venues other than NATO to address them.

Rather than **expend precious resources** and continue to use NATO as an instrument to grapple with all manner of cooperative security issues, a Biden administration should instead **reorient** the **alliance’s strategic focus** toward the more pressing task of adjusting to China’s rise. Not doing so risks turning NATO into nothing more than a **glorified discussion club**. To avoid this fate, the Biden team will have to move quickly. At stake is not just alliance unity but NATO’s future utility.

**That’s key to deter a looming Russian invasion of the Baltics.**

**Deni, '22** – Dr. John R. Deni is a research professor at the U.S. Army War College’s Strategic Studies Institute and a nonresident senior fellow at the Atlantic Council. (Dr. John R. Deni; "Yes, Russia Might Invade a NATO Country. Here’s How the Alliance Should Prepare."; POLITICO; https://www.politico.com/news/magazine/2022/03/04/nato-spread-itself-too-thin-00013933; 3-4-2022, Accessed 6-26-2022)//ILake-NoC

Russia’s invasion of Ukraine has triggered a careful balancing act on the part of NATO allies, who are eager to see Russia fail but also unwilling to jump into the war directly. This reflects the same challenge that has confronted the West vis-à-vis Ukraine for two decades: how to foster a sovereign Ukraine independent of Russia without necessarily inviting Kyiv into NATO or the EU.

The bottom line is that militarily, NATO will only offer limited assistance to Ukraine. Under Article 5 of the North Atlantic Treaty, allies are obligated to treat an attack on one as an attack on all. But the flip side is that they are under no obligation to help countries that aren’t members of the club.

While NATO’s short-term role in Ukraine may be limited, its bigger role now is to **keep Russia out of the rest of Europe**. For years, many have taken for granted that Putin will stop at NATO’s borders, deterred by the promise of an Article 5 response. But this is no longer a given in light of the Russian leader’s **belligerence** and **unpredictability**.

Although NATO’s Article 5 has not been triggered, Article 4 has — the provision of the treaty allowing member states to request consultations if they believe their “territorial integrity, political independence or security” is threatened. Requesting consultations may sound weak-kneed, but this in fact carries enormous political and diplomatic weight, with the potential to trigger serious military moves. Last week, no fewer than eight allies — Bulgaria, the Czech Republic, Estonia, Latvia, Lithuania, Poland, Romania and Slovakia — called for Article 4 consultations because they believe Putin’s actions threaten them, too.

The serious concerns of these eight allies are yet another indication that NATO may have **spread itself too thin**. Since the end of the Cold War, NATO has become something of an ‘**all of the above’** alliance, simultaneously engaged in collective defense in Europe, crisis management in places like Afghanistan and Iraq, and building cooperative security relationships across the globe from Morocco to Japan. Now, **NATO needs to recommit to its original mission**. In the short term, it should **expand** its **frontline battlegroups** **in** the **Baltic States** and Poland. In the longer term, the alliance needs to prepare to admit new members, equip itself to fight Russian hybrid aggression and expand its permanent presence in Eastern Europe.

Although the early days of the invasion seemed marked by some major setbacks for Russia and surprising momentum for Ukraine, the weight of evidence still points toward a brutal Russian victory. Russia retains overwhelming military advantage, and its drive to encircle Kyiv continues unabated. The Russian military has yet to commit all of the available forces that sit just across Ukraine’s borders. And the most likely outcomes remain a Ukrainian state dominated and/or dismembered by Russia and neighboring Belarus, which hosts an enduring, offensive Russian presence close to NATO territory.

NATO’s primary response — made after Article 4 was invoked — has been activating the NATO Response Force and its leading element, the Very High Readiness Joint Task Force, parts of which can deploy in as little as 48 hours. Notably, the alliance has never deployed any part of the NRF for collective defense purposes, not even in 2014 when Russia first invaded Ukraine. Sending this force to the alliance’s most exposed members in Eastern Europe, even though NATO has no intention of taking part in the war, is a powerful, tangible indicator of NATO’s commitment to defend every inch of allied territory and to deter Russia from expanding the conflict. Deploying the NRF is more than symbolic; it’s a response to genuine fears that the West may have its work cut out when it comes to deterring Putin.

Beyond this collective response, several NATO countries individually have committed to sending more defensive forces to Eastern European members and to continuing or increasing the flow of military assistance to Ukraine. These measures include the deployment of thousands of additional U.S. troops to Europe for both defensive purposes and to assist in managing the influx of Ukrainian refugees, an additional $350 million in U.S. security assistance for Ukraine, Germany’s groundbreaking decision to send anti-tank weapons and man-portable surface-to-air missiles, and an array of other steps.

The **question is whether all of this is enough to prevent** **Putin from looking** beyond Ukraine **to** the **Baltic States** or elsewhere in Eastern Europe. He may intend to create more buffer space along Russia’s western border, regain some lost semblance of Russian greatness, bolster his declining approval ratings at home or solidify his legacy. The point is, **Putin’s evident unpredictability** — and his government’s blatant lies on the eve of the invasion — create doubt that **Western defense** and deterrence **thus far are adequate.**

To reduce the risk that Putin will expand the conflict beyond Ukraine and prepare for the new reality of post-conflict Europe, **NATO should expand** **the scale, mission and capabilities** of the units that would be on the front lines of any Russian attack on Eastern European NATO countries. The Enhanced Forward Presence battlegroups, located in Estonia, Latvia, Lithuania and Poland, were established in 2017 as a somewhat belated response to Russia’s first invasion of Ukraine. Since 20 out of NATO’s 30 members contribute troops to these battlegroups, they represent a “tripwire”: If Russia was to invade one of the four host nations, several alliance members would likely sustain casualties, which would spur a faster, more unified NATO response. In this way, the EFP **battlegroups** help deter Russia by signaling NATO’s **increased willingness to take a risk** — the basic game theory at the heart of deterrence.

But shortcomings persist. Each battlegroup consists of roughly 1,200 troops, which probably isn’t enough to deny Russian advances. The EFP units also lack persistent American contributions (except for the unit in Poland, which is U.S.-led), struggle to share information internally and with one another, and lack the ability to tackle hybrid Russian threats.

It’s reasonably clear that Russia understands it will incur costs if it invades a NATO country — what international relations scholars call “deterrence by punishment.” What’s less clear is whether Russia sees the NATO military presence as foreboding enough to rule out the idea of invasion altogether — or “deterrence by denial.”

To change Putin’s calculation about a potential invasion of the Baltics or Poland, NATO can take a number of steps. First, it should expand each EFP unit to an enhanced brigade of 5,000 troops. This would dramatically increase the deterrent effect given that a typical Western brigade is a far more capable, self-sufficient combat formation in a way that a battlegroup simply is not.

Second, the United States should contribute at least a battalion to each of the expanded EFP units. There’s no substitute for American boots on the ground in Europe, which are a **physical manifestation of** the United States’ commitment to **Article 5.**

Third, the alliance should quickly provide each EFP unit (and the four nations that host them) common advanced, secure voice and data communications equipment and network tools, perhaps supplied by the United States. It’s here — in communications — where the number of allies involved in EFP is an Achilles heel instead of a strength. Twenty contributing allies can mean 20 different types of radios and computers, leading to serious internal communication challenges — a problem not faced by the Russians, who operate largely without allies. A common, off-the-shelf solution will not only enable the individual contributors to each EFP battlegroup to communicate, but also permit more effective communication between EFP units so they can operate together across borders.

Fourth, NATO should expand the mission of the EFP units. Currently, the units are almost entirely focused on conventional military missions. They are not equipped to conduct operations in the information space, with electronic warfare and signals jamming, or in cyberspace. Yet when I visited the units last year, I learned that they struggle against Russian information, electronic and cyber attacks almost every day. The alliance ought to authorize the EFP units to engage in these domains (only in accordance with host-nation policies, of course).

Beyond immediately strengthening EFP, NATO needs to **think more strategically** about how to adjust in the aftermath of Russia’s dramatic upending of European security. **Given** the challenges posed by Russia (and to a lesser degree, China) and the **requirements of collective defense,** **NATO probably can’t do it all**. It will either need to pare down its appetite and **focus almost entirely on collective defense** as in the Cold War, or receive increased resources from the allies to maintain the global set of tasks it’s taken on since the 1990s, including in crisis management and security cooperation in Africa, Asia and elsewhere.

**Baltics invasion causes nuclear war. Only strengthening traditional defense caps escalation.**

**Brands, '19** – Hal Brands is an American scholar of U.S. foreign policy. He is the Henry A. Kissinger Distinguished Professor of Global Affairs at the Johns Hopkins University School of Advanced International Studies and a Resident Scholar at the American Enterprise Institute. (Hal Brands; "How Russia Could Force a Nuclear War in the Baltics"; American Enterprise Institute - AEI; https://www.aei.org/op-eds/how-russia-could-force-a-nuclear-war-in-the-baltics/; 11-7-2019, Accessed 6-27-2022)//ILake-NoC

Yet a series of reports by the nonpartisan RAND Corporation shows that the **possibility of nuclear escalation** in a conflict between the North Atlantic Treaty Organization and Russia over the Baltic region is higher than one might imagine. The best way of averting it? **Invest more in the alliance’s conventional defense.**

There was a time when it seemed quite normal to risk nuclear war over the sanctity of European frontiers. During the Cold War, NATO was outnumbered by Warsaw Pact forces, and it would have had great difficulty stopping a Soviet attack with conventional weapons. From the moment it was formed, NATO relied on the threat of nuclear escalation — whether rapid and spasmodic, or gradual and controlled — to maintain deterrence. American thinkers developed elaborate models and theories of deterrence. US and NATO forces regularly carried out exercises simulating the resort to nuclear weapons to make this strategy credible.

After the Cold War ended, the US and its allies had the luxury of thinking less about nuclear deterrence and war-fighting. Tensions with Russia receded and nuclear strategy came to seem like a relic of a bygone era. Yet today, with Russia rising again as a military threat, **the grim logic of nuclear statecraft is returning.**

The spike in tensions between Russia and the West over the past half-decade has revealed a basic problem: NATO doesn’t have the capability to prevent Russian forces from quickly overrunning Estonia, Latvia and Lithuania. Russian invaders would be at the gates of the Baltic capitals in two to three days; existing NATO forces in the region would be destroyed or swept aside. NATO could respond by **mobilizing** for a **longer war** to liberate the Baltic countries, but this would require a bloody, dangerous military campaign. Critically, that campaign would require striking targets — such as air defense systems — located within Russia itself, as well as suppressing Russian artillery, short-range missiles and other capabilities within the Kaliningrad enclave, which is situated behind NATO’s front lines.

Moreover, this sort of NATO counteroffensive is precisely the situation Russian nuclear doctrine seems meant to avert. Russian officials understand that their country would lose a long war against NATO. They are particularly alarmed at the possibility of NATO using its unmatched military capabilities to conduct conventional strikes within Russian borders. So the Kremlin has signaled that it might carry out **limited nuclear strikes** — perhaps a “demonstration strike” somewhere in the Atlantic, or against NATO forces in the theater — to force the alliance to make peace on Moscow’s terms. This concept is known as “escalate to de-escalate,” and there is a growing body of evidence that the Russians are serious about it.

A NATO**-Russia war could thus go nuclear** if Russia “escalates” to preserve the gains it has won early in the conflict. It could also go nuclear in a second, if somewhat less likely, way: If the U.S. and **NATO initiate their own limited nuclear strikes** against Russian forces to prevent Moscow from overrunning the Baltic allies in the first place. And even the limited use of nuclear weapons raises the question of further escalation: Would crossing the nuclear threshold lead, through deliberate choice or **miscalculation**, **to** a **general nuclear war** involving intercontinental ballistic missiles, strategic bombers and **apocalyptic destruction**?

So what to do? One option would be for the West to pull back — to conclude that any game that involves risking nuclear war over the Baltic states is not worth the candle. The logic here is superficially compelling. After all, the US could survive and thrive in a world where Russia dominated Estonia, Latvia and Lithuania, just as it survived and thrived during the Cold War, when those countries were part of the Soviet Union. The problem is that **failing to defend** the **Baltic states** would devalue the Article 5 guarantee on which NATO rests: the principle that an attack on one is an attack on all. And given that one could raise similar questions about so many US commitments — would declining to meet a Chinese attack on the Philippines really endanger America’s existence? — this failure could **undermine** the **broader alliance system** that has delivered peace and stability for so many decades.

**2NC – OV – AT: Hybrid War**

**Conventional war outweighs cyberwar – cyberattacks are de-escalatory and replace more violent means.**

**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

Imagine two universes. In the first one, information systems are impervious to manipulation from the outside. No unauthorized person one can change the instructions that systems run and systems react to all input as they are supposed to (that is, consistent with the common understanding of designers and users). This is a world in which the **potential effects of cyberwar are**, at most, **weak** and largely irrelevant to the conduct of violent (i.e., kinetic) conflict. In the second universe, cyberwar is potentially consequence; it where we live today.

In which universe is violent conflict – war, if you will – more likely? In recent years, two scholars who agree on little else, Tomas Rid and John Arquilla, have put forward the case that the second universe, today’s is less likely to be warlike than the first universe, where cyberwar is impossible or at least inconsequential.[1] **Cyberwar**, in effect, **is good for peace**. Both scholars pivot their argument over Stuxnet, a piece of malware that was responsible for the destruction of roughly a thousand centrifuges in Iran’s uranium-enrichment facility, Natanz. Had the means of cyberwar not been available, they argue, there is a serious likelihood that Israel or even the United States would have tried to destroy Natanz using air raids. Such **air raids would likely have produced casualties**. Furthermore, the use of violence might have begotten violence in return – more likely terrorism (given Iran’s modus operandi) than **open war**, but the latter could not have been ruled out. Thus, the existence of Stuxnet allowed the problem created by Iran’s desire to enrich uranium (in order to making nuclear weapons) to be dealt with in a nonviolent way. To the extent that Stuxnet is archetypical, **cyberwar is good for peace.**

This paper argues that the case that cyberwar is good for peace is by no means so clear, something that can be demonstrated by a more rounded analysis of what cyberwar does and what the alternatives to cyberwar really are. To start, consider another attack on the (supposed) nuclear facility being constructed in Syria with North Korean help. [2] In 2007, Israeli jets destroyed this facility (Operation Orchard). According to Richard Clarke (and others), the air strike was aided by a cyberattack on Syria’s air defense system which essentially erased radar images of incoming aircraft allowing all the aircraft to make it back safely.[3] Now suppose that a cyberattack really was employed (other accounts say that more conventional electronic warfare was used[4]). Further suppose that, without the confidence that cyberwar would have disabled the radar, the raid’s planners would have been deemed it too costly in terms of lost aircraft and pilots and hence called it off. In the first universe, where the tools of cyberwar were unavailable, no raid would have taken place, no destruction would have ensued, and no casualties (Operation Orchard left one to two dozen dead) would have resulted. In that calculus, the cyberwar capabilities lead to more rather than less violence. Had Syria retaliated, a further cycle of violence might have commenced.

This example suggests that the picture is a little more complicated than the notion that cyberwar allows **nonviolent means to replace violent** **means**. A full analysis must ask (1) what choices are available with and without cyberwar, (2) what responses are likely to a cyberwar attack, and (3) what does the threat of cyberwar say for the likelihood of conflict, qua stability. Such analyses also have to be sensitive to different contexts. What may hold for a conflict among comparably strong countries may not hold for a conflict among countries, one of which is clearly stronger than the other. Furthermore, the possibility of operational cyberwar (used against an opponent’s military forces) may lead to different answers than the possibility of strategic cyberwar (used against an opponent’s infrastructure and society, usually away from the battlefield).

But first: why does this question matter? Normally, comparing the world as it is to a counterfactual world in which something had not taken place is a completely academic exercise. Un-invention never takes place (even if people do walk away from some technologies – nuclear power comes to mind). Weapons control is oft pursued and only occasionally succeeds (chemical and biological weapons provide the best example, but such weapons have low military utility, anyway). Although people worry about cyberattacks, the fact that they are not heinous – and, indeed, **have yet to hurt anyone directly** – coupled with the technical difficulties of enforcing arms control on virtual instruments of war suggests that they are unlikely to be banned. Norms against certain uses of cyberwar may have better chances, but they may also be worth less in terms of assurance.

**Card run**

**Stimpson, '15** – (Maj R.T. Stimpson; ""; No Publication; https://www.cfc.forces.gc.ca/259/290/317/305/stimpson.pdf; xx-xx-xxxx, Accessed 6-27-2022)//ILake-NoC

Cyberweapons have been hyped as an attractive alternative to conventional weapons due

to their affordability. Amy Chang a research associate in the technology and national security

program at the Center for a New American Security states, “cyber warfare is a great alternative

to conventional weapons, it is cheaper for and far more accessible to these small nation-

3

states.”3Ross Rustici argues that “Cyberweapons are a cheap way to build a global strike

capability against networked states.”4 He argues that poor states, who were incapable of

challenging larger more technologically advanced states with conventional weapons can now

take can now them on in cyber.

They are both partially correct. A cyberwarfare capability can be purchased on the

internet for a couple hundred dollars; one can purchase malware and botnets or hire the services

of a self-trained hacker.5

Gabriel Weimann identifies that “all terrorists need is an online

connection and personal computer.”6 What could be purchased at this price can be crude but very

effective. The ILOVEYOU virus was able to shut down businesses for hours and caused around

6 billion dollars in damages.7 Why would one waste money on expensive conventional weapon

that need upgrades and become obsolete when they can drop $200 on Craigslist for a virus or the

services of a ‘weekend cyberwarrior’?

Not all cyberweapons are created equally. As effective (causing damage to unprotected

computers) as it was, ILOVEYOU was not a militarized cyberweapon; it could not be directed

against a specific target, could not be controlled and was not sophisticated enough to penetrate

sensitive military networks. It proved to be more of an annoyance by indiscriminately attacking

hundreds of countries and millions of random emails.8

Thomas Rid points out that exceptional

cyber weapons require a lot of technical expertise and funding, hence they would not be the

preferred weapons of poor countries or non-state actors.9

A true cyberwarfare capability is

3

Ibid.

4 Ross Rustici, "Cyberweapons: Leveling the International Playing Field," Strategic Studies Institute (2011).37.

5 M. Lee and L. Hornby, "Google Attack Puts Spotlight on China's "Red" Hackers." Reuters (2010).

6 Gabriel Weimann, "Cyberterrorism: How Real is the Threat?" USA Institute of Peace (2004).

7

S. Kirschner, "I Love You...Not." Popular Science., 2000, .48-49.

8

Ibid.

9 Thomas Rid, Cyber War Will Not Take Place (London: Hurst and Company, 2013a).45.

4

expensive. The technologically advanced Stuxnet was able to discern targets and could be

controlled by the user after launch. It is estimated that Stuxnet cost around US$3 million dollars

to create.10 Additionally it is believed that the virus was tested by experts for many months

before it was actually launched.11 As malware and viruses become more and more complex so do

the defenses that prevent them from infecting computers. Advanced defenses will only raise the

costs and the entry requirements into militarized cyberspace.

Accessibility

Launching a real cyberattack is harder to achieve than media and movies portray it. An

obvious disadvantage to the state that wishes to replace physical weapons with cyber weapons is

that all future opponents 1) need to be present in cyberspace and 2) they need to be vulnerable to

cyberattack.

The first element is self-evident. You can’t attack someone in cyberspace if they don’t

have a presence in cyberspace. There are many countries, mostly poor and not technically

advanced, whose government, military and citizens are minimally connected. An attempted

cyberattack against such an unconnected country would have little to no effect and might even

go unnoticed. An advantage of physical weapons is that they can be employed against anyone

within range. Declaring cyberwar on a group that is not networked or dependent on IT systems

will not be all that productive.

Cyberattack, the critical component of cyberwarfare is reliant on, vulnerability. “One

distinction between cyberwarfare and warfare in all other media must be made: cyber warfare

requires that the targets have made mistakes in their implementation and use of digital

10 A. Hesseldahl, "Computer Worm may be Targeting Iranian Nuclear Sites," Bloomberg (2010).

11 Ibid.

5

equipment”12 If the adversary has a tight cybersecurity perimeter that is not penetrable, then

there is no cyberattack that can occur. A country that is in cyberspace can at any time reduce or

remove their presence. Making cyberattack difficult is not impossible. One way to protect

oneself against cyberattack is electronic isolation. By “air-gapping” a network from the rest of

the world a state makes it very difficult for outsiders to penetrate a system.13 The majority of

classified US Defense and other Western defense networks are air-gapped making if very

difficult to conduct a cyberattack.14 “Air-gapping” can reduce one’s vulnerability, however

human error plays a role in even the most perceptively secure systems, as was the case with

Buckshot Yankee. Buckshot Yankee, “the most significant breach of U.S. military computers

was caused by a flash drive inserted into a U.S. military laptop on a post in the Middle East in

2008.”15 The virus compromised a large amount of defense related sensitive material. Whether a

network is connected to the internet or not, cyberwarfare in all cases requires a window of

opportunity that is not necessarily going to be open when and where you need it to be.

Even when the opportunity exits to penetrate a system, an advanced country reliant on

cyberspace is going to employ advanced cyber defenses. Vulnerabilities will be hard to exploit.

It is not difficult to immunize one’s networks from cyberattack. Advanced cyberdefenses are

layered with other security measures to include “computing instructions that can only be

manipulated by hands on access to the hardware, preventing malware or malicious software with

12 Martin Libicki, "Why Cyber War Will Not and should Not have its Grand Strategy," Strategic Studies Quarterly

(2014).31.

13 Bruce Schneier, "Want to Evade NSA Spying? Don'T Connect to the Internet," Wired (2013).

14 Ibid.

15 Ellen Nakashima, "Defense Officials Discloses Cyberattacks," The Washington Post2010.

6

rogue instructions being placed on the machines.”16 This makes cyberattack against an advanced

state target very challenging.

Vulnerability is requisite but so is preparation time. It is true a cyberattack could be

launched at the click of a keyboard and the cyber projectile can arrive at target destination

instantaneously. There is however a substantial amount of preparation that needs to occur prior

to an attack whether retaliatory or pre-emptively. The Stuxnet attack would have needed

extensive knowledge of the nuclear facilities in Iran but also people with nuclear reactor

expertise.17

The need for so many pre-conditions to exist makes cyber not a particularly responsive

means to retaliate. When attacked by a physical weapon it is relatively easy to respond with

another physical weapon. If you are in range, your adversary is probably in range. For a

cyberattack to be effective as a pre-emptive strike option, the target needs to be known well in

advance, time is needed to probe the opponent’s system for vulnerabilities before attack. This is

one of the reasons cyberattack was not used during the NATO attack on Libya in 2011. The

attack was not foreseen in time to employ cyber means.18 One is not necessarily vulnerable to

your cyberweapon by virtue of their cyberspace presence.

Network vulnerabilities when found, are fleeting, especially with technologically

advanced states. When they are exploited and attacked they will be sensed by the defender and

repaired quickly. “Even if a potent cyber-weapon could be launched successfully once, it would

16 Libicki, Why Cyber War Will Not and should Not have its Grand Strategy30.

17 R. Langner, Cracking Stuxnet: A 21st Century Cyberweapon, Cracking Stuxnet: A 21st Century Cyberweapon.

Ted.com, 2011 .

18 Ellen Nakashima, "US Cyberweapons had been Considered to Disrupt Gaddafi's Air Defenses," The Washington

Post2011.

7

be highly questionable if an attack, or even a salvo, could be repeated in order to achieve a

political goal.”19

There are many things that can be done to reduce cyber and network weakness. If an

attack was impending there are substantially even more measures that can be taken. Just because

one has a cyberweapon does not mean one can use it at a time and place of choosing. It needs to

be enabled by the opponent’s carelessness and ignorance. For this reason alone cyberweapons

will never be a replacement for conventional weapons.

Risk and Cyberwarfare

Patrick Lin in his Atlantic article sees cyberwarfare as a low risk alternative to

conventional warfare.

This also means new channels for warfare. Indeed, a target in cyberspace is more

appealing than conventional physical targets, since the aggressor would not need

to incur the expense and risk of transporting equipment and deploying troops

across borders into enemy territory, not to mention the political risk of casualties.

Cyberweapons could be used to attack anonymously at a distance while still

causing much mayhem.20

Cyberwarfare is not a riskless affair to the user. A characteristic of cyberspace is that it is very

difficult to determine the follow-on effect of actions taken in cyberspace and even more difficult

to try to control these effects. Physical weapons are tangible; they can be inventoried, expended

and destroyed if required. When cyberweapons are used in cyberspace the user may not always

be able to contain the weapon’s effects or control its use and eventual destination. This can have

three very negative consequences:

19 Thomas Rid and Peter McBurney, "Cyber-Weapons," Rusi Journal 157, no. 1 (2012).

20 Patrick Lin, "Is it Possible to Wage just a Cyberwar?" The Atlantic (2012).

8

Firstly, a state’s cyberweapon will not necessarily discern enemy from friendly in

cyberspace. A launched cyberweapon could seep into the attacker’s networks and infect the

systems of the employer resulting in negative consequences. Conventional weapons effects are

observable and finite. It is not easy to tell what kind of damage a cyberweapon has done or

where a virus ultimately ends up. When a state loses control of the effects of its weapons, the

attacking state could do more damage to itself that to the intended target. Consequences of cyber

blowback would not be contained to defense systems and would include the technologies that are

integral to the state’s citizens. Major efficiencies and economic production could be

compromised. The secondary effects caused by engaging in cyberwarfare could undermine a

state’s citizen’s trust in cyberspace well into the future.

Secondly, a country that uses and creates advanced cyberweapons will need to be very

reliant on IT systems. This serves to increase a state’s vulnerability to the very cyberweapons it

is producing. It also increases the attractiveness of that state to other states wishing to employ

cyberattack.21

Thirdly, the most lucrative targets and typically most vulnerable in cyberspace are nonmilitary. Attempting to defeat the adversary by attacking the economy and industry of a country

through cyber will have global consequences given the interconnectedness of the world. Power

generators and communications networks are intertwined with other cities and countries. IT

infrastructure and private networks are connected globally.22 Due to the interconnectedness of

the financial systems, a successful attack against for example Wall Street will more than likely

21 James Adams, "Virtual Defense," Foreign Affairs 80, no. 3 (2001).98.

22 Andrew Krepinevich, "Cyberwarfare: A "Nuclear Option"?" Centre for Strategic and Bugetary Assessments

(2012).65.

9

have negative consequences to an attacker’s allies and the country itself. Interdependencies are

not always obvious in cyberspace.23

PART II

Cyberdeterrence

Threat and deterrence are unique psychological aspects within the concept of war. The

aim of deterrence is to persuade an adversary not to initiate action for fear the retaliation would

not be outweigh potential benefits.

A state deploys a deterrent strategy to protect an interest. To keep adversaries

from attacking the interest, a state makes a deterrent declaration, ‘Do not do this,

or else that will happen.’ This is any adversary action that would threaten the

[state’s] interest. That includes either denial measures, penalty measures, or

both.24

There is a significant body of knowledge that shows wars have been averted due to the

perception of strength or perception of powerful weapons that were in reality not as powerful as

they appeared.25 If arguing for cyberwar as a legitimate form of war, it would be rational to

assume that the associated negative costs and risks of engaging in cyberwar could act as a

deterrent. Will Goodman who has served as an advisor to US Defense dept. argues cyberwarfare

can be used as an effective deterrent. He states that “Cyberdeterrence proves easier in practice

than it seems to be in theory because cyberattacks are ultimately inseparable from the physical

domain, where deterrence has a long-demonstrated record of success”.

26

Cyberwarfare however does not represent an effective means to apply the functions of

deterrence. Deterrence requires two key elements: a credible threat and ability to communicate

23 S. Borg, "Economically Complex Cyber Attacks," IEEE Security and Privacy 3, no. 6 (2005).

24 Will Goodman, "Cyber Deterrence," Strategic Studies Quarterly (2010)., 105-106.

25 Geoffrey Blainey, The Causes of War (New York: Free Press, 1973).35-56

26 Goodman, Cyber Deterrence102.

10

the threat. Cyber unfortunately does neither effectively. Cyber coercion cannot compel like

physical means can. A physical force in a tangible environment is still preferred.

Known cyberwarfare capability on its own is not compelling. “All publicly known

cyberweapons have far less ‘firepower’ than is commonly assumed”.27 To deter, you need to

make the adversary believe that an attack will cause some level of pain and suffering. Though

the Stuxnet example might be an example of how physical damage can be delivered via cyber

(albeit indirectly), for now it is the exception rather than the rule in cyberwarfare. The cyber

attacker in reality is very limited in what can be achieved. Interrupting a state’s industry or

military communications network are irritating notions and could weaken the state temporarily,

they are however temporary and any resulting destruction could be fixed fairly quickly as

previous examples have indicated. Retired US Marine General James Cartwright has been urging

the US military to be more overt with their cyber capability.

We've got to step up the game; we've got to talk about our offensive capabilities

and train to them; to make them credible so that people know there's a penalty to

this," said Cartwright. "You can't have something that's a secret be a deterrent.

Because if you don't know it's there, it doesn't scare you.28

Cartwright is correct, if you want to deter, having the capability is important but you also need to

communicate to your enemy your ability. What Cartwright fails to realize, is how hard this is to

do in cyberspace. When it comes to deterrence, actions speak louder than words. In

cyberwarfare deterrence is difficult.

Pointing to one’s ability to use cyberweapons effectively in the past would not

necessarily be all that compelling. If a computer virus was launched in the past and discovered, it

can be safe to say an attack employing an identical or similar virus and using similar

27 Rid and McBurney, Cyber-Weapons

28 Shane McGlaun, "DARPA Wants More Money for Cyber Weapons," Daily Tech Magazine, 2011, .

11

vulnerabilities would be nearly impossible to deliver again. Additionally the cyberweapon design

utilized will have been dissected and access points patched. As soon as Stuxnet was discovered it

was globally “outted” and neutralized.

Once you know that it's there it's not that difficult to reverse engineer.

Neutralization of Stuxnet, once its operation is understood, would not be that

difficult as it was precisely engineered to disrupt a specific item of machinery,

once Stuxnet’ s signature is identified it can be eliminated from a system .29

Launching a lesser show of force attack like overtly probing an enemy’s servers or causing

minor network disruptions to illustrate a capability would work well in an observable world, but

not so much in the virtual world. By conducting a show of force you telegraph your intent to use

cyberwarfare. Lupovici sees this as a significant drawback stating, “exposing the offensive

capabilities as the consequence of repeated attacks may serve as the basis of knowledge or

inspiration for the challenger, it is also likely to allow enemies to prepare for a future threat.”30

Attribution is another challenge in cyberdeterrence. The advantage of easily being

anonymous in cyberspace has its benefits and drawbacks. When trying to coerce in cyberspace it

is a drawback. Cyberspace is not an exclusive club where all members are known, like the

‘nuclear club’ of the Cold War. The majority of the world is operating in cyberspace.31 This

poses a problem in deterrence as the sender of a cyberdeterrence message may not be known.

When the sender is not known the message can be misinterpreted, misread, misidentified or

perhaps not even detected. There is a difference between a cyberattack that originates from a

domestic hacker and one that is external and state sanctioned. The attack against Estonia in 2007

used hundreds of thousands of computers from 178 countries against 90% of the key information

29 Peter Sommer, "Experts Say, Iran has Neutralized Stuxnet," YNet News- Middle East, 2012, .

30 A. Lupovici, "Cyber Warfare and Deterrence: Trends and Challenges in Research," Military and Stategic Affairs

3, no. 3 (2011).55.

31 J. Nye, "Cyber Power," Belfer Centre for Science and Int'L Affairs Harvard Kennedy School (2010).4.

12

systems in the country.32 The origin of the attack could not be determined; without knowing who

was attacking it is difficult to determine what the purpose of the attack even is. Estonia is an

example of how difficult it might be to attribute what the message is and where it is coming

from.

Cyberspace is not a good venue to achieve deterrence. Physical weapons and their effects

are observable and their effects are understood making deterrence compelling. Deterrence

through cyber is not effective as one cannot effectively communicate the threat in which one

should fear.

Cyberpower

Could cyberpower replace conventional military means in other domains? Cyberpower,

as a new form of warfare has been compared to the emerging airpower theory of the 20th century.

Andrew Krepinevich states, “in the context of the historical analogies discussed, the state of

cyber weapon development appears to most closely approximate that of airpower during the

1930s.”33 He further states that a “cyberattack on an advanced state’s critical infrastructure

achieves results more similar to those of the strategic bombing campaigns of World War II”34It is

argued that cyberweapons can strike at strategic targets like industry supporting the war effort

and the state infrastructure so crucial in holding the will of the people together. Conceptually,

there are obvious similarities between airpower and cyberpower, however the domains of

cyberspace and air are vastly different. The most glaring difference is in the potential to create

destruction. During WWII, Allied aerial bombing campaigns could effectively strike deep into

Nazi Germany, degrading support to the war effort.

32 Charles Clover, "Kremlin Backed Group Behind Estonia Cyber Blitz," Financial Times- Europe (2009).

33 Krepinevich, Cyberwarfare: A "Nuclear Option"?79.

34 Ibid.65.

13

The German experience suggest that even a first class military power- rugged and

resilient as Germany was- cannot live long under full-scale and free exploitation

of air weapons over the heart of its territory. By the beginning of 1945, before the

invasion of the homeland itself, Germany was reaching a state of helplessness.

Her armament production was failing irretrievably, orderliness in effort was

disappearing, and total disruption and disintegration were well along.35

Bombing campaigns targeted civilian targets like transportation, electricity and manufacturing

infrastructure that enabled war production. Assessment reports post Second World War

determined irreparable physical damage needed to occur to inflict strategic victory over the

means of production.36

Cyberattacks cannot achieve destruction of infrastructure like

conventional weapons can. Networks can be disrupted temporarily but the hardware and

machines that enable cyberspace will still be intact. “Because cyberwar does not involve

bombing cities or devastating armored columns, the damage inflicted will have a short-term

impact on targets”.37

Another effect of aerial bombardment is the immediate delivery of shock and destruction.

It is seen and felt. Cyberweapons are incapable of delivering this sensation. Empirical evidence

shows that a cyberweapon has never caused immediate direct damage and destruction on the

same level as bombs. Stuxnet took many months to damage Iranian nuclear facilities.38

Aerial bombardment can be overwhelming on first strike, but usually requires multiple

waves and re-attack to achieve strategic goals. This was noted in the US Strategic Bombing

Survey, “no indispensable industry was permanently put out of commission by a single attack.

Persistent re-attack was necessary.”39

Attacks were rarely successful on the first attempt and if

35 . The United States Strategic Bombing Surveys, Summary Report (Maxwell Airforce Base, Alabama: Air

University Press,[1945]).37-38.

36 Ibid.

37 Eric Gartzke, "The Myth of Cyberwar," International Security 38, no. 2 (..57.

38 Langner, Cracking Stuxnet: A 21st Century Cyberweapon

39 . The United States Strategic Bombing Surveys, Summary Report39.

14

they were, the German industry was very capable of replacing and rebuilding infrastructure.40

Persistent attacks is not a luxury in cyberwarfare.

Cyberattacks “are most effective as an opening salvo in war”.

41 Once an attacker has

infiltrated a network the defender will quickly move to patch the vulnerability and perhaps even

close the network from the outside. For a re-attack to occur, another vulnerability in the system

would need to be found. The more attacks that are launched against a system the harder it

becomes to find future vulnerabilities.

Though cyberattacks can achieve disruption of critical industry in depth for minimal

expenditure, they are not a replacement for airpower as they are incapable of delivering the

carnage of bombs and cannot be employed persistently. The more pragmatic use of

cyberweapons is in a combined force environment which may be alongside strategic bombing

campaigns but always synchronized with conventional warfare assets

**2NC – T/C – OCOs**

**2NC – T/C – Cohesion**

**2NC – UQ – Collective Defense Now**

**NATO is shifting priorities towards Baltic conventional defense now, but that requires massive resource re-allocation.**

**Foy, 6/27** – FT's European Diplomatic Correspondent, based in Brussels. He reports on the EU's foreign policy, relations between Brussels and other world powers, and the diplomatic intrigues between member states. Previously he was Moscow Bureau Chief, where he interviewed president Vladimir Putin and charted his regime's descent into repression (Henry Foy; "NATO to increase forces on high alert to 300,000 "; Financial Times; https://www.ft.com/content/39caeff3-38cf-44e2-9270-835ab28f13c8; xx-06-27-2022, Accessed 6-28-2022)//ILake-NoC

Nato is to increase its forces on high alert by **more than sevenfold** to 300,000 in response to Russia’s invasion of Ukraine as part of a sweeping overhaul to **better protect its eastern flank.**

In a historic shift from the post-cold war era, when military spending was cut and troops pulled back from eastern Europe, secretary-general Jens Stoltenberg said the western alliance would also increase deployments close to Russia, **shifting** the **focus** from deterring any invasion **to** a **full defence of allied territory**.

The pledge to increase the number of troops on high alert across allied countries from 40,000 came as G7 leaders vowed to impose new sanctions to curb Moscow’s import of technology for its arms industry, amid efforts by western countries to respond to Russia’s invasion of Ukraine.

Speaking before the announcement, Stoltenberg told the Financial Times that the new military blueprint would **drastically upgrade its eastern** **defences**, tearing up a model that could have meant relinquishing and then attempting to recapture the Baltic states in the event of a Russian invasion.

Estonia’s prime minister has claimed that the current doctrine accepted that the **Baltic states would be “wiped off the map**” in the event of a Russian assault before Nato attempted a counter-attack to liberate them after 180 days.

“We never share the details of operational plans,” Stoltenberg said. “But I can assure you that we have been able to protect countries bordering Russia for decades, adjusting our presence in light of the threat assessment. We have done that before and we will do it again.”

The alliance would “significantly reinforce” its defences in eastern Europe, he said, pledging that Russia would not be able to capture the Estonian capital Tallinn “just as they have not been able to seize the city of Kirkenes in northern Norway or West Berlin during the cold war”.

The new “strategic concept”, to be signed off at an annual summit of alliance leaders that begins on Tuesday in Madrid, would define its goals and approaches for the next decade, and agree on a vastly expanded plan to defend its easternmost allies in response to Russian president Vladimir Putin’s invasion of Ukraine.

That will include new structures in which western Nato allies, such as the US, UK and France, would pledge their ships, warplanes and a total of more than 300,000 troops to be ready to deploy to specific territories on the alliance’s eastern flank, with graded response times starting from the opening hours of any attack.

**Yes – CUT lower para ab cyber too**

**Machi, '22** – reporter based in Stuttgart, Germany, contributing to Defense News' European coverage (Vivienne Machi; "NATO to boost readiness numbers, approve new Ukraine aid at Madrid summit"; Defense News; https://www.defensenews.com/global/europe/2022/06/27/nato-to-boost-readiness-numbers-approve-new-ukraine-aid-at-madrid-summit/; 6-27-2022, Accessed 6-28-2022)//ILake-NoC

STUTTGART, Germany — NATO plans to approve increased readiness objectives and provide more support to Ukraine, as well as formalize a key strategic document at its annual summit this week, alliance Secretary-General Jens Stoltenberg said Monday.

At the summit held Tuesday and Wednesday in Madrid member nations will agree to increase the number of high-readiness forces to “well over” 300,000 troops, in what Stoltenberg called the biggest overhaul of the alliance’s collective defense and deterrence since the Cold War. The alliance plans to enhance many of its forward-deployed battlegroups currently stationed in its eastern member countries up to brigade levels, he noted in a press conference broadcast online from Brussels.

The readiness increase will be matched with more prepositioned equipment and supplies stockpiles, notably air defense capabilities, he added. NATO is also planning to upgrade its defense plans, and pre-assign troops to defend specific allies.

“These troops will exercise together with home defense forces, and they will become familiar with local terrain facilities and our new prepositioned stocks, so that they can respond smoothly and swiftly to any emergency,” Stoltenberg said.

The ongoing war in Ukraine will be at the top of the summit’s program, particularly as President Volodymyr Zelenskyy is expected to attend. NATO plans to approve a new comprehensive aid package for Kiev, to include “partial deliveries” of capabilities like secure communications, unmanned systems and fuel, per Stoltenberg.

NATO’s identification of Russia as its most significant threat will be reflected in the ongoing deliberations over whether Finland and Sweden will become the alliance’s newest members. While Stoltenberg and other stakeholders have called for the two partner nations to join NATO as quickly as possible, member Turkey has promised to veto their accession, claiming Sweden has harbored members of the Kurdish Worker’s Party (PKK), which Ankara considers a terrorist organization.

On Monday, Stoltenberg reasserted the need to “take into account concerns expressed by allies” and said that the leaders of Finland, Sweden, and Turkey would meet at NATO headquarters in Brussels later that day, as well as on the sidelines of the Madrid summit this week.

“I will not make any promises, but I can just assure you that we are working actively to ensure progress, because the applications of Finland and Sweden to join NATO – they are historic,” Stoltenberg said. “It will strengthen the security of Finland and Sweden, it will strengthen NATO, and it will be something that will contribute to stability across the Euro-Atlantic area, Europe and North America.”

NATO member nations are also expected to formally approve the new “Strategic Concept” document which lays out the alliance’s defense and security vision. Members tasked NATO to update the Strategic Concept document at the 2021 summit. Per the alliance, the document has been updated about once every 10 years to reflect the current security environment.

This latest concept will reflect a “fundamental shift in NATO’s deterrence and defense” and will focus on NATO’s “evolving approach” to current and new threats and challenges, to include terrorism, cyber attacks, and hybrid warfare, Stoltenberg said Monday.

**NATO’s new strategic concept prioritizes collective defense over cooperative security to counter Russian aggression.**

**Simón & Arteaga, '22** – Director of the Research Centre for Security, Diplomacy and Strategy (CSDS) and a Research Professor in International Security at the Brussels School of Goverance (Luis Simón & Félix Arteaga; "NATO gets an update: the Madrid Strategic Concept"; Real Instituto Elcano; https://www.realinstitutoelcano.org/en/analyses/nato-gets-an-update-the-madrid-strategic-concept/; 01-17-2022, Accessed 6-24-2022)//ILake-NoC

Deterrence and defence

NATO endorsed its **posture of deterrence and defence** after the ratification of the Lisbon Strategic Concept as a means of having a combination of capabilities appropriate to a range of possible scenarios.[7] In the absence of a specific adversary, the capabilities to be established could only be generic, but the Russian invasion of Crimea in 2014 and its burgeoning hostility forced the Alliance’s military posture to be redefined. NATO had to deploy forces on its Eastern border to reassure the allies and strengthen its capacity for deterrence.

The Russian aggression forced the natural procedure to be inverted and, since 2014, NATO has had to adapt its deterrence and defence posture to the new situation without waiting for the formal review of the Lisbon Strategic Concept. It began by strengthening its reassurance and adaptation measures on its eastern flank (its Readiness Action Plan) in 2014,[8] followed by a review of its military strategy (MC 400/4) in 2019, the adaptation of its defence and deterrence in the Euro-Atlantic region (Defence and Deterrence in the Euro-Atlantic Area, DDA) in 2020 and NATO’s fundamental concept of combat (NATO Warfighting Capstone Concept, NWCC) in 2021.[9] In recent years NATO’s military authorities have thus been establishing the doctrine, goals and capabilities needed to confront the Russian threat before the political concept that will require them is approved.

The new military developments are not known in detail given their confidential nature, but amid a specific threat such as Russia’s they will have been tailor-made to address it, and therefore will be less reactive than those envisaged in the current Strategic Concept, which are restricted to awaiting an armed attack before responding. The new military strategy will need to address the new forms of confrontation in all domains (land, sea, air, outer space and cyberspace) and in their conventional and non-conventional forms (hybrid war), a more proactive and anticipatory shift in focus that now requires a political justification. As matters stand, the necessity now arises of reconciling the political component of the Madrid Strategic Concept with the military strategy already adopted, which could present problems if one or several allies disagree with the new terms of military planning.

Spain has contributed and will continue to contribute to collective deterrence on NATO’s eastern borders, meaning that it will not be difficult to adapt itself to the new deterrence and defence guidelines from a military point of view. It may be more difficult to acknowledge the Russian Federation as a threat and to act accordingly from the political perspective, because Spanish strategic culture is reluctant to put a name to threats to national security and because adopting the necessary measures would incur major political and economic costs.

Russia, China and strategic competition

The North Atlantic Council described Russia’s aggressive conduct as a ‘threat’ at its June 2021 meeting in Brussels,[10] together with terrorism and other asymmetrical threats such as hybrid threats, disinformation and cyberattacks. Numerous acts jeopardising Euro-Atlantic security were listed and laid at Russia’s door, and consequently Russia is going to provide the adversary that the Alliance lacked in the Lisbon Strategic Concept. With China, the Council’s communiqué was more cautious: the country was described as a ‘systemic challenge’ to the international order and it was called upon to behave more responsibly within this order. However, while the NATO 2030 report drawn up by a group of experts did not deem China a ‘military threat’ like Russia, it placed it on an equal footing in terms of threat to the security of the Alliance.

The allies, including Spain, will need to endorse the characterisations in the Madrid Strategic Concept and the respective measures to reverse these types of behaviour. The measures to be taken against the Russian threat already seem to be **defined** **in the new allied strategy**, but it remains to be seen what measures are adopted against China. The allies are faced with the dilemma of how to address the geopolitical rivalry between China and the US and to take preventative measures to deter and defend their security interests against Chinese power in the European region, the scope of its global capabilities and, above all, the application of its disruptive technologies to erode NATO’s military superiority.[11] In this context, the NATO 2030 report warns about China’s strategy of civil-military fusion, whereby Beijing seeks to acquire the intellectual copyright and advances of European and Western research centres and companies with the goal of boosting its own military development.

All the foregoing presents the Madrid Strategic Concept with the need to use a public language of diplomacy that explains the reasons and consequences of returning to a strategy of **deterrence and containment**. This constitutes a significant communication effort because the allies and their citizens have become accustomed over the course of various decades to **prioritise crisis management to** the **detriment of collective defence and deterrence**. It was a habit they hurriedly had to abandon in 2014 after the Russian annexation of Crimea and required halting the freefall in military spending and committing to investing 2% of GDP by 2024 (NATO Defence Investment Pledge). Spain is not one of the allies most affected by geographical proximity to Russia or the Asia-Pacific, but it must share its allies’ concern about the growing physical presence of these countries in its space of strategic interest in the Mediterranean and Africa and about the virtual reach of their hybrid capabilities to destabilise national security. The tendency of Spanish strategic culture is inclined to prioritise détente over deterrence, but it will have to revise this inclination if the Madrid Strategic Concept incorporates binding containment measures against the Russian and Chinese threats.

The Alliance’s functions

NATO has three fundamental functions: collective defence, crisis management and cooperative security, with none of these taking precedence. The Madrid Strategic Concept will have to address the situation on NATO’s eastern flank and experiences such as Afghanistan so as to **prioritise collective defence** against the Russian threat, **to** the **detriment** **of** its functions of crisis management and **cooperative security**. As well as priorities, the allies will have to weigh whether to add new functions to the traditional list, and candidates such as resilience, cybersecurity, pandemics and technological disruption, among others, are all under consideration.

Prior to the Lisbon Strategic Concept, the usefulness of crisis management operations –referred to variously as international, humanitarian or, in Spanish terminology, peace-keeping missions– was being called into question. It was agreed in Lisbon to halt combat missions in Afghanistan in 2014 and promote the construction of local capabilities as a way of avoiding new interventions within the function of cooperative security. The outcome of operations in Libya and Afghanistan had the effect of discrediting the crisis management function, at least whenever it involves mass troop deployments on the ground, and the Madrid Strategic Concept should **reduce** its **priority** compared to deterrence, which is necessary against the Russian threat, and cooperative security, which is necessary in order to strengthen local partnerships.

**More**

**Morcos, '22** – Visiting Fellow, Europe, Russia, and Eurasia Program (Pierre Morcos; "NATO and the South after Ukraine"; Center for Strategic & International Studies; https://www.csis.org/analysis/nato-and-south-after-ukraine; 5-9-2022, Accessed 6-24-2022)//ILake-NoC

“We, the Heads of State and Government of the 30 NATO Allies, have met today to address Russia’s aggression against Ukraine, the gravest threat to Euro-Atlantic security in decades.” In this solemn statement released after an extraordinary summit in Brussels on March 24, 2022, NATO leaders sent a clear signal: Russia poses an unprecedented threat that the alliance needs to address as a matter of priority. Beyond its decisions to assist Ukraine and reassure frontline allies, NATO is also preparing for the long-term implications of the return of war to the European continent. Incidentally, this reorientation coincides with the preparation of a new strategic concept that will be adopted in Madrid.

The strategic concept is arguably NATO’s most important political document as it scans the international security context, identifies the main threats and challenges to Euro-Atlantic security, and outlines an approach to addressing such challenges. The previous strategic concept, adopted in Lisbon in 2010, signaled a meaningful rebalancing among NATO’s so-called core tasks, namely collective defense, crisis management, and cooperative security. Inter-state competition took a back seat because the alliance still hoped it could strike a cooperative relationship with Russia despite the invasion of Georgia in 2008. The return of great-power competition in Europe—arguably best illustrated by Moscow’s illegal annexation of Crimea in 2014—forced allies to put collective defense once again at the center of NATO strategy. Russia’s full-scale invasion of Ukraine in February 2022 is further compounding this shift. A renewed commitment to territorial defense will undoubtedly be at the forefront of the Madrid strategic concept.

**2NC – UQ – Yes Russia Invasion**

**2NC – UQ – AT: Ukraine Disincentives Invasion**

**2NC – L – T/L**

**NATO must prioritize military defense against Russia – non-traditional threats blur strategic focus.**

**Coffey, '20** – Director of the Allison Center for Foreign Policy Studies at The Heritage Foundation (Luke Coffey; "NATO needs to remain focused on Russia"; SAUDI RESEARCH & PUBLISHING COMPANY; https://www.arabnews.com/node/1772621; 12-05-20, Accessed 6-24-2022)//ILake-NoC

This week, foreign ministers from NATO’s 30 member nations gathered for a virtual meeting during which they were presented with a lengthy report on the future of the alliance.

Researched and written over the course of the past year by a team of 10 external experts from different NATO countries, it offered a number of recommendations for the organization to consider.

The motivation for the report came, in part, from French President Emmanuel Macron describing NATO as “brain dead” last year. Soon after, Secretary-General Jens Stoltenberg announced that the organization would undergo a “period of reflection,” during which it would start to chart a path for the future.

This reflective phase was sorely needed. The last time the alliance conducted a comprehensive review was in 2010 — clearly the world has changed a lot since then.

Debate about the future of NATO is nothing new. It was founded in 1949 as a mechanism to prevent the expansion of the Soviet Union into western Europe. Since the collapse of the USSR and the end of the Cold War in the early 1990s, therefore, there has been much discussion about the organization’s relevancy.

Now the mainstream debate has shifted from whether NATO is still relevant to discussions about what it should be doing. Some argue that although the Soviet Union is gone, Russia remains the biggest threat, and that **collective** and territorial **defense** remains its core task. Others suggest that NATO must re-tool to become a counterterrorism force and focus on emerging challenges such as the rise of China.

While the report published this week highlighted the continued threat posed by Russia to the alliance, most of the focus was on dealing with new and emerging threats — and the two issues that really stand out are terrorism and China. Sadly, the focus on these issues is likely to disappoint many. This is because NATO was **neither founded nor designed to confront such threats.**

Take China for example. Among other things, the report states that “NATO should enhance its ability to coordinate strategy and safeguard allies’ security vis-a-vis China.” A sizable section of the report is devoted to the country, and the word “China” appears no fewer than 62 times throughout the document.

However, it fails to acknowledge NATO’s **limitations** when it comes to **confronting non-military threats** originating from China. Some of the biggest challenges it poses to member states involve questionable investments in critical infrastructure, disinformation campaigns, and encroachments in the technology sector using Huawei’s 5G networks.

As an intergovernmental security alliance lacking any legislative powers, NATO should not pretend to lead on an issue for which it lacks the necessary policy competencies. While the organization should be aware of the challenges posed by China, only national capitals, and on occasion the EU, have the political and economic tools that can address the non-military threats from Beijing.

Counterterrorism is another issue that received a lot of attention in the report but which NATO is not fully equipped to address. The authors state: “NATO should more explicitly integrate the fight against terrorism into (its) core tasks” — but again there is no mention of the limitations that exist.

The organization can be one tool in the box to help confront terrorism but it cannot itself be the entire toolbox. Sometimes a military operation is needed to confront terrorists but most of the time it is not. More often than not, non-military means are the most effective tools in the fight against terrorism.

This is where NATO is lacking. It does not possess any legislative powers to confront terrorism, nor does it have the ability to implement sanctions and block terrorist funding. It also lacks many other capabilities required to fight terrorism, such as policy competency over law enforcement, and border and immigration controls.

As long as Russia remains on the march in Central and Eastern Europe, as it has been in places such as Georgia and the Ukraine, it will remain the primary military threat to NATO.

Many in North America and Europe are concerned about the terrorist threat, and reasonably so. While NATO needs to be aware of this concern, as an alliance it must also be realistic about its ability to conduct counterterrorism operations. Since the organization lacks many of the key policy competencies to fight terrorism, the responsibly to do remains with individual member states.

The report also addresses a number of other issues, ranging from climate change to the role of women in security.

When it is all said and done, the organization **really needs to refocus** **on** its raison d’etre, which is **collective defense**. It does not have to be present everywhere in the world, trying to do everything and solve every problem that exists — but it does have to be able to defend the territory of member states. Right now, there is only one major threat that NATO is fully equipped to handle — and that is Russia. The alliance must **get back to basics** and focus on its eastern flank, where the threat from Moscow remains the top challenge.

Make no mistake, individual member states should be concerned about issues such as terrorism and China, but NATO as an institution should not try to take the lead on these.

As long as Russia remains on the march in Central and Eastern Europe, as it has been in places such as Georgia and the Ukraine, it will remain the **primary military threat** to NATO. As the organization’s secretary-general considers the recommendations in the report, he must not forget this important fact.

**2NC – L – Cyber**

**Peripheral commitments like cybersecurity spread NATO too thin – obfuscates a focus on the operational capabilities that sustain collective defense.**

**Peter van Ham, '08** – senior research fellow at the Netherlands Institute of International Relations Clingendael in The Hague (About The; "NATO Review"; NATO Review; https://www.nato.int/docu/review/articles/2008/03/18/nato-and-the-madonna-curve-why-a-new-strategic-concept-is-vital/index.html; 3-18-2008, Accessed 6-24-2022)//ILake-NoC

If NATO aspires to deal with terrorism and WMD proliferation, the **timing and legitimacy of military force** **will be a key issue** on which the allies have to see eye to eye. But as a look at some core strategic documents shows, this is not the case today. The EU Security Strategy of 2003 opens with the sanguine observation that “Europe has never been so prosperous, so secure, nor so free”, whereas the US Security Strategy of 2006 starts with the ominous statement that “America is at war.” This testifies to the potential of infecting the Alliance with a level of **strategic ~~schizophrenia~~ [irrationality]** that is unhealthy and untenable.,

The current ostrich-reflex, with the head in the sand in the hope that the problem will go away, will no longer do. A commitment must be made to turn NATO into a true, functioning political organisation, prepared to debate key strategic challenges facing the Alliance. That this is not happening today explains the diverging threat perceptions which make collective NATO-action problematic. The North Atlantic Council (NAC), NATO’s key political governing body, now focuses its deliberations largely on the Alliance’s on-going operations, with **too little time spent on potential crises** lurking over the horizon. A new strategic concept should bring an end to this **imbalance**, for example by changing procedures for agenda-setting within the NAC.

Second, **choices must be made** regarding NATO’s future as a **defence organisation**. Obviously, **collective defence** remains the backbone of the Alliance. But what does this mean in an era where **energy cut-offs** and (**cyber**-)terrorism are the preferred lines of attack? NATO’s collective defence clause under Article 5 was duly invoked after 9/11, which means in theory that NATO as a whole remains in a quasi-state of war. The fact that we simply forget this indicates that the Alliance needs to **rethink the nature of collective defence**, its responses, and the importance of **retooling its operational** kit to address new security challenges more effectively. NATO’s military operations suggest a new strategy of “forward **defence**”, where allied interests and values are protected “at the Hindukush.” But with energy security topping the agenda and relations with Russia at freezing point, the true, and possibly novel, meaning of Article 5 requires serious collective thought.

All this implies that NATO has to **set priorities**. The expectations–capabilities gap of the Alliance is becoming dangerously large. As an organisation, NATO cannot bring many policy tools to the table and depends on member states’ willingness to work together and pool their collective resources and capabilities. But the continuing acrimony over **funding** and **force generation** for NATO-led operations exposes the **crumbling consensus within the Alliance**, especially in the case of ISAF. NATO should begin to **cut its coat according to its cloth.** The new strategic concept should clearly explain what Article 5 means in the 21st century, and, based on that new assessment, set limits to the scope and nature of NATO-led missions.

Third, NATO should bring its relationship with new, often global partners and key players like the EU and UN on a new level. In Afghanistan, ISAF includes crucial allies such as Australia, whose 1000 soldiers are engaged in the country’s risky southern province of Uruzgan. Since numerous NATO member states remain reluctant to risk life and limb in these dangerous missions, the Alliance risks becoming a “**coalition of the willing**”, which would undermine **internal solidarity,** and hence NATO’s raison d'être. If NATO chooses to go truly global, it must draw global partners closer to the organization, and clarify their rights and obligations under new and transparent rules of the game.

There is no perfect time for a strategic extreme makeover of the Alliance. So today is as good a time as any.

This also applies to NATO’s ties with the EU and UN. The Alliance takes prides in the “comprehensive approach” it takes towards operations. In reality, however, this can only be realized by bringing the resources of key international organisations (IOs) such as the EU, UN, and World Bank into play. This is why these IOs were invited for the first time to discuss the reconstruction of Afghanistan during NATO’s informal meeting of defence ministers in Noordwijk, in October 2007. Since 21 EU states are also members of NATO, more coordination and joint action between both organisations is obviously required.

The Berlin Plus-arrangement foresaw the EU using NATO resources. Now it is time for a so-called Berlin Plus in reverse, as the Alliance may want to draw upon EU tools like the European Gendarmerie Force (EGF), as well as the EU’s civilian crisis management capabilities. Since the UN’s Department of Peacekeeping Operations (DPKO) now has 90,000 troops deployed under its authority (based on a US$ 5 billion annual budget), NATO-UN ties obviously need to be strengthened and formalized. Numerous modalities are informally discussed, but choices have to be made urgently.

Fourth, **confronting NATO’s strategic choices** and dilemmas head-on will have a cleansing effect within the Alliance.

**2NC – L – Cyber – PC**

**Cyber-security investments sap diplomatic energy crucial to doubling down on territorial defense.**

**Peter van Ham, '08** – senior research fellow at the Netherlands Institute of International Relations Clingendael in The Hague (About The; "NATO Review"; NATO Review; https://www.nato.int/docu/review/articles/2008/03/18/nato-and-the-madonna-curve-why-a-new-strategic-concept-is-vital/index.html; 3-18-2008, Accessed 6-24-2022)//ILake-NoC

That is why NATO needs policy entrepreneurs who are willing to give the Alliance a new lease of life and a new focus.

Today, there is hardly a challenge facing the West that NATO has not been obliged to add to its already **crowded agenda**. **On top of traditional tasks** such as territorial defence and peacekeeping, the Alliance now deals with WMD proliferation, missile defence and **cyber-security.**

In its multifunctionality, NATO begins to resemble a Swiss pocket-knife with all its tools exposed. But as we all know, unfolded pocket-knives are unwieldy affairs, and whilst prepared to do everything, are actually good at nothing. This is why NATO needs to retool itself, starting with a revision of its outdated strategic concept.

The current strategic concept, which is the core mission statement of the Alliance, was adopted in April 1999, in the midst of NATO’s Kosovo-campaign. This key document therefore predates the strategic paradigm-shift of 9/11, as well as NATO’s Afghanistan mission, the first outside the Euro-Atlantic area.

In the past, allies have not prepared strategic concepts frequently (in 1952, 1967, 1991 and 1999), but history seems to go at fast-forward speed these days. This is why NATO Secretary General Jaap de Hoop Scheffer called for a new strategic concept in February 2007, arguing that on-going operations in Afghanistan and Kosovo have offered the Alliance “lessons of 21st century security. We need to enshrine them in our guiding documents so that they are implemented in practice.”

The “ if it ain’t broke, don’t fix it” mentality underestimates the strategic challenges facing NATO today

However, many officials in NATO capitals are concerned that the risks of such a strategic review are too great. They fear that it might revive the transatlantic controversies of 2002-3, and open wounds that have just begun to heal. They also suggest that with the Comprehensive Political Guidance-document that was endorsed in November 2006 at the Riga Summit, a solution has been found to NATO’s predicament.

Still, merely kicking the can down the road would be a serious mistake. This “if it ain’t broke, don’t fix it” mentality underestimates the strategic challenges facing NATO today.

In the current debate, German chancellor Angela Merkel is the only political leader who has clearly stated she would like to see a new strategic concept endorsed at NATO’s Summit in 2009. This will be difficult to achieve given the electoral calendar in the United States where a new administration will take office in January 2009, and will need several months to get a new team together.

Presenting a new strategic concept at NATO’s 60th anniversary would be a welcome birthday present. But more important than nice timing is that at NATO’s Summit in Bucharest, allies commit themselves to **biting the bullet** and doing what is necessary: accept the inconveniences of temporary disagreements and aim for a new NATO strategic concept that clarifies the Alliance’s political and **military strategy** - and communicates this clearly to the wider world.

Why? And why now?

The current debate about a new strategic concept is déjà vu to strategic analysts: all arguments, pro and con, which could be heard in the 1990s, are now rehearsed. Why open Pandora’s Box? **Why** **waste diplomatic energy** **that could be spent on** more important, **operational matters**? Why risk failure by **washing NATO’s dirty linen in public?**

Interestingly, both the 1991 and 1999 strategic concepts were innovative and instrumental in getting NATO ready for new members and missions. So recent experience does not support a cautious approach, but rather suggests that a more daring spirit serves the Alliance well.

Arguably, NATO is facing a **litmus test** which determines whether the organization is really still an “Alliance”, based on shared interests and values, or **merely a glorified security coalition.** There are four pressing reasons why a strategic recalibration of NATO is required.

To be successful, NATO needs a **package-deal of painful compromises**, where each member state has to give and take.

First, allies need to find a workable consensus about the legitimacy of using military force in non-article 5 operations (i.e., for purposes other than self-defence), and, in the extreme, even without an explicit UN Security Council mandate. In a way, this has been the most controversial, **unresolved** issue of the 1999 strategic concept, which has gained even greater relevance with the US invasion of Iraq and the American doctrine of preventive wars.

**2NC – I/L – AT: OCOs Turn**

**Baltic info-sharing is sufficient to deter Russian covert activities now BUT vulnerabilities remain in their military readiness.**

**Radin, '15** – political scientist at the RAND Corporation. His research interests include European security, NATO, and Russia's foreign and security policy; state building and security sector reform; and peace operations (Andrew Radin; "Hybrid Warfare in the Baltics"; RAND corporation; https://www.rand.org/content/dam/rand/pubs/research\_reports/RR1500/RR1577/RAND\_RR1577.pdf; 2015, Accessed 6-28-2022)//ILake-NoC

Like Crimea and eastern Ukraine, the eastern portions of Estonia and Latvia are proximate to Russia and do have a significant Russian-speaking population that might make them similarly vulnerable to Russian covert action. In general, however, the **Baltic countries** appear to be a **less fertile ground for covert subversion** than Ukraine. While Russia was able to seize and maintain control over Crimea, where its conventional forces maintained dominance, the success of covert actions in eastern Ukraine was ultimately less successful, as discussed above. The Baltic countries are better positioned than Ukraine to defend against and deter Russian covert action. They have greater control over their own territory, through the development of their internal security forces, as outlined below. Furthermore, they are members of NATO, and so benefit from assistance from other NATO countries, including under Article 5. Unlike Ukraine, where NATO support to Ukraine was limited to nonlethal equipment after Russia used conventional forces to support the separatists, NATO member countries are committed to respond to an attack on any of the Baltic states as if it were an attack on themselves.

Indeed, both Estonian and Latvian Ministry of Defence officials indicated **confidence in their ability to deal with covert Russian activity** because of their greater state capacity and NATO’s conventional deterrent.56 Their policy to address covert Russian aggression is relatively straightforward—they plan to shoot the “little green men.”57 The Estonian Chief of Defence explains, “If Russian agents or special forces enter Estonian territory, ‘you should shoot the first one to appear. . . . If somebody without any military insignia commits terrorist attacks in your country you should shoot him . . . you should not allow them to enter.”58 By rapidly deploying civilian and military forces to quickly defeat Russian covert elements, the Baltic countries hope to defeat Russian special forces, and leave Russia with the choice of either backing down or risking conventional escalation that would bring NATO into the war. By relying on NATO to provide a conventional deterrent, the Baltic states thereby hope to deter Russian covert action.59

This strategy is uncertain, however. In practice, the Baltic countries may hesitate before attacking Russian forces operating in their territory because of fears of Russia’s willingness to escalate. Russia may also be able to seize territory and establish a new status quo before the Baltic states are able to respond. Indeed, the Baltic countries recognize the importance of rapidly alerting NATO of Russian aggression under Article 4 or 5.60 The Baltic countries may also not receive full NATO support if the presence of Russian forces is ambiguous and there is reason to believe that opposition is primarily carried out by Baltic Russian speakers.

Hence, despite the confidence of the Baltic officials, it remains important to evaluate the **readiness, capabilities, and coordination** of the security forces in the Baltic countries. Estonia appears have a relatively well-prepared security structure, albeit small and dependent on rapid mobilization of reservists. Estonia has an active duty ground force of 5,500 soldiers, of whom 2,700 are conscripts, organized into two brigades. With the exception of one professional highreadiness mechanized battalion, these two brigades are at low readiness and mainly serve to train conscripts for eight to 11 months before they are moved into the reserves.61 There are also four teams of American-trained special operations forces, who have repeatedly deployed to Afghanistan. The Kaitseliit, a 15,000-strong National Guard, contains some well-trained and -equipped fighting units that would coordinate with the special operations forces in the event of an invasion. Based on their own estimates of Russian special forces capabilities, Estonian officials claim that a two-battalion force—their own plus a U.S. or NATO battalion—would be able to hold off Russian special forces, at least until a broader mobilization occurred.62

Estonian government officials are confident in their ability to monitor Russian activity within their territory, highlighting the capability of the Internal Security Service, although it is uncertain how effectively this information can be shared with other NATO members. A July 2015 visit to Narva revealed a modern multilayered border post that would require a not insignificant effort to circumvent.63 While Western officials were skeptical of the extent of coordination between the Ministry of Defence and internal security forces, Estonian government officials claimed that **coordination was quite good** and straightforward in large part due to the small size of the Estonian security establishment. Estonia has undertaken regular war games and exercises to understand how to respond to different forms of Russian aggression, including practicing handoffs of responsibilities from the internal security forces to the Ministry of Defence forces and determining when to seek assistance from NATO. The Hedgehog exercise in May 2015, for example, involved 13,000 Estonian personnel and revealed gaps in mobilization times that the government is currently seeking to address.64

The **readiness and preparation** of the Latvian military is **more questionable**. Despite Latvia’s greater population (2 million compared with 1.3 million in Estonia), Latvian forces are smaller than Estonia’s, in large part because Latvia spends only 0.94 percent of GDP on defense, in comparison with Estonia’s 1.93 percent in 2014.65 Latvia does not have conscription, and the overall size of the active ground force is 3,900. This force is organized into a single brigade with two active duty battalions, and also includes highly trained special forces. Latvia also has a volunteer National Guard of approximately 8,000.66 The focus of the military has been on out-of area NATO deployments, and some Western trained observers in Riga have expressed **doubts about the force’s readiness** to counter either serious covert violent action or a conventional attack.67 As with Estonia, Latvian officials were also **confident of their intel**ligence **gathering** related to Russian covert actions. They observed that they had dealt with the Russian covert threat for many years. Although Latvian defense officials noted **good interagency information sharing**, contingency planning, and coordination,68 Western-trained observers noted serious interagency coordination problems, including the **absence of regular exercises** to practice crisis coordination between the Ministry of Defence and internal security forces. Latvian and foreign observers have also questioned the effectiveness of the Latvian border guard relative to those of Estonia and the Nordic countries.69

**Strengthening conventional defense is key to keep up with Russia – that matters most for territorial, cross-border conflicts.**

**Boston et al., '18** – senior defense analyst at the RAND Corporation. His research focuses on land warfare, with particular emphasis on Russian military (Scott Boston, Michael Johnson, Nathan Beauchamp-Mustafaga, Yvonne K. Crane; "Assessing the Imbalance of Military Power in Europe"; RAND; https://www.rand.org/pubs/research\_reports/RR2402.html; 02-05-2018, Accessed 6-28-2022)//ILake-NoC

This report outlines how NATO and Russian force levels and capabilities have evolved in the post–Cold War era and what recent trends imply for the balance of capabilities in the NATO member states that border Russia in the Baltic Sea region. It is intended to inform debate over appropriate posture and force structure for NATO forces to respond to the **recent growth in Russian military capability** and capacity and to **increased Russian assertiveness in the use of force**. Given NATO's current posture and capability, including European battalions and a rotational U.S. armored brigade combat team, Russia can still achieve a rapid fait accompli in the Baltic states followed by brinksmanship to attempt to freeze the conflict. Nothing about this analysis should suggest that Russian conventional aggression against NATO is likely to take place; however, prudence suggests that steps should be taken to mitigate potential areas of vulnerability in the interest of ensuring a stable security relationship between all NATO members and Russia. NATO has sufficient resources, personnel, and equipment to **enhance conventional deterrence** focused on Russia; a more robust posture designed to considerably raise the cost of military adventurism against one or more NATO member states is worthy of consideration.

Key Findings

Current Imbalance of Military Power on the Russian Border a Result of Different Motivations

In the years following the end of the Cold War, **NATO's ground forces have substantially declined** in size and shifted focus away from high-intensity conventional combat.

By contrast, while Russia also saw a major decline through the 1990s and 2000s, more-recent efforts have led to effective changes in Russian warfighting capabilities and a gradual spread of more-modern systems to much of the Russian armed forces.

Recent **improvements to readiness** and to the ability to move forces quickly within Russia, combined with the density of anti-access/area denial capabilities arrayed to defend the Russian heartland, provide Moscow with a much greater ability to project force against countries on its borders.

The Russian Threat to NATO in the Baltics

While NATO militaries have retooled to focus on stability operations and lighter forces that can be more easily deployed out of area to such places as Afghanistan, Russia has retained a combined-arms force that **emphasizes mobility and firepower** and trains to conduct larger-scale combined-arms operations. This **gives Russian forces** an **important advantage** in conflicts between mechanized forces **close to their border**.

There has been a notable increase in the quality of Russian forces over the last decade: a growing number of volunteer soldiers, fielding of modernized weapons, improvements to readiness, and **experience gained from** large-scale exercises and combat operations in **Ukraine** and Syria.

The highest density of Russia's most-capable ground and air forces is in its Western Military District, which borders the NATO allies in Estonia, Latvia, and Lithuania, which have very small conventional forces.

Russia's demonstrated ability to mass ready forces from elsewhere within its borders, leveraging its internal rail and road networks, means it is likely to enjoy a significant time-distance advantage in generating combat forces during the opening period of a crisis.

**Baltic states are invulnerable to irregular warfare; Russia will exploit their conventional inferiority which risks nuclear escalation.**

**Radin, '15** – political scientist at the RAND Corporation. His research interests include European security, NATO, and Russia's foreign and security policy; state building and security sector reform; and peace operations (Andrew Radin; "Hybrid Warfare in the Baltics"; RAND corporation; https://www.rand.org/content/dam/rand/pubs/research\_reports/RR1500/RR1577/RAND\_RR1577.pdf; 2015, Accessed 6-28-2022)//ILake-NoC

I find that the **most significant threat** from Russia to the Baltics **lies in Russia’s conventional forces**, **not** its capacity for **irregular warfare** or political subversion. I divide potential Russian aggression in the Baltics into three distinct categories of scenarios: nonviolent subversion, covert violent actions, and conventional warfare supported by political subversion. I find that the Baltic countries are not especially vulnerable to nonviolent or covert violent actions by Russia. Given the loyalty of many Russian speakers in the Baltics to their home countries, and their greater economic well-being within the EU, Russia will have difficulty provoking large-scale protests or separatist movements. Covert violent Russian actions are also unlikely to succeed, given preparations in these countries to deploy security forces sufficient to either defeat Russian covert forces or compel Russia to escalate to conventional war. A large-scale conventional Russian incursion into the Baltics would almost inevitably be hybrid in the sense that it would include some effort at political subversion. Nevertheless, the **danger of such an attack lies in NATO’s local conventional inferiority**, not in Russian propaganda or proxy warfare, and as such NATO needs to establish a more **credible conventional deterrent**.

The limited vulnerability to irregular warfare does not mean that a U.S. or NATO policy can focus exclusively on conventional warfare in deterring or defeating Russian aggression. Effective defense of the Baltics depends on reducing vulnerabilities to all forms of Russian aggression. The greater the perceived vulnerabilities of the Baltic countries to a particular form of aggression, the more likely that Russia is to undertake it. Even if the objective risk of success is limited, Russia could miscalculate or determine that the possible benefit is great enough that risk is justified. Alternatively, war or conflict could emerge by accident. Russia and NATO forces could unintentionally come into conflict, as they did when Turkish forces shot down a Russian plane in November 2015. Or, Russia could become involved if groups allied with the Russian state, but not controlled by them, engage in aggressive action.5 The failure of Russian-backed armed groups could lead Russia to escalate to avoid defeat, a cycle which could lead to large-scale conflict and even **nuclear use**. Hence, even if Russia prefers to avoid conflict, a crisis could nevertheless emerge. Strengthening the overall resilience of the Baltic States can reduce the risk of low-level aggression and unintentional escalation.

I conclude this report by suggesting several implications for U.S. and NATO policies to limit the potential for Russian hybrid aggression. First, with regard to nonviolent subversion, pressure from Western allies to improve language and citizenship rights for Russians in the Baltics is probably impractical. Instead, the United States and NATO should pursue the development of a more sophisticated and subtle strategic communication campaign, starting with supporting local Russian-language broadcasters within the Baltic countries.

Second, with regard to covert violent action, continued support for the Baltic countries’ security forces is clearly beneficial. The U.S. Air Force can help improve the intelligence, surveillance, and reconnaissance capabilities of the Baltic states by **strengthen**ing their **technical capabilities** for border control and air and maritime domain awareness. NATO and its member states can also do more to share intelligence of Russian policies and actions and help conduct whole-of-government exercises to better prepare for covert or denied Russian aggression. Additional research would also be beneficial to develop and evaluate responses to a wide range of Russian covert tactics.

Third, in developing a **credible conventional deterrent in the Baltics**, the United States and NATO should attempt to reduce the risk of low-intensity conflict. While there is no way to definitively prevent Russia or Russian speakers in the region from misperceiving NATO’s intent, the United States and NATO may be able to deploy forces in a way that would reduce the risk of Russian aggression or subversion. Such actions may include avoiding basing forces in areas dominated by Russian speakers, increasing transparency, limiting activities that appear intended to achieve regime change in Russia, and developing a comprehensive public relations campaign aimed at the Baltic Russian speakers.

**Baltic hybrid war goes nuclear unless NATO shores up their local conventional forces.**

**Radin, '15** – political scientist at the RAND Corporation. His research interests include European security, NATO, and Russia's foreign and security policy; state building and security sector reform; and peace operations (Andrew Radin; "Hybrid Warfare in the Baltics"; RAND corporation; https://www.rand.org/content/dam/rand/pubs/research\_reports/RR1500/RR1577/RAND\_RR1577.pdf; 2015, Accessed 6-28-2022)//ILake-NoC

A final category of hybrid warfare involves a conventional attack by Russian ground, air, naval, and airborne forces, justified and legitimized by covert or denied activities focused on the Russian speakers. Such an attack could seek to capture territory, replace the government of the Baltic countries, or shift the military balance in an ongoing internal conflict, as in eastern Ukraine. Even if the value to Russia of occupying the Baltic countries is low, Russia could seek to demonstrate that NATO’s security guarantees are not credible and the United States is unable to defend its allies.

Russian conventional forces could adopt a range of courses of action. They might seek to drive ground forces across the Baltic countries to their capitals, and attempt to seize the countries before a significant Western response. Russian forces might limit their offensive to a small “bite” of the Baltic countries, capturing a Russian-dominated city near the border, such as Narva, or an area of strategic importance, such as a land bridge between Belarus and Kaliningrad. Russia may bargain that NATO is unwilling to risk war to recapture an area of strategic importance to Russia, or a Russian-dominated territory where there is some ambiguity about whether there is support for Russian action by the local population. Russia would likely use its anti-access and area-denial capabilities to inhibit NATO deployments in the region and give it more time to consolidate its gains. However Russia uses its conventional forces, it will likely **threaten the use of nuclear weapons** to deter a response from NATO. Russia has discussed the possibility of **deploying tactical nuclear weapons** to Crimea and **nuclear-capable ballistic Iskander missiles** to Kaliningrad, and emphasized that it would use such weapons to defend its territory. Russia would likely do the same if it attacked the Baltics.70

RAND has recently undertaken a series of tabletop exercises to better understand the prospects for a Russian conventional attack in the Baltics. Based on open source estimates, Russia could muster approximately 27 maneuver battalion tactical groups to attack the Baltic countries in a short-warning attack, supported by significant long-range fires. Assuming a week of warning, NATO could deploy 12 maneuver battalions. NATO forces, however, would be light, outgunned, and outmaneuvered by Russian heavier units, and fixed in place or destroyed while Russian forces maneuvered toward the capitals. Furthermore, while NATO could deploy significant air forces, without heavy NATO ground forces present, Russia would have significant freedom to deploy its forces to limit its vulnerability to air power. Across multiple iterations of the scenario, Russian forces were on the outskirts of Riga and Tallinn between 36 and 60 hours after the start of the war. It would likely take at least several weeks until armored reinforcements from the United States could arrive in numbers that would be capable of ejecting Russian forces.

By that point, NATO may be reluctant to risk nuclear war and bear the heavy casualties necessary to retake the Russian-occupied areas in the Baltics.71 The success of Russia’s actions in the “small bite” scenario may vary depending on the degree of surprise, but the chances for Russia’s conventional success in the short term appear high, given the substantial numerical superiority of Russian conventional forces in the region.

While Russia could theoretically only use conventional forces and eschew political subversion or covert action, these unconventional tactics have the potential to reduce the likelihood of a NATO response. Russia could provoke a conflict between Russian speakers and the Baltic governments, which may create the perception that local Russian speakers support Russian military action. Because the North Atlantic Council makes decisions based on consensus, any disagreement about Russian intent could delay or vitiate a NATO-backed response to Russian provocations. Russian leaders made an extensive effort to rationalize and justify their actions in Crimea, and it seems likely that Russian aggression in the future would be accompanied by similar activities to justify their actions.72 Russian covert action could also be used to delay or undermine the Baltic countries’ ability to deploy their security forces to respond to Russian forces.

Even in the absence of consensus within the North Atlantic Council, individual member states could come to the defense of the Baltics under Article 5, which states that each member state can take “such action at it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.”73 So long as the United States is willing to respond, and the transit countries of Germany and Poland permit the U.S. deployment, opposition from other member states cannot prevent a large-scale military response to a potential Russian invasion.

In summary, the **greatest danger** posed by Russia in the Baltics **appears to be** its **local conventional superiority**. Without the threat or actual use of a conventional attack to inhibit a decisive response to Russian subversion, the efficacy of nonviolent or covert efforts would be limited against competent states such as the Baltics. Offsetting Russia’s geographic advantages with a **strengthened NATO defense posture** may therefore be the essential precondition for maintaining political stability in this region. The nature of such a deterrent is the focus on other research and beyond the scope of this report.74 It suffices to note that such a deterrent will likely involve a **significant deployment of NATO forces** to the region. The Baltic countries, for example, have requested that the United States permanently deploy a U.S. Army battalion in each country. Determining the types and numbers of forces and where they will be deployed will have important ramifications for the relations between the Russian speakers and their governments.

**2NC – I/L – AT: Cohesion Turns**

Our internal link comes first

**2NC – I/L – Deter Russia**

**Collective defense k2 russia**

**Kochis et al., '22** – Senior Policy Analyst in European Affairs, Margaret Thatcher Center for Freedom (Daniel Kochis; "The Russian Threat: Bolstering NATO Deterrence at a Critical Time"; Heritage Foundation; https://www.heritage.org/defense/report/the-russian-threat-bolstering-nato-deterrence-critical-time; 3-14-2022, Accessed 6-26-2022)//ILake-NoC

The security and prosperity of the transatlantic community, including the United States, rests on the foundation of the North Atlantic Treaty Organization (NATO). Russia’s ongoing war of naked aggression against Ukraine, a NATO non-member state, should put to rest any lingering questions about the modern utility of the Alliance and about which threat should be the focus of NATO’s upcoming strategic concept.

The answer is clear: The U.S. must lead the Alliance to a wholesale refocusing on the organization’s raison d’être of collective defense. While the Alliance faces challenges emanating from an unstable Mediterranean basin and terrorism originating from the Middle East, the fact remains that Russia continues to be the only existential threat to member states. NATO must send a strong signal that it is strengthening deterrence measures explicitly in response to the increased threat from Russia.

Deterrence measures should include an Alliance-wide recommitment to defense spending; a persistent and continuing U.S. presence in Eastern European member states; updated Alliance operational planning in light of Russia’s position in Belarus and Ukraine; and an increase in U.S. air, ground, and naval forces in the European theater as a sign of continued commitment to the NATO treaty’s Article 5.

These deterrence measures must be carried out with the recognition that, from a long-term perspective, China is the largest peer challenger from whom the U.S. must expect hostile action. Any improvements to the U.S. force posture must not be to the detriment of the nation’s ability to counter China.

The Importance of NATO Deterrence Has Only Increased

From the Arctic to the Levant, Russia remains an aggressive and capable threat to NATO and the interests of its members. For member states in Eastern Europe, Russia represents a real and potentially existential threat. Russia’s entrenched position in Belarus, along with its ongoing actions to cleave Ukraine, a nation that borders four NATO members, in two, scramble the geostrategic map of Europe and necessitate changes to NATO operational planning, exemplifying the need for the Alliance to take swift and resolute steps to bolster deterrence measures along its eastern flank.

Russia’s ongoing war against Ukraine will hopefully be the push that some allies need to finally live up to their commitments to the NATO defense spending benchmark. As an intergovernmental security alliance, NATO is only as strong as its member states. Weak defense spending on the continent has led to a significant loss of capabilities and embarrassing gaps in readiness for NATO allies. As a result, American Presidents of both political parties have long called for increases in defense spending by NATO allies.

Although most are familiar with Article 5 of the North Atlantic Treaty—an attack on one is an attack on all—Article 3 is the most important when it comes to the overall health of the Alliance. Article 3 states that member states, at a minimum, will “maintain and develop their individual and collective capacity to resist armed attack.” Only a handful of NATO members can legitimately say that they are living up to their Article 3 commitment.

In 2006, in an effort to encourage defense investment, NATO set a target for its 30 member states to spend 2 percent of gross domestic product (GDP) on defense. At the 2014 Wales Summit, member states recommitted to spending 2 percent of GDP on defense and committed to spending 20 percent of their defense budgets on “major equipment” purchases by 2024.

NATO allies have made real and sustained increases in defense spending in recent years, but it is far from enough. In 2021, 10 members of the Alliance spent 2 percent of GDP on defense, and 24 members met the 20 percent benchmark.1

Procuring capabilities does not happen overnight, and allies in NATO must commit today to investing the necessary political and economic capital to fulfill their Article 3 treaty commitments.

U.S. Deployments in Europe Can Magnify NATO Deterrence

U.S. basing structures in Europe harken back to a time when Denmark, West Germany, and Greece represented the front lines of freedom. The security situation in Europe has changed, not least of which due to Russia’s force posture in Belarus and occupied portions of Ukraine. The U.S. must account for this shift by establishing a persistent and continuing military presence in allied nations further east. A robust presence displays the long-term U.S. resolve to live up to its NATO treaty commitments. The U.S. should lead by example, while also encouraging other NATO allies to base forces in Eastern European member states.

Over the course of the past few weeks, the U.S. has deployed additional rotational forces in Europe. On Thursday, 7,000 troops from the Army’s First Brigade, Third Infantry Division, deployed to bases in Germany.2

Helene Cooper, “Pentagon Orders 7,000 More Troops to Europe,” The New York Times, February 24, 2022, https://www.nytimes.com/2022/02/24/us/politics/us-troops-deploy-europe.html (accessed February 25, 2022).﻿

In total, the U.S. has deployed an additional 14,000 troops to Europe in response to Russia’s actions in Ukraine. The U.S. has also redeployed aircraft further east on a temporary basis, including 20 Apache helicopters (AH-64s) based in Germany deploying to Baltic allies, 12 AH-64s based in Greece deploying to Poland,3

and six F-35 fighter jets from Utah deploying temporarily to bases in Estonia, Lithuania, and Romania.4

Furthermore, two B-52s from the 5th Bomb Wing deployed on a “long-planned Bomber Task Force Europe mission over the Arctic and Baltic Sea regions.”5

Ibid.﻿

Earlier in February, the U.S. deployed 3,000 forces to Poland and Romania to bolster deterrence and aid in preparations for refugees crossing the border from Ukraine. The U.S. Department of Defense noted that “[t]hese moves are temporary in nature, and are part of the more than 90,000 U.S. troops already in Europe on rotational and permanent orders.”

Some NATO allies have also increased their presence further east. Germany, which serves as the framework nation in Lithuania for NATO’s enhanced forward presence battalion stationed there, added 350 troops.6

NATO allies have battlegroups stationed in Estonia (U.K.-led), Latvia (Canadian-led), and Poland (U.S.-led); France has offered to lead a similar battalion in Romania, and stated that it is “accelerating” the deployment of forces to the nation.7

On Friday, NATO activated its Very High Readiness Joint Taskforce (VJTF), with Secretary General Jens Stoltenberg stating: “We are now deploying the NATO response force for the first time in the context of collective defense.”8

NATO will partially deploy a portion of the VJTF to Eastern Europe; the deployment will include air, land, and naval assets.9

[**The Baltic States Need Advanced NATO Weapons to Compensate for Their Geographical Disadvantages | RealClearDefense**](https://www.realcleardefense.com/articles/2022/05/06/the_baltic_states_need_advanced_nato_weapons_to_compensate_for_their_geographical_disadvantages_831021.html)

**2NC – I/L – Deter Russia – Baltics**

[Opinion | Lithuanian President Gitanas Nauseda: Now is the time to make NATO even stronger - The Washington Post](https://www.washingtonpost.com/opinions/2022/06/23/lithuanian-president-gitanas-nauseda-strengthen-nato-russia-war-ukraine/)

**i/l but sussy**

**Brands, '19** – Hal Brands is an American scholar of U.S. foreign policy. He is the Henry A. Kissinger Distinguished Professor of Global Affairs at the Johns Hopkins University School of Advanced International Studies and a Resident Scholar at the American Enterprise Institute. (Hal Brands; "How Russia Could Force a Nuclear War in the Baltics"; American Enterprise Institute - AEI; https://www.aei.org/op-eds/how-russia-could-force-a-nuclear-war-in-the-baltics/; 11-7-2019, Accessed 6-27-2022)//ILake-NoC

A second option, emphasized by the Pentagon’s 2018 Nuclear Posture Review, would be to devise new limited nuclear options as a way of strengthening deterrence and dissuading Russia from pursuing a strategy of escalate to de-escalate. For example, the US might develop low-yield nuclear weapons that could be used, in a relatively limited fashion, against a Russian invasion force or the units supporting it.

This approach is probably worthwhile, because it would help fill in missing steps on the escalatory ladder between conventional conflict and general nuclear war. The knowledge that the US has its own “tactical” nuclear options might inject greater caution into the calculations of Russian planners. It is possible, RAND analysts note, that limited nuclear strikes early in a Baltic conflict could convince the Kremlin that the risks of proceeding are unacceptable.

The dangers here are, well, obvious and drastic. There is always some possibility — although informed analysts debate how much of a possibility — that Russia might mistake a limited strike against military targets in the Baltics for part of a larger or more dangerous nuclear strike against Russia itself. And if the plan is to use limited nuclear strikes against Russian military assets involved in an invasion of the Baltic states, the implication is that NATO would be using nuclear weapons on the territory of its own members.

A third, and best, option is to strengthen the weak conventional posture that threatens to bring nuclear options into play. The root of NATO’s nuclear dilemma in the Baltics is that the forces it currently has stationed there cannot put up a credible defense. Yet as earlier studies have noted, the US and its allies could make a Russian campaign far harder and costlier — with a much-diminished chance of rapid success — by deploying an enhanced NATO force of seven to eight brigade combat teams, some 30,000 troops. That force would include three or four armored brigade combat teams (as opposed to the one NATO periodically deploys to Eastern Europe now), along with enhanced mobile air defenses and other critical capabilities.

Russia couldn’t claim credibly that such troops posed any real offensive threat to its territory. But the force would be large and robust enough that Russian troops couldn’t destroy it in a flash or bypass it at the outset of a conflict. It would therefore obviate many of the nuclear escalation dynamics by making far less likely a situation in which NATO must escalate to avoid a crippling defeat in the Baltics, or one in which Russia can escalate to protect its early victories there.

Developing this stronger conventional deterrent in the Baltics would not be cheap: Estimates run from $8 billion to $14 billion in initial costs, plus $3 billion to $5 billion in annual operating expenses. Yet neither would it be prohibitive for the richest alliance in the world. The best way of reducing the danger of a nuclear war in the Baltics is to ensure that NATO won’t immediately lose a conventional one.

[**https://www.cnbc.com/2022/06/22/russia-and-nato-member-lithuania-are-clashing-over-kaliningrad.html**](https://www.cnbc.com/2022/06/22/russia-and-nato-member-lithuania-are-clashing-over-kaliningrad.html)

**collective defense k2 baltics**

**Coffey & Kochis, '21** – Director of the Allison Center for Foreign Policy Studies at The Heritage Foundation (Luke Coffey and Daniel Kochis; "NATO Summit 2021: Reinforcing Collective Defense in the Baltics"; Heritage Foundation; https://www.heritage.org/defense/report/nato-summit-2021-reinforcing-collective-defense-the-baltics; 6-11-2021, Accessed 6-26-2022)//ILake-NoC

The North Atlantic Treaty Organization (NATO) summit in Brussels on June 14, 2021, offers an opportunity for the Alliance to continue its focus on bolstering collective defense in the Baltic region. While great strides have been made over the past seven years to deter Russian aggression, the effort is far from complete. The Alliance must keep a focus on the region, avoiding any premature belief that additional measures are no longer necessary.

The Baltic region is one of the most complex regions that the Alliance is obligated to defend. While small in size and population, the Baltic states represent something much bigger geopolitically: They are staunch defenders of economic freedom, liberal democracy, and human rights. They experienced Russian treachery during more than five decades of Soviet occupation in ways that few other countries did. This horrific experience means that the Baltic states do not take for granted the democracy, liberty, and security they enjoy today.

Defending the Baltic states and deterring Russian aggression will be far easier and cheaper than liberating them. In Brussels, the U.S. must ensure that NATO thinks strategically about continuing to put in place durable, robust measures to deter Russian aggression in the region. Deterrence requires more than token actions; it requires a sustained commitment to reinforcing the security of the Baltic region while addressing the Baltics’ unique security challenges.

Get exclusive insider information from Heritage experts delivered straight to your inbox each week. Subscribe to The Agenda >>

A Complex Region

The Baltic region presents distinctive military and political difficulties that NATO needs to overcome. These challenges include:

The Baltic states’ geographical isolation. Militarily speaking, the three Baltic states—Estonia, Latvia, and Lithuania—are isolated from other NATO members. To the north of the Baltic states are non-NATO, but friendly, Finland and Sweden. To the south and east are Russia and Belarus. To the west, Lithuania shares a border with the Russian exclave of Kaliningrad. Only Lithuania shares a land border with another non-Baltic NATO member—a 65-mile border with Poland, to the southwest between Kaliningrad and Belarus, known as the Suwalki Gap.

The Baltic states’ small size. The Baltic states are small in population and size. Combined, the three have roughly the same geographic size and population as Missouri. The Baltic region is probably the only region inside NATO that is too small to depend on rapid reaction forces based elsewhere for its defense.

The Baltic states’ inability to reinforce their defenses. Key to any potential liberation of the Baltic states would be the swift arrival of robust reinforcements and equipment to the region. However, contested airspace, especially in light of Russia’s anti-access, area-denial (A2/AD) capabilities in the region, would make reinforcing the region difficult—if not initially impossible. Even NATO’s Joint Air Power Strategy cautions that “the future operating environment may be one in which air superiority can neither be assured at the onset of operations nor, once obtained, be an enduring condition.”1

North Atlantic Treaty Organization, “NATO’s Joint Air Power Strategy,” June 26, 2018, https://www.nato.int/nato\_static\_fl2014/assets/pdf/pdf\_2018​\_06/20180626\_20180626-joint-air-power-strategy.pdf (accessed June 28, 2018).

NATO’s critical dependence on non-NATO countries. While not impossible, it would be extremely difficult for NATO to respond to an incident in the Baltic region without the acquiescence of non-NATO Finland and Sweden.

Important Progress Has Been Made

NATO has taken good steps for safeguarding the Baltic region in recent years, including the adoption of a new defense plan for the Baltics and Poland in July 2020.2

“NATO Puts Defence Plan for Poland, Baltics into Action, Officials Say,” Reuters, July 2, 2020, https://www.reuters.com/article/us-nato-baltics-turkey​/nato-puts-defence-plan-for-poland-baltics-into-action-officials-say-idUSKBN24320B (accessed May 26, 2021).

The four Enhanced Forward Presence (EFP) multinational battalions stationed in Poland and the Baltic states, announced in 2016, have so far been a success. The U.S. serves as the framework nation for the battle group in Poland, the United Kingdom is in Estonia, Canada is in Latvia, and Germany is in Lithuania. EFP troops are under NATO command and control; a multinational divisional headquarters located in Elblag, Poland, coordinates the four battalions.

One issue that remains controversial within the Alliance is the question of permanently stationing NATO troops in the Baltic states. The only way to guarantee the security of the Baltic states against a conventional Russian military threat is by having robust troops and military capabilities on the ground. The Baltic states are too small to rely on a strategy of defensive depth that could buy NATO enough time to mobilize and deploy a sizable force to the region.

In order to protect NATO’s pre-positioned equipment, rotational troops, and key infrastructure and transport nodes required for rapid reinforcements in the Baltic region, NATO needs to develop a strategy promoting air defense, not just air policing. In 2020, NATO scrambled jets 350 times for Russian aircraft approaching or violating NATO airspace, many of these incidents in the Baltic region.3

News release, “NATO Intercepts Hundreds of Russian Military Jets in 2020,” North Atlantic Treaty Organization, December 28, 2020, https://www.nato​.int/cps/en/natohq/news\_180551.htm?selectedLocale=en (accessed May 14, 2021).

Air defense would require a robust fast-jet and airborne surveillance presence in addition to air defense assets. Despite positive discussions and aspirational talk, NATO has not agreed on a common position for a Baltic Air Defense.

Another matter to consider is the role of the Kaliningrad oblast in regional security. Kaliningrad is a small Russian exclave along the Baltic Sea (slightly larger than Connecticut), bordering both Lithuania and Poland. Kaliningrad is part of Russia’s Western Military District, and approximately 25,000 Russian soldiers and security personnel are stationed there. It is home to Russia’s Baltic fleet, which consists of around 50 vessels, including submarines. Perhaps most important for Moscow is that Kaliningrad is at the heart of Russia’s A2/AD strategy.

Russia’s permanent stationing of Iskander missiles in Kaliningrad in 2018 occurred a year to the day after NATO’s EFP deployed to Lithuania.4

Sergey Sukhankin, “Kaliningrad: From Boomtown to Battle-Station,” European Council on Foreign Relations, March 27, 2017, https://www.ecfr.eu​/article/commentary\_kaliningrad\_from\_boomtown\_to\_battle\_station\_7256 (accessed June 20, 2019).

Iskander missiles can carry nuclear or conventional warheads and have a range of 250 miles, placing Riga, Vilnius, and Warsaw within their reach.

Russia reportedly has deployed tactical nuclear weapons, the S-400 air defense system, and P-800 anti-ship cruise missiles to Kaliningrad.5

Michael Krepon and Joe Kendall, “Beef Up Conventional Forces; Don’t Worry About a Tactical Nuke Gap,” Breaking Defense, March 28, 2016, http://​breakingdefense.com/2016/03/beef-up-conventional-forces-dont-worry-about-a-tactical-nuke-gap/ (accessed June 20, 2019), and ibid.

Russia also has facilities for storage of tactical nuclear weapons in Kaliningrad. Russia is modernizing runways at its Chernyakhovsk and Donskoye air bases in Kaliningrad, providing Russia with nearby bases from which to fly near NATO airspace.

Many of the aerial incidents that cause NATO planes from Baltic Air Policing to scramble involve Russian planes flying from or to bases in Kaliningrad. Additionally, Russia plans to re-establish a tank brigade and a “fighter aviation regiment and naval assault aviation (bomber) regiment” in Kaliningrad and to re-equip the artillery brigade with new systems.6

State Security Department of the Republic of Lithuania, Second Investigation Department Under the Ministry of National Defence, “National Threat Assessment 2019,” p. 22.

Keeping a Baltic Focus

While progress in defending the Baltics has been made, the Alliance should not become complacent. Rather, NATO should use the upcoming Brussels Summit to:

Prepare to reinforce the Baltic defenses quickly. The exercise Defender Europe 20 focused on large-scale troop movements from the U.S. to the Baltic region and Poland, and, despite being scaled back due to the COVID-19 pandemic, was successful. The U.S. and NATO should analyze lessons from Defender Europe 20 (and the ongoing Defender Europe 21 with a focus on the Balkans and Black Sea), identifying roadblocks and implementing fixes.

Maintain the military-mobility focus. NATO must ensure that the Baltic states have the infrastructure and ability to receive large numbers of forces and their equipment. Improving military mobility is one security vector where the Alliance and European Union cooperation could bring positive results.

**Sdfsf**

**Gallo, '22** – William Gallo is the VOA Seoul bureau chief and regional correspondent. His main focus is U.S. policy in Northeast Asia. Prior to coming to Seoul, William covered U.S. foreign policy and international affairs for VOA at the White House, Pentagon, and State Department. (William Gallo; "After Russia’s Ukraine Invasion, Baltics Push for Permanent NATO Presence "; VOA; https://www.voanews.com/a/after-russia-s-ukraine-invasion-baltics-push-for-permanent-nato-presence-/6497246.html; 3-23-2022, Accessed 6-26-2022)//ILake-NoC

The small Baltic countries, whose militaries have long been dwarfed by that of neighboring Russia, are renewing their push for NATO to establish a larger and more permanent presence on their territory following the Russian invasion of Ukraine.

Estonia, Latvia, and Lithuania — with a combined population of only about six million people — have long been seen as some of NATO’s most vulnerable nations. The countries joined the Western military alliance in 2004 but are connected to the rest of European NATO countries by only a narrow corridor, which lies between the heavily armed Russian exclave of Kaliningrad and Russia-allied Belarus.

The Baltics, former Soviet states, have watched with concern as Moscow tries to reassert influence across Eastern Europe. However, they have also been encouraged as Western countries fortify the NATO alliance in response to Russia’s invasion of Ukraine.

NATO had no forces in the eastern part of the alliance until 2014, when it decided to deploy four multinational battlegroups on a rotational basis to the Baltics and Poland in response to Russia’s annexation of Crimea. The NATO presence was further strengthened this year after Russia attacked Ukraine. In total, the Baltics now host about7,700 foreign NATO troops — nearly twice as many compared to earlier this year.

But even with those reinforcements, NATO forces in the Baltics likely could not defeat a large-scale Russian invasion, Baltic leaders warn. “If we want to be ready from the first minute of any kind of attack to defend our citizens, and if you want to give citizens of Latvia the same feeling of security as the citizens of France, Britain, Spain, (and) Germany…then there must be this permanent presence and more firepower and capabilities,” Latvian Minister of Defense Artis Pabriks told VOA in an interview.

Artis Pabriks, Latvia's Minister of Defense, tells VOA that if Russia does not like NATO expansion, then Moscow can stop threatening its smaller neighbors. March 18, 2022.

Baltic leaders have long pushed for a permanent basing of U.S. troops, seeing it as the ultimate deterrent against a Russian invasion. Currently, U.S. troops are part of NATO’s Baltic rotational battlegroups, which are led by Germany, Britain, and Canada. During a Baltics tour earlier this month, U.S. Secretary of State Antony Blinken said “more permanent deployments” were being considered as part of a larger review of NATO’s defense posture. He did not offer details. But the United States has been reluctant to permanently station forces on Russia’s doorstep, fearing it would further upset relations with Moscow.

Many Baltic leaders hope a permanent NATO presence will be discussed this week when U.S. President Joe Biden visits Brussels, Belgium, for meetings with NATO and other European leaders. Asked about Biden’s visit, Latvian Minister of Foreign Affairs Edgars Rinkēvičs told VOA he believes “it is time that NATO states clearly that (its) presence in the Baltic states and Poland and Romania, in what we call the ‘eastern flank,’ is permanent.”

Edgars Rinkēvičs, Latvia's Minister of Foreign Affairs, speaks to VOA on March 18, 2022. Rinkēvičs wants a permanent NATO presence on the alliances eastern flank.

Estonian Minister of Foreign Affairs Eva-Maria Liimets also told VOA she hopes NATO leaders meeting in June in Spain will “make permanent decisions about how to strengthen defense and deterrence posture in our region.” Even though she conceded Estonia does not currently face a “direct military threat,” she said Europe’s security situation “has changed as a whole and therefore we must continue to strengthen the defense and deterrence posture of NATO so that we would be more protected.”

It’s not clear what a more permanent NATO presence in the Baltics would entail in terms of weapons. During the Cold War, the United States alleviated European security fears by positioning tactical nuclear weapons in countries such as Germany, pointed out Dan Plesch, a professor of diplomacy at the SOAS University of London. “Is that what is going to satisfy (Baltic) security concerns?” Plesch asked in an interview with VOA.

The Baltic nations are already protected by NATO’s commitment to defend its members in the event of an attack. NATO also has overwhelming air power superiority that would factor into any battle with Russia in the Baltics, Plesch pointed out. And at the moment, he added, Russia’s military looks even weaker than normal after sustaining significant losses in Ukraine.

Eva-Maria Liimets, Estonia's Minister of Foreign Affairs, hopes a NATO meeting in June will "make permanent decisions" about how to strengthen Baltic security. Interview with VOA on March 14, 2022.

The challenge is how to address Baltic security concerns while avoiding steps that would lead to a more unstable situation with Russia in the future. But with NATO and Russia each blaming the other for creating instability in Eastern Europe, that may be a difficult task.

Any NATO expansion is sensitive for Russian President Vladimir Putin, who cited the issue as a justification, among others, for his invasion of Ukraine. Putin still fumes over the Baltics’ decision to join NATO, seeing it as a betrayal of Western promises. Analysts say he would likely see the establishment of a permanent NATO presence in Eastern Europe as a violation of past agreements, including the 1997 NATO-Russia Founding Act (NRFA).

However, those agreements “can be regarded in significant part as null and void given Russian actions,” Plesch said. Another factor: the NRFA is not a legally binding document, added Mary Elise Sarotte, a Cold War historian and professor at the Johns Hopkins University School of Advanced International Studies. “This reality gives the alliance flexibility with regard to NRFA’s terms,” she told VOA by email.

Experts are mixed when it comes to predicting whether NATO will establish a permanent presence in the Baltics anytime soon. According to Plesch, much depends on how the situation in Ukraine progresses. Sarotte said it depends on how “permanent” is defined, but that “it is clear that a larger NATO presence in the east will happen, and will endure.”

In the view of Pabriks, the Latvian defense minister, NATO’s new approach to the Baltics should mean “much more capabilities, a classical strong presence in the region and also support to our national armies.” If Russia does not like the prospect of a more powerful NATO, he said, then it can always choose to “not threaten its neighbors.”

**2NC – !! – Baltics**

<https://www.foreignaffairs.com/articles/ukraine/2022-04-06/ukraine-russia-war-return-conquest>

**DA – NATO Tradeoff [Climate]**

**1NC – DA**

**Climate is a priority, but resources are strapped – NATO defense initiatives directly trade off.**

**Kochis, '21** – senior policy analyst in European affairs in the Margaret Thatcher Center for Freedom (Daniel Kochis; "Biden Wants NATO To Focus on Climate Change. What About Russia?"; Heritage Foundation; https://www.heritage.org/global-politics/commentary/biden-wants-nato-focus-climate-change-what-about-russia; 8-13-2021, Accessed 6-24-2022)//ILake-NoC

The recent NATO summit in Brussels was, by and large, a big disappointment. Its big “achievement” was the misguided adoption of a climate change agenda. At best, that agenda is a distraction from the critical security challenges facing the alliance. At worst, it will actively undermine the alliance’s ability to defend its member states.

For quite some time, NATO has been grappling with divergent threat perceptions among its member states. The summit did nothing to reconcile or systematize these views. Instead, the alliance opted for an umbrella approach where every threat is deemed equally acute.

This **oversized umbrella** may have kept everyone’s threat perceptions dry for now, however, there is **only so much focus, money, and political willpower** to go around. Sooner or later the alliance will need to **prioritize**.

For those nearest Russia, it’s crystal-clear Putin is not only NATO’s greatest threat, but also one which the alliance is best suited to confront. In the 21st century, NATO needs to return to basics, with territorial defense as its primary goal. **NATO cannot try to be everywhere** in the world doing everything all the time. Keeping Russia at bay requires the alliance to address the full range of Russian aggressions against NATO members: aerial incursions, cyber-attacks, energy coercion, espionage, and propaganda. It must also be able to deter Russia’s use of conventional and nuclear arms.

Facing daily arrivals of migrants from North Africa, our Mediterranean allies view migration and terrorism as NATO’s greatest security threat. And then there is the gnawing reality of China’s rise, with its implications for transatlantic security. These are secondary threats to the alliance. Nonetheless, NATO has some (albeit limited) role to play in keeping them in check.

Yet in the Brussels Summit Communiqué, **climate change gets top billing** as a threat to the alliance. This suggests that NATO, now with Team Biden calling the shots, views climate as NATO’s greatest threat, or at least as important as the other threats mentioned: Russia, China, instability in Europe’s near abroad, and the proliferation of weapons of mass destruction.

At the summit, NATO adopted a “Climate Change and Security Action Plan.” Among other things, it commits the alliance to conducting an “annual Climate Change and Security Impact Assessment” and to mapping and analyzing greenhouses gases from military installations and military activities. “Furthermore,” the plan states, “data on energy demand and consumption in the military could inform Allies’ investment decisions, help define the role of Emerging Disruptive Technologies and innovative energy efficient and sustainable technologies, as well as inform operational planning.”

The Summit Declaration goes further, inviting the Secretary General to “formulate a realistic, ambitious and concrete target for the reduction of greenhouse gas emissions by the NATO political and military structures and facilities and assess the feasibility of reaching net-zero emissions by 2050.”

This is not to say that climate change isn’t real, nor that it has implications for NATO member states or theaters (particularly the Arctic). NATO, however, is not the right organization to lead on addressing these issues.

There is now a very real possibility that the alliance’s new climate focus, with its reporting and consultation requirements, will become a distraction which undermines collective defense.

Worse yet, NATO’s drive to hit arbitrary emission targets could lead some nations to make choices which weaken transatlantic security. Why invest in emissions belching tanks when you can buy light armored cars? Why invest in fifth-generation fighters when many new aircraft consume more fuel than older platforms? Why invest in capabilities at all when you can invest in carbon capture technology and wind farms?

Scaling up to challenge Russia’s increased presence in the High North? Expect headwinds ahead under NATO’s climate turn. How about joint exercises, the lifeblood of NATO’s continued interoperability and readiness? Could they one day be reduced to lower emissions?

And what of the alliance’s adversaries? The idea that Russia, the world’s fourth-largest carbon emitter, or China, the world’s largest emitter by far, are going to allow emissions targets and climate change concerns restrain their military acquisitions, basing, or operations is farcical.

Many of our NATO **allies are still struggling to meet** their **defense** **spending commitments**. Their militaries suffer from glaring capability gaps. Siphoning scarce resources away toward a green agenda will only further **enervate** alliance **collective defense**.

**NATO is key to climate mitigation. Otherwise, extinction.**

**Shea, '22** – Former Deputy Assistant Secretary General for Emerging Security Challenges at NATO Headquarters in Brussels, Belgium (Jamie Shea; "NATO and Climate Change: Better Late Than Never"; GMFUS; https://www.gmfus.org/news/nato-and-climate-change-better-late-never; 3-11-2022, Accessed 6-25-2022)//ILake-NoC

Yet the past few years have underscored that the future is now. There is no more luxury of time to respond to this challenge. The planet is sending repeated warnings that climate change has reached a **tipping point** and poses a **constant threat** to the functionality of economies and societies. This will make larger areas of the **globe uninhabitable**, as living with 50 degrees Celsius (122 degrees Fahrenheit) or hotter becomes the norm rather than the exception. The past three summers have been the hottest on record; the past five years have seen the largest numbers of category 4 and 5 hurricanes. Devastating forest fires have displaced people from the west coast of the United States, western Canada, Siberia, Greece, Portugal, and Australia. Colorado recently experienced such a fire in the middle of the winter. In January, meteorologists recorded the most extreme temperature vortex ever, with minus 50 degrees Celsius (minus 58 degrees Fahrenheit) in the Arctic and plus 50 degrees Celsius (plus 122 degrees Fahrenheit) in Australia. We have become used to **heavier rainfalls** and more **widespread flooding**. Rising sea levels have placed entire cities and even countries in jeopardy, as we heard in the powerful words from Bermuda’s prime minister, representing the small island states, at 2021 United Nations Climate Change Conference (COP26) in Glasgow last November. Indeed, 50 percent of Asia’s population today lives in coastal cities. The biodiversity that has regulated the smooth functioning of our natural habitat for thousands of years is being rapidly depleted. Prolonged droughts affect freshwater availability and put acute stresses on food production and rural livelihoods, leading the United Nations to forecast that by mid-century, 40 percent of the globe’s land surface will be subject to acute water stress. We will need to contend with more climate refugees than those today on the move because of conflicts or poverty (currently an all-time high of 26 million).

Only belatedly have we become aware of the role that droughts play in **exacerbating social and political tensions** in places such as Syria, Darfur, and Afghanistan. Of course, not every natural disaster can be laid at the door of climate change, as earthquakes in Haiti or the recent eruption of an undersea volcano near Tonga attest. Moreover, the planet’s climate has rarely been stable, and historians have documented extreme cold spells in the 17th century or devastating droughts in biblical times. It was, after all, the catastrophic Lisbon earthquake in 1757 that for Voltaire ended the 18th century’s age of optimism. Yet the mountain of scientific evidence produced by the UN’s Intergovernmental Panel on Climate Change points to the role of global warming as a **force multiplier** for more frequent and extreme weather events, giving the planet less time to recover from one natural disaster before the next one strikes, thereby producing a **cumulative destructive effect**. Climate change is arguably the **first truly global security challenge** in that, according to UN reports, only 11 out of the current 193 UN member states do not currently experience its impact in one form or another. Any organization, like NATO, that tries to address climate change thus faces the dual challenge of responding to individual flash points (such as extreme weather events putting lives at risk or leading to social breakdown), while simultaneously understanding how climate change is shaping the future of global geopolitics, making fu ture conflicts over land, water, or resources more likely in the longer term. Getting these predictive models right is essential if the allies are to devise the preventive strategies to **head off** the **worst-case scenarios** while **mitigating the worst consequences**. Thus, it was no surprise that US President Joe Biden’s administration ordered a National Intelligence Estimate of the security implications of climate change as one of its first acts upon taking office.

The military forces of NATO countries have played an increasing role in responding to extreme weather events in recent years. In fact, the first time the NATO Response Force (NRF) deployed was to Kashmir in 2006 to help Pakistan restore infrastructure and communications after a major earthquake. In recent years, alliance military forces have been increasingly pulled into civil defense tasks. British, French, and Dutch marines and engineers have gone to the Caribbean to restore order in the wake of hurricanes that have paralyzed the normal process of government. Military firefighters and aircraft have been mobilized to combat forest fires in the United States, Canada, and Europe. British and German forces have been called up to build flood defenses, evacuate flood victims, and build pontoon bridges or reconnect power lines. Military hospitals and medical personnel have helped local authorities cope with extreme heatwaves affecting the elderly and other populations at risk. The **military with** their **rapid-response capabilities** have become the **partner of choice** to the civil emergency authorities within NATO countries in responding to climate-driven events. This has also been the case with other shocks that may well be linked indirectly to climate change, such as the coronavirus pandemic, which result from stresses on the natural environment and the interface between animals and humans. The pace of military deployments within alliance member states has reached such an extent that some NATO commanders are worried that this could have deleterious consequences for training and the retention of war-fighting skills.

In the process of deploying to climate-stressed zones, characterized by extreme weather events or hotter or colder conditions, NATO’s military forces have become aware of how climate change impacts their own ability to operate. For instance, the Pentagon has assessed that two-thirds of US military bases, especially along coastlines, are vulnerable to rising sea levels or extreme weather events. Hampton Roads in Virginia, which is important to NATO as the home of Joint Forces Command Atlantic and the US Second Fleet, has been assessed as especially vulnerable. Hotter temperatures, greater frequency of high winds, storm surges, or increased salinity in the oceans have led NATO military commanders to review both the resilience of their equipment (for instance, the performance of ship turbines) or the dependency of military operations on fossil fuels. In Afghanistan, for instance, helicopters and vehicles needed more than average maintenance because of dust storms and persistent high temperatures, while the high consumption of gasoline required lengthy and dangerous supply lines from Pakistan into Afghanistan that jihadists targeted. At one stage, NATO planners calculated that a $2 gallon of gasoline cost over $100 by the time it reached a NATO ISAF unit in Helmand or Kunduz.11Amory Lovins, “DOD’s Energy Challenge as Strategic Opportunity,” Joint Forces Quarterly, Issue 57, second quarter, 2010. This certainly motivated the allies to experiment with smart energy camps, powered by solar and wind generators, which were demonstrated at NATO trials such as the annual Capable Logistician exercise. The Pentagon, with an annual fuel bill surpassing $ 25 billion, has been graded as the 43rd “country” in the world in terms of fossil fuel emissions.22Neta Crawford, Pentagon Fuel Use; Climate Change and the Costs of War, Boston University paper, June 2019. Accordingly, NATO military forces have faced the twin task of fine-tuning their modus operandi and added value in supporting the humanitarian response to climate change, while adapting their own doctrine, training, and capabilities to operate in these more demanding conditions.

NATO planners calculated that a $2 gallon of gasoline cost over $100 by the time it reached a NATO ISAF unit in Helmand or Kunduz.

NATO’s purpose has always been to defend its populations against challenges that evolve into concrete security threats and that require military forces or military organizations. The criterion has been the added value that the alliance can bring to bear. Sometimes this means that NATO is in the lead and generates the bulk of the response from within its own ranks and capabilities. This is obviously the case with territorial collective defense, particularly as it applies to Russia’s military buildup on NATO’s eastern borders at the present time. In other cases, the alliance functions in a supporting role, integrating its capabilities with those of other institutions and actors as part of a networked, comprehensive approach. What NATO brings to the table here are its analytical and intelligence cells, its strategic planning and foresight capabilities, its political consultation, joint assessment and information-sharing structures, its web of partnerships with non-member states and other international organizations, and its political-military command and control and operations network from HQ to the regional level. Few other organizations have all this machinery under one single roof. Consequently, as the climate change community has gradually accepted a role for the military in addressing climate change—after initially fearing that this would put too much emphasis on adaptation at the expense of the primary political goal of reducing carbon emissions—pressure has built on NATO to use its spectrum of capabilities in a more coherent, systematic way. The mounting urgency and universality of global warming **require every institution to step up** **and play its part** within its means and capabilities. The broad spectrum of NATO assets means that it can contribute in multiple supporting ways to a UN-led effort both to reduce global warning and adapt to the climate impacts that are already locked in, even if that warming can be **limited to 1.5 to 2 degrees** Celsius over pre-industrial levels. The question now is how to optimize all these NATO assets so that the alliance can receive and transmit expertise and make its contribution count.

NATO Secretary General and former UN climate envoy Jens Stoltenberg has usefully led the way. At the Brussels summit in June 2021, he declared that climate is not just a trans-boundary ecological crisis but a **security crisis** as well. Stoltenberg skillfully used his NATO 2030 reflection exercise and the review carried out by the group of experts he appointed to generate public pressure and build the case (against initial skepticism from some allies) for a formal NATO role in addressing climate change. Before the summit, NATO foreign ministers endorsed a joint analysis of the security implications of climate change. One paper recognized climate change not only as a **threat to human security** per se, but also as a **force multiplier** which could **accelerate** and intensify **preexisting tensions and conflicts**, many of which, because of their location close to NATO’s borders, could impinge directly on the security of the alliance.33Neta C. Crawford, Pentagon Fuel Use, Climate Change, and the Costs of War, Brown University, 2019. At the Brussels summit, the allies adopted a Climate Change and Security Action Plan broken down into four broad implementation categories. These are awareness, mitigation, adaptation, and partnerships.

**2NC – UQ – Climate**

**Climate change will be a top priority in the upcoming Madrid summit – focus is key.**

**NATO, '22** (North Atlantic Treaty Organization; "NATO continues to adapt to rapid environmental changes"; NATO; https://www.nato.int/cps/en/natohq/news\_195079.htm; 5-5-2022, Accessed 6-25-2022)//ILake-NoC

Rapid environmental changes resulting from climate change have a direct impact on our shared security and call for innovative technological solutions. **NATO** has **started** a **new project using Big Earth** Datacube Analytics for transnational security and environmental protection. Today (5 May 2022) marked its kick-off, at an event hosted at NATO Headquarters in Brussels by the NATO Science for Peace and Security (SPS) Programme, featuring the participation of project stakeholders and experts from Denmark, Germany, Israel and Switzerland.

The Sixth Assessment Report of the United Nations Intergovernmental Panel on Climate Change (IPCC) published this year highlights that changes in **extremes** such as heat waves, **heavy precipitation**, **droughts and tropical cyclones**, are more and more frequent. Although NATO is not the first responder for every challenge related to climate change, the Alliance has a role to play in a comprehensive response to climate change. This is why, at the 2021 Brussels Summit, Allies endorsed a Climate Change and Security Action Plan. Furthermore, **climate change** may feature in the next Strategic Concept that will be adopted at the NATO Summit in Madrid scheduled at the end of this June. A major challenge for the future is to enable **continuous monitoring of climate change** and establish early warning capabilities to ensure the security and protection of our populations.

Cube4EnvSec is a new multi-year project supported by the NATO Science for Peace and Security (SPS) Programme, which will involve experts from Germany, Israel and Denmark. “As **climate change and security are a growing priority** for the Alliance, the NATO SPS Programme is boosting its engagement with Allies and partner nations on this shared challenge,” stated Dr. Deniz Beten, Senior SPS and Partnership Cooperation Advisor. In line with the Programme's decades of experience addressing environmental security issues, Cube4EnvSec will demonstrate how datacubes can contribute to agile insights on Big Earth Data for observing natural and human-made threats of any kind, combining ground, space, and airborne sources ad-hoc and in real-time, with particular emphasis on security-relevant aspects. According to Rene Heise of the Climate and Energy Security Section at NATO Headquarters "This **new generation** of high-resolution (1 to 10 cm) imagery will provide greater quality and accuracy to procedures such as change analysis for airfields on unstable ground (e.g. thawing permafrost), flood simulations, harbour security in case of sea level rise or land slide risk.”

The application of this technology will be demonstrated in a number of cases, such as thunderstorm warning for aviation and harbour protection. Attempting to integrate warnings from space weather events will be particularly relevant for areas in the High North. The project will demonstrate the benefit of spatio-temporal datacubes such as satellite, climate and high-dynamics meteorological/oceanographic (METOC) data offered in a ready-to-use analysis. "We aim at showing the benefits of massive space/time federated datacubes as a particular enabler for better understanding our planet", explained Dr. Peter Baumann, one of the project’s co-directors based at Jacobs University in Bremen, Germany.

**2NC – UQ – AT: Ukraine**

**Climate remains high priority post-Ukraine.**

**Kirton & Warren, 3/22** – professor of political science and the director and co-founder of the G7 Research Group, co-director and founder of the G20 Research Group (John Kirton and Brittaney Warre; "Will the War in Ukraine Crowd Out G7 Climate Action in 2022?"; G7 Information Center; http://www.g7.utoronto.ca/evaluations/2022elmau/kirton-warren-ukraine-crowd-out.html; 3-22-2022, Accessed 6-24-2022)//ILake-NoC

G7 Performance on Security and Sustainability on March 10 and 11

The Ukraine crisis could still easily derail the G7's climate-focused agenda. And there are signs it has done so to some extent. On March 11, G7 leaders released a statement focused solely on Ukraine. It therefore did not mention climate change at all (see Appendix B-1). It did make two energy commitments, but neither spoke of a clean energy transition (see Appendix B-2). However, the G7's energy ministers, who met on March 10, the day before their leaders, made a **clean energy transition a high priority in** their own **statement on Ukraine**. The G7 energy ministers stated: "We remain **steadfastly committed** and convinced that the most important contribution towards energy security is an accelerated clean energy transition based on energy efficiency and a shift to the use of clean, safe and sustainable energies." Of their 13 commitments, nine (69%) explicitly referenced clean energy, the energy transition, climate change or the Paris Agreement (see Appendix C). Although the following day the agriculture ministers put less emphasis on climate change, two of their 15 commitments, for 13%, committed to support food security in line with climate, environment and sustainable development commitments (see Appendix D). This suggests that the **Ukraine crisis will not** totally **overshadow** **climate governance** before or at Elmau.

**2NC – L – Resources**

**The aff clouds NATO’s focus – info-sharing makes the organization a glorified clearinghouse that trades off with NATO security initiatives.**

**Moller, '20** – Assistant Professor at the School of Diplomacy and International Relations (Sara Bjerg Moller; "It Will Take More Than a Biden Victory to Solve NATO’s Strategic Malaise"; War on the Rocks; https://warontherocks.com/2020/09/it-will-take-more-than-a-biden-victory-to-solve-natos-strategic-malaise/; 9-25-2020, Accessed 6-24-2022)//ILake-NoC

If and when the Biden team embarks on its grand European tour, it seems virtually certain that, beyond the expressions of gratitude for America’s “return” that will surely follow them wherever they go, the delegation can expect to be met with a lengthy list of items requiring their immediate attention. Moreover, appeals for Washington’s assistance are likely to differ from capital to capital, with each NATO ally arguing that their particular issue or concern represents the most pressing challenge and therefore requires the most attention and resources. In Warsaw and the capitals of the Baltic states, the U.S. delegation will hear that, despite a new U.S. rotational troop deployment, a revanchist Russia necessitates additional NATO (but especially U.S.) military commitments along the Eastern flank of the alliance. In Rome, Athens, and Madrid, U.S. policymakers will learn that the Mediterranean countries represent the “soft underbelly” of NATO and that the alliance must do more to project stability along its southern arc of instability. In Ankara, the message will be one of anger directed at what the Erdogan government perceives as NATO’s collective failure to support Turkish actions in Syria and elsewhere. In Paris, the message for the U.S. delegation will be that the alliance must strengthen its counter-terrorism efforts in the Middle East and North Africa, while in Berlin the focus will be on reforming NATO’s nuclear posture and salvaging expiring arms-control agreements. Meanwhile, securing the Arctic and halting the effects of climate change will be at the top of the agenda in Copenhagen and Oslo.

In short, wherever the Biden presidential delegation goes, it will be met with requests that Washington — and with it, the NATO alliance — **prioritize** **everything**, thereby fulfilling the old adage that, “**When everything is a priority, nothing is a priority**.” Given the precarious state of international relations today, the temptation to do more is understandably strong. It is easy to understand why, in the present climate of global instability, calls for the transatlantic alliance to reinforce and strengthen its existing commitments while simultaneously adding new mandates, missions, and programs are popular. Rather than adding more items to its **already crowded agenda**, however, the time has come for not just the United States but also NATO to consider **doing less but** doing it **better**.

When More Is Less, and Less Is More

For an alliance that has long prided itself on its commonality of purpose and interests, the truth is that NATO is in danger of losing both. On paper and in public, the members still agree the core purpose of the 71-year-old alliance is deterrence and defense of the North Atlantic region. When internal disagreements are aired publicly, other allies are quick to dispel reports of rifts by pointing out that differences of opinion are nothing new. But unlike during the Cold War, when a single adversary occupied all of the alliance’s attention, today’s security environment — as the allies routinely remind each other — is multifaceted and complex. In an effort to address members’ often disparate security requirements, NATO has taken on additional tasks over the past three decades almost as quickly as it has taken on additional members. The NATO-ization of every security challenge has meant that issues once considered the purview of individual nations or other international organizations — such as migration, terrorism, and foreign security force assistance — are now lumped onto NATO’s agenda under the guise of fulfilling its ambitious (and potentially limitless) post-Cold War mandate of “projecting stability.”

For far too long now, alliance leaders have tasked the NATO military infrastructure with a seemingly impossible undertaking: weighing down the military organization with new responsibilities like peacekeeping and counter-terrorism while simultaneously allowing members to shirk on contributing the resources required to fulfill old and new alliance missions. To date, much of the criticism surrounding NATO’s current strategic deadlock has focused on the resource issue and the strains caused by uneven burden-sharing within the alliance. Far less attention has been paid to the first part of the “ends-means-ways” formulation of strategy, namely NATO’s original purpose. While addressing “means” and “ways” are crucial elements in any strategic enterprise, it is past time the Allies got around to focusing on NATO’s strategic ends once more.

Confronting NATO’s present strategic dilemma will require looking beyond existing strategic documents like the 1949 North Atlantic Treaty, which proclaimed the signatories’ commitment to the “preservation of peace and security” in the North Atlantic area. As the past three decades of NATO transformation have shown, there is not much that does not fit under the rubric of fostering “peace and security” and consequently cannot be tacked onto the alliance’s agenda. True strategy requires setting (and adhering to) actual goals and priorities, as well as developing plans to achieve them. Although the alliance’s past strategic documents have often sought to define NATO’s evolving strategic purpose with more precision than the founding treaty, the alliance has not adopted a new strategic concept since 2010 for fear that embarking on such an exercise would only further inflame the deep rifts within the alliance that such strategic endeavors are meant to help address.

Officially, NATO members still assert collective defense is the alliance’s primary task, despite the inclusion of two other core tasks — projecting stability and cooperative security/crisis management — in all three of its post-Cold War Strategic Concepts (1991, 1999, 2010). The addition of these latter two core tasks — coupled with members’ differing threat perceptions about what rises to the level of an existential security threat — has **clouded the organization’s focus**. After **three decades** of continual adaptation, the danger that the alliance’s original raison d’étre of collective defense gets further downgraded to the point where it risks becoming primus inter pares among NATO’s many other responsibilities is real. As with previous critical junctures in transatlantic relations, it will take American leadership to change NATO’s future course. Come January 2021, a Biden administration should move swiftly to announce its intention to commission a new NATO strategic concept by 2022. Should Trump win, all bets are off.

Defenders of NATO’s post-Cold War emphasis on projecting stability and collective security argue that NATO has a proven track record of crisis management and capacity-building beyond its borders in places like Bosnia and Herzegovina, Kosovo, Afghanistan, and Iraq. The alliance’s cooperative security track record, however, is hardly stellar. This past June, the NATO-led international peacekeeping force in Kosovo entered its 22nd year of operation. Almost 17 years after the alliance’s Integrated Military Command first assumed responsibilities in Afghanistan, the NATO flag continues to fly in Kabul, where some 15,000 allied troops remain as part of NATO’s Resolute Support mission. Nor can the alliance’s intervention in Libya in 2011 be considered a resounding success, judging by the state of affairs there today. That NATO remains engaged in some of these places decades afterward is not an impeachment of the men and women who served in these operations and performed the tasks demanded of them. It is, howevwer, evidence of NATO’s failure to give sufficient consideration to its core strategic purpose.

While one can debate the wisdom of NATO having accumulated such an expansionist security agenda in an era marked by American unipolarity, an all-encompassing approach to security is harder to justify in a time of waning American power. Just as the diminishing threat of great-power competition in the 1990s and early 2000s freed NATO to take on additional security tasks beyond its traditional mission of collective defense, its return should prompt a reexamination to determine whether NATO is still the appropriate entity for handling such tasks.

Another center of excellence, special representative, or office will not fix what ails NATO. As the authors of a recent Heritage Foundation report on “NATO in the 21st Century” put it, it is time for NATO to get “back to the basics.” There are limits to what an international institution — even one as successful as NATO — can accomplish: “When policymakers expect or want NATO to do what it was never designed to do, that is when the Alliance risks failure.”

The launch of NATO Secretary Gen. Jens Stoltenberg’s #NATO2030 reflection process earlier this year to address political reforms within the alliance presented just such an opportunity to tackle these and other big-picture questions. It is still unclear to what extent the pandemic has delayed the work of the group of experts begun last March. The Biden team will have to move quickly if it hopes to help shape the working group’s deliberations, as Stoltenberg is slated to brief members on the path forward for the alliance at the April 2021 Leaders’ Summit.

Back to the Future: Narrowing (Not Broadening) NATO’s Remit

Looking ahead, alliance leaders should consider ways to streamline current NATO missions and tasks so that responsibilities that fall below the threshold of existential challenges can be unloaded onto other multilateral institutions or global partnerships. In addition to bringing an end to the Resolute Support Mission in Afghanistan, alliance leaders should consider getting NATO out of the security assistance and stabilization business altogether. Calls for NATO to look for opportunities to do more in the MENA region should also be rebuffed. Few would dispute that this region poses real security challenges to European states or that these challenges are particularly acute for the southernmost members of the alliance, some of whom might even view migration and refugee flows as rising to the level of existential threats. But while the 21st century challenges to the “stability and well-being” of member states may be numerous and growing, there is only one NATO. A single organization cannot tackle every national security challenge its members face. To remain useful, the alliance must choose which threats to prioritize.

Doing so requires recognizing that not every security issue rises to the level of an existential threat to the alliance. Terrorist attacks were a common occurrence in many West European nations in the 1970s and 1980s, yet NATO did not fundamentally transform its agenda back then because members recognized that the threat posed by the Soviet Union was greater. While neither Russia nor China as yet represents a threat on par with the Soviet Union, NATO should prepare for the possibility that the latter (either alone or in combination with Moscow) could pose an existential challenge to the Atlantic community in the coming decades.

Nor is it evident that NATO was ever the appropriate venue for tackling threats like terrorism in the first place. Effective counter-terrorism requires intelligence-sharing; local policing and counter-radicalization programs; and financial instruments that agencies like Europol, Interpol, the Global Counterterrorism Forum, and others are better equipped to lead than an overstretched military alliance. The same is true when it comes to other activities the transatlantic alliance has added to its roster since 1991, like stabilization missions and security sector reform. In fact, organizations such as the United Nations, the Organization for Security and Co-operation in Europe, and the European Union provide more appropriate venues for tackling many of the collective security duties the alliance has assumed since the 1990s. As a regional defensive military alliance, NATO’s comparative advantage lies in providing territorial defense against other states or groups of states. This is a comparative advantage that should be preserved, not diluted by the addition of other security tasks. True comparative advantage arises from specialization. Continuing to add more and more security responsibilities to NATO’s already-full plate risks **transforming** the **military alliance into** a **glorified clearinghouse** or administrative apparatus whose sole task is the **facilitation of information-sharing** rather than the provision of **collective defense.**

**2NC – I/L – Resources Finite**

**NATO climate security requires tradeoffs and resource allocation.**

**Lipert, '16** – Policy Analyst, Lawyer, and Data Scientist (Tyler H. Lippert; "NATO, Climate Change, and International Security: A Risk Governance Approach"; RAND; https://www.rand.org/pubs/rgs\_dissertations/RGSD387.html; 10-2016, Accessed 6-24-2022)//ILake-NoC

NATO finds itself in a complicated and crowded institutional environment in the context of climate security risk. A variety of international organizations—as well as NGO and member state agencies—share responsibility for the potentially adverse and wide ranging impact of a changing climate. Yet, NATO has the resources and relationships to allow it to play a role in shaping, guiding, and implementing actions on the climate-security nexus.

The landscape of institutions with responsibility or interest in climate change and security is comprised of a mosaic of organizations. It should, therefore, come as no surprise that these 82 organizations have so far been unable to find a coordinated response. NATO will also struggle to articulate a formal position on climate change and security because of its consensus-based decision-making process. Still, a risk governance analysis can facilitate a discussion because it harnesses a broad array of risk considerations that could promote insights on whether NATO has adequately addressed the climate security risk it faces.

The problem of climate security risk requires **difficult tradeoffs** of attention and **resource allocation**. Policy makers must weigh various dimensions to make decisions. Even though the comprehensive view is preferred to individual analytic conclusions, information on climate security risk is nevertheless insufficient to render a complete understanding of the scope and implications because the location and magnitude of risks to be mitigated are deeply uncertain, global in nature, and highly complex (discussed in Chapter 2).

**2NC – I/L !! – Climate**

**Climate change is an existential risk and a threat multiplier. Integrating it with NATO risk assessment is vital to avoid extinction.**

Amar **Causevic 17**, researcher at Global Economic Dynamics and the Biosphere program at the Royal Swedish Academy of Sciences, “Facing an Unpredictable Threat: Is NATO Ideally Placed to Manage Climate Change as a Non-Traditional Threat Multiplier?,” Connections: The Quarterly Journal, Vol. 16, Iss. 2, 2017, http://connections-qj.org/article/facing-unpredictable-threat-nato-ideally-placed-manage-climate-change-non-traditional-threat

Climate Change as a **Non-Traditional Threat Multiplier**

Since its formation, the earth’s climate has been changing. The planet has witnessed multiple periods of climate change that lasted for **thousands of years**, during which the earth’s climate has been warming. The current global warming phenomenon is mostly caused by **increasing concentrations of GHGs** and other **anthropogenic activities**. Based on the measurements in **ice core samples**, scientists have come to the conclusion that present-day GHGs levels are the **highest they have been** since **800,000 years ago**.

In the early nineteenth century, the concentration of CO2 in the atmosphere was 280 parts per million by volume (ppmv). By the 1960s, emissions rose to 316 ppmv. Today they are around 420 ppmv.[26] The Intergovernmental Panel on Climate Change (IPCC) temperature threshold defined a “tolerable” increase in global average temperatures as an increase of only 2 degrees Celsius (°C). If the current emissions trajectories hold, however, humanity is heading towards a **5°C** increase in average global temperature by the end of the twenty-first century.[27] Even though a 5°C increase sounds like an insignificant number, when observed on a **planetary scale**, it certainly represents a **tremendous fluctuation**. The temperature difference between today’s temperature and the average global temperature during the last Ice Age was -5°C. During that period, significant parts of North America, Northern Europe, the Atlantic, and the Pacific oceans were covered with huge ice sheets.

Climate change is not principally an environmental concern, however. It is actually a problem that is closely **linked** to national **economic policy**, **strategic planning**, **public health**, **infrastructure**, **finance**, and international **security**.[28] The impacts of climate change are **already** dramatically affecting **food** security, **weather** patterns, **trade** relations, access to **fresh water**, and **mass migration**. Scientists have already provided mountains of convincing **ev**idence that global warming is **distressing** the **life-support systems** on which **human beings** and **other species depend**.[29] More importantly, these impacts are occurring much **more quickly** than some security experts and scientists had predicted. Sea levels are rising, snow and ice cover are decreasing, and both rainfall patterns and growing seasons are changing.

The biggest problem is that these changes are happening in a very **short geological time scale**. The earth’s climate has certainly changed over time, but in the **past** these alterations—barring extraordinary events like meteor impacts—developed slowly and lasted for thousands of years. This slow **pace** of climate change gave flora and fauna enough **time** to **adapt** and evolve. Scientists Ignacio Quintero and John J. Wiens discovered that species evolve at steady rates at around 1°C per million years.[30] Researchers from the IPCC stated that temperatures are going to rise between 2°C and 4°C in the next hundred years.[31] When calculated, the results lead us to the grim finding “that **matching** projected changes for 2100 would require rates of niche evolution that are **10,000 times faster** than rates **typically observed** among species.”[32]

A recent study by the Organization for Economic Co-operation and Development (OECD) shows that the most economically vulnerable regions are Africa and Asia. Based on data compiled since the 1990s, the OECD projects that gross domestic product (GDP) losses in 2060 will amount to 3.3 percent for the Middle-East and Northern Africa; 3.7 percent for South-and South-East Asia; and 3.8 percent for Sub-Saharan Africa.[33]Furthermore, GDP surges in Latin America, -1.5 percent by 2060, and Eurasia, which includes Europe, China, and Russia, in 2.1 percent GDP loss by 2060. In total, societies across the globe are facing a global average 2 percent of GDP loss.[34]

Climate change will negatively affect **food production** in tropical and temperate climates. Crops are adversely affected by drought and other extreme weather events. In the last hundred years the world significantly increased its food production and experienced dynamic growth in population. “Exposed and/or vulnerable regions will suffer from risks to **all aspects** of food security, including food **access**, **utilization**, and price **stability**, and could even experience **full breakdowns** of food systems.”[35] In the summer of 2013, for instance, Russia was hit by an extremely destructive drought. A state of emergency was declared in twenty regions across the country. In the end, a ten percent drop in Russian production caused a forty percent increase in global wheat markets.[36] Since the early 2000s, Syrian President Bashar al-Assad enforced an agricultural strategy with a goal of attaining self-sufficiency in national food production. During the effort to increase agricultural output, the country overused its water reserves. To make matters worse, Syria was home to one million Iraqi refugees, which contributed to additional social stress. From 2006 to 2010, large parts of the country were hit by consecutive droughts. When drought hit again in 2011, desperate farmers went to the cities and started protesting; when mixed with a complex ethnic composition and social structure in crisis, the drought certainly contributed to increasing tensions.[37] It is hard to claim that drought sparked the Syrian Civil War; however we can state that socio-economic despair triggered by successive droughts between 2006-2011 accelerated social unrest in that nation.[38]

Climate change will create public **health issues** through increases in **heat-stress mortality**, tropical **vector-borne diseases**, urban **air pollution problems**, and decreases in cold-related illnesses. “Areas where malaria is currently endemic could experience intensified transmission (on the order of fifty to eighty million additional annual cases, relative to an estimated global background total of five hundred million cases).”[39] Natural disasters between 1990 and 1999 killed 600,000 people.[40] Extreme and unpredicted fluctuations in temperatures cause heat stress (hyperthermia) or extreme cold (hypothermia) that often end in heart and respiratory failure. In the summer of 2003, high temperatures caused an estimated 70,000 more deaths as compared to the average death rate in previous years.[41] Warmer temperatures increase levels of evaporation and disturb rainfall patterns. This increases the risk of diarrhea, a disease that on average takes around two million lives annually. Diarrhea also increases the spread of trachoma, an eye infection that can lead to blindness.[42]

Environmental disasters are able to severely hurt **modern economies**. When hurricane Sandy ravaged the east cost of the U.S. and parts of the Caribbean, an estimated 1.8 million structures and homes were destroyed or damaged. Economic losses surpassed US$ 65 billion. Tourism was the hardest hit industry, with 10,000 job cuts and losses of US$ 1 billion.[43] In the aftermath of hurricane Katrina, US$ 40 billion in claims were filed and the city of New Orleans’ population decreased by 18 percent when compared to pre-storm levels.[44] In one of their reports that surveyed more than 1,500 leading global private companies, the Carbon Disclosure Project stated that climate change is the main threat to business security. The report also stated that more than one third of companies experienced disruption in production from rainfall or drought which caused a 31 percent increase in production costs.[45]

Pre-existing **poverty** **multiplies** the chances of failure when a state or region is faced with a massive flood or long drought. The majority of low-income countries are situated in tropical zones closer to the equator. On average they are hotter, which has traditionally limited their agricultural outputs, and as temperatures increase, the amount of agricultural output decreases further. For example, negative climate impacts are predicted to generate a welfare loss equivalent to a quarter of total income in sub-Saharan Africa and certain parts of Asia.[46] In 2011, Thailand was hit by unusually destructive floods. In total, sixty-five out of country’s seventy-seven provinces were affected. They lasted from July 2011 until January 2012, affecting the everyday lives of 13 million people. Total losses were US$ 45 billion, which classifies this event as one of the top five natural disasters in recorded history.[47]

Climate change can be classified as a **threat multiplier** for countries suffering from **political instability** and **ethnic tensions**. Socio-economic differences in the northern part of Nigeria, particularly in the Sahel region, are **stark**. In the last decade, more than hundred villages have been abandoned due to desertification. Migration and unrelated population growth have **added** supplementary stress to already unstable relations between ethnic groups in the Muslim north and Christian south. In 2010, this led to land disputes and uprisings that were fueled by religious differences in which approximately a thousand people lost their lives.[48] Moreover, amplified desertification of the Nigerian Sahel left many people in despair, strengthening the influence of terrorist organizations, such as Boko Haram, an **al-Qaeda** affiliate. Boko Haram used the power vacuum and inefficiency of the central national government to position itself as an ambassador, representing the grievances of northern Nigerians. **Boko Haram**’s actions infringed upon the Nigerian government’s ability to provide security.

NATO and Climate Change

NATO first defined and recognized environmental challenges as potential threat to security in 1969. The first organizational mechanism focusing on environmental challenges was the Committee on the Challenges of Modern Society (CCMS). CCMS utilized knowledge gained through networks of national experts working on scientific publications examining defense-related environmental issues. Teams of experts funded by member states tackled problems affecting ecosystems and quality of life through three to five year pilot studies, shorter term projects, conferences, workshops, and roundtables.[49]

In 2006, CCMS merged with NATO’s Science for Peace and Security (SPS) Program. SPS is a policy tool and platform for dialogue based on scientific research, innovation, and knowledge exchange. It provides funding, expert advice, and support to NATO-led operations and activities developed with partner states. NATO defines the environmental sphere within two concepts: security and protection. First, environmental security reflects responses to security challenges originating from the physical and natural environment. Second, environmental protection is defined as safeguarding physical and natural environment from the detrimental impact of military activities.

Since the formation of the CCMS, NATO has tried to respect environmental principles and policies under all authorized conditions. For that reason, the Alliance formed two different bodies, the Environmental Protection Working Group (EPWG) and the Specialist Team on Energy Efficiency and Environmental Protection (STEEEP). The EPWG drafts NATO policies that diminish possible harmful impacts of military activities on the environment. The STEEEP integrates environmental protection and energy efficiency regulations into technical requirements and specifications for military hardware, equipment, and machinery.

However, the notion of climate change as a security threat remains underdeveloped, especially when compared to traditional security risks such as traditional war, weapons of mass destruction, and terrorism. The non-traditional threat of climate change was first institutionalized in NATO’s agenda in the 2010 Strategic Concept for the Defense and Security of the Members of NATO. Point fifteen in the Security Environment section mentions the climate change in the following context,

Key environmental and resource constraints, including **health** risks, **climate** change, **water scarcity** and increasing **energy needs** will further **shape the future security environment** in areas of concern to **NATO** and have the potential to significantly **affect NATO planning and operations**.[50]

Former Secretary General de Hoop Scheffer highlighted climate change as a non-traditional threat in 2008. His successor, Secretary General Fogh Rasmussen, integrated climate concerns into NATO’s functioning mechanism. In 2009, General Secretary Rasmussen stated, “NATO should begin a discussion on how we—NATO as an organization, and individual Allies as well—can do better to address the security aspects of climate change.”[51]

It is clear that climate change has been on the Alliance’s priority list for years prior to the 2010 Strategic Concept, but until the beginning of this decade it was not integrated into the NATO’s agenda. The Emerging Security Challenges Division (ESCD) was established the same year as the Strategic Concept. The ESCD was established to respond to a growing range of non-traditional risks and challenges, with climate change being one of them. The division’s goal is to monitor and anticipate threats arising from non-traditional risks and catapult non-traditional security challenges to the center of NATO’s radar.

In 2013, NATO adopted the Green Defense framework, which “seeks to increase the Organization’s operational effectiveness through changes in the use of energy, while saving resources and enhancing environmental sustainability.”[52] The framework highlights NATO’s readiness to explore the smart energy domain. Additionally, work within the framework gave birth to the Smart Energy Team (SET), a working group that advises NATO on its efforts to help lower fuel and electricity consumption and identify practical energy-efficient solutions to the Alliance’s military forces. The SET should lead to cuts in CO2 emissions by the world’s biggest armed force.

In January 2014, Jens Stoltenberg became the United Nations Special Envoy on Climate Change. The 2014 Wales Summit Declaration stated that climate change and increasing energy needs will shape the global security arena in the future. The Wales Declaration underlined that climate change-induced security concerns such as environmental and resource constraints, including health risks and water scarcity, will result in crises that will directly affect NATO. The declaration reinforced the Alliance’s stance on the issue that climate change represents a new and growing threat to all NATO member states.

Shortly after the Wales Declaration, the NATO Parliamentary Assembly adopted Resolution 427 on Climate Change and International Security.[53] The document acknowledges that climate change-related risks are significant threat multipliers, recognizes the need to work on climate action with efforts to strengthen the resilience of states, and praises the formation of the Green Defense Framework and the SET. NATO showed readiness and willingness to invest in collective defense and to work to develop capabilities to respond to climate change challenges. During his visit to Croatia in July 2015, General Secretary Stoltenberg emphasized:

Environment, climate change is **critical** for promoting **development** and **peace** and **stability**. Development is important both for development and for security. And **security** is important to provide the **foundations** for development and for addressing climate change.[54]

At the moment, NATO is undergoing an evolutionary process in integrating the threat of climate change into the organization’s modus operandi. While the notion of climate change has been recognized, acknowledged, and analyzed, it has not yet been fully integrated into the Alliance’s operations. To date, climate change has been a strategic security threat that has for the most part been more actively pursued on the national level.

Consider the fact that the melting of the **ice** in the **far north** is making the Arctic more and more **accessible**. As the Arctic ice continues to **retreat**, trade routes will **remain open** for **longer** periods of time, increasing annual traffic of ships carrying goods and resources in the North. At present, no one owns the Arctic, but Canada, Denmark, Norway, Russia, and the United States have all laid different claims to territories on the Artic. In 2007, Russia sent a diving team to position its flag on the sea floor underneath the ice cap. NATO member state Norway is already adopting a Smart Defense Strategy that centers around a strong focus on the Arctic, both with regards to funding and resource allocation. In 2009, the Norwegian Defense Force made a decision “to relocate the Army’s Headquarters functions to the Arctic town of Bodø—1,700 kilometers north of Oslo—[bolstering] Norway’s commitment to establishing an integrated High North defense system.”[55]

Canada is another NATO member state that cares greatly about the Arctic sovereignty issue. Canada deployed Canadian Ranger units to help the indigenous population of the Canadian Arctic to ensure that northern communities are equipped with all necessary goods so that they may reap the benefits of economic activities. Maintaining functional population centers in the Arctic helps Canada protect its national sovereignty in the far North.

The United Kingdom (UK) has incorporated climate change in its national defense planning, introducing climate change study programs in its military staff colleges. In 2009, the British Ministry of Defence published guidance entitled “Defence in Changing Climate,” a document that outlines principal objectives and identifies concrete targets for GHGs reduction in the sphere of the UK’s military concerns.[56] The Ministry’s climate change strategy became effective in March 2012. Soon after the adoption of the strategy, the Ministry created the position of Climate and Energy Security Envoy to act as a focal point for representing this institution in the climate change and security realm.[57]

Spain formed a Military Emergencies Unit to respond to climate disasters. By 2012, this military unit had responded to ninety climate change-ignited disasters, most of them on domestic territory.[58] Defense strategy documents in Denmark, the Czech Republic, Germany, Italy, the Netherlands, and Poland all mention climate security, but do not yet have concrete mechanisms, units, and departments that respond to these security threats. The French military developed several climate and security projects, but has admitted that its leadership is just starting to acknowledge more seriously the importance of climate change in the national security nexus. In 2011, close to 4.5 percent of the French defense budget was allocated to financing environment and future defense policy. The Dutch government has invested millions of Euros in strengthening costal flood defense mechanisms, and Denmark has allocated 2.2 percent of its defense budget to improve the climate change disaster response capacity of the Home Guard Command.[59]

The issue of climate change encompasses a broad spectrum of human security, which may or may not include national security. So far, the U.S. has made the most progress in addressing this issue, as compared to the other twenty-eight NATO members.

Under the 2007 Global Climate Change Security Oversight Act, the United States initiated a far more systematic program of research on global climate change impacts on military requirements, operations, doctrine, organization, training, material, logistics, personnel, and facilities and on the actions needed to address such impacts.[60]

The 2008 U.S. National Defense Authorization Act directed the U.S. Department of Defense to evaluate the capability of armed forces to respond to natural disaster (e.g. floods, wildfires, droughts, etc.) and other missions the armed forces may be asked to conduct domestically or in foreign countries.[61]

The Pentagon’s 2014 Climate Change Adaptation Roadmap is a concise document that outlines the effects of extreme weather events and rising temperatures on military training, operations, acquisitions, and infrastructure. The document is designed to become the basis for long-term planning for security risks that arise from the increase in global temperatures. This report is significant because it utilizes strong language implying that climate change is not only a future, but rather a present security threat multiplier. In response to this document, the U.S. Department of Defense has: (i) collected historic data and potential future vulnerabilities from coastal locations and developed regional sea-level rise scenarios for 704 coastal locations; (ii) evaluated military installations’ vulnerability to global warming impacts and directed military planners to incorporate climate change considerations into certain installation planning efforts; and (iii) demanded that the hazardous impacts of climate change be included in installation master planning as we all as natural resource exploitation planning.[62]

The U.S. armed forces have been actively engaged in studying climate change as a security threat since the end of the Cold War. The U.S. Naval War College was the first institution that pointed out the potential impact of climate change on future policymaking. The U.S. intelligence community, as well, has been monitoring risks emerging from climate change within the MEDEA program—a collaborative initiative among climate scientists and U.S. intelligence agencies—and has been issuing intelligence reports based on analysis of climate change-related security impacts since 2008.[63]

Although the national defense agendas of some member states are ahead of NATO in responding to climate change impacts, NATO has been engaged in helping Partnership for Peace Program countries to mitigate natural disasters caused by or exacerbated by global warming. In May 2014, a low-pressure cyclone in Bosnia and Herzegovina caused the biggest floods and landslides in recorded history, with flood damages costing close to US$ 2.2 billion.[64] Although fewer than a hundred people died, a significant percentage of critical infrastructure—such as schools, hospitals, roads, and railroads—were destroyed or heavily damaged. In addition, the disaster created 2,100 active landslides across the mountainous Bosnian terrain and dislocated many of the 9,000 marked minefields. Twenty-one NATO members provided humanitarian aid, helicopters, rescue teams, medicines, blankets, and tents across Bosnia and Herzegovina. Upon the request of the Bosnian government, NATO activated the Euro-Atlantic Disaster Response Coordination Centre (EADRCC), which conducted operations in flooded Bosnian territory. Eighteen NATO member states sent boats, water pumps, power generators, humanitarian aid, and helicopters. Without the engagement of NATO’s EADRCC and NATO troops on the ground, Bosnia and Herzegovina would have faced serious if not impossible obstacles in its recovery efforts.

Climate change has **already** become a **dangerous reality** in the five Central Asian republics. Environmental mismanagement and limited climate-related disaster adaptation, combined with a naturally arid climate that has been profoundly affected by the global rise in temperatures, transformed the region into one that is now increasingly vulnerable to the effects of temperature fluctuations and water shortages. Over the last fifteen years, the rise in temperature melted one-third of all the region’s glaciers.[65]

Melting **glaciers** disrupt **regional water flaws**. The largest rivers in the region originate in the mountainous republics of Tajikistan and Kyrgyzstan; both republics are home to some of the Soviet era’s largest dams. At the same time that these glaciers are retreating, fresh water levels are additionally impacted by hydroelectric dams. Turkmenistan, Uzbekistan, and Kazakhstan are feeling the consequences of reduced downstream river flows. Tajikistan and Kyrgyzstan are trying to fight their water shortages by retaining a larger amount of water in the dam reservoirs, but as shortages are becoming more severe, there is less water left for the agricultural economies of downstream countries. From 2004 to 2009, NATO worked to support integrated water resources management for a wetlands restoration project in the Aral Sea basin.[66] Additionally, NATO was engaged in a project using a comprehensive multidisciplinary approach to assess the geo-environmental security of the Toktogul hydroelectric power station, which is the largest of its kind in Central Asia.

It is clear that **threats** emanating from global warming will **exceed national and regional scopes.** Climate change is a threat operating on a **planetary scale**, simultaneously activating multiple security challenges. Climate impacts will directly affect **military facilities**, **personnel**, and **hardware**. NATO **cannot ignore the perils** of climate change. Conversely, the Alliance will become more actively engaged in dealing with it. Since the publishing of the Strategic Concept in 2010 NATO started addressing this problem. Nevertheless, the Alliance can improve and catch up in institutionalizing the notion of climate change at the heart of organization by harmonizing its policy with the efforts already done by American, British, Canadian, Norwegian, or any other member state governments that could offer good solutions. In 2009, the former General Secretary Fogh Rasmussen laid out a robust list of objectives for NATO which are still relevant when applied to current context.

Future prospects for NATO’s involvement in the realm of climate change security could be paralyzed by U.S. President Donald Trump. Since the beginning of his presidential campaign as well as his presidency, Donald Trump has demonstrated skepticism towards climate change phenomenon.[67] Moreover, key members of Trump’s administration are climate change deniers (i.e. head of U.S. Environmental Protection Agency Scott Pruitt), fossil fuel industry lobbyists (i.e. U.S. Secretary of Interior Ryan Zinke), and former fossil fuel industry executives (i.e. U.S. Secretary of State Rex Tillerson). The new American administration has already started abolishing domestic initiatives to protect the climate and environment and seems likely to ignore climate change security as a component of wider NATO policy and operations. It is still early to predict changes in the U.S. official climate strategy within the Alliance; however, the U.S. withdrawal from the Paris Climate Agreement in June 2017 might have a negative impact on the Alliance’s ability to integrate further climate change mitigation and adaptation measures as a security component of NATO’s policy and operations.

Conclusion

Climate change is a non-traditional threat that has profound ramifications on a **planetary scale**. It simultaneously affects **every person**, **rich and poor**, as well as **every state**, **big or small**, **developed or developing**, **young or old**. Climate change is a **threat multiplier** that will **shape the security environment** in the twenty first century.

Although NATO is already engaged in developing policy and conducting operations responding to climate change impacts, it is easy to understand why climate change considerations are not yet fully integrated into the Alliance’s modus operandi. After all, NATO was conceived in the Cold War and—at least until the September 11 attacks—its main purpose has always been to react to traditional threats. Climate change is just one of many threats to which NATO must respond. Realism offers good solutions to analyses of war, conflict, geopolitics, alliances, and balancing behaviors, but it lacks effective solutions when it comes to confronting environmental security threats originating from climate change.

Climate change is a novel non-traditional type of threat with multiplier effects that must be effectively addressed. Hence, as the discussion above demonstrated, the Alliance should address climate change through utilization of a non-traditional approach to security. Beck’s risk society theory defines solid strategies to deal with climate change as a non-traditional threat multiplier. Risk society provides a theoretical framework for a systematic approach to dealing with hazards and insecurities induced and introduced by the process of modernization, of which climate change is a perfect example.

NATO will need to implement a stronger and more coherent approach to dealing with climate change. More precisely, the Alliance needs to develop more concrete policies as well as the capacities of partner nation forces to manage environmental security crises. This can include a faster process of sharing climate change-related knowledge between member states and the Alliance. This encompasses learning from capacities that exist on the member state level and upgrading them to work on the Alliance level. NATO militaries need to **integrate** issues related to **climate risk** into their **training** and **exercise routines**. Moreover, member states need to work on developing a common Alliance strategy for responding to the negative impacts of climate change on military planning and operations. Because there is currently a disparity about how this issue is addressed, all member states must be encouraged to integrate the mitigation of climate risks into their national defense strategies. The United States is currently led by a government that will most probably not focus on the issue, while its European allies such as France, Germany, and the UK already consider the mitigation of and adaptation to climate change to be one of their most crucial national security priorities. This difference in views has the potential to cause a certain level of disparity in strategic planning of the alliance. Nevertheless, the current U.S. administration’s dismissal of this security concern could potentially complicate stronger engagement of the Alliance in the field of climate change security.

At present, NATO exists in a world where it is facing both traditional and non-traditional threats. It has **proven itself** as an organization that can **master** traditional **threats**, but the Alliance must upgrade and accelerate current efforts to develop a more efficient and concrete strategy to respond to the non-traditional threat multiplier of climate change as a security risk. This will require leaders to encourage efforts for deeper **integration** of climate change **threat analysis** into policy and planning within the Alliance’s strategic thinking, because by doing so the Alliance will avoid paying higher security, economic, and social costs for the **greatest problem that will confront humanity in the decades to come.**

**2NC – !! – Warming**

**Runaway warming causes extinction**

Nathan Alexander **Sears 21**, PhD Candidate in Political Science at The University of Toronto, Former Professor of International Relations at the Universidad de Las Américas, Trudeau Fellow in Peace, Conflict and Justice at the Munk School of Global Affairs, “Great Powers, Polarity, and Existential Threats to Humanity: An Analysis of the Distribution of the Forces of Total Destruction in International Security”, Conference Paper: International Studies Association, 2021 Annual Conference, March/April 2021, https://tinyurl.com/bfbfspzx

*Climate Change*

Humanity faces existential risks from the large-scale destruction of Earth’s natural environment making the planet less hospitable for humankind (Wallace-Wells 2019). The decline of some of Earth’s natural systems may already exceed the “planetary boundaries” that represent a “safe operating space for humanity” (Rockstrom et al. 2009). Humanity has become one of the driving forces behind Earth’s climate system (Crutzen 2002). The major anthropogenic drivers of climate change are the burning of fossil fuels (e.g., coal, oil, and gas), combined with the degradation of Earth’s natural systems for absorbing carbon dioxide, such as deforestation for agriculture (e.g., livestock and monocultures) and resource extraction (e.g., mining and oil), and the warming of the oceans (Kump et al. 2003). While humanity has influenced Earth’s climate since at least the Industrial Revolution, the dramatic increase in greenhouse gas emissions since the mid-twentieth century—the “Great Acceleration” (Steffen et al. 2007; 2015; McNeill & Engelke 2016)— is responsible for contemporary climate change, which has reached approximately 1°C above preindustrial levels (IPCC 2018).

Climate change could **be**come an **existential threat** to humanity if the **planet**’s climate reaches a **“Hothouse Earth”** state (Ripple et al. 2020). What are the dangers? There are two mechanisms of climate change that threaten humankind. The direct threat is **extreme heat**. While human societies possesses **some** capacity for **adaptation** and **resilience** to climate change, the physiological response of humans to heat stress imposes **physical limits**—with a hard limit at roughly 35°C wet-bulb temperature (Sherwood et al. 2010). A rise in global average temperatures by 3–4°C would increase the risk of heat stress, while 7°C could render some regions uninhabitable, and 11–**12°**C would leave much of the planet **too hot for human habitation** (Sherwood et al. 2010). The **indirect** effects of climate change could include, inter alia, rising **sea levels** affecting coastal regions (e.g., Miami and Shanghai), or even swallowing entire countries (e.g., Bangladesh and the Maldives); extreme and unpredictable **weather** and **natural disasters** (e.g., hurricanes and forest fires); environmental pressures on **water** and **food scarcity** (e.g., droughts from less-dispersed rainfall, and lower wheat-yields at higher temperatures); the possible inception of new **bacteria** and **viruses**; and, of course, large-scale human **migration** (World Bank 2012; Wallace-Well 2019; Richards, Lupton & Allywood 2001). While it is difficult to determine the existential implications of extreme environmental conditions, there are historic precedents for the **collapse of human societies** under environmental pressures (Diamond 2005). Earth’s **“big five” mass extinction events** have been **linked** to dramatic shifts in Earth’s **climate** (Ward 2008; Payne & Clapham 2012; Kolbert 2014; Brannen 2017), and a Hothouse Earth climate would represent **terra incognita for humanity**.

Thus, the assumption here is that a Hothouse Earth climate could pose an **existential threat** to the habitability of the planet for humanity (Steffen et al. 2018., 5). At what point could climate change cross the threshold of an existential threat to humankind? The complexity of Earth’s natural systems makes it extremely difficult to give a precise figure (Rockstrom et al. 2009; ). However, much of the concern about climate change is over the danger of crossing **“tipping points,”** whereby **positive feedback loops** in Earth’s climate system could lead to potentially **irreversible** and **self-reinforcing** **“runaway”** climate change. For example, the melting of **Arctic “permafrost”** could produce additional warming, as glacial retreat reduces the refractory effect of the ice and releases huge quantities of methane currently trapped beneath it. A recent study suggests that a “planetary **threshold**” could exist at global average temperature of **2°**C above preindustrial levels (Steffen et al. 2018; also IPCC 2018). Therefore, the analysis here takes the 2°C rise in global average temperatures as representing the **lower-boundary** of an existential threat to humanity, with **higher temperatures** increasing the risk of **runaway** climate change leading to a Hothouse Earth.

The Paris Agreement on Climate Change set the goal of limiting the increase in global average temperatures to “well below” 2°C and to pursue efforts to limit the increase to 1.5°C. If the Paris Agreement goals are met, then nations would likely keep climate change **below the threshold** of an **existential threat** to humanity. According to Climate Action Tracker (2020), however, current policies of states are expected to produce global average temperatures of 2.9°C above preindustrial levels by 2100 (range between +2.1 and +3.9°C), while if states succeed in meeting their pledges and targets, global average temperatures are still projected to increase by 2.6°C (range between +2.1 and +3.3°C). Thus, while the Paris Agreements sets a goal 6 that would reduce the existential risk of climate change, the actual policies of states could easily cross the threshold that would constitute an existential threat to humanity (CAT 2020).

**It’ll be rapid, overwhelming adaptation, there’s multiple positive feedbacks AND it causes extinction from food, water, resource wars, ocean collapse, and disease**

John **Coviello 21**, Senior Technical Writer at Total Technology, Inc., Author of One Last Breath: A Look Back at 200 Years of Global Warming, Degree in Environmental Science from Susquehanna University, “Are Humans Facing Near-Term Human Extinction Due to Global Warming?”, Soapboxie, 7/23/2021, https://soapboxie.com/social-issues/Are-Humans-Facing-Near-Term-Human-Extinction-Due-to-Global-Warming

Looking back on the history of life on Earth, the main driver of species’ extinctions have been **changes in climate** over time that species could **not adapt to**, even when provided long spans of time to adapt. Given the unnaturally **fast rate** of global warming climate change now occurring, humans would have to adapt to the **rapid loss** of **habitat** and **food sources**, as well as all the other impacts, at an unprecedentedly fast speed. Adding to concerns regarding our survival as a species, pessimists point out that Homo sapiens are the last of several humanoid species (Neanderthals, Homo erectus, etc.) that made Earth their home for millions of years until these prior humanoid species eventually went extinct because they could not adapt to their environment and competition for food.

Why the Concern Now About Our Survival as a Species?

While some scientists started raising concerns about the burning of fossil fuels eventually warming the Earth’s atmosphere as far back as the middle 20th century, a consensus among scientists that global warming is a problem we have to address didn’t form until the later part of the 20th century.

Now that we’re progressing through the 21st century, why are some in scientific circles raising concerns about our near-term survival as a species? In recent years, the effects of global warming have become **exceedingly extreme**. In fact, from record-breaking **heatwaves** to unprecedented **forest fires** to melting **polar ice** sheets, the effects of global warming are occurring **fast**er than the scientific community had projected they would just a decade or two ago. The concern about our viability as a species on Earth is due to the fast-developing effects of global warming. If we don’t address the causes of global warming or take mitigative actions, it could **transform** into **runaway** global warming that would heat up the Earth **so rapidly** that humans and many other species will likely be **imperiled**.

Many scientists wrongly had confidence that mankind would come to its senses when faced with the stark reality that our survival as a species is threatened and we’d collectively take actions to avert catastrophic global warming by discontinuing our burning of fossil fuels and replacing them with renewable non-carbon energy sources. However, despite some tepid efforts to cut carbon emissions, such as the 2016 Paris Agreement, it appears that due to a combination of ignorance and a concerted effort by the fossil fuels industry to stop any efforts to move away from carbon-based products, we will likely not address our continuing release of global warming gases into Earth’s atmosphere until it’s too late and the global warming we’ve experienced in recent decades transforms into irreversible and catastrophic runaway global warming.

This will occur because human-caused global warming will eventually trigger natural climate warming **feedback loops** to take over. At that point, global warming will be like an **unstoppable** runaway train, as the Earth’s atmospheric temperatures rise to life-threatening levels. These warming feedback loops include such things as releases of global warming gases from melting polar ice sheets and from frozen methane deposits beneath the oceans, as well as the loss of polar ice causing the Earth to absorb more of the sun’s heat energy. All of which will cause additional warming, which then results in **additional releases** of global warming gases that will cause additional global temperature rises in an **unstoppable loop** that will continue until the planet is warmer than it has been in many millions of years (long before humans existed).

Such rapid and uncontrollable warming of Earth’s atmosphere could warm the planet by 4 to 5 degrees Celsius (7 to 9 degrees Fahrenheit) within the current century and perhaps eventually lead to a planet that is 8 to 9 degrees Celsius (14 to 16 degrees Fahrenheit) warmer than it was before humans started burning fossil fuels in large quantities starting in the 19th century.

Some might wonder, what’s the big deal if the planet is 4 to 5 degrees Celsius or even 8 to 9 degrees Celsius warmer than it has been as humans evolved on Earth? After all, many parts of the planet routinely experience temperature swings of this magnitude on a daily or weekly basis. There are several ways that **rapid** global warming on a planetary scale could **threaten human survival**.

Warming is not evenly distributed. Some areas, including currently farmable land, will warm well in excess of the global average, which would lead to **desertification** and **crop failures**. This would obviously **imperial humans** due to **massive food shortages**.

Oceans, **a**nother major source of food that **humans need to survive**, are impacted by rising global temperatures, as higher ocean temperatures lead to **acidification** of ocean water, which will eventually lead to **massive die-offs of sea life** that provide much-needed food for humans.

Water resources will completely dry up in many arid parts of the world, making those areas **uninhabitable**.

Dwindling food and water resources will inevitably lead to **wars** between competing nations that could be **catastrophic**.

Humans can’t survive at wet-bulb temperatures above 35 degrees Celsius (95 degrees Fahrenheit), even in the shade, as the human body loses its ability to cool itself off. Higher global temperatures and the higher humidity levels that will occur with the higher temperatures could make large parts of the Earth uninhabitable due to wet bulb temperatures that are lethal.

Would Runaway Global Warming Actually Lead to Human Extinction?

It’s a very big step go from runaway global warming to the extinction of all human beings on Earth. Humans possess the intellectual skills necessary to design and build technologies that can help us adapt to climate change. We’re also able to move to places with more hospitable climates. However, some scientists are concerned that humans will **not** have time to **adapt** to the **quick pace** of runaway global warming and some of the impacts will be **too harsh** for us to **survive**.

If farmlands and oceans are no longer capable of providing food for humans, where will we turn to obtain life-sustaining food? It is possible that humans could migrate towards the poles and try to farm on land in those areas that is freed up from the ice. However, it is unclear if the currently frozen areas in and around the polar regions will have topsoil suitable for farming. What about freshwater fish? Unfortunately, freshwater lakes and rivers will also undergo acidification that will likely wipe out most or all fish species that can provide humans nourishment. Our only hope might be some sort of synthetic food that is created in factories using basic elements (a technology that is certainly viable).

There will be other life-threatening factors that humans will face in a fast warming world. Massive **fire balls** from **methane releases** will create **havoc** for humans. These fireballs will start enormous forest fires driven by the warmer and in many places a more arid world, which will cause turmoil for humans. A lack of freshwater in areas that undergo desertification will make **survival impossible** in such areas. **Wars** over **dwindling resources** will be **fought** out of **desperation** and could **end in catastrophe**.

The stress of a warmer world will weaken human immune systems. If **industrial society collapses** or is greatly reduced, **health**care and medicines might become **very limited**, lowering life expectancy dramatically. Humans that survive all the dangers associated with runaway global warming might **succumb** to **pandemics** that will likely sweep the world as opportunistic pathogens take advantage of weakened human systems and cause a **large loss of life** in the **remaining human populations**.

**Defense doesn’t assume simultaneous shocks AND cascading societal collapse**

Simon **Beard 21**, Centre for the Study of Existential Risk, University of Cambridge, Lauren Holt, Centre for the Study of Existential Risk, University of Cambridge, Asaf Tzachor, Centre for the Study of Existential Risk and Cambridge Global Food Security Interdisciplinary Research Centre, University of Cambridge, Luke Kemp, Australia National University, Shahar Avin, Centre for the Study of Existential Risk, University of Cambridge, Phil Torres, Institute of Philosophy, Leibniz University Hannover, Haydn Belfield, Leverhulme Centre for the Future of Intelligence, University of Cambridge, “Assessing Climate Change’s Contribution to Global Catastrophic Risk”, Futures, Volume 127, March 2021, ScienceDirect

As part of their discussion of BRIHN Baum and Handoh (2014) note that climate change is the planetary boundary for which the risk to humanity has received most meaningful consideration and they suggest that this attention is deserved. Yet little research attention has been paid to climate change’s extreme or catastrophic effects. Kareiva and Carranza (2018) argue that, despite currently falling outside of the area of high risk, climate change has the clear potential to push humanity **across a threshold** of **irreversible loss** by “changing major **ocean circulation** patterns, causing massive **sea-level rise**, and increasing the frequency and severity of **extreme events**… that displace people, and ruin economies.” **Even if** humanity was resilient to **each** of these individual impacts, a **global catastrophe** could occur if these impacts were to occur **rapidly** and **simultaneously**.

One scenario that has received comparatively more attention is that of the global climate crossing a **tipping point** that would trigger environmental **feedback loops** (such as **declining albedo** from melting ice or the release of **methane** from clathrates) and **cascading effects** (such a **shifting rainfall patterns** that trigger desertification and soil erosion). After this point, anthropogenic activity may cease to be the main driver of climate change, making it accelerate and become harder to stop (King et al., 2015).

Other scenarios can be discerned from the numerous historical cases in which the modest, usually regional, climatic changes experienced during the Holocene have been implicated in the **collapse of** previous **societies**, including the Anasazi, the Tiwanaku, the Akkadians, the Western Roman Empire, the lowland Maya, and dozens of others (Diamond, 2005, Fagan, 2008). These provide a precedent for how a changing climate can **trigger** or contribute to **societal breakdown**. At present, our understanding of this phenomena is limited, and the IPCC has labelled its findings as “low confidence” due to a lack of understanding of cause and effect and restrictions in historical data (Klein et al., 2014). Further study and cooperation between archaeologists, historians, climate scientists and global catastrophic risk scholars could overcome some of these limitations by identifying how the impacts of climate change translate into social transformation and collapse, and hence what the impacts of more rapid and extreme climatic changes might be. There is also the potential for larger studies into how global climate variations have coincided with collapse and violence at the regional level (Zhang, Chiyung, Chusheng, Yuanqing, & Fung, 2005; Zhang et al., 2006). However, these need to be interpreted and generalized with care given the differences between pre-industrial and modern societies.

Societies also have a long history of adapting to, and recovering from, climate change induced collapses (McAnany and Yoffee, 2009). However, there are two reasons to be sceptical that such resilience can be easily extrapolated into the future. First, the relatively stable context of the Holocene, with well-functioning, resilient ecosystems, has greatly assisted recovery, while anthropogenic climate change is more **rapid**, **pervasive**, **global**, and **severe**. Large-scale states did not emerge until the onset of the Holocene (Richerson, Boyd, & Bettinger, 2001), and societies have since remained in a surprisingly narrow climatic niche of roughly 15 mean annual average temperature (Xu, Kohler, Lenton, Svenning, & Scheffer, 2020). A return to agrarian or hunter-gatherer lifestyles could thus have more devastating and long-lasting effects in a world of rapid climate change and ecological disruption (Gowdy, 2020).7 Second, modern human societies may have developed **hidden fragilities** that **amplify the shocks** posed by climate change (Mannheim 2020) and the complex, **tightly-coupled** and **interdependent** nature of our socio-economic systems makes it **more likely** that the **failure** of a **few key states** or industries due to climate change could **cascade** into a **global collapse** (Kemp, 2019).

A third set of plausible scenarios stem from climate change’s broader environmental impacts. Apart from being a planetary boundary of its own, Steffen et al. (2015) point out that climate change is intimately connected with other planetary boundaries (see Table 1). Climate change is thus identified by the authors as one of two ‘core' boundaries with the potential “to drive the Earth system into a new state should they be substantially and persistently transgressed.” This transformative potential was elaborated on in subsequent work exploring how the world could be pushed towards a ‘Hothouse Earth’ state, even with anthropogenic temperature rises as low as 2 °C (Steffen et al., 2018).

The connection between climate change and biosphere integrity (the survival of complex adaptive ecosystems supporting diverse forms of life) is particularly strong. The IPCC is highly confident that climate change is adversely impacting terrestrial ecosystems, contributing to desertification and land degradation in many areas and changing the range, abundance and seasonality of many plant and animal species (Arneth et al., 2019). Similarly, the Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services (IPBES) has reported that climate change is restricting the range of nearly half the world’s threatened mammal species and a quarter of threatened birds, with marine, coastal, and arctic ecosystems worst affected (Diaz et al., 2019). According to one estimate, climate change could cause 15–37 % of all species to become ‘committed to extinction’ by mid-century (Thomas et al., 2004).

Disruption to biosphere integrity can have profound economic and social repercussions, ranging from loss of ecosystem services and natural resources to the destruction of traditional knowledge and livelihoods. For instance, desertification, which threatens a quarter of Earth’s land area and a fifth of the population, is already estimated to cost developing nations 4–8 % of their GDP (United Nations, 2011). Many other rapid regime shifts involving loss of biosphere integrity have been observed, including shifts in arid vegetation, freshwater eutrophication, and the collapse of fish populations (Amano et al. 2020). There is a theoretical possibility of still more profound regime shifts at the global level (Rocha, Peterson, Bodin, & Levin, 2018). However, the contribution of loss of biosphere integrity to GCR is yet to be assessed. Kareiva and Carranza (2018) argue that it is unlikely to threaten human civilization, due both to a lack of plausible mechanisms for this threat and the fact that “local and regional biodiversity is often staying the same because species from elsewhere replace local losses.” However, in their classification of GCRs, Avin et al. (2018) suggest the potential for ecological collapse to threaten the safety boundaries of multiple critical systems with diverse spread mechanisms at a range of scales, from the biogeochemical and anatomical to the ecological and sociotechnological. Note that both these studies were conducted for largely conceptual purposes and should not be taken as rigorous analyses of this risk, this topic warrants further investigation.

3.2. Classifying climate change’s contributions to global catastrophic risk

Climate change's contribution to GCR goes well beyond its impact on the earth system. Taking Avin et al.’s list of critical systems, we note that previous studies have mostly focused on the effects of climate change on physical and biogeochemical systems (e.g. global temperature and sea-level rise) or the lower-level critical systems that are most directly related to human health and survival (e.g. Heath Stress). However, these represent a very limited assessment of risk as it only accounts for climate change as a direct hazard/threat and our "ontological" vulnerabilities to it. A more comprehensive risk assessment must consider the higher-order critical systems threatened by climate change passively (through a lack of alternatives) and actively (through intentional design).

The probability of a **global catastrophe** is higher when **sociotechnological** and **environmental** systems are **tightly coupled**, creating a potential for **reinforcing feedback loops**. If environmental change produces social changes that perpetuate further environmental change, then this could actively work against our efforts at adaptation. When this change has the potential to produce significant harm, via human vulnerabilities and exposure, we describe such loops as **‘global systems death spirals.’** These spirals could produce self-perpetuating catastrophes, whereby the energy and resources required to reverse or adapt to collapse are beyond the means of dwindling human societies. Feedback loops like this could thus create tipping points beyond which returning to anything like present conditions would become extremely difficult. Global systems would shift to very different states in which the **prospects for humanity** would likely be **bleak**er.

**2NC – !! – Warming – War**

**Even lower increments make nuclear war inevitable in every region**

Dr. Michael T. **Klare 20**, Five Colleges Professor of Peace and World Security Studies at Hampshire College, Ph.D. from the Graduate School of the Union Institute, BA and MA from Columbia University, Member of the Board of Director at the Arms Control Association, Defense Correspondent for The Nation, “How Rising Temperatures Increase the Likelihood of Nuclear War”, The Nation, 1/13/2020, https://www.thenation.com/article/archive/nuclear-defense-climate-change/

Climbing world **temperatures** and rising **sea levels** will diminish the supply of **food** and **water** in many **resource-deprived areas**, increasing the risk of widespread **starvation**, social **unrest**, and **human flight**. Global **corn production**, for example, is projected to fall by as much as **14 percent** in a 2°C warmer world, according to research cited in a 2018 special report by the UN’s Intergovernmental Panel on Climate Change (IPCC). **Food scarcity** and **crop failures** risk **pushing hundreds of millions** of people into **overcrowded cities**, where the likelihood of **pandemics**, ethnic **strife**, and severe **storm damage** is bound to increase. All of this will impose an immense burden on human institutions. Some **states may collapse** or break up into a **collection of warring chiefdoms**—all fighting over sources of water and other vital resources.

A **similar momentum** is now evident in the emerging **nuclear arms race**, with all three major powers—**China, Russia, and the U**nited **S**tates—rushing to deploy a **host of new munitions**. This dangerous process commenced a decade ago, when Russian and Chinese leaders sought improvements to their nuclear arsenals and President Barack Obama, in order to secure Senate approval of the New Strategic Arms Reduction Treaty of 2010, agreed to initial funding for the modernization of all three legs of America’s strategic triad, which encompasses submarines, intercontinental ballistic missiles, and bombers. (New START, which mandated significant reductions in US and Russian arsenals, will expire in February 2021 unless renewed by the two countries.) Although Obama initiated the modernization of the nuclear triad, the Trump administration has sought funds to proceed with their full-scale production, at an estimated initial installment of $500 billion over 10 years.

Even during the initial modernization program of the Obama era, Russian and Chinese leaders were sufficiently alarmed to hasten their own nuclear acquisitions. Both countries were already in the process of modernizing their stockpiles—Russia to replace Cold War–era systems that had become unreliable, China to provide its relatively small arsenal with enhanced capabilities. Trump’s decision to acquire a whole new suite of ICBMs, nuclear-armed submarines, and bombers has added momentum to these efforts. And with all three major powers upgrading their arsenals, the other nuclear-weapon states—led by India, Pakistan, and North Korea—have been expanding their stockpiles as well. Moreover, with Trump’s recent decision to abandon the Intermediate-Range Nuclear Forces (INF) Treaty, all major powers are developing missile delivery systems for a regional **nuclear war** such as might erupt in **Europe**, **South Asia**, or the **western Pacific**.

**DA – NATO Tradeoff [Cyber]**

**Notes**

OCOs tradeoff w/ cyber ops in Estonia to deter russia

**2NC – L – OCOs – CYOC**

**OCOs would be integrated by the CYOC.**

**Maigre, '22** – Non-resident Senior Fellow with CEPA's Transatlantic Leadership Program and CEPA's Digital Innovation Initiative, as well as the Senior Cyber Security Expert at Estonia’s e-Governance Academy, a non-profit that helps governments go digital. (Merle Maigre; "NATO’s Role in Global Cyber Security"; GMFUS; https://www.gmfus.org/news/natos-role-global-cyber-security; 4-6-2022, Accessed 6-24-2022)//ILake-NoC

CyOC is the first cyber-dedicated entity within the Command Structure. The “eyes and ears” of the respective commanders in cyberspace, CyOC aims at enhancing situational awareness in cyberspace and helping integrate cyber into NATO’s planning and operations at all levels. While CyOC operates within the existing NATO frameworks, its main aim is to equip the Supreme Allied Commander Europe with any necessary tools to operate in cyberspace. As CyOC moves toward initial then final operating capacity, it will be critical that it is staffed with sufficient—and sufficiently expert—personnel.2222NATO, NATO's Role in Cyberspace, February 19, 2019.

During NATO’s July 2018 summit, the allies affirmed, for the first time, their determination “to employ the full range of capabilities, including cyber, to deter, defend against, and counter the full spectrum of cyber threats,” shifting away from securing cyberspace with defensive measures only. The “full range” of cyber capabilities means that both defensive and **offensive capabilities** can be deployed by NATO, in line with its defensive mandate and in accordance with international law. As NATO will not develop or acquire any offensive capabilities, it will rely, like in other operational domains, on the voluntary contributions of allies.

**CYOC operations drain expertise from other NATO cyber operations.**

**Ablon et al., '19** – information scientist at the RAND Corporation and a professor at the Pardee RAND Graduate School. (Lillian Ablon, Anika Binnendijk, Quentin E. Hodgson, Bilyana Lilly, Sasha Romanosky, David Senty, Julia A. Thompson; "Operationalizing Cyberspace as a Military Domain"; RAND; <https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE329/RAND_PE329.pdf>; 2019, Accessed 6-24-2022)//ILake-NoC

Workforce

NATO will need staff officers, civilian personnel, and other augmentees who not only are **steeped in the technical aspects of cyberspace** but also understand how cyberspace operations can contribute to the overall success of NATO operations and how other domains can reinforce the cyber domain. NATO is starting to adapt its educational curriculum to address the full array of cyberspace issues. The NATO Communications and Information Agency has built a new school in Portugal to support its mission and teach staff about the operation of NATO IT systems.53 Other academic institutions, such as the NATO Defence College, the NATO School Oberammergau, or the Cooperative Cyber Defence Centre of Excellence, should also implement courses focusing on cyberspace as a domain of operations.

The competition for skilled cybersecurity personnel is well documented. The cybersecurity certification organization, (ISC)2 , noted in a recent report that the workforce **shortage of these professionals** is growing globally, reaching almost **three million positions** in 2018.54 Nearly half of the surveyed organizations for that report expected to increase cybersecurity staffing in the next year, underscoring that **demand will grow,** not diminish. NATO undoubtedly will be among those organizations competing in the labor marketplace for skilled cybersecurity professionals, but as we have seen, it will **require more than technical** **staff**. It will need to educate its leadership, both military and civilian, in the technical, operational, legal, and policy topics of cyberspace.

Officers and civilian personnel assigned to NATO on rotations will come with varied backgrounds and experience for the positions they will fill. Some positions, such as in the cyber offices at Allied Command Operations (ACO), ACT, and the new **CyOC** will clearly **need personnel** who have a deeper experience than the broader organization, something that will likely rely on personnel from a subset of the member nations for the near future, given the wide variance in national experience in cyberspace. But **other parts of NATO** will **also need to draw on cyber expertise** to ensure cyberspace integration into operations, including at the various operational headquarters. A first step to ensuring that qualified personnel are assigned (part of which has already been completed by the NATO Command Structure Adaptation that reviewed, among others, ACT and ACO cyber positions) is to evaluate and enumerate the specific job functions and associated qualifications for cyber-related positions across the alliance. These can include planners, operators, cyber defenders, acquisition personnel, and even less-obvious areas such as public diplomacy.

NATO relies on its member nations to send qualified personnel on rotation, but NATO also has longer-serving staff among its civilian personnel. Whether employees have served for three years or 30, NATO will want to ensure that its cyber workforce has a baseline of skills and knowledge and develop progressive educational modules to grow and sustain its human capital. As already noted, the baseline will vary depending on the work roles and job series a person occupies. The U.S. Department of Defense (DoD) has developed a DoD Cyber Workforce Framework that encompasses four main categories of personnel: cyberspace IT, cybersecurity, cyberspace effects, and intelligence.55 NATO could also look to bring in expertise on short-term assignments similar to the U.S. Defense Digital Service.56 It could also develop industry fellows programs to give its permanent staff experience in the private sector, similar to the U.S. Secretary of Defense Executive Fellows program.57 These programs could inject new thinking and bring valuable private-sector experience to bear. NATO’s educational institutions will play a critical role in developing and sustaining the cyberspace workforce for the alliance, starting with instituting courses that cover relevant topics, from strategy and policy to more technical areas. Some suggested topics to include in a first orientation course that establishes the baseline (some of which are already being taught) would include

• NATO organizational structure and national-level organizations that interface with the alliance. This would include covering the roles and responsibilities of the NCIRC, ACO Cyber Division, ACT Cyber Capabilities Branch, and the CyOC, as well as national-level cybercommands and EU institutions strategic and operational planning, including how cyber operations fit into the COPD and the NATO Crisis Management Process.

• technical topics for those less familiar with the layers of the cyber domain, from the physical infrastructure to the virtual or “cyber persona” domain.

• cyberspace capabilities in the alliance and at the national level, including defensive capabilities.

• the legal and policy frameworks for cyber operations, including the law of armed conflict and its application to the cyber domain, operational authorities, and NATO declarations and policies. Finally, NATO will need to address how it recruits and retains personnel to identify opportunities for attracting talent and taking advantage of expertise. Initiatives could include offering limited-term appointments from the private sector, scholarship-for-service, and developing stronger ties with academic institutions across the alliance.

Conclusion

For NATO to achieve the ambitious goals it has set for itself in Ministerial statements, it will take sustained effort and dedication. Each member has a role to play, at the very least in shoring up its own cyber defenses, as well as contributing to the extent it can and is fit for purpose to the overall defense of the alliance. In this section, we highlighted key areas to focus on in terms of defining cyberspace functions, exercises and training, and workforce development, but as is often the case, there are numerous other areas requiring focus. Numerous members large and small have clear capabilities in cyberspace. Harnessing those capabilities in an integrated manner will not happen overnight, but NATO

has the capacity and mechanisms to accomplish its goals.

Preparing for the Future:

Indications and Warning Against

Cyber Threats to NATO

Why I&W Against Cyber Threats?

Effective and timely I&W of cyber threats is a vital component of any cyber strategy because they can provide early detection and advance notification of cyber threats. This early warning can facilitate avoidance or mitigation of potentially harmful attacks by providing decisionmakers with needed time to consider options and authorize and implement preventive actions. Yet none of the cyber strategies released by the United States or its federal agencies discuss I&W in detail. National cyber strategies of other NATO members likewise do not elaborate on I&W of cyber threats, likely due to the lack of clearly established definitions or best practices on how to construct I&W frameworks in the cyber domain. The need to constantly refine and adapt these frameworks to the evolving threat actors provides further challenges for establishing a standardized cyber I&W model.

It is specifically because of these challenges that it becomes critical to identify the main parameters of an effective cyber I&W framework. For example, cyber I&W will help to ensure robust defense of the alliance’s cyberspace and continuous operation of NATO’s cyber infrastructure in support of strategic and operational planning. I&W capabilities for the cyber domain are also directly related to the functional areas of as described in Figure 1. To be effective at predicting and detecting threats to cyberspace, I&W frameworks require both horizontal (NATO-wide and across NATO members) and vertical (within NATO entities, nations, and sectors) integration and collaboration, including national contributions and collaboration between nation-states and national entities at multiple levels. Thus, designing rigorous I&W frameworks in cyberspace is a complex challenge that requires a number of key steps: crafting a strategy for cooperation and communication among NATO entities, NATO members and partners, and other public-private entities; developing information-sharing protocols that ensure timely and continuous data exchange; and integrating I&W cyber frameworks in joint cyber exercises to improve I&W applications.

Despite the significance of the field and some promising steps toward improving cyber I&W capabilities, frameworks for cyber I&W are still evolving and are not yet mature.58 The importance of I&W methods, combined with their relatively recent and underdeveloped application to cyberspace, suggests this issue warrants special attention.

In their process of designing a robust and adaptable cyber I&W framework, NATO entities may benefit from understanding how mature I&W frameworks from other domains in U.S. intelligence can be adapted to the cyber domain. Such I&W frameworks offer a way of thinking about security threats and provide methods for designing and structuring detection and response mechanisms.

In this section, we first define I&W, and then outline the publicly known progress that NATO has already achieved in relation to building its cyber I&W capabilities. We then propose a general framework for cyber I&W and discuss how NATO can further develop, adopt, and integrate cyber I&W capabilities within its current planning processes and operations. We conclude with an overview of several critical issues that we believe NATO entities should address to ensure that the alliance meets its missioncritical objectives in cyberspace.

What is Cyber Indications and Warning?

Cyber I&W focuses on collecting actionable information about threats to cyberspace that may provide early detection and warning of impending malicious cyberactivity. However, there is still no consensus regarding the concept of indications and warning. Some liken it to cyber threat intelligence and therefore focus on information directly pertaining to impending threats without analyzing broader strategic-level factors that can affect the behavior of a threat. Others define cyber I&W as a methodology that includes monitoring for indications of an impending threat, understanding the context in which this information is being collected, and performing strategic-level assessments of these indicators that can affect the behavior or nature of an impending cyberattack.5

Publicly available U.S. doctrine offers some insights applicable to the NATO context that can serve as a starting point for discussion. U.S. Joint Publication 2.0 stipulates that warning intelligence—a concept the DoD has recently adopted instead of indications and warning—includes “those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention.”60 Joint Publication 3-12 further stipulates that warning intelligence should be based on “all-source analysis in order to factor in political, military, and technical warning intelligence” and that “cyberspace threat sensors may recognize malicious activity with only a very short time available to respond.”61 While these definitions characterize the nature of cyber I&W concepts, they do not provide a full explanation of how to design an I&W framework.

The term indications and warning has a formal meaning in NATO and is supported through a set of processes governed by the member states with strong involvement by their intelligence communities.62 Yet NATO does not publicly offer a formal definition of what constitutes I&W in the cyber domain. Official public NATO documents provide only some insights; for instance, NATO’s 2018 Glossary of Terms and Definitions defines strategic warning as “[a] notification that hostilities may be imminent. This notification may occur at any time prior to the initiation of hostilities.” The document also defines tactical warning as “[a] notification that a local enemy attack is imminent. This notification may occur at any time from the indication of a probable attack until just prior to the target being struck or engaged.”63 The glossary defines indicator as “an item of information which reflects the intention or capability of a potential enemy to adopt or reject a course of action.”64 Although informative, these definitions provide only a general understanding of what activities constitute I&W. One distinction that can be made is separately defining indications from warnings. One may consider that there are indicators at various levels: strategic indicators (usually based on intelligence); operational indicators (combining intelligence and technical information); and tactical indicators (technical intrusion—malware, phishing, etc.). Warnings describe how and when to relay the indicators to the field.

Finally, the Intelligence and National Security Alliance (INSA), a U.S.-based nonprofit organization that facilitates collaboration between the private and public sectors concerning national security and intelligence,65 defines I&W against cyber threats as “an analytic process where an anticipated scenario in cyberspace is decomposed into indicators that can be continuously monitored to provide warning of the scenario coming to fruition.”66 We propose to adapt this definition to the NATO context and emphasize NATO’s primary area of responsibility and the political utility of I&W frameworks. We therefore define I&W for cyber threats as “an analytical process focused on collecting and analyzing information from a broad array of sources to develop indicators which can facilitate the prediction, early detection, and warning of cyber incidents relative to one’s information environment.”67 These indicators are then continuously monitored to provide warning of the scenario coming to fruition as much in advance as possible, allowing NATO to take preventive action.

Before we outline our framework, we first describe how NATO has already prepared its infrastructure for addressing, at least in part, cyber I&W

How Has NATO Already Prepared for Cyber I&W?

NATO has made significant progress in elevating the importance of the cyber domain and setting up the structural foundations for the effective adoption and integration of cyber I&W frameworks. In particular,

• At the Wales Summit in September 2014, NATO adopted an action plan for enhancing cyber defense, which was subsequently updated in February 2017.68

• At the Warsaw Summit in 2016, NATO members agreed to prioritize the strengthening of the cyber defenses of their national infrastructure and networks.69

• At the Brussels 2018 summit, NATO members discussed collaboration between NATO entities and nation-level cyber capabilities and teams. In the Brussels Summit Declaration, issued by NATO’s heads of state and government, the allies asserted that NATO “will continue to optimise NATO intelligence to facilitate timely and relevant support to Allied decision-making and operations, including through improved warning and intelligence sharing, particularly on terrorism, hybrid, and cyber.”70

• NATO claims to continuously update its cyber policy and its action plan, which contains “concrete objectives and implementation timelines on a range of topics from capability development, education, training and exercises, and partnerships” to include, for example, allied nations agreeing to a Cyber Defense Pledge to prioritize maturing their security controls.7

NATO has made significant progress in standing up NATO entities and capabilities to implement or be involved in the implementation of I&W frameworks for cyber threats. Some of the principal NATO organizations include

NCIRC, operated by NCIA and based at SHAPE in Mons, Belgium, is responsible for protecting NATO’s networks. NCIRC monitors, prevents, detects, and responds to cybersecurity incidents and provides centralized cyber defense support to NATO sites.72 In 2006, NCIRC obtained its initial operating capability and started to build more robust cyber situational awareness for NATO’s networks. In 2013, NCIRC expanded its intrusion detection monitoring capabilities to more NATO critical sites under the Full Operating Capability program. The sites were expanded again in 2017.73

• NATO’s CyOC, established at the Brussels Summit in 2018 as a part of NATO’s Command Structure and located at SHAPE. Among other responsibilities, the CyOC acts as a focal point for planning, preparation, conduct, and coordination of cyberspace operations, which will involve the processing and analysis of data.74 The CyOC is established to support I&W decisions, though it does not maintain a separate cyberspace I&W framework.75

• ACO Task Force Cyber is a multidisciplinary team acting as a part of Supreme Allied Commander Europe’s task to provide the Council with advice on I&W on threats to NATO’s collective security.7

• ACT is NATO’s warfare development command and capability requirements authority, responsible for NATO common funded capability delivery.

• NATO’s Intelligence and Security Division, supported by SHAPE Comprehensive Crisis and Operations Management Centre, NATO Intelligence Fusion Centre, and the national representatives, is responsible for the NATO I&W System, which incorporates I&W capabilities in cyberspace.77

• NATO Intelligence Fusion Centre, a multinational organization operating under a memorandum of understanding (MOU) with SHAPE, provides the primary intelligence analytical support.7

NATO’s educational structures have also substantially evolved and expanded their cyber education and training. NATO’s principal educational institutions include

• the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, a NATOaccredited research and training center providing education, consultation, research, and development in the area of cybersecurity

• the NATO Communications and Information Systems School in Latina, Italy, which provides training on operating and maintaining NATO’s communication and information systems to personnel from NATO members and allied nations79

• the NATO School in Oberammergau, Germany, which provides cyber defense education and training in support of NATO operations, policy, doctrine, strategy, and procedures

• the NATO Defense College in Rome, Italy, which emphasizes strategic education on cyber defense issues.80

NATO entities and allies have also recognized the importance of partnering with the private sector. Some of the benefits of such cooperation include establishing sharing of best practices and lessons learned and ensuring the timely supply and analysis of actionable cyber threat information. One of the primary channels through which NATO strengthens its collaboration with private partners is the NATO Industry Cyber Partnership. The partnership includes NATO structures, national CERTs, and industry representatives of NATO members. The partnerships include information-sharing activities, training, exercises, and multinational Smart Defence81 projects.8

Adopting Strategic Intelligence Frameworks to Cyberspace in the NATO Context

Despite significant progress in building cyber capabilities and integrating them into existing NATO planning, operations, and C2 structures, I&W for cyberspace is still a relatively immature discipline. Therefore, NATO and its components can benefit by adopting well-established and tested frameworks from more mature disciplines, which provide actionable policy-relevant recommendations related to the detection and assessment of security threats. For instance, cyber I&W concepts can leverage the I&W frameworks used by U.S. strategic intelligence, the Department of Homeland Security, or Cyber Command. The U.S. intelligence community has been developing and improving these frameworks since World War II to assess and monitor potentially threatening actions by U.S. adversaries in an attempt to avoid surprise attacks, such as the attack against Pearl Harbor in 1941.83

Among the most well-known warning intelligence frameworks are former senior intelligence analyst Cynthia Grabo’s comprehensive methodology for warning intelligence, Jonathan Lockwood’s Analytical Method for Prediction, and the U.S. Defense Warning Network conceptual framework.84 However, the cyber I&W framework produced by INSA reflects components of these traditional I&W intelligence frameworks and provides an appropriate model that can be adapted to the NATO context.85 INSA’s framework is a useful starting point for building a cyber I&W foundation because it was based on tradecraft from the U.S. intelligence community in consultation with governmental, academic, and private sector representatives and is one of the only publicly available documents on this topic. INSA’s original I&W framework contains the following seven steps: (1) identify and prioritize assets, (2) refine the threat, (3) assess threat courses of action, (4) break down scenarios into indicators, (5) plan and exercise countermeasures, (6) align to the intelligence cycle (collect information for each indicator from Step 4), and (7) execute proactive countermeasures.

While this framework is valuable and While this framework is valuable and fills a gaping void for publicly available information on cyber I&W, its steps are too broad for our purposes. Therefore, we will adapt it to the NATO context and outline how NATO can apply these stages below. We closely adhere to the steps proposed by INSA but modify the sequence of Steps 5 and 6 to emphasize the need to establish data collection mechanisms for the indicators identified in Step 4 first, before planning and practicing countermeasures. In effect, one needs to be assured that the indicators are properly collected before responding to them.86 We further discuss establishing standard operating procedures, exercising the planned countermeasures, and aligning them to NATO’s communication and command structure in Step 6—this is necessary due to the tightly interconnected nature of these aspects of the process. For each step, we propose how NATO entities, allies, and partners can apply it to increase the effectiveness of their I&W capabilities by standardizing their operational protocols and decisionmaking processes. The RAND modified cyber I&W framework consists of the following steps:87

1. Identify and prioritize mission-critical assets.

2. Maintain an updated list of top cyber threats.

3. Construct scenarios of potential cyberattacks.

4. Decompose scenarios into observable indicators.

5. Establish data collection methods and sources and set up a collection requirement and prioritization matrix.

6. Establish standard operating procedures and exercise chain of communication and command in different scenarios.

Finally, it is important to recognize that some of the steps described below relate to common cybersecurity practices. However, the steps involving scenario development and identification of appropriate indicators are distinct and unique to a cyber I&W framework. This exercise is not meant to define a highly detailed framework but merely to highlight the key first steps the alliance should consider on its journey to operationalizing cyberspace.

Step 1: Identify and Prioritize Mission-Critical Assets

NATO’s high visibility and central role in the Western security architecture make it an attractive target for a variety of malicious cyber intrusions.88 The chief of cybersecurity at the NATO Communications and Information Agency (NCIA) asserts that NATO detects about 550 million suspicious events daily. Although NATO is constantly seeking to improve its cybersecurity, **it is challenging to monitor, analyze, and** **act upon all of these events**.89 NATO’s cyber I&W capabilities, therefore, must be able to differentiate between security alerts that represent a **meaningful threat** to the alliance (or are precursors to an attack) from activities that constitute operational noise that can be ignored.90

Suggested actions: To achieve this goal, NATO should leverage its mission assurance efforts to first determine a list of **priority assets**. The continued development of such a list should stem from NATO’s primary mission to ensure collective defense and security of all its members, including the protection of communications systems that are owned and operated by the alliance.91 NATO can further focus on supporting the protection of C2 nodes on NATO-based military sites that coordinate operations of major offensive military platforms, as well as telecommunications and electric grid systems, on which militaries heavily rely for intelligence, logistics, operations, and communications.92

**2NC – I/L – Resources Finite**

**NATO cyber resources are limited – we must pick and choose.**

**Waterman, '22** – journalist and communicator who has worked for the BBC, United Press International and POLITICO, and an expert on cybersecurity and counterterrorism (Shaun Waterman; "Cyber Troops Stretched Thin in Ukraine Response as NATO Builds Common Air Picture"; Air Force Magazine; https://www.airforcemag.com/cyber-troops-stretched-thin-ukraine-response-nato-common-air-picture/; 3-14-2022, Accessed 6-24-2022)//ILake-NoC

The war in Ukraine has provided a wake-up call for U.S. military cyber defenders, who are facing hard choices about **how to deploy limited resources**, said Air Force Brig. Gen. Chad D. Raduege, the chief information officer of U.S. European Command.

“There’s been a realization that, quite frankly, **we can’t protect everything we have**,” Raduege told a virtual luncheon hosted by the Gabriel Chapter of the Air Force Association on March 9.

He added that this realization had been growing for some time. In his prior job in 2021 as chief information officer of Air Combat Command, “we found ourselves … identifying the key [IT] components for us to fly, fight, and win. And we were applying mission defense teams from a cyber component against those weapon systems and saying, these are our crown jewels that we need to protect.”

But faced with a **crisis that is demanding agile U.S. deployments** alongside a wide variety of partners, meaning small teams operating from unfamiliar locations, there **weren’t enough cyber defense teams** to go around, Raduege said, answering an audience question from retired Maj. Gen. Burke E. ”Ed” Wilson, the former deputy assistant secretary of defense for cyber policy, who previously commanded Air Forces Cyber.

“I think the area that we’ve got to continue to figure out is this idea that we were going [to] protect the weapon systems themselves, protect those smaller groups, with our mission defense teams. That’s a really great vision. What we found is we didn’t have enough capacity in the cyber realm to even stand up some of those capabilities,” Raduege said.

He said the Air Force is deciding which weapon systems it can **afford to protect**.

**Cyberspace resources are scarce and on demand – prioritization is key.**

**Cavegn, '18** – Managing Board Of Saunders & Cavegn Übersetzungen und Texte (Dario Cavegn; "Director of cyberdefense center points to decision-makers' lack of skills"; ERR; https://news.err.ee/683497/director-of-cyberdefense-center-points-to-decision-makers-lack-of-skills; 2018, Accessed 6-24-2022)//ILake-NoC

Authorities show lack of skills that needs to be addressed

In her article Maigre also pointed to the worrying global shortage of relevant skills. According to the White House's **cybersecurity** coordinator, the United States alone is short of some 300,000 personnel.

Adding to this are **scarce resources** and **talent constraints** in the public sector, along with a lack of coordination among agencies even of single governments and authorities in countries around the world only slowly reacting to developments that often happen at break-neck speed.

And though political leaders by now are making cybersecurity a campaign and policy issue, their understanding just how and why the subject should be approached in detail is often insufficient.

To make up for this lack of readiness and skills, organizations as well as governments should invest in preparation, which in turn requires knowledge. A solid knowledge base for cyber defense can only be developed in practice, which means that what is needed is a community of specialists and teams.

In practice, this means that both the military and civilian authorities **need to know about cross-dependencies** and **the different systems** in use. As it is already done at the cyberdefense center in Tallinn, exercises need to be based on scenarios that are as close as possible to real life.

Apart from the technological dimension there is also the **legal** and the **diplomatic** realm, both of which are important here. How should a country react to being attacked if it isn't immediately obvious where exactly the attack is coming from? Once the country of origin is identified, what then?

A hostile operation in cyberspace is taxed as an attack not based on whether it is directed against public or private infrastructure or against military or civilian personnel, but by the scale and effects of the operation. This is where international law comes in, as it is important to interpret an individual attack based on the existing legal means.

All of this is of great importance in a domain where politics can get lost in technical and legal matters. Identifying, spoiling, tracking, and reacting to cyberattacks takes skills and a level of preparation that in too **many** cases the **current generation** of **decision-makers don't have.**

**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.