## 1AC---Full Text

### 1AC---CT ADV

#### Contention 1 is Counterterror.

#### Expansive Article 5 coverage for non-state actors precludes necessary adaptation.

Sara B. Moller & Sten Rynning 3-23, Assistant Professor in the School of Diplomacy and International Relations at Seton Hall University; Professor in the Center for War Studies at the University of Southern Denmark, "Revitalizing Transatlantic Relations: NATO 2030 and Beyond," The Washington Quarterly, Vol. 44, Issue 1, pg. 192-193.

Protect Old and New Defense Spaces

Following the 9/11 terrorist attacks on the United States, NATO modernized its collective defense clause, Article 5, by invoking its provisions for “an armed attack against one or more” allies in the case of commercial aircraft hijacked for terrorist attacks. In subsequently invoking its collective defense clause for the first and only time, NATO explicitly noted that its treaty “was first entered into in circumstances very different from those that exist today, but it remains no less valid and no less essential today.” 47 The 2010 Strategic Concept affirmed allies’ commitment to deter and defend against “any threat of aggression, and against emerging security challenges where they threaten the fundamental security” of allies.48 A new Strategic Concept therefore needs only to reaffirm this modernized understanding of Article 5.

However, NATO needs to advance its thinking about the spatial implications of its collective defense commitment. NATO’s Article 6 delineates NATO’s commitment to national territory in the North Atlantic area (north of the Tropic of Cancer), but a broadened approach has become necessary. In 2016, NATO recognized cyberspace as a domain of operations; in 2019, it recognized outer space as such a domain. Cyber and outer space are limitless, and NATO should impose limits for its engagement: a focused approach would entail priority to issues that carry a risk of war. In a Strategic Concept, NATO could delineate this concern and task its staff to operationalize it. Because China occupies a central place in each of these domains, NATO must also do more to counter Beijing’s dominance in AI, cyber, space, quantum computing, and other high-tech military spheres.49

The new Strategic Concept must also address the Arctic, which has become an incipient arena of great power competition and was left out of the 2010 version. Since then, China has described itself as a “near-Arctic” state and published its own Arctic strategy. China’s state-owned companies have also entered into several development projects with Russian companies aimed at developing the Northern Sea Route.50 To guard against the potential for Chinese or Russian malignant activities in the Arctic, where both powers are increasingly active, and beyond, European militaries must expand their maritime, icebreaker, and rotorcraft capabilities.51

It is in NATO’s interest to define how China’s growing presence in NATO’s remit relates to its collective defense interests and how surveillance and maritime capacities—NATO-owned or reinforced—can help preempt tensions. 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 become so in the coming decades.

Conclusion

NATO’s continued transformation in the coming years seems all but certain; less certain is what it will transform into. The alliance has survived this long by adapting. But unlike during previous rounds of adaptation that involved the alliance taking on more responsibilities and tasks, the coming decades—whose defining feature will be the continued rise of China—will require a much more narrowly focused alliance. For nigh on three decades, NATO had the luxury of pondering what kind of alliance it wanted to be as it searched for a new raison d’etre in the reduced threat environment following the end of the Cold War. But the contrast between the 1990s and today’s deluge of challenges and threats is stark, and NATO no longer has the luxury of time.

To ensure the alliance’s future operational utility, the alliance must embrace its original collective defense identity and look for ways to streamline, and where possible reduce, its existing collective security and crisis management activities. In addition to offloading existing responsibilities to the EU and UN, NATO should think twice before taking on new mandates and avoid elevating new tasks like resiliency or counterterrorism missions and assigning them equal importance to Article 5. The alternative to the vision outlined here is an alliance increasingly weighed down by a myriad of tasks, unable to prioritize among them, and lacking both the political will and financial resources to perform its main function. An overburdened NATO risks being unable to fulfill its chief purpose of collective defense, thereby increasing the risk of further fracturing within the alliance. The proposed course of action will by no means be an easy one. But it provides the best chance to guarantee that the transatlantic alliance will have the capabilities and assets needed to meet the challenges posed by China’s rise.

#### Only clarifying ambiguity over Article 5 thresholds for non-state actor attacks ensures NATO cohesion AND resolve.

David H. Ucko 10, Adjunct fellow at the Department of War Studies, King's College London, "Resetting Article 5: Toward a New Understanding of NATO's Security Guarantees," World Politics Review, 10/26/2010, https://www.worldpoliticsreview.com/articles/6838/resetting-article-5-toward-a-new-understanding-of-natos-security-guarantees.

The Deceptive Decisiveness of Article 5

Of course, Georgia is not a NATO member, and while Afghanistan has sapped some of NATO's strength in Europe, the alliance still far outspends the rest of the world on defense. NATO's proponents insist that should a member state face outright attack, the alliance would come to its rescue, not least to defend NATO's credibility.

While such a scenario is imaginable, it rests on two problematic assumptions: that an eventual attack on a NATO member would be unambiguous, and that NATO could mount a swift and effective response. Neither assumption is likely to hold. In the case of the Georgian war, Russia acted as overtly as it did precisely because Georgia is not a NATO member. Against an actual member of the alliance, any worthy adversary, be it Russia or another actor, would opt for more-indirect means of exerting influence, so as to avoid prompting the invocation of Article 5 or even a concerted response. The point would be to operate under the threshold for triggering NATO's security guarantees, preferably with plausible deniability -- or at least some significant measure of ambiguity -- so as to confound, split and [freeze] ~~paralyze~~ NATO's decision-makers over a suitable response.

The potential means include cyber attacks, the use of armed or destabilizing nonstate proxies, energy-related threats or coercion, or even a limited military provocation or saber-rattling that nonetheless does not constitute an outright attack. Such acts of subversion and harassment could have severe consequences for the stability of NATO's most vulnerable members, but it remains unclear in which cases and under what circumstances they would warrant an Article 5 response. In the absence of a shared understanding of the article's current meaning, the scope for interpretation, disagreement, delay and even inaction is substantial.

The cyber attack against Estonia is illustrative. In April 2007, Estonia was hit by a distributed denial-of-service attack that also involved vandalism of key Web sites. The attack was not terribly sophisticated, but it nonetheless disrupted government services, communications and banking, to say nothing of the month-long campaign's psychological effect. Estonia appealed for help, but as a neophyte in the cyber domain, NATO could not muster a swift or effective response. In the end, NATO sent just a few advisers to Tallinn to help ascertain the source and nature of the attack, leaving the alliance's newest and most exposed members to question whether NATO's Article 5 guarantees could still be counted upon.

The Estonian crisis demonstrated that today's attacks are unlikely to be the unambiguous, military and territorial attacks imagined during the Cold War, and that NATO, as a military alliance, remains ill-equipped to operate in less-traditional domains or against less-readily identifiable actors. Similar conclusions can be drawn from NATO's sole invocation of Article 5, on Sept. 12, 2001. NATO's response then centered on Operation Eagle Assist, the deployment of Airborne Early Warning aircraft (AWACS) to protect U.S. airspace, and Operation Active Endeavor, the deployment of naval forces to the eastern Mediterranean "to help detect, deter and protect against terrorist activity." The alliance also pledged to share intelligence on the terrorist threat, provide overflight rights and access to ports and airfields as part of any retaliatory operations, and to assist any state whose support for these measures would prove destabilizing.

At first sight, NATO's response reflected an agile use of structures and capabilities configured for Cold War-era threats. But the first invocation of Article 5 also illustrated the limited relevance of its guarantees against less-conventional foes. Unlike the Soviet Union, al-Qaida was not deterred by the threat of collective NATO action. Nor were NATO's actions following Sept. 11 effective in punishing the transgressor or in forestalling future attacks. Indeed, it took nearly a month for NATO to confirm its invocation of Article 5 and launch Active Endeavor and Eagle Assist, as it first had to establish that the perpetrators of the attack were not domestic actors within the United States. And although the AWACS that NATO provided did free up some U.S. assets for the campaign in Afghanistan, Operation Eagle Assist was peripheral to the broader effort against al-Qaida and was terminated after a mere six months. The Mediterranean operation looked good on paper, but its relation to the al-Qaida threat was unclear, and the ships involved also operated under a limited mandate that precluded involuntary boarding of suspicious vessels.

Some European nations did deploy special forces to Afghanistan in 2001, yet even this response was a far cry, in terms of scale and effectiveness, from the type of reaction associated with Article 5. By the time the U.S. made more concrete appeals for European forces to come stabilize "postwar" Afghanistan, the mood of solidarity had already begun to wane. Having had their initial offers of assistance rebuffed by the then-bullish Bush administration, there was not much appetite in Europe to deploy, and the campaign basically had to be sold as another Balkans peacekeeping operation before European troops began arriving. By that point, the link between the Afghan campaign and the invocation of Article 5 had already substantially eroded.

In short, the threat and actual invocation of Article 5 does not deter less-traditional adversaries and types of attack, nor does it provide for a swift or effective response to these threats. As a military alliance, NATO is ill-equipped and ill-structured to deal with the security risks of terrorism, cyber attacks, political subversion and harassment (over energy or natural resources, for instance). The ambiguity of these acts, whether in their origins, effects, and nature, is also likely to delay NATO decision-making and undermine the alliance's resolve. As a result, the categorical response implied by the wording of Article 5 will be difficult, if not impossible, to put into practice.

Even in the case of a conventional military threat against a member state, getting NATO to react to anything short of an entirely unambiguous and -- quite unlikely -- territorial attack would still be an intensely political process, resulting in a delayed or circumscribed response. NATO's own war games have revealed the difficulties of galvanizing swift action in the consensus-based alliance, where several members face military shortfalls and others require U.N. or parliamentary approval to launch military operations. Relying on a predominantly American response has long been the norm, but this hedging strategy is becoming increasingly problematic as U.S. priorities shift away from Europe, and in light of Washington's own financial limitations and military commitments elsewhere.

The need for consensual political agreement has bedeviled previous attempts by NATO members to seek Article 5 guarantees in the face of military threats. In early 2003, Turkey grew concerned that its support for the imminent U.S. invasion of Iraq might provoke an Iraqi retaliation. But Ankara's requests for alliance assistance, mainly in the form of surveillance aircraft and missiles, quickly became mired in the alliance's internal rancor over the Iraq War. Ultimately, NATO was unable to arrive at a joint position on the matter or offer any security guarantees. A similar scenario occurred in 1991, during the first Gulf War, when the German government argued that it would be inappropriate to grant Turkey Article 5 security guarantees because of a war of choice, as opposed to an unprovoked attack. Both instances illustrate the intensely political nature of invoking Article 5, much as the experience following the Sept. 11 attacks points to the difficulties of following through with a timely, effective response.

Article 5: Abort, Retry, Fail?

The declining credibility of Article 5 has prompted two diametrically opposed reactions. On one side stand the "traditionalists," who see NATO's difficulties in honoring its security guarantees as an unfortunate oversight that can and should be remedied. By this line of argument, the alliance overstretched itself but can restore meaning to Article 5 by taking certain necessary steps. In a report entitled "Alliance Reborn," a group of Washington analysts propose some possible measures to do so. These include ensuring that NATO's Response Force is able to respond to likely attacks, holding exercises to improve NATO's ability to quickly reinforce a force or country under attack, investing in the infrastructure needed to offload such reinforcements -- particularly in NATO's easternmost members -- and stationing NATO common assets in one of these member states, or else creating a new NATO multinational corps composed of their armed forces. Others have arrived at similar proposals.

Though bold, these recommendations are not impossible. They do, however, face obstacles. First, in terms of sheer capability, they ask NATO members to boost their investments and act in a concerted manner to ensure the relevance of the alliance. Previous attempts to prod NATO members in this direction have not fared well, and in today's economic climate, progress is even less likely. Second, if the guarantees are to cover threats that are not military in nature, NATO would need to branch out into new areas, including the cyber domain, energy security, and others. NATO has developed some limited capacity to deal with cyber attacks since the 2007 strike on Estonia, but in general terms, it is uncertain whether, as a military alliance, it is able or willing to take on these less-traditional challenges.

Quite aside from the issue of capability, political will is a fundamental obstacle. There is a strong risk that the effort to bolster NATO's readiness against potential attack may itself heighten the threat against which these measures are ostensibly taken. It is hard, for example, to picture Russia, always the imagined adversary, standing idly by while its western neighbors militarize. This points to a broader problem: How interested is "old NATO" in providing unconditional support to "new NATO" in case of attack? Rather than representing an unfortunate but addressable oversight, the current malaise over Article 5 may in fact reflect the very limited interest on the part of NATO's more-powerful members in committing to the cause of collective defense.

Following this logic, and in marked contrast to the traditionalists who ask NATO to put its money where its mouth is, a small clique of "revolutionaries" argue that the best way forward is to formally renounce the Article 5 security guarantees. At present, they argue, those at the receiving end of these guarantees rightly worry that NATO will not be there when the time comes, whereas those who continue to peddle these promises do so while slashing their defense budgets -- or in the case of the U.S., its presence in Europe, its ability to respond to an attack there and its interest in the continent in grand-strategic terms. To analysts like Thomas Fedyszyn, dropping the Article 5 guarantee would signal an end to this charade and allow NATO to concentrate on its "non-Article 5" commitments -- that is, the gamut of operations that the alliance has undertaken since the Cold War -- without any distracting pretentions about collective defense or unmet expectations arising from misleading rhetoric. It is also possible, Fedyszyn adds, that dropping the security guarantees would ameliorate relations with Russia and open the door for NATO membership to a whole range of like-minded nations worldwide, whose support would serve the alliance well but who would refrain from joining so long as it implied a commitment to the collective defense of Eastern Europe.

The revolutionary proposal has its merits but underestimates the benefits of the Article 5 regime, however dysfunctional it may be. First, even the vague promise of collective security has encouraged NATO's newest members to partake in operations in Afghanistan, Iraq and elsewhere. There would be no real incentive for such participation if NATO did not provide these countries something in return, nor would these countries be so willing to accept risk at home by deploying their troops far away. Second, there is a constructive ambiguity to the current status quo: If Russia did indeed feel free to act more aggressively against Georgia because it was not a NATO member, then Article 5, however imperfect, retains a deterrent effect. Would-be adversaries might know that NATO's will and ability to defend a targeted ally is at times limited, but for them to assume NATO inaction or ineffectiveness in response to aggression would represent a monumental wager, given the consequences of getting it wrong.

Seen in this light, a dysfunctional Article 5 regime may, perversely, be in old NATO's interest. At present, in return for what are mostly token gestures of solidarity toward the East, Article 5 nonetheless produces a generalized deterrent effect, all while avoiding unnecessary provocation of Russia or letting NATO's easternmost allies dictate Western strategic priorities. This may also explain the lack of progress in addressing many of the shortcomings and problems facing Article 5 today.

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

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

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

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

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

#### Clear and consistent US leadership is key.

Ian Ward 05, Professor of Law at the University of Newcastle, "The Challenges of European Union Foreign and Security Policy: Retrospective and Prospective," Tulane Journal of International and Comparative Law, Vol. 13, 2005, pg. 47-54. error edited.

Throughout much of the 1990s, as we have seen, the testing ground for the European Union's evolving relations with the United States and with NATO could be found in the Balkans. And, as we have also seen, the test remains current. The events of September 11, 2001, however, changed everything, on both sides of the Atlantic. Indeed, as Prime Minister Blair suggested, it "changed the psychology of the world. 3 2 ' The idea of global security, previously so nebulous, has emerged as a very immediate and very real concern.

Overall, there is no doubt that European commentators favour a more differentiated approach to terrorism. As Stanley Hoffmann observes, there is a clear distinction between the "dogmatism" of the United States, which refuses to countenance any such differentiation, and European "empiricism," which is inclined to admit that terrorism is not a uniform experience.37 This has led, perhaps predictably, to accusations that Europe is just plain soft on terrorism.3 There is just too much "handwringing and vacillation," as former Secretary of State Albright put it." ' By way of repost, of course, European politicians and commentators have tended to voice a haughty disdain with regard to the seeming simplicity of the American "with us or against us" position.340

Regardless of the different intellectual and political attitudes assumed on alternate sides of the Atlantic, the European Union has remained consistent in its pursuit of multilateral responses to the challenges of global security. Even as it voiced sympathy for the United States in the wake of 9/11, the Council was quick to caution the need for a multilateral "global coalition against terrorism," one that must be pursued "under United Nations aegis."3 ' The security of the European Union must be secured outside its borders, and cannot, accordingly, be secured by any one global actor alone.3 ' The challenges of global security, it is repeatedly argued, require global solutions. As Javier Solana has rightly urged, "We need to think globally and to act locally," for in "an era of globalisation, distant threats may be as much a concern as those near at hand.""3 For this reason, Europeans must realise that the "first line of Defense will often be abroad."" The challenges of terrorism and weapons of mass destruction require "concerted" European and international action.3 5

The sentiment has been echoed at recent Council meetings. The Brussels Council of Foreign Ministers, in December 2003, affirmed that the "fight against terrorism is one of the highest priorities of the European Union."" 6 It also affirmed that the only legitimate means for conducting this "fight" was through multilateral institutions, most obviously the United Nations."7 Four months later, in the wake of the Madrid bombings, the full Council adopted a Declaration on Combating Terrorism. 48 "The threat of terrorism," it declared, "affects us all," and so, accordingly, a "terrorist act against one country concerns the international community as a whole."3'49 The multilateral tone was again pronounced. The Declaration further confirmed an EU "Plan of Action to Combat Terrorism," together with a Counter-Terrorism Coordinator, as well as a series of legislative measures in the form of framework directives intended to reinforce various provisions for "combating terrorism"-for example, freezing the assets of suspected terrorists, as well as measures intended to ease the workings of a European arrest warrant and facilitate a more rigorous collection and exchange of intelligence on suspected terrorist movements.350

The security of Europeans within the European Union is then entirely dependant on the responsibilities of the European Union without."' The Iraq crisis, and in particular the issue of WMD, was cast in precisely this context (or at least it was by those, most obviously the United Kingdom, who pressed the European Union to rally behind the American-led coalition of the willing). The European Union readily acknowledged the potential threat of WVMD at the Thessaloniki Council in 2003, where it devised a "Strategy Against Proliferation of Weapons of Mass Destruction.3 ' 2 This particular "threat to international peace and security" could not, the Council confirmed, be "ignored. 3 Moreover, the Council further acknowledged the implicit link between WMD and the "global fight against terrorism.""' Significantly, the Council confirmed the European Union's view that "effective multilateralism is the cornerstone" of any viable policies for "combating" the proliferation of WMD." ' Proliferation of WMD, it concluded, "is a global threat, which requires a global approach.'3 The Council further resolved to implement more rigorous procedures for monitoring the export of WMD-related materials, a commitment reaffirmed at the Washington EU-U.S. summit in Summer 2003.2" Most recently, in June 2004, the Council confirmed the European Union's commitment to United Nations Security Resolution 1540 which is directed against the proliferation of 351 such weapons.

Moreover, the Thessaloniki strategy went on to voice a very European concern with what it perceived to be the broader context of WMD and unrest in the Arab world. It identified a series of the "root causes" of "instability" which nurture rogue states and terrorist groups.359 These, it suggested, were primarily economic rather than cultural or moral, and being economic were readily surmountable by "development assistance" and the "reduction of poverty."36 This "root causes" approach has been articulated further by the current External Relations Commissioner, for whom the European Union owes a particular responsibility to share the potential fruits of globalisation. According to Commissioner Chris Patten, the "root of the problem" in the Mideast is not an inability to locate WMD anywhere, but a pressing need to promote wealth and democracy."' As the United Nations Development Programme Report on the Arab world concluded in 2002, the real problem is "poverty of opportunity.""36 The need to address this poverty, and the need to do so multilaterally, Patten adds, is a "salutary reminder" of the limitations of "occasional American exceptionalism."'36 Invasions can oust dictators, but they feed no one. The "alienated and the dispossessed" feel no less alienated and are no less dispossessed.364

Although the Council might pretend to hold a uniform position, the depth of division became only too apparent during the Iraq crisis. Whilst President Bush and Prime Minister Blair desperately strove to align WMD and the need to remove the present Iraqi regime, much of the rest of Europe remained stolidly unconvinced."5 Famously, United States Secretary of Defense, Donald Rumsfeld, declared that there were now two Europes, an old and a new: the former being led by the likes of France and Germany, the latter by the United Kingdom and a majority of newer Member States. 6 Certainly, French opposition was conspicuous and loud, as evidenced by their blocking of a second United Nations Resolution. 7 But what was perhaps most striking about the French position was President Chirac's determination to assume the leadership of a European opposition. 68 The European Union also ventured to voice its discontent; perhaps most conspicuous was Commissioner Patten's observation that the United States should not presume that the European Union will feel obliged to open up its cheque book in order to clear up the mess from a war it did not support.369

Of course, as Timothy Garton Ash has suggested, such a schismatic picture is misleading."' Just as many in America voiced reservations regarding the war, so, too, many European citizens voiced at least hesitant support. With regard to popular political support, the picture was, and is, far from clear. Much the same can be said of the question of legality. Certainly, there is no clear answer to the question whether the supposed breaches of United Nations Resolution 687 actually justified military engagement. Presuming some kind of customary jurisprudence, founded on a creative understanding of the doctrine of self-defence and the redefining of a collateral doctrine of preemption, the U.S. and U.K. governments maintained that it did. 7 ' Citing the fact that Resolution 1441 patently refrained from providing explicit authority for military intervention, the French government, along with the governments of most other European Union Members, argued that it did not."2

All in all, as Brian Crowe suggests, the events of the Iraq war "humiliatingly exposed" the continuing weaknesses of the European Union's CFSP when faced with a real life crisis. 373 Moreover, it was not just a matter of internal disagreement. Even if the European Union could have agreed on a "common foreign policy" position, the conduct of the war revealed once again that, in comparison with the United States and NATO, Europe's military capabilities remain limited.374 The United Kingdom did its best. Spain sent a few units along.3 7 But otherwise, as in the Balkans, the Iraq war was very much an American enterprise. Once again, it seems, if someone has to actually do something about a pending crisis, whether it be humanitarian crises in the Balkans or WMD proliferation in the Mideast, there is really only one credible option. The United States, acting within NATO or in the alternative guise of some kind of "coalition of the willing," must be persuaded to act. Alternatively, nothing happens. And the situation is not likely to change, not for the immediate future at any rate.376

The crisis in Iraq is ongoing, even if disagreements in the European Union have been largely papered over. The challenges of terrorism, counter-terrorism, and WMD, however, remain. At present, the same kind of tensions, both within the European Union and between the European Union and the United States, can be seen in attitudes towards Iran. Last June, the European Union, along with the United States, expressed its "continuing serious concern" regarding Iran's nuclear programme.377 Significantly, however, the United Kingdom has already joined France and Germany in articulating a clear preference for diplomacy rather than guns and, moreover, for working through the offices of the European Union rather than NATO or any ad hoc coalition."8 It may work. But if it does not, then it will be a matter of picking up the phone to Washington once again, which is the only, as Henry Kissinger famously remarked, 911 number in the international system.379

And yet the case for multilateralism is compelling. The postmodern world order, as Robert Cooper describes it, is defined by threats which are distinctive in their lack of clear distinction.38 It requires a post-modern response, a response that is effected by more than one, or even a coalition of nation-states determined to act as sovereign political bodies."' No one nation-state can effectively counter the terrorist threat, and neither can any one particular transnational body, whether it be the United Nations, NATO, or the European Union.382

At the same time, however, it must never be forgotten that, in the real Hobbesian world, power talks. It is for this reason that the European Union's relations with the United States will retain their central importance. Whilst the organs of security must remain multilateral, the tools will, for the foreseeable future, be supplied by NATO and, in reality, by the United States. The European Union must work within this context. As the European Union's new Coordinator for CounterTerrorism has recently confirmed, the effectiveness of an international response to terrorism will be geared by the strength of the EU-U.S. partnership. 83 It has become fashionable to argue for the continuation of a "good cop, bad cop" approach, with the European Union sweet-talking the terrorists and dictators, whilst the United States and NATO hover menacingly in the background threatening apocalyptic intervention.384

As Timothy Garton Ash concludes, for now and the foreseeable future, the prospects for a credible EU foreign and security policy depends upon working through a viable relationship with the United States and NATO. 8 The present standoff is absurd, and it can profit neither party. The future, not just of the United States and Europe itself, but of the cause of freedom in the wider world, depends on its resolution.36 In making this plea, Garton Ash repeatedly invokes President John E Kennedy's famous Declaration of Interdependence: "[W]e don't regard a strong, united Europe as a rival, but as a partner.387 It may, in military terms, be a subordinate partner. But that does not mean that it should be either supine or uncommitted. Neither stance will suit either party. Europe's role, Garton Ash concludes, must be to provide the Lockean constraint on sovereign power, which in this context means to provide a "check and balance" on the one "solitary hyperpower" in the world today.388

#### Revitalizing cohesion on CT threads the needle between total alliance dissolution and overexpansion AND enables a full spectrum alliance focus---that streamlines NATO’s crisis response to numerous emerging risks.

Thierry Tardy 21, Director of the Research Division at the NATO Defence College. Visiting Professor at the College of Europe. Ph.D, Political Science, National Session of the Institute of Higher National Defence Studies, "The Risks of NATO’s Maladaptation," European Security, Vol. 30, Issue 1, 2021, T&F.

This article deals with the process of adaptation that NATO has gone through over the last decade in the context of the so-called new Cold War. It contends that while seeking congruence with its environment, NATO is facing a risk of maladaptation that pertains to its positioning as a defence or security actor. On the one hand, NATO has adapted by going back to the basics of deterrence and defence in the new Cold War context provoked by Russia’s annexation of Crimea; in the meantime though, this move has created tensions for the organisation as it had to simultaneously cope with an increasingly diverse security environment that tends to pull NATO away from a narrow defence-focused agenda. This leads to a dilemma by which either NATO focuses on the narrow segment of military defence at the risk of becoming inadequate to a large range of threats; or it embraces a broader segment of security governance, with all associated risks, spanning legitimacy deficit, a weakening expertise, and dilution of its core military role.

By looking at this dilemma in the context of the new Cold War, this article provides an empirical case study of the side-effects of NATO’s adaptation, characterised in this study as the risks of maladaptation. The institutionalist literature is abundant on why and how NATO has survived the end of the Cold War through adaptation (Duffield 1994, McCalla 1996, Wallander 2000); the academic and policy literature is equally rich on NATO’s shift from collective defence to crisis management in the 1990s (Yost 1998, Rupp 2000, Frantzen 2005) and then back to collective defence in response to Russia’s resurgence (Sperling and Webber 2016, Ringsmose and Rynning 2017); however, the issue of the side-effects of adaptation policies during the latest episode of NATO’s organisational change has been under-researched, and we aim to fill this gap.

Our study is grounded on three premises. A first premise is that organisations need to constantly adapt to the environment they are operating in, so that they remain relevant to their constituencies and to the task for which they were established (Wallander and Keohane 2002). For the purpose of this article, “relevance” is understood as congruence or alignment between an organisation and the nature of its environment (Sarta et al. forthcoming 2021). It draws on the institutionalist literature that sees international institutions as being established by states to further their goals (Koremenos et al. 2001, p. 762). With this in mind, an international security or defence organisation is considered relevant if it demonstrates a certain efficacy in delivering on its mandate of protecting the citizens of its member states while adapting to environmental changes. Organisations that fail to adapt run the risk of being inadequate (or irrelevant) to the threats they are supposed to tackle and to their member states’ objectives. When this is the case, they may become obsolete, can be absorbed by other organisations or cease to exist. Relevance is a subjective concept and, in the particular case of NATO, is largely a question of the priorities set by its own member states and their perception of NATO’s core tasks. The point here is not to explore how much NATO is the product of its member states (it surely is to a large extent) versus how it can partially shape its own environment. This article is less about the nature of international organisations than it is about their adaptation to their environment and their quest for relevance. Nonetheless, we argue that congruence between what NATO is and does on the one hand, and the nature of the security environment on the other hand, is essential to NATO’s relevance in the twenty-first century.

Second, while organisational adaptation is a response to evolving needs and environmental changes, it is seldom linear and seamless (Olsen 2009). Indeed the process of adaptation often creates tensions and dilemmas for any organisation as it implies a number of changes to its structure, mandate, or policies. Change can be evolutionary or revolutionary (Gersick 1991); internally or externally driven, i.e. determined by the environment (Hrebiniak and Joyce 1985). Organisational adaptation can take many forms (Adegbite et al. 2018, Hardt 2018) driven by the nature of the organisation (Wallander and Keohane 2002) or the transformation dynamics; it may abide by the “punctuated equilibrium” model (Tuschman and Romanelli 1985) by which an organisation evolves in slow motion punctuated by more radical reorientations, which leads, in a NATO context, to the notion of critical junctures (Johnston 2017).

Most importantly, adaptation is likely to create unintended consequences. This draws on what economists call “negative externalities” (Mankiw 2020), or on what the literature on climate change calls “maladaptation” (Scheraga and Grambsch 1998, McCarthy et al. 2001, Magnan 2014). The term of “maladaptation” is used to characterise policies that lead, unintentionally, to adverse side effects or increased vulnerability. In other words, while an adaptation process aims at making an institution more congruent or relevant, it can generate costs for the institution or its member states, as a by-product. We believe that NATO’s adaptation policies over the last decade have created such adverse effects and costs that may increase NATO’s vulnerability rather than strengthen its relevance. For example, for NATO to focus on a narrow military segment, or to broaden too much its security agenda, would be examples of maladaptation. Shedding light on these side effects inform the academic debate on organisational change, contribute to the structure-agency framework of institutional analysis, and further advance the policy conversation on NATO’s optimal adaptation.

Third, in the context of this analysis, we believe it matters to distinguish variations of public policies along a security-defence spectrum. Our approach here is less concerned with theoretical debates (in reference to the different conceptualisations of security and defence) than it is with the practical implications of the conceptual distinction on adaptation policies. Security refers to a broad range of threats, risks and policy responses that span political, economic, societal and environmental dimensions (Buzan et al. 1998). In contrast, defence is a narrower concept, signifying “the act of shielding against an existential threat with military means” (Dönges and Hofmann 2018, p. 29). While security implies a large range of tools, defence is essentially a function of the use of military force or the threat to use it.

This distinction ought not to be overstated and the continuum between security and defence is well understood. As a matter of fact, such continuum has characterised NATO’s evolution over the last 30 years, as illustrated by its operations in the Western Balkans and Afghanistan, where the use of force has come in parallel with, or in support of, broader security policies. In the same vein, NATO’s role in counter-terrorism, both in Afghanistan and in its wider contribution to the Coalition against ISIS, has provided examples of the security-defence nexus. Nonetheless, the dichotomy between security and defence is useful to distinguish between what NATO does in the field of hard-core deterrence – or what the military would call kinetic activities – on the one hand, and what it does as a response to a humanitarian emergency, in the capacity building domain, or in the management of the COVID crisis, on the other hand. This distinction tells different stories about NATO’s strategic posture, institutional identity, capabilities, and of course operational activities. In other words, whether NATO does primarily defence or security matters to its adaptation, and therefore its relevance. This is all the more important as we furthermore assume that there are limits to what a security institution can do in terms of breadth of its mandate. Defence is part of a broader security agenda, yet this does not imply that a credible defence mandate is compatible with a large security agenda. What needs to be emphasised is the intrinsic tension between the need to specialise (being a credible defence actor) and the pressure to expand tasks (to cover a broader security spectrum). It is this tension that leads to maladaptation.

With these three premises in mind this article aims to unpack the risk of maladaptation that NATO is facing while responding to Russia’s resurgence by looking at the following questions: how has NATO adapted to the recent evolutions in the security environment? To what extent has this adaptation responded to NATO’s quest for relevance and reinforced the congruence between its mandate and the nature of the environment? What side-effects and maladaptation has the quest for congruence produced and how NATO should respond to the generated risks? In answering these questions we show that NATO is facing risks of maladaptation that are the consequence of the efforts to combine credibility in the defence domain with a presence on a broader security agenda. While we believe this is illustrated by the Russian context since 2014, the analysis is pertinent for NATO’s relevance beyond Russia.

The research relies on an extensive analysis of the NATO-related literature on NATO’s recent adaptation as well as on regular interactions with NATO officials from Headquarters and Strategic Commands since the Spring of 2018, as well as with representatives of NATO member states.

We proceed in three sections. In the first one, the article looks at how NATO went back to its collective defence role in response to Russia’s policy in Ukraine, and how this adaptation has supported the Alliance’s renewed congruence with the international security environment.

With the New Cold War starting in 2014, NATO has been given a new mission that it knows well – deterring and defending against Russia. This came at a moment when NATO was largely pulling out from Afghanistan, thus nearly putting an end to a 25-year involvement in crisis management operations. In a way, this “back-to-basics” moment was welcome for an institution on a quest for a new mission. At that stage, NATO was positioning itself in the narrow segment of collective defence, with all the credibility and legitimacy that come with it.

The second section examines the limits of NATO’s evolution and how it leads to possible maladaptation, i.e. some sort of asynchrony between what NATO does and what the environment looks like; and points to the inevitability of a broader positioning for NATO so that it embraces the widest range of security threats. While NATO adapts to the resurgence of Russia, the threat has evolved in a way that calls into question the centrality of collective defence, and with it the appropriateness of the narrow defence segment. In the hybrid, cyber, political warfare, digital world or age, the extent to which the deterrence paradigm would fully build NATO’s relevance is open to debate. If the threat materialises in a non-military manner, at the nexus between internal and external security (i.e. from within member states), and below the threshold of Article 5 of the Washington Treaty, will NATO’s traditional response suffice?

In the third part, the article delves further into the risk of maladaptation by looking at how embracing a broad security agenda can create vulnerabilities for the Alliance. To overcome the limits of a positioning on too narrow a segment, the Alliance has to an extent enlarged its mandate, for example by acquiring competence on a broader spectrum of activities, at the periphery of the military domain. But by trying to respond to threats for which it displays little added-value, does NATO not then run the risk of maladaptation and dilution of its core military comparative advantage, and in the end undermine its own relevance? In other words, by seeking congruence with the widened security agenda, NATO may face side-effects of adaptation that will in the end increase its vulnerabilities. This is not entirely new; adaptation in the post-Cold War era and the move to crisis management in the 1990s have raised similar questions. Yet, the “Russian context” sheds new light on NATO’s dilemma as it is simultaneously at the core of NATO’s adaptation and questioning the appropriateness of such adaptation.

The paper concludes on the necessity for NATO to make trade-offs, by which it combines the maintenance of a certain credibility as a military alliance with demonstrating relevance in non-strictly military domains. In doing this, the article suggests that partnerships are to be strengthened, so that, through burden-sharing, other institutions help maximise the congruence between NATO and its environment while minimising the risk of maladaptation.

NATO’s quest for congruence with its environment in a post-Ukraine world

From crisis management back to collective defence

International security institutions have often been faced with the difficulty of calibrating their own sphere of operation so that they respond to the concerns of their member states and meet the intent of their original mandate. This is what congruence is about. It draws on the comparative advantages of the organisation under consideration, analysed against the evolution of the security environment and member states’ policies. One aspect of this debate relates to how an institution and its member states define the scope of activities to be covered; how specialised versus how broad-ranging an institution’s mandate must be (See Koremenos et al. 2001, Guzman 2013). This, in turn, feeds into the adaptation process, as a particular balance of activities may need to be changed to respond to new needs.

With the end of the Cold War NATO has been faced with this debate in different ways: with the embrace of crisis management in the early 1990s at a time when collective defence was no longer central (See Rupp 2000, Galen Carpenter 2001); with the counter-terrorism turn post-911; and more recently with the move back to collective defence in the aftermath of the Ukraine crisis in 2014. Back in the early 1990s, NATO’s purpose was deeply challenged, most notably due to the fading away of its collective defence core task, and the mismatch that it implied between the Alliance’s character as a defence actor and the nature of the security needs. NATO needed to adapt. This debate, both in academic and policy circles, raised existential questions about NATO’s nature and purpose (see McCalla 1996, Wallander 2000, Menon and Welsh 2011). This was inter alia encapsulated by the “out of area or out of business” formula, by US Senator Richard Lugar (1993), which implied that crisis management operations conducted outside of the North Atlantic area were a response to the risk of irrelevance provoked by the absence of an existential threat.

Crisis management was undoubtedly important; as a matter of fact, crisis management operations in the 1990s and 2000s were by far the most visible NATO activity (Frantzen 2005, Edström and Gyllensporre 2012). Yet these operations were also challenges to NATO’s core defence function. Among the key questions raised was that of the need for NATO to adapt to a constantly evolving security environment, yet raising the risk that embracing an increasingly broader security mandate would undermine NATO’s core defence character. The “winning the peace” agenda would not substitute or even complement the war-fighting core role without (negative) consequences for the latter (Yost 1998, Nelson 2006).

In a post-911 context, the role of NATO in counter-terrorism (CT) raised similar questions. NATO had to adapt to the new environment, and thus respond to the terrorist threat (for which its Article 5 had been invoked for the first time), yet the comparative advantage of the Alliance in CT was not obvious to everyone, both for political and operational reasons (Valasek 2001/2002).

These two examples of crisis management and counter-terrorism show how an adaptation process can generate side-effects that in the end may increase the vulnerability of the institution, through maladaptation.

In this context, 2014 has been a key moment in NATO’s congruence quest (Webber et al. 2014). The 2014 Ukraine crisis and with it the annexation of Crimea by Russia have significantly changed the European security landscape and, for European security actors, their own perception of threats. While Russia was beforehand seen as a partner by most European states (NATO 2012, para. 36), 1 the Ukraine crisis brought it back to the category of threats. The New Cold War had begun (Lucas 2008, Trenin 2014, Kroenig 2015).

For NATO, this meant a return to the so-called deterrence and defence agenda, 2 and to the core task of collective defence, as defined in the 2010 Strategic Concept (NATO 2010). A few months after the annexation of Crimea, NATO member states meet at the Wales Summit, and state that “Russia’s aggressive actions against Ukraine have fundamentally challenged our vision of a Europe whole, free, and at peace” (NATO 2014, para. 1), and that “the greatest responsibility of the Alliance is to protect and defend our territories and our populations against attack, as set out in Article 5 of the Washington Treaty” (NATO 2014, para. 2).

Since then most of NATO’s attention has been towards the menace of a resurgent Russia, be it in terms of narrative (or securitisation process) and policy-making, capability development, military posture or exercises (see Ringsmose and Rynning 2017), leading NATO’s Secretary General to talk about “the largest reinforcement of our collective defence” since the end of the Cold War (NATO Secretary General 2018). Decisions taken include (Turner 2019): the strengthening of NATO’s rapid reaction forces, with the trebling of the size of the NATO Response Force, and the creation of a “spearhead force” within it, known as the Very High Readiness Joint Task Force (VJTF); the deployment of multinational battlegroups in Estonia, Latvia, Lithuania and Poland, known as the enhanced Forward Presence (eFP); the increasing of the exercise programme, with a new stress on collective defence exercises; the adoption of the NATO Readiness Initiative that aims at increasing the readiness of NATO forces with an additional 30 manoeuvre battalions, 30 major naval combatants and 30 kinetic air squadrons, with enabling forces, at 30 days’ readiness; and the building of resilience, including defence against cyber-attacks and other forms of “hybrid” attacks.

At the national level, those initiatives are paralleled by the US European Deterrence Initiative (EDI) that aims at strengthening Eastern European armed forces and infrastructures (see Marmei and White 2017); but also by the stabilisation and then slight increase of European defence budgets, in line with the 2014 Wales Summit Defence Investment Pledge (DIP). 3 This is particularly the case in Eastern European countries, that move towards the target of 2% of their GDP dedicated to defence spending. Overall, prior to the COVID-19 crisis, NATO’s projections were that European NATO allies would have spent an additional USD100 billion on defence between 2015 and the end of 2020 (NATO Secretary General 2019).

These various efforts should not hide the on-going political crisis about burden-sharing and the American narrative on the need for European states to spend more on defence (see Cordesman 2018, Newton et al. 2018). The burden-sharing debate has arguably undermined the cohesion of the Alliance, as much as it has raised longer-term questions about the nature of the US commitment. In the same vein, NATO’s defence posture on the Eastern flank is accompanied by a vivid debate on whether NATO indeed deters Russia, be it in operational terms through its enhanced Forward Presence or in more political terms, in relation to the solidity of the transatlantic bond (see Schlapak and Johnson 2016, Veebel 2018, Vershbow and Breedlove 2019). While these two sets of questions are evidence of the difficulty for NATO to be fully credible as a military Alliance, they nonetheless do not call into question the post-2014 shift towards deterrence and defence. In the name of relevance, NATO adapted so that it would serve best the security interests of its member states, and as of 2014 this arguably meant a focus on the collective defence agenda.

The virtue of “deterrence and defence”

The shift to “deterrence and defence” allows NATO to demonstrate full relevance as a defence actor facing a peer competitor that must be deterred or, if need be, militarily defeated. This, in turn, provides grounds for a discussion about NATO’s raison d’être. Indeed the shift towards collective defence leads NATO back to its core military identity and role, at the possible expense of any other non-military function. For neo-realist scholars who had long predicted the death of NATO in the absence of a unifying existential threat, the Ukraine episode may even offer a moment of respite (Walt 2014). This is all the more the case as 2014 is also the year when the largest NATO-led operation, the International Security Assistance Force (ISAF) in Afghanistan came to an end. Although ISAF was replaced by a sizeable training operation, 4 and NATO is still present in Kosovo, the withdrawal of ISAF symbolically marked the end of 20 years of NATO’s involvement in out-of-area crisis management, raising anew the question of NATO’s purpose and adaptation.

Already in the early 2010s, the prospect of NATO pulling out from Afghanistan and in general playing a lesser role in crisis management was questioning the raison d’être of the Alliance, at a time when neither Russia nor any other peer competitor could easily justify the level of investment that NATO implies (Interview with Michta 2014). The “what is NATO for?” question was not as blunt as in the early 1990s, yet concerns were expressed on the added-value of an Alliance searching for an enemy (Berdal and Ucko 2009). If there is no peer competitor to the Alliance, and if crisis management is no longer a priority, then where is the congruence between the Alliance and its environment, and what is it that justifies the maintenance of a transatlantic military pact?

With the Ukraine crisis, the relevance debate changes in nature, as peer competition comes back, and as NATO is unquestionably a first responder to the new threat. De facto, NATO moves away from crisis management and back to its core collective defence role. The discussion on relevance draws on NATO’s comparative advantages, in relation to those of other security actors. NATO’s comparative advantages stem from the organisation’s nature as a political-military Alliance furthermore composed of some of the most powerful and militarily experienced states. Those assets can be put in two categories. At the political level, one talks about the capacity to: deter the most powerful military actors; be a forum for strategy-making (Ruiz Palmer 2019); be the framework for the definition and implementation of the defence policies of most of its member states; be a source of legitimacy for operations; provide political clout. In more operational terms, one talks about a capacity to: carry out military operations covering the entire operational spectrum, including the most complex tasks; carry out large-scale exercises; provide interoperability among its member states; provide planning assets and a command and control structure for complex operations; provide expertise on a wide range of military-related issues, including defence capacity-building, defence sector reform, training, counter-IED, etc.

In this military-focused role, the right balance is to be struck between capacities and doctrines for counter-insurgency operations and other types of asymmetrical warfare on the one hand, and those for more traditional war-fighting on the other, for which the know-how may need to be re-learned (Greenwood and Savage 2019). The current policy literature talks about the need for NATO to keep the military edge in an ever interconnected environment; to remain militarily credible, acquire high-end capabilities, enter the digital age and constantly anticipate (See ACT 2017, SHAPE and ACT 2018). For those activities, NATO displays un-matched potential and legitimacy, and can, therefore, proport to be in the lead.

Finally, NATO’s focus on its core military task seems to take stock of the premise that in the current security environment, no security actor can respond to all threats alone (Petersen et al. 2010). Contemporary security governance must be multi-actors, with a division of tasks that results from a fair assessment of the respective comparative advantages of the actors involved. For NATO, a focus on collective defence also suggests that some of the “new threats” are not for it to tackle but will be better handled by others, and that the Alliance can, as a result, only be one part of the answer, very seldom the answer. In this context, NATO must focus on what it does best, and seek partnerships with others for the tasks where it will most likely play no role.

To summarise, the 2014 events have led NATO to adapt by going back to basics, in the sense that the Alliance has clearly re-embraced its collective defence agenda, backed up by its military/defence identity, and this has furthermore given NATO a new relevance that could not be provided by any other activity. In the following section, we offer that such adaptation was not as adequate as it appears, as it contains risks of maladaptation.

The limits of the narrow defence segment

What we have seen in the previous section is that there is a case for NATO’s focus on a military-centric posture, which is furthermore vindicated by the Ukraine crisis and what it says about the nature of Russia as a potential enemy. Such focus is rational and offers a coherence that apparently no other posture offers.

What we want to argue now is that the repositioning of NATO on a narrow, military-centric segment, generates side-effects that in the end may lead to maladaptation. More specifically, the question posed is that of how narrow and focused NATO’s mandate can be in a world characterised by the multifaceted nature of threats. Indeed, the conclusion by which NATO can, as the new situation in Russia illustrates, concentrate on its military role, is difficult to reconcile with a/ the nature of the security environment, and b/ the nature of the Russian threat. In other words, if the post-2014 aspect of NATO’s adaptation leads to a form on incongruence with the environment, then the adaptation process is to be questioned.

The widened security environment

The nature of current threats to international security and to NATO in particular plays against the Alliance’s core business and comparative advantages. At the core, NATO is a military instrument. It “thinks” and acts in military terms, in contrast to, say, the European Union, that is fundamentally a civilian actor. In the world that NATO is facing, threats such as Russia or ISIS show how central a military posture needs to be; how deterrence, or coercion, are indispensable to the preservation of stability. The narrative on the resurgence of great power competition also hints to the virtues of a strong defence posture (Brustlein 2019, Colby and Mitchell 2020).

This said, the evolution of the international system since at least the 1970s in parallel with the globalisation process, and the related implications for the concept of security (shift away from state security to human security), are also part of the picture (UNDP 1994; Buzan, Wæver, de Wilder 1998, Commission on Human Security 2003, Burgess 2008).

Looking at the current environment, many of the threats are simply not of a military nature and therefore do not necessarily elicit a military response. Current threats can take the form of random urban attacks using ramming vehicles (in the case of terrorism), the disruption of communication channels and IT networks (in the case of cyber), overt and covert activities using applications of artificial intelligence, automation and big data processing (in the case of political warfare), or the mix of some traditional modus operandi and covert, non-state-led, violent actions (in the case of hybrid threats), not to mention organised crime or the potential destabilising effect of illegal migrations. The fact that the perpetrators of these criminal and malicious acts are not necessarily military nor use military means to attack (nor even fire a shot) must inform about the nature of the response, in a discussion that operates the shift from defence to security, or maybe that is simply about the evolution of warfare (Fassi, Lucarelli, Marrone 2015).

The shift away from military threats is partly addressed by NATO’s Projecting Stability agenda, formalised at NATO’s Warsaw Summit in 2016 (NATO 2016a). Projecting stability is defined as “a range of military and non-military activities that influence and shape the strategic environment in order to make neighboring regions more stable and secure in support of both NATO’s strategic interests and those of its neighbors” (NATO 2016b). To an extent “projecting stability” operates the merger between crisis management and cooperative security, and de facto becomes one of the two main NATO’s missions, together with “deterrence and defence”.

Projecting Stability cannot though be put on a par with “deterrence and defence”; for reasons that have to do with the tangibility of the Russian threat versus the diffuse nature of the threats coming from the South, “deterrence and defence” is politically and operationally predominant. Nonetheless, the projecting stability agenda depicts a parallel agenda for NATO, as well as it informs on member states policy preferences. Projecting stability is supposed to contribute to the response to threats that emerge or re-emerge, mainly from the South, from terrorism to the potentially destabilising effects of illegal migrations. Some Allies push for an increased role of NATO in this field (See Vershbow and Speranza 2019). This, in turn, points to the so-called East-South divide within the Alliance, by which NATO member states diverge on their threat perceptions, based on their geographical origin (See Jakobsen and Ringsmose 2018). While some Eastern European States tend to see Russia as the main threat to the Alliance, countries of the South rather look at their Southern flank, which shapes their own threat perceptions (Sakkov 2019). Some member states, like France, even advocate some sort of reset with Russia in the name of European long-term stability (see Macron 2019).

Furthermore, the above-described threats are located along a spectrum that ignores national borders and that, for some of them, do not even have an external connection or cannot be located at all. Home-grown terrorism can be as devastating as externally driven attacks. This is what the internal-external security nexus is about, i.e. the intertwining of the internal/national and external security spaces that can, as a consequence, no longer be conceived of as distinct (Eriksson and Rhinard 2009). These characteristics of the security environment challenge NATO’s latest adaptation as they require a set of policy responses that is arguably far broader than what can be produced by a military institution focused on external defence. In the context of our research, this implies that NATO’s organisational change has generated costs that can be read as maladaptation. Indeed a side-effect of the shift back to collective defence is a form of incongruence with the environment. Even more importantly, maladaptation is also observed in the context of Russia’s resurgence.

The evolving nature of the Russian threat

The Russian threat is to be analysed in the more general context of the evolution of threats. Russia may well be a peer competitor that needs to be militarily deterred and/or defeated, and in this respect NATO’s military posture responds to a tangible need. Russia’s military modernisation has been well documented (see IISS 2016, Pifer 2016, Crane, Oliker, Nichiporuk 2019, RAND Corporation 2019). At least since 2008, learning the lessons from the Georgia war, Russia’s efforts have concentrated on ground and airborne capabilities, force generation and readiness, professionalisation (of some units), ballistic and cruise missiles, strategic and operational air defences, to an extent force projection, training, as well as exercises. Furthermore, Russia’s narrative on its nuclear power status and the threat to use nuclear weapons, have fuelled Western concerns and vindicated the deterrence and defence response (Crane, Oliker, Nichiporuk 2019).

In terms of materialisation of the threat, for states such as the Baltic States or Poland, the Ukraine crisis has depicted what could potentially happen in a NATO member state, i.e. a military incursion that must be fought by military means (see Schlapak and Johnson 2016, Barrie et al. 2019, Estonian Foreign Intelligence Service 2019). This does not necessarily imply a large-scale military operation, but the military component of the attack, with the crossing of borders by military units, is most often present in the hypothetical scenarios. How likely those scenarios are is difficult to assess, but NATO and its member states cannot simply dismiss these hypotheses. The necessity to respond at the highest military level is therefore prima facie justified.

This being said, the range of threats emanating from Russia cannot be equated to their sole military dimension. As a matter of fact, threats coming from Russia embrace the broad spectrum of contemporary threats, from hard core military to political warfare, information operations, cyber attacks, under-the-radar covert and/or criminal action (see Rumer 2016, Hagen Karlsen 2019). Many of these threats can furthermore materialise from within the territory of the Alliance.

Alongside the above-presented scenarios of a Russian occupation of a NATO member state’s territory, are situations were a Russian action would look very different from a military invasion. Those hypotheses include cases where the Russian move would take the form of “little green men” taking key positions in cities of a Baltic state, together with multi-tracked cyber attacks against critical infrastructure, disinformation campaigns, which would most likely start much earlier than any physical incursion (if any)(see O’Hanlon 2019, p. 198, McKew 2018). Some phases of such scenarios are possible without any physical crossing of a border between Russia and the state under attack; and some of these actions may have already started (see Estonian Foreign Intelligence Service 2019). 5 “Little green men” could also come from within and be “men in jeans” (see Radin 2017, Braun 2019), with actions being covertly orchestrated from abroad. This can unfold over a long period of time. These scenarios may produce destabilising effects without the firing of a shot (Stangl 2019). They contain economic, political, social, societal, civil protection, civil liberties implications, encapsulated in the notion of “hybrid war” (Galeotti 2019).

This raises the issue of the adequacy between the nature of the threat as above-described, and NATO’s posture and comparative advantage. Through the concept of societal resilience and total defence, states of Northern Europe and the Baltic region have adapted to the evolving threat (Flanagan et al. 2019), yet NATO as an organisation is still largely lagging behind. If the threat materialises in a non-military manner, at the nexus between internal and external security (i.e. from within member states), then the question of the added-value of NATO and of the appropriateness of its adaptation is legitimately raised.

This is all the more the case as the latter threats are less likely to lead to the invocation of Article 5 of the Washington Treaty than a clear-cut military intrusion. Over the last few years, NATO has made cyber an operational domain, and both cyber and hybrid attacks can theoretically trigger NATO’s defence clause. In practice though, this is likely to be difficult whenever the attack is diffuse, multi-faceted, and for some aspects of it not attributable.

To summarise and to put it bluntly, what is the purpose of the Very High Readiness Joint Task Force (VJTF) if the threat is “men in jeans” operating from within? Or, more fundamentally, what is the comparative advantage of NATO if most attacks that materialise do so under the Article 5 threshold? If NATO’s positioning on the narrow segment of deterrence and defence does not suffice, should NATO then broaden its mandate to cover tasks that are today part of threat response, though not strictly military-related?

Dilemmas and trade-offs

In the debate about congruence, one logical conclusion of the above-described elements about the character of the Russian threat is that NATO has to embrace a broader agenda than the one defined by the “deterrence and defence” mantra. To remain relevant, NATO needs to go beyond a too narrow defence-focused agenda, the argument goes. It needs to engage into a securitisation process, by which issues that were not previously belonging to its portfolio of tasks, would now appear on its agenda.

As a matter of fact, the shift to security is not new. Since the end of the Cold War, the Alliance has indeed broadened its agenda through activities in the fields of crisis management, implementing mandates often closer to police tasks than to genuine military undertakings. In doing this NATO demonstrated a sense of adaptability and resilience (Menon and Welsh 2011). NATO’s role in Afghanistan’s Provincial Reconstruction Teams (PRTs), or in humanitarian relief operations, provides more specific examples of NATO operating at the frontier of military core tasks to respond to broader security needs (see Gallis 2007, Jakobsen 2010, Williams 2011).

Similarly, NATO’s role in counter-terrorism, energy security (Bocse 2020), security sector reform, training, or more recently in the cyber domain, also attest to a broadening of the agenda. The entire discussion about hybrid threats and warfare epitomises this evolution. NATO has also developed expertise on these issues, both within its own staff in Brussels and through its network of Centres of Excellence. To a large extent thus, the defence agenda is subsumed into a broader security agenda and the challenge is therefore to make trade-offs between different types of activities.

We believe though that not only are these activities politically and operationally less prominent than what the “deterrence and defence” agenda has implied since 2014, but a key argument of this research is also that further developing these tasks carry risks of maladaptation. Maladaptation may result from issues spanning a lack of expertise and legitimacy deficit on many of the new tasks embraced, inter-institutional duplication and competition, uneven members states’ backing, to dilution of the Alliance’s core military role.

Enlarging the scope: towards security and internal threats

Acquiring a mandate or a capacity to tackle a broad range of threats implies that NATO moves in two directions: towards more security-type activities as opposed to defence-focused ones; and towards more internal issues. In both directions, a more assertive role for NATO implies three levels of activity: policy development, i.e. the ability to produce policy documents that frame NATO’s role in a particular domain; capability development, i.e. the ability to acquire expertise or resources that can be used for the implementation of a particular policy; and operations, i.e. the ability to act through operational activities, be they exercises, training or actual use of NATO and member states’ capabilities placed under NATO command. These three levels allow us to distinguish between domains where NATO would only act in a coordination or information-sharing role (for which capability development and operations are not necessary), and domains where NATO would be having a more central function.

Applied to the current landscape, the broadening security agenda beyond what is already done would imply a more assertive role for NATO in defensive/offensive cyber activities (with the cyberspace being an operational domain and covered by Article 5), in the fight against organised crime networks, inter alia through maritime security, as well as in the broad security sector reform (SSR) agenda of partner countries, to take just a few examples. In all these tasks coercion and military effect are not absent, yet they are less central than in traditional defence activities.

The second direction of the move – inward-looking – would mean that NATO plays an increased role in the defence against internal threats, by contributing to: critical infrastructure protection and resilience building; civilian protection tasks; police-type activities such as anti-terrorist operations in European capitals; operations that aim to tackle the security consequences of (massive) migrant flows; or support to police forces facing under-the-radar hybrid-type non-conventional attacks. This would imply establishing relations with a set of national actors, from law enforcement entities to municipalities, public companies (in the energy and transport sectors among others) and the private sector (Machi 2017). The role of NATO in these various activities could vary in ambition, spanning information-sharing, awareness rising, coordination, exercises, and more operational tasks.

The implied risks of task expansion

Although these various tasks make sense when assessed against the broad security needs of NATO member states and societies, and may be justified for political reasons, they carry a number of risks of maladaptation.

First, NATO would have to further develop or acquire an expertise on issues that can be very technical, or human resources-heavy, and for which even the member states may have a deficit (as in the cyber domain, energy security, or critical infrastructure protection). The added-value of NATO’s role would be all the more challenged as its expertise is being questioned. Second, the legitimacy of NATO’s role in some areas may be challenged due to a lack of expertise or because of the possible intrusiveness of NATO’s activities; this leads to sovereignty considerations, with states – be they NATO member states or not – having issues with any attempt from NATO to interfere with their internal sphere, in the law enforcement domain for example. Third, any task expansion would require a degree of consensus within member states on the merits of the enlarged mandate, and this will prove to be difficult, as illustrated by the sensitivities of broadening NATO’s agenda towards the South, to include counter-terrorism and migration policies for example (NATO official 2019). Even an agreement on broadening NATO’s mandate on the Eastern flank to embrace security issues would be difficult. Securitisation is inherently subjective (Buzan and Waever 2003, Sperling and Webber 2016); it is the outcome of a political choice that in turn results from an intersubjective understanding of what constitutes a threat. It follows that consensus-building on newly identified threats or policies is all the more difficult. Fourth, the broad security field is already crowded with institutions that in some areas would appear in a stronger position. NATO’s positioning on the broad field of activities would potentially duplicate existing capacities, and place it in direct competition with others, often in a weaker position. From the SSR domain in Sub-Saharan Africa to police or border tasks within European states, actors like the EU, national administrations, police forces and NGOs would not necessarily welcome a NATO role. Fifth, any broadening of NATO’s mandate would be resisted as it would carry the risk of diluting NATO’s war-fighting capability. Contemporary war-fighting is arguably politically, financially and operationally demanding; any parallel effort can, therefore, be seen as a deleterious diversion (see Stapleton 2016).

Cyber security provides a good example of these risks. Cyber is arguably a key dimension of NATO’s mission. It is part of “NATO’s core task of collective defence”, and its qualification as an operational domain implies that NATO “must be able to operate as effectively in cyberspace as [it does] in the air, on land, and at sea to strengthen and support the Alliance’s overall deterrence and defence posture” (NATO 2018, para. 20) At the 2014 Wales Summit, Allies have also stated that a cyber attack could lead to the invocation of Article 5 of the Washington Treaty. Furthermore, NATO has developed a fair amount of doctrinal and policy documents in that domain.

Yet the extent to which NATO can play an important role in cyber security is uncertain for reasons that have to do with expertise, capabilities, the nature of the threat and of its possible targets, and therefore the nature of the response. In terms of expertise, while NATO may provide support to the states that suffer shortfalls, notably through its Cyber Rapid Reaction teams, the Alliance does not display obvious comparative advantages vis-à-vis most member states (NATO Official 2019). As for capabilities to conduct cyber attacks, NATO has so far relied exclusively on its member states, through the concept of “sovereign cyber effects, provided voluntarily by Allies”, and integrated “into Alliance operations and missions” (NATO 2018, para. 20). The fact that cyber attacks (on NATO member states) would most likely target entities that are either private actors, or in any case under the protection of domestic police forces, is also an issue. As put by a NATO official, while what can be sought is a “military outcome, it cannot be achieved solely through military means”, and “what may be a military challenge is in fact inextricably linked with both civilian government, private industry and even individuals” (Brent 2019, p. 2). These issues lead back to the question of how much NATO can deter cyber attacks, in relation to both deterrence by punishment and deterrence by denial. Those limitations apply beyond the cyber domain, to most of the current threats, for which a military response can be necessary, but very seldom sufficient nor even central.

Conclusion – overcoming maladaptation

This article has offered an analysis of the risks of maladaptation that NATO has been exposed to while seeking congruence with its environment. As any security organisation, NATO has since the end of the Cold War sought to align with the needs and policies of its member states; yet such adaptation has generated side effects that can undermine the Alliance’s own relevance. We have looked at the context of the new Cold War to explore this maladaptation. As of 2014, the resurgence of Russia as a peer competitor has given NATO a new role as a collective defence organisation; Russia constitutes a threat and NATO offers a response to it; through the shift to collective defence NATO seemed to align with its environment. What we have seen in this article though is that the pure defence-focused response is insufficient to NATO’s alignment with its threat environment. Because the threats are diverse and embrace a large range of possible actions, the policy response needs to be equally broad-ranging and multi-domain.

This leads to the dilemma by which NATO must play with two imperfect policy options: either it focuses on the narrow segment of defence but then risks being ill-equipped for the multifaceted threats; or it enlarges its mandate to a broad range of tasks but then it runs the risks of diluting its core military function. The dilemma is here to stay. Member states are unlikely to agree on a strategy that would clearly identify one path at the expense of the other. And security institutions inherently struggle to demonstrate relevance and adjust their own mandate to the evolving environment.

In this context, the challenge comes from the exposed dilemma as much as it is about a trade-off between the narrow and the broad paths; in lieu of a binary choice the way forward is probably to calibrate the scope of the broadening (see Shea 2019). Here is the relevance challenge: for NATO to keep the military edge and being able to prevail in future military operations, while sufficiently enlarging the scope of its mandate so that it can respond to the most acute contemporary threats. Such trade-off builds a slightly different notion of congruence that is in the end more equivocal than initially asserted.

Further research is needed on this calibrating exercise as a potential response to maladaptation. When doing this, three sets of considerations will have to be taken into account, and one possible path is recommended.

First, the NATO of the Cold War is no longer a useful point of comparison; the threat environment is simply too different today and adaptation has, as a consequence, become a very different process. Second, maintaining a comparative advantage in the military domain will most likely remain a priority and therefore the starting point of any adaptation policy. Failing that, NATO’s added value would be at stake. Third, the nature of the threats means that NATO must to a degree embrace a wider security agenda: hybridity calls for it, and resisting task expansion will be difficult.

In this context, one possible way out comes from burden-sharing through institutional partnerships (Flockhart 2014). Back in the 2000s, the idea of the Comprehensive Approach (CA) emerged from the acknowledgement that “NATO cannot do it all”, and must, therefore, rely on partners which, because of their own expertise and comparative advantages, would maximise the broad international efforts, be it in Kosovo or in Afghanistan (see Williams 2011, Tardy 2012, Jakobsen 2018). This is no less valid today. Partnerships carry benefits that alliances bring, be it in terms of capability aggregation, strategy coordination, or burden-sharing (Wallander and Keohane 2002). Partnering with others is imperative as there are issues that are simply not for NATO to tackle and that are nonetheless essential to NATO’s mission. How to organise this new type of comprehensive approach goes beyond the remit of this article. The thinking relates to other institutions such as the EU or the UN, but also to sub-state actors such as municipalities, law enforcement entities or regions, as well as the private sector. At least two principles should guide the reflection so as to minimise the risk of maladaptation: first is the fact that any task expansion be based on NATO’s added value as a defence institution. It is this defence added value that must determine the nature of NATO’s role in any broader partnership. Any task expansion that would not make the military nature of the Alliance the starting point of the discussion would potentially lead back to the unintended consequences of adaptation and create incongruence. Second, any burden-sharing implies that NATO may not be in the lead, but rather in support of other actors, and even, theoretically, coordinated by others. This implies a sense of modesty in some areas of multi-domain threat response, where NATO’s added value is not central. Making these points takes us far from the alleged pertinence of the post-Ukraine collective defence agenda. Yet, this is what NATO’s relevance and congruence with the twenty-first-century security environment are about.

#### It ensures coordination across multiple environments:

#### First, counter-terror---ambiguity wrecks effective operations.

Stefano Santamato & Marie-Theres Beumler 13, Senior Visiting Research Fellow in the Institute for National Strategic Studies at the National Defense University; Research Intern in INSS. M.A. in Peace and Conflict Studies from the European Peace University, “The New NATO Policy Guidelines on Counterterrorism: Analysis, Assessment, and Actions,” Institute for National Strategic Studies, Strategic Perspectives, No. 13, February 2013, pg. 14-21.

More consequential is the last paragraph. In it, three short sentences reveal first-class policy and drafting skills by capturing the essence of four key assumptions of NATO’s response to counterterrorism. First, terrorism has never been a static challenge, and NATO’s efforts to counter it will remain dynamic and adaptive. Second, while recognizing the primacy of other national and international organizations, NATO will always be ready to lead counterterrorism efforts, in general or in specific areas, should the situation warrant. Third, notwithstanding the many facets of NATO’s actual and potential contribution, it is Allies’ capabilities that will make the difference in its response to terrorism, something that NATO defense planners will need to keep in mind when applying the concepts and principles of Smart Defense to the full spectrum of Alliance capabilities.

Fourth and final, the last 11 words of the document open and close a sensitive debate that is germane to the whole of NATO’s emerging security challenges, from cyber defense to energy security: the extent to which the Article 5 collective defense commitment applies to the terrorist threat. In the case of cyber attacks, Allies have stumbled against the “attribution” hurdle. In the case of energy security, the nonmilitary nature of possible energy coercion or intimidation has led more than one Ally to question the very competence and mandate of NATO. When it comes to terrorism, both arguments may apply, with the additional temptation of setting magnitude thresholds for an attack to “be eligible” for Article 5 invocation.

In this case, however, NATO brings to the table the power of precedent. NATO has invoked Article 5 following a terrorist attack. In fact, the September 12 declaration is the only occasion in the history of the Alliance of Article 5 invocation.58 Therefore, when the policy guidelines state, in the very last sentence, that “collective defense remains subject to decision by the North Atlantic Council,” one should not be misguided in thinking that Allies have decided to delay the debate through an if and when approach. The contrary is true. The sheer mention of collective defense in NATO’s policy guidelines on counterterrorism should be read like a stark warning to enemies and a reassurance to allies: if NATO did it once, it can do it again.

The Bad News

The overall judgment on the new policy guidelines can, and should, be positive. However, three “shadow areas” remain and will need to be clarified for the policy to express all its potential. Unsurprisingly, one of them is related to NATO cooperation, or lack thereof, with the European Union (EU). The second is a challenge common to all emerging security challenges, from nonproliferation to cyber defense: the need to reconcile the horizontal and cross-cutting nature of the terrorist threat with the vertical reality of NATO’s structures. The third is the Alliance’s need to establish a clearer link between its political-military nature and the fundamentally nonmilitary, counterterrorism constituencies within nations.

The Looming Shadow of NATO-EU Cooperation. These are the days when almost every debate on the future of NATO, European defense, or transatlantic relations writ large includes in its title “in an age of austerity.” Experts concur that the lack of real cooperation between the two organizations generates the single largest waste of transatlantic defense resources, and worse, of security capital. At regular intervals, summits and ministerial communiqués call for stronger NATO-EU cooperation.59 However, no solutions appear on the horizon due to a mix of political obstruction, bureaucratic resignation, and leadership hesitation. NATO’s Chicago Summit Declaration confirms this deadlock. While recognizing the importance of strengthening the NATO-EU strategic partnership, the Chicago Declaration steers away from clear commitments or taskings, focusing instead on operational cooperation and capability development. While aspiring to “broaden political consultations,” the inter-institutional dialogue has been reduced to an individual relationship between the NATO Secretary General and the EU High Representative.60

The accepted narrative is that NATO-EU relations work well on the ground and that the lack of strategic dialogue is compensated for by more pragmatic approaches at the operational level, from Kosovo to Afghanistan and from the Gulf of Aden to Libya. However, such an approach would be particularly risky in the realm of counterterrorism. It is clear that terrorists do not operate as self-contained individuals or groups. Be it the result of strategic partnerships or simple shared approaches,61 the growing link among terrorist groups, insurgents, and international criminality requires a networked effort by security, law enforcement, and justice authorities at both the national and international level. The risk is that NATO-EU theater-level cooperation may not work outside NATO-led operations, where the Alliance is engaged with thousands of deployed forces. In other words, it would be extremely difficult to promote NATO-EU practical cooperation in areas such as counterterrorism, where the EU and its member states are not demandeurs of NATO’s contribution. To make things more complicated, the policy guidelines further inhibit NATO’s engagement ambitions with the EU by introducing, in footnote and in text, the condition that NATO’s activities related to international organizations will be conducted “in accordance with the Comprehensive Approach Action Plan (CAAP) and the relevant decisions.”62 The reference to the CAAP is code language for another standard proviso of NATO-EU official texts known as “the agreed framework,” limiting the cooperation between the two organizations to the areas and conditions determined by the Berlin Plus Agreement63 and the related Security Agreement and Exchange of Letters.

The agreed framework de facto excludes Cyprus from any possible exchange of classified information between the two organizations.64 On the EU side, the political and legal argument that the European Union is a “single entity” that includes Cyprus prevents variable geometry relations. The resulting deadlock does not bode well for any substantial cooperation beyond mere exchange of information on activities such as training and exercises, protection of civilian populations against CBRN attacks, and civil emergency planning.

Unfortunately, there is no easy way out of this situation and NATO and EU staffs’ creativity will have to adapt to the pace of political evolution, hoping that breakthroughs are not preceded by loud explosions or images of chaos and suffering innocents.

A Round Peg in a Square Hole: The Challenges of a “Matrix Management” Approach to Counterterrorism. To segue into the second challenge the policy guidelines did not address, one could paraphrase a famous Henry Kissinger remark on Europe. The establishment of a counterterrorism section at NATO headquarters should answer the question: “Whom do I call when I want to speak to counterterrorism in NATO?” However, this leaves the door open to another European-inspired telephone joke: “Dial one for critical infrastructure protection; dial two for civil emergency planning; dial three for intelligence-sharing,” and so on. In other words, the policy guidelines do not support conceptual and strategic consolidation with structural amalgamation and executive consistency. The guidelines make no reference to the existence and role of NATO’s counterterrorism section and leave to the Terrorism Task Force (TTF) the task to report to council. Given that the TTF is an informal coordinating body with no real executive powers,65 it does not introduce a “matrix management”66 approach to NATO’s counterterrorism activities.67 NATO remains essentially a functional organization, and the policy leaves a management vacuum that reflects the enduring territorial resistance among various parts of the NATO International Staff organization and the struggle to reconcile the horizontal and crosscutting nature of the terrorist threat with the vertical reality of NATO’s structures. Unless specified elsewhere, NATO’s counterterrorism section has no authority to define or at least deconflict activities and resources68 for the execution of the policy guidelines across the NATO spectrum. To use a fitting military analogy, the guidelines do not clarify NATO’s command and control structure for counterterrorism. The long-term risk of this approach is that counterterrorism activities will remain byproducts of other, predominantly military, mainstream activities of the Alliance, reducing the overall impact of NATO’s counterterrorism policy.

Connecting to the Homeland Constituency. On the opposite side of the command and control spectrum sits the third unresolved challenge of NATO’s policy guidelines on counterterrorism: the absence within NATO of a homeland security constituency. Currently at NATO, only the Civil-Emergency Planning Committee and its subgroup on Civil Protection provide a forum for a number of national homeland security representatives. However, representation in these bodies is not very homogeneous, ranging from civil defense organizations, to civil protection agencies, to homeland security departments. The result is a lack of a coherent vision of the mandate of these committees and, as far as counterterrorism is concerned, the absence of authoritative national counterparts. The importance of this aspect should not be underestimated for at least two reasons. First, counterterrorism is intrinsically linked to a nation’s territory and populations. Citizens expect their national and local authorities to protect their lives and property from terrorist attacks. Conversely, one of the destabilizing aims of terrorist actions is to undermine national sovereignty, seen as the government’s ability to control the national territory and to guarantee security. This creates a responsibility and trust relationship between nations and their citizens that cannot—and should not—be transferred to a “third party” multinational organization. It therefore becomes crucial for NATO to establish a closer relationship between the support it provides to the counterterrorism efforts of Allies and partners and their respective populations.

The second important aspect is related to the nature of NATO as an organization. Even in its primary military defense responsibility, NATO has no direct access to all the necessary capabilities. With few exceptions, most notably for political consultations and command and control, NATO’s assets and capabilities belong to its members. It is therefore not a coincidence that its planning process (the NDPP) represents one of the pillars of its integrated military structure. Through the NDPP, nations coordinate and apportion their capabilities to the Alliance’s level of ambition. In case of need, a Transfer of Authority (ToA) mechanism allows national forces to fall under the control of NATO’s Supreme Commander. In recent years, as a result of NATO’s operational experience and the development of a comprehensive approach to operations, the NDPP was expanded to include selected nonmilitary capabilities, mainly in the area of logistics, stabilization, and reconstruction. However, no provisions have been implemented concerning the possible transfer of these capabilities under NATO command should a situation warrant. If and when they are made available by national organizations, civilian capabilities will always remain under national control. This requires a considerable effort to ensure national contributions to NATO’s requirements,69 and this challenge would extend also to counterterrorism assets. While the policy guidelines succeed in establishing a fundamental link between NATO’s counterterrorism capabilities and the NDPP, they fall short of creating the equally important nexus between NATO and those organizations responsible for implementing national policies and controlling national assets. Mediated access through NATO’s Defense Policy and Planning Committee, the Deputy Permanent Representatives Committee, or the Policy and Partnership Committee would load this relationship with the burden and challenges of national interagency processes.

More Good News?

None of these shortcomings should belittle the contribution of the policy guidelines on counterterrorism efforts to NATO’s continuous transformation process into a collective security organization. The mere fact that the Allies reached consensus on a role for NATO in countering terrorism is possibly the best news of all, irrespective of the caveats and nuances included in the guidelines.

More importantly, the guidelines jump-started a dynamic process that will culminate with the development of an “Action Plan to further enhance NATO’s ability to prevent, deter and respond to terrorism” through initiatives that will improve NATO’s threat awareness, capabilities, and engagement.70 As work on the Action Plan progresses along these lines, many ongoing activities, already mentioned by the policy itself, will be consolidated into a single consistent program. Others will require new approaches and initiatives, and in identifying these, NATO policymakers have the opportunity to design new activities and adapt structures to optimize NATO’s contribution to counterterrorism.

Awareness, capability, and engagement are mutually reinforcing dimensions of a broad counterterrorism effort. Partnerships multiply these capabilities and increase international awareness. Shared intelligence and strategic communications require outreach. Training and education are the result of continuous analysis and assessment. Naturally, some initiatives will fall under one category or the other. However, the opposite is also true. Much of NATO’s value added in countering terrorism rests in the Alliance ability to bring together awareness, capabilities, and engagement so that the total is larger than the sum of its parts.

In line with these considerations, this report will focus on six cross-cutting proposals that should find their way into the Action Plan. The table on page 19 summarizes the potential value added of the proposals to the three dimensions of NATO’s counterterrorism policy guidelines.

[Chart omitted]

Apply Net Assessment to Counterterrorism. Shared awareness is a critical component of any counterterrorism strategy. We need to understand the terrorists’ motives and anticipate their intentions if we are to plan effective prevention and response campaigns. We need to also be aware of our societal and material vulnerabilities to design effective mitigation and resilience plans. More importantly, all these components must be cross-analyzed to identify weaknesses, allocate resources, and create opportunities. This exercise of comparative analysis is inspired by the concept of Net Assessment, developed in the United States during the Cold War to “provide an even-handed look at both sides of complex military competitions.”71 While applying Net Assessment to asymmetric threats such as terrorism in a multilateral environment is a complex effort, it has the potential to yield significant results for NATO’s contribution to countering terrorism. Successful Net Assessment is the synthesis of close-hold and open source data. It relies on intelligence input, expert analysis, and public information. In this respect, NATO is most certainly a privileged environment where intelligence-sharing, cross-cutting expertise, and lessons learned come together. Threat and vulnerability scenarios can be developed in support of national preparedness efforts and multinational exercises designed to improve responses and consequence management.

The policy guidelines have already indicated that enhanced intelligence-sharing and strategic analysis will be at the center of NATO’s strategy. The Alliance has greatly improved the quantity and quality of its intelligence analysis through a reform that culminated in 2010 with the establishment of the Intelligence Steering Board (ISB) and the creation of an Intelligence Unit (IU) at NATO headquarters. Downstream from intelligence, NATO’s Strategic Analysis Capability has introduced Net Assessment methodologies in staff work, although its focus is still more “geographical” than functional. A number of NATO organizations, such as the headquarters’ Situation Center and the Allied Command Operations’ Civil-Military Fusion Center have the ability to collect and combine large amounts of open-source information. Greater effort should go to ensuring that all these assets work together consistently and coherently.

The Action Plan should ensure that coordinated net assessments of the global terrorist threat and of NATO’s response (and potential responses) are produced on a yearly basis. These reports should also become the basis for designing regular counterterrorism training and exercises and act as an authoritative contribution to the NDPP

Develop Effective Counterterrorism Strategic Communications. The policy guidelines contemplate strategic communications as a contribution to “promote common understanding of [NATO’s] counterterrorism role as part of a broader international effort.”72 As important and innovative as it is to increase a shared awareness of NATO’s contribution, the role of strategic communications in NATO’s counterterrorism efforts should not be limited to mere outreach.

As a means to an end, terrorism is often used to spread a destabilizing message. Its impact on public opinion is immediate. Social media and the 24/7 news cycle provide terrorists with unprecedented opportunities to disseminate their narrative, boast about their successes, and expose their victims’ vulnerabilities. Media coverage of terrorist acts becomes an unintentional ally of terrorist groups, forcing national and international authorities into defensive postures to maintain public confidence and support.

In countering terrorism, much like countering insurgency, strategic communications become the instrument to fight for and win public opinion.73 Terrorist actions and rhetoric aim to provoke overreactions that undermine the authorities’ credibility and weaken the democratic foundations of nations. The counterterrorism message must be unwavering and unequivocal. Above all, it should be credible. NATO should develop a Counterterrorism Strategic Communications Strategy that speaks with equal force to Allies’ public opinion and to possible adversaries. As counterterrorism and counterinsurgency share methodologies and lessons learned, NATO’s experience in marshalling public support within and for its operations could be an asset in countering terrorists’ propaganda. Mindful of General David Petraeus’s “under-promise and over-deliver” guidance for Afghanistan,74 NATO’s Counterterrorism Strategic Communications Strategy should bring together the doctrinal and conceptual contributions of NATO’s Center of Excellence for the Defense Against Terrorism (CoE/DAT) in Ankara, Turkey,75 as well as those of national civilian counterterrorism organizations. In doing so, NATO must engage with its target audience in a two-way communications process through “strategic listening” opportunities.76 NATO’s Allied Command Transformation project on Human Environment Capabilities is a clear example of the importance of bringing together strategic communications, civil-military interaction, cultural advisors, and the Comprehensive Approach when facing emerging security challenges.77

#### Europe is the locus of CBRN terrorism.

Dr. Elena Lazarou 20, Acting Head of the External Policies Unit of the European Parliamentary Research Service and an associate fellow in the US and the Americas Programme at Chatham House. Assistant professor of international relations at the Getulio Vargas Foundation, "EU Action to Counter Threats to Peace and Security," in Peace & Security in 2020, Chapter 2, September 2020, pg. 63-64.

The threat of a terrorist attack comprising chemical, biological, radiological and/or nuclear (CBRN) elements has become a realistic scenario.226 \*\*\*FOOTNOTE BEGINS\*\*\* 6 B. Immenkamp, ISIL/Da'esh and non-conventional weapons of terror, EPRS, European Parliament, May 2016.\*\*\*FOOTNOTE ENDS\*\*\* Repeated chemical attacks by both State and non-state actors in the Syrian conflict, the Novichok attack in Salisbury (UK), and foiled terror plots in France, Germany and Italy that involved chemical or biological agents have sharpened the EU's resolve to tackle the growing CBRN threat.227 Moreover, the ongoing coronavirus pandemic, even though it is believed to have occurred naturally, provides a real-life example of the potential for large-scale disruption of certain biological agents228 and how a 'bio-terrorist attack might unfold in the world.'229

2.6.1. Terrorism in Europe

For Europe, the terrorist threat has grown significantly over the past two decades. Groups with an explicitly anti-Western and anti-European ideology, such as al-Qaeda and ISIL/Da'esh, have expanded in size and importance. Nevertheless, the number of deaths from terrorism fell for the second successive year, from over 200 people in 2017 to 62 in 2018. In the EU, deaths from terrorism fell to 13 people in 2018, with all fatalities the result of jihadist attacks. However, it is noticeable that arrests and attacks linked to right-wing terrorism have increased consistently over the same period (see Figure 29).

Virtually all terrorist acts that Europe has witnessed since 2004 have been perpetrated by individuals either directly linked to or inspired by extremist groups with centres outside Europe's borders. The realisation that there is a connection between internal and external security has come to shape EU action. The EU has therefore addressed the terrorist threat both within the EU and beyond its borders.

#### Attacks are likely due to new production, transportation, and dispersion tech.

Ioannis Galatas 20, Editor-in-Chief of C2BRNE Diary, Senior Research Associate at the Center for Security Studies, CBRN consultant for the Emergency Department, Gemelli Policlinico at the Catholic University of Sacred Heart, “Prevention of CBRN Materials and Substances Getting into the Hands of Terrorists,” in “Handbook of Terrorism Prevention and Preparedness,” International Centre for Counter-Terrorism, 2020, https://icct.nl/handbook-of-terrorism-prevention-and-preparedness/

Technical innovations can weaken control over the illicit use of CBRN agents and materials, but at the same time they can also assist in the prevention of CBRN attacks.

Drones

A drone, in technological terms, is an unmanned aircraft. Drones are more formally known as unmanned aerial vehicles (UAVs) or unmanned aircraft systems (UASs). Essentially, a drone is a flying robot that can be remotely controlled or fly autonomously through software-controlled flight plans in their embedded systems, working in conjunction with onboard sensors and GPS. 39 Drone swarms consist of multiple unmanned platforms and/or weapons deployed to accomplish a shared objective, the platforms and/or weapons autonomously altering their behavior based on communication with one another or with a ground pilot approving (for the time being) firing decisions. The interconnectivity of drone swarms enables them to exhibit more complex behaviors than their component drones. There is a significant distinction between drone swarms and drones en masse. 40 Drones en masse are the use of multiple drones without autonomous communication between the drones.

Drone-swarm technology is possible to increase/improve delivery of CR agents. 41 The incident with a drone carrying a vial with a radioactive liquid that landed on the roof of the building where the office of the Japanese Prime Minister is, represents an example of future drones’ possibilities.42 A possible scenario could be based on drones positioned on rooftops programmed to remotely take off at a given time, providing enough time to terrorists to escape the area or the country. In such a scenario the combination of chemical weapons with conventional munitions might trigger panic and chaos since responding to an attack while in personal protective equipment with limited dexterity, vision, and communication is not very effective. In a parallel scenario, a conventional drone attack might mask a simultaneous biological dispersal to a totally unprotected population. It is of note that most cities are not equipped with air defense systems capable to intercept or destroy drones as it was recently witnessed repeatedly times in London’s Gatwick and Heathrow airports.43

It is worth considering that one or more drones can attack the incident command post supervising a chemical or radiological incident site not to mention their ability to interfere in communications by using sophisticated jamming equipment. The “aerial terrorist” of the future might also coordinate a swarm with a variety of specialized drones that will maximize the deadly consequences of the attack.

Hacking

The threat of cyber-attacks targeting chemical or nuclear facilities is a growing possibility.44 Given that chemical plants are now largely controlled by the use of networked computers, it is possible in some countries that cyber-attacks similar to the Stuxnet targeting of Iranian nuclear could cause critical systems failure.45 By hacking into computer networks, an adversary could reprogram an industrial control system so that it commands the equipment to operate at unsafe speeds or opens valves when these should remain closed.46

Critical systems, like those of public utilities, transportation companies, and firms that use hazardous chemicals, need to be made much more secure. One analysis found that only about one-fifth of companies that use computers to control industrial machinery in the US even monitor their equipment to detect potential attacks - and that in 40% of the attacks they did catch, the intruder had been accessing the system for more than a year.47

The Internet

When it comes to terrorism, the internet is considered the proverbial Pandora’s box. Numerous websites, social media pages, and chat rooms in the world wide web and many more in the dark web provide information and detailed instructions, offer manuals and books about practically everything48 – from constructing an IED to how to produce ricin from castor beans at home. 49 Not all sources on the internet are reliable but some can lead amateurs to the construction of a real weapon with the help of ingredients available over-the-counter or from suppliers on the internet. Is it possible to control the internet? Unfortunately, it is too late now in open societies – terrorists know that and we know that. What can be done to minimize the spread of malignant knowledge? Existing technologies make identification of internet interactions a very difficult and sometimes impossible task, given encryption and other hiding techniques.

Prevention

To prevent access to CBRNE weapons, government and corporate and other security actors must focus on a number of areas including theft and smuggling; rogue state trade; trafficking; scientist recruitment; orphan sources; the use of toxic industrial chemicals as weapons; dual biotechnologies; dirty bombs; nuclear trafficking; and the nexus of organized crime and terrorist organizations.

Theft and Smuggling

The Soviet Union’s chemical weapons program was in such disarray in the aftermath of the Cold War that some toxic and radioactive substances got into the hands of criminals or those who tried to sell these to them. While nerve agents degrade over time, if the precursor ingredients for nerve agents were smuggled out in the 1990s and stored under proper conditions and mixed more recently, these agents could still be deadly.

Attacking a nuclear power plant is difficult but not impossible. Terrorists could find a way to sabotage a plant, causing radiation to escape into the environment. In 1992, for example, a hacker named Oleg Savchuk was arrested for trying to sabotage the Ignalina Nuclear Power Plant in Lithuania using a computer virus.50

In August 2019, the Nuclear Threat Initiative (NTI) released an annual Global Incidents and Trafficking Database, 51 produced by the James Martin Center for Nonproliferation Studies (CNS). In 2019 alone, CNS recorded 167 incidents in 23 countries where nuclear and other radioactive materials were found outside of a regulatory control regime (this was an increase from 156 incidents in 2018). Among them: the loss of 1g of weapons-gram plutonium from a university laboratory in the US. Trends remain consistent with the data collected between 2013 and 2017. In 2018, 58 losses were recorded while there were 45 thefts. 64 incidents occurred during transport. 52

Rogue State Trade

According to a 2017 UN report, two North Korean shipments to a Syrian government agency responsible for the country’s chemical weapons program had been intercepted in a six months period. The goods were part of a Korea Mining Development Trading Corporation (KOMID) 53 contract with Syria’s Scientific Studies and Research Centre (SSRC).54

Trafficking

While Slovakia is not a likely target for chemical weapons attacks, the substances needed for such an attack may have been smuggled through the country due to its geographic position and close proximity with areas where trafficking flourish. The Slovak Police Corps along with the Ukrainian police have been cooperating in detecting illegal CBRN materials at the Slovak-Ukrainian border for several years. 55

In 2009, U.S. counterterrorism officials authenticated a video by an al Qaeda recruiter threatening to smuggle a biological weapon into the US via tunnels under the border with Mexico. 56 Smuggling a modern nuclear weapon across a border would be almost as easy as people smuggling and would present no trouble for professional people or drug smugglers. Approximately 350,000 people have been smuggled across the US- Mexico border in a typical recent year. The main issues are portability, which is really about size and weight (similar to that of a man) and weight and the probability of detection. Simulations of detection of mock-up nuclear bombs have been carried out in red teaming exercises. 57 In a widely reported stunt in 2002, ABC News smuggled a mock-up of a nuclear bomb (7 kg of depleted uranium shielded by a steel pipe with a lead lining) in a suitcase by rail from Austria to Turkey crossing several border checkpoints without inspection. 58

In its Dabiq magazine issue No 9 (p.77), 59 one ISIS writer noted:

“Let me throw a hypothetical operation onto the table. The Islamic State has billions of dollars in the bank, as they call on their wilayah in Pakistan to purchase a nuclear device through weapons dealers with links to corrupt officials in the region. The weapon is then transported overland until it makes it to Libya, where the mujahidin move it south to Nigeria. Drug shipments from Columbia bound to Europe pass through West Africa, so moving other types of contraband from East to West is just as possible. The nuke and accompanying mujahidin arrive on the shorelines of South America and are transported through the porous borders of Central America before arriving in Mexico and up to the border with the US. From there it’s just a quick hop through a smuggling tunnel and hey presto, they’re mingling with another 12 million “illegal” aliens in America with a nuclear bomb in the trunk of their car.” 60

Such statements highlight the potential risks in relation to the trafficking of weapons of mass destruction.

Recruitment of Scientists

Recruitments of scientists with a CBRN background can take several forms: it could take place following religious conversion; it could be an act of revenge against a previous employer; or it could be an embittered individual. Furthermore, it could follow after a direct threat against his/her life or against family members or relatives; the result of an impending job loss; the outcome of a business deal, or could also be a case of promising support to a scientist’s ambitions to make a new invention. For example, in 2014 when the Islamic State seized Mosul, geologist Suleiman al-Afiari was recruited and given the task to organize a supply chain for mustard gas, outfitting a small cluster of labs and workshops. He accepted because “I was afraid that I would lose my job. Government jobs are hard to get and it was important to hang on to it.”61

Orphan Sources

‘Orphan sources’ are radioactive sources, which are not under regulatory control, or have never been regulated, or were left without attendance, were lost, placed at an inappropriate location, transferred without proper permission from the government or were stolen.62 An “orphan source” falling into the hands of a regular citizen may lead to lethal consequences for those who touch these or get close to these radioactive objects. An example of such a situation was a radioactive contamination of 249 people with cesium-137 which occurred in 1987 in Brazil, costing the lives of four persons when the Institute of Radiotherapy in the town of Goiania moved to a new location, abandoning old radiation equipment.63

It should be mandatory to ensure that a radioactive source may only be used by individuals or enterprises who have proved to the state that they are capable of ensuring safety and security of the source. Governments should enforce accountancy and monitor and control all radioactive sources. Another preventive method is counteracting the potential threat of IRS (Industrial Radiation Sources) converted into the “orphan” category. The sources that may be abandoned are categorized as vulnerable. 64 Vulnerable sources are those radioactive sources, which are presently under control, but such control is insufficient for ensuring continuous safety and security.

Toxic Industrial Chemicals as Weapons

Toxic industrial chemicals can also be used as weapons. For example, an industrial catastrophe took place in India in 1984 when 3,800 people were killed while more than 11,000 others were injured when methyl isocyanate was released from the Union Carbide India Ltd (UCIL) pesticide plant in Bhopal. 65 While this was an accident, a deliberate attack on a chemical plant by terrorists might have an even larger effect.

The largest concern after the events of 11 September 2001 was for a while that chemical plants might be among the next targets. A terrorist could crash an aircraft or an armed drone against a chemical plant, resulting in the release of chemicals and expose the surrounding area to a plume of toxic gases. A bomb could damage storage tanks or transport vehicles carrying chemicals, releasing deadly toxins. Terrorists could get into an industrial plant and release toxic chemicals from within, or a disgruntled company employee could intentionally release toxic chemicals into the atmosphere. Most chemical plants around the globe are located close to urban areas; therefore, depending on the location, if toxic chemicals were released from one of those plants, as many as one million citizens could be killed, injured, or evacuated (US estimate). Approximately 850,000 U.S. businesses use, produce, or store toxic industrial chemicals (TICs). 66

Military or civilian food or water supplies could also be threatened, directly or indirectly, by a terrorist attack with TICs. Contaminating animal feed is an indirect method of poisoning the food supply, spreading toxins to people who eat contaminated animal products. Depending on the chemical, the residual toxins indigested by animals could be enough to cause mass illness and possibly even death within a meat-eating human population.67

Dual Biotechnologies and Terrorists

Although the potential impact of a biological weapons attack can be significant, the likelihood is currently not believed to be high. Back in 1984, the Rajneeshee cult performed the first biological attack in the recent history of the US by poisoning with Salmonella typhimurium the salad bars of 10 restaurants in an effort to influence local elections in a town in Oregon. 68 In 1993, the Aum Shinrikyo cult was involved in bioterrorism exploitation with Bacillus anthracis to be used against the citizens of Tokyo first with a homemade sprayer from the roof of a cult building located in a residential neighborhood and later from a modified truck.69 Days after the 9/11 massacre in 2001, five US citizens were killed and 17 got sick following exposure to Bacillus anthracis spores send by the regular mail service.70

Genetic engineering, toxicology, molecular biology, and related sciences could contribute to the development of new generations of biological weapons by increasing the virulence and antibiotic resistance of pathogens, enhancing non-transmissible agents for airborne transmission and creating organisms or biological agents capable to attack humans and entire ecosystems.

The Biological and Toxin Weapons Convention (BTWC)71 entails prohibition of the development, production, stockpiling and acquisition of biological and toxin weapons. This convention is also apprehensive regarding the development of dual-use technologies in the areas of genetic engineering, biotechnology, and microbiology, for growth of products and processes that are capable of being used for purposes inconsistent with its objectives and provisions.

Rapid advances in gene editing and so-called “DIY biological laboratories” which could be used by extremists, threaten to derail efforts to prevent biological weapons from being used against civilian targets. 72

One might wonder why one should spend money and scientific expertise to create novel bio-weapons for which currently no defenses are available, when at this moment a dynamite-loaded properly loaded truck (VBIED), with or without chemicals or a radioisotope, could do much harm and produce the effect intended by terrorists at a reasonable cost? One possible answer could be found in the sphere of scientific ambition when a scientist [goes rogue] ~~turns mad~~. 73 A gifted but frustrated scientist could cause havoc and spread a pandemic much more deadly than some of the known biological weapons of the past. A scientifically trained bioterrorist could get hold of the DNA of a virus and program it to disrupt or suppress certain cellular functions in human populations. [They] ~~He or she~~ could also create chemical-resistant insects and then use these against the agricultural production of a country. Therefore, the scientific community, together with governments worldwide should create a framework regarding the extent and the depth of scientific research in critical areas because a rogue scientist might become terrorists too. This has apparently happened in the case of the anthrax attacks of 2001 in the United States. There Bruce E. Ivins, a microbiologist from a national biodefense laboratory, was found to be the chief suspect in the distribution of weapon-grade anthrax spores by mail. This is why better state supervision is mandatory - whether it is inside state, hospital, university or pharmaceutical industry laboratories.

Dirty Bombs and Terrorists

A “dirty bomb” or radiological dispersal device (RDD) is an explosive improvised device that combines conventional explosives, such as dynamite or C4, with radioactive materials. Most RDDs would not release enough radiation to kill more than a few people or cause severe illness. The conventional explosives would kill or injure more people in close proximity to the site of the explosion than the radioactive materials themselves. However, a RDD attack would create fear and panic, contaminate people and property, and require a costly cleanup. For “dispersal” no explosives are needed. It could involve adding radioactive materials to a ventilation system (inhalation threat; expensive cleanup cost), spraying radioactive materials over a populated area with a crop duster or a drone, or contamination of water supplies (although the high dilution is not likely to result in individually significant injuries). In addition, radiological materials can be used in a radiation emitting device (RED, uncovered lead container) hidden in mass gathering places like a subway car or in the outpatient clinics department of a hospital. In addition, placing an IED in an area where radioisotopes are stored (nuclear medicine departments of hospitals) or used (cesium irradiators in hospitals’ blood banks or radiotherapy units) may result in an outcome similar to the one of exposure to a dirty bomb. A capsule of Cobalt 60 ( 60Co) used for cancer treatment typically contains about 7.4⋅1013 Bq (2000 curie), which corresponds to a mass of about 1.8 grams.74 The same applies for sabotage of spent fuel transport cask and the corresponding release of radioactive aerosol.75

Until now no dirty bombs have successfully been detonated. However, the threat is not imaginary. A vivid example is the 2008 case of the millionaire James Cummings. In his home in in Belfast, Maine, USA, police found both radiological materials and technical literature on how to construct a dirty bomb.76 Such a case indicates that the threat is real. Another example of potentially planned use was the discovery of explosives together with a radiological source (cesium-137) buried, by Chechen rebels, in the Izmailovsky Park in Moscow in 1995. 77 For a terrorist organization with even rudimentary IED capabilities, the design and building of the explosive elements of a dirty bomb would be relatively easy. Obtaining radioactive material in sufficient quantities to create a major radiological dispersal is, however, a much harder challenge and one which can be countered by appropriate monitoring of radioactive sources, their regulation and effective law-enforcement.

Improvised Nuclear Devices

An Improvised Nuclear Device (IND) is a primitive type of nuclear weapon. When an IND explodes, it gives off four types of energy: a blast wave, intense light, heat, and radiation. The idea of terrorists accomplishing such a big bang is, unfortunately, not out of the question; it is far easier to make a crude, unsafe, unreliable nuclear explosive that might fit in the back of a truck than it is to make a safe, reliable weapon of known yield that can be delivered by missile or combat aircraft.78

Could resourceful terrorists design and build a crude nuclear bomb if they had the needed nuclear material? Unfortunately, repeated examinations of this question by nuclear weapons experts in the US and elsewhere have concluded that the answer is yes – for either uranium or plutonium nuclear bomb, provided they can get hold of the required radioactive materials through theft or from trafficking. 79

Nuclear Trafficking

The Black Sea region is a vital strategic crossroads between Europe, Asia, Transcaucasia, Russia, and the Middle East, and has long been used for smuggling of licit and illicit goods, including nuclear materials since the end of the Cold War. Over 630 nuclear trafficking incidents were recorded in Black Sea states between 1991 and 2012, almost half of them in or from Russia. Five of the recorded incidents involved highly enriched uranium (HEU), raising concerns about the region’s use as a transit route for nuclear material smuggled from the former Soviet Union to the Middle East. 80

The seizures of HEU samples in Georgia in 2010, 81 and Moldova in 2011, 82 suggest that some quantities of previously stolen weapon-grade nuclear materials may still be available for illegal transfer and sale to state and non-state actors. Therefore, it is important that efforts to counter nuclear trafficking in the Black Sea region are continued and enhanced.

The terrorism-organized crime nexus could provide not only the basic nuclear material required for a radiological dispersal device or an improvised nuclear bomb but even an actual nuclear warhead to be delivered to the targeting site in the back of a truck or as payload of a drone.

IED – WMD Networks

Nexus Convergence between IED facilitation and WMD proliferation networks could also potentially lower existing thresholds, making the proliferation of WMD not only easier but more widespread. Networks are composed of people, material, infrastructure, money/finance, information, and lines of communications, which can be both physical and virtual. Perhaps the most notable WMD proliferation network was Abdul Qadeer Khan’s nuclear technology network which stood at the basis of Pakistan becoming a nuclear power currently possessing more than 100 atomic bombs. While A.Q. Khan’s network sold critical technology he stole from his time with URENCO in the Netherlands to state actors (e.g., Libya, North Korea) from his base in Pakistan, the father of Pakistan’s atomic bomb could have sold know-how and nuclear materials to non-state actors as well. 83 This does not imply that a terrorist could easily develop and employ a nuclear weapon, but rather that there are profit-minded suppliers willing to sell crucial components to them.

#### Nuclear terror causes catalytic escalation---extinction.

Dr. James Johnson 21, Assistant Professor in the School of Law and Government at Dublin City University and a Non-Resident Fellow with the Modern War Institute at West Point. He was previously a Postdoctoral Research Fellow at the James Martin Center for Nonproliferation Studies, "‘Catalytic Nuclear War’ in the Age of Artificial Intelligence & Autonomy: Emerging Military Technology and Escalation Risk between Nuclear-armed States," Journal of Strategic Studies, 01/13/2021, T&F. language edited.

The main concern about ‘catalytic nuclear war’ – and ‘Nth country problem’ more broadly – in the late 1950s and early-1960s centered on the fear that a small or new nuclear power would deliberately set a major exchange in motion between the United States and the Soviet Union. 1 As its name suggests, the concept was inspired by chemical reactions where the catalyzing agent (a third-party actor) would remain unscathed by its initiated process. 2 In his seminal work on ‘catalytic nuclear war’ in 1962, Donald Kobe defines the notion of ‘catalytic war’ as the possibility that a third party’s actions induce a nuclear war between the two nuclear-armed opponents. A third-party attack on nuclear-power would be misattributed to another state, thus sparking a catalytic ‘chain reaction of retaliation and counter-retaliation.’ 3 A broader definition of ‘catalytic nuclear war’ encompasses situations in which the catalyzing actor (non-state or another third party) initiates a simulated attack (e.g., a false alert) that produces the effect of an imminent attack on one or both of the nuclear-armed adversaries, for which pre-emption is considered the most expedient (or only) strategic recourse. 4 This broadened definition, and used in this article, includes any process by which a third-party actor uses its capabilities to involve nuclear-armed strategic rivals in a war intentionally or to increase the scope or intensity of a situation. 5 The paper’s originality lies in revisiting the ‘catalytic nuclear war’ concept, considered by many as unworkable, and reconceptualizing it in light of technological change, as well as improved understanding of human psychology and other factors.

Because nuclear powers must have some policy of retaliation (i.e., massive, proportional, finite, or random) in order to act as a deterrent, this chain reaction may, under certain circumstances, become a self-fulfilling prophecy. For instance, the common fear of pre-emption caused by one or both states is vulnerable to a first strike, or if a state’s command, control, and communication structures are compromised following an attack. 6 This situation would be compounded by the presence of higher numbers of nuclear-armed states – or nuclear multipolarity – with varied, and possibly conflicting, retaliation and deterrence postures. 7 Moreover, miscalculation, misperception, or an irrational act, would also increase the risk of catalytic war.8 \*\*\*FOOTNOTE BEGINS\*\*\* Therefore, a catalytic war would still be possible if a third-party instigator believed that the potential benefits from the war outweighed the risk of receiving a retaliatory attack. Ibid., p.128.\*\*\*FOOTNOTE ENDS\*\*\* At the root of these conditions is human psychology, which strains the credibility of arguments that human-rationality, perceptions, and nuanced signaling ensure that deterrence will prevail.

Classical nuclear deterrence policies, premised on the assured threat of a retaliatory second strike (or mutually assured destruction (MAD)), are a fundamentally psychological-political-technical phenomenon that has worked to reduce the chances of deliberate use of nuclear weapons. 9 This article argues that increasingly sophisticated, interdependent, and vulnerable nuclear command, control, and communications (NC3) systems – the bedrock of the mutual deterrence regime between nuclear-armed states – increases the risks associated with unintentional catalytic nuclear war. 10 The article is not a treatise on the motives or goals of non-state motives for committing such acts, but rather the evolving means at the disposal of actors to actualize their malevolent goals – or ‘apocalyptic world views’ – in the digital age. 11 There is a rich body of literature on the intersection of emerging technology and the nuclear enterprise – and the potential for warfare more broadly defined. 12 However, there is a relative paucity of research on how existing concepts of escalation, nuclear terrorism, and classical deterrence theories might apply (or be tested) in the digital age, which are increasingly defined by developments in artificial intelligence (AI) and autonomy perfect information and rational decision-making cannot be assumed. 13 Are existing theories of military escalation still applicable in the era of AI and autonomy?14 \*\*\*FOOTNOTE BEGINS\*\*\* ‘Artificial Intelligence’ (AI) refers to a machineability to perform tasks that generally require human-level intelligence. For example, recognizing patterns, learning from experience, making predictions, or taking action – whether digitally or as smart, behind autonomous physical systems. Today’s AI systems use ‘narrow’ AI – or task-specific intelligence. For more on definitions of AI, see Nils J. Nilsson, The Quest for Artificial Intelligence: A History of Ideas and Achievements (Cambridge: Cambridge University Press, 2010). ‘Autonomy’ is the ability of a system to respond to uncertain situations by independently composing and selecting among different courses of action to accomplish goals based on knowledge and a contextual understanding of the world, itself, and the situation. Autonomy is categorized by degrees of unsupervised behavior (i.e., degrees of autonomy) that range from fully manual to fully autonomous. United States Air Force, ‘Artificial Intelligence Annex to DoD AI Strategy’, Tech. Rep., United States Air Force (2019); and Andrew P. Williams and Paul D. Scharre eds., Autonomous Systems – Issues for Defence Policy Makers (NATO Allied Command Transformation, Norfolk, VA, 2015).\*\*\*FOOTNOTE ENDS\*\*\*

The remainder of the article proceeds as follows. First, it contextualizes the concept of ‘catalytic nuclear war’ with emerging security technologies, particularly AI. The article uses this analytical framework to examine how and under what circumstances the nefarious (mis)use of these technologies by non-state actors (i.e., terrorists, criminals, and state-proxy actors) might create or exacerbate escalation pathways leads to an accidental nuclear confrontation between nuclear-armed powers. Next, in the articles’ empirical core, it considers four aggravating features in the interaction of emerging technology with nuclear weapons and the pathways to nuclear escalation examined in the article – information complexity and asymmetry; greater automation of NC3; disinformation, misinformation, and information manipulation; and nuclear multipolarity.15 \*\*\*FOOTNOTE BEGINS\*\*\* The concept of ‘emerging technologies’ is a loose and ill-defined one that is often used interchangeably when discussing the impact of technologies such as cyberspace, social media, autonomous weapons, quantum computing, rail guns, directed energy weapons, 3D printing, and AI. Emerging technologies can mean different things to different people and are analytically very distinct. For example, cyber capabilities can enable offensive capabilities to penetrate and compromise an adversary’s systems, while social media can permit attackers to influence perceptions, create false memes, or otherwise disrupt or upend prevailing norms. AI can amplify and enhance the potency and efficacy of these effects. This distinction also implies that there will be variation among third party non-state actors in their relative capabilities to achieve their malevolent objectives in the context of nuclear weapons, which the article will highlight.\*\*\*FOOTNOTE ENDS\*\*\* This article posits that AI-enhanced capabilities will likely amplify these underlying conditions (or second-order effects), thus increasing the risk of sparking unintentional escalation between strategic nuclear-armed powers – especially in crisis and conflict conditions. The next section uses four fictional scenarios – cyber false flag operation, cyber-attack on nuclear early-warning systems, drone swarming targeting ISR systems, and deepfake disinformation – to demonstrate how AI-enhanced capabilities in the hands of non-state actors might accidentally or inadvertently drag a competitive nuclear dyad into conflict. The final section considers possible ways of reducing catalytic escalation risk caused by non-state actors, particularly how militaries can maintain effective command and control of their nuclear forces in a rapidly evolving and complex conflict environment.

Catalytic nuclear war in the digital age: Evolving nuclear strategies of non-state actors

During the later 1950s and early 1960s, the notion of a ‘catalytic nuclear war’ centered on the possibility that a minor nuclear power would deliberately trigger a full-scale nuclear exchange between the United States and the Soviet Union. In a seminal article on the topic, Donald Kobe argued that the notion of ‘catalytic war’ was inspired by chemical reactions whereby the catalyzing agent remains unchanged by the process it has triggered. 16 Several scholars also raised the specter that a minor nuclear power might be tempted to catalyze a devastating exchange that would inflict maximum damage on the superpowers but leave it relatively unscathed and thus dictate conflict termination outcome. 17

Some scholars have questioned the plausibility of this hypothesis. Even in the unlikely event that a minor power successfully concealed its role in sparking a global war, the prospect of its plot being discovered would almost guarantee decapitation, making any potential gains outweighed by the overwhelming risks thus, illusionary. 18 In the event, improvements to nuclear early-warning systems and communication channels – and broader tactic cooperation – between the United States and the Soviets did much to reduce the (albeit remote) possibility of a minor power creating the conditions inadvertently dragged the superpowers into nuclear war. 19 What if the risk and rationality considerations mattered less to non-state actors (especially terrorists) in possession of a nuclear weapon to incite chaos and other disruptive means to fulfill its apocalyptic ends? 20

The nuclear terrorism threat discourse began in the mid-1970s. The terrorist attacks on the United States in 2001, coupled with the 2003 exposure of a secret network (led by Abdul Qadeer Khan) supplying Libya, North Korea, and Iran with the know-how for manufacturing critical nuclear equipment, which increased the sense of urgency. In particular, concerning non-state actors (especially those motivated by extreme political or religious goals), global nuclear security regimes and approaches.21 \*\*\*FOOTNOTE BEGINS\*\*\* For example, evidence revealed that Al-Qaida actively sought nuclear weapons and expressed a clear desire to use them. Rolf Mowatt-Larssen, ‘Al Qaeda’s pursuit of weapons of mass destruction: the authoritative timeline’, Foreign Policy, 25 January 2010.\*\*\*FOOTNOTE ENDS\*\*\* Experts consider the probability of the successful theft of nuclear grade materials (i.e., highly enriched uranium or plutonium) and detonation of atomic weapons or manufacturing an improvised device (or a ‘dirty bomb’) by non-state actors as extremely low; but it cannot be entirely discounted. 22 To be sure, experts have continued to warn about the opacity of materials safety and security in smaller nuclear-armed states such as Iran, Israel, Pakistan, and most notably, North Korea. 23

If a non-state group realized that the possession of nuclear weapons could trigger a total catalytic war between two or more major nuclear-armed states, what possible situations might set these dynamics in motion? The potential success of a catalytic nuclear detonation by a terrorist group during a crisis between two nuclear-armed states (i.e., the original target of the nefarious attack and the victim of a subsequent inadvertent retaliatory strike), when tensions are running high, and a heightened state of alert is in place – at a nuclear or sub-nuclear level – would likely be amplified. That is, a broader nuclear exchange would likely occur. Moreover, a non-state actor might exploit a tense situation by making provocative false claims that its attack had been sanctioned by the state with which the victim of the attack was already in a crisis, or worse still, nuclear brinkmanship. Against the backdrop of fear, acrimony, and paranoia – when decision-makers are more susceptible to misperception and misunderstanding – any denials or assurances would [fail] ~~fall on deaf ears~~. 24 If a repeat of the 1999 Kargil crisis or the more recent Indian-Pakistani stand-off in 2019, a non-state nuclear detonation (or the credible threat of one) could spark an accidental or inadvertent nuclear exchange. 25 Thus, any confidence Indian or Pakistani has in their ability to manage a conflict below the nuclear-level would likely be unreliable in the event of a non-state nuclear attack. Absent unambiguous and incontrovertible evidence to the contrary, an unprovoked non-state attack may compound mutual suspicions about the other side’s intentions and behavior, and in turn, confirm worst-case scenario assessments.26 \*\*\*FOOTNOTE BEGINS\*\*\* The broader notion that escalation can occur inadvertently (or unintentionally) is attributed to a failure to appreciate the pressures that one’s actions put on an adversary. These pressures generate perceived first-mover advantages and associated with the ‘security dilemma’ concept – when defensively motivated actions can appear and be perceived as offensive. See, Robert Jervis, ‘Cooperation under the Security Dilemma’, World Politics 30:2 (1978), pp.167–214.\*\*\*FOOTNOTE ENDS\*\*\*

In the contemporary digitized landscape, the theft of nuclear grade materials, the detonation of atomic weapons, and ‘dirty bombs’ by non-state actors are not the only threats that states must worry about. Emerging technologies – most notably cyber, AI technology, and drones – are rapidly creating new (and exacerbating old) low-cost and relatively easy means for non-state actors to fulfill their nefarious goals; without the need for actual physical contact with or manufacture of nuclear weapons to have the ‘power to hurt’ – or the power to get others to hurt each other. 27 One of the critical potential ‘threat vectors’ (i.e., a mechanism or means by which an actor can gain access to a network in order to deliver a malicious payload) is the severe consequences that would result from a non-state actors’ deliberate actions to penetrate or manipulate nuclear command, control, and communication (NC3) systems with AI-enhanced conventional capabilities. Above all, cyber operations targeting early-warning satellites and radars are central to this article’s central focus. 28

The presumption of immunity or overconfidence in the robustness of NC3 networks to external (or insider) threats may increase the chances that states underestimate nuclear weapon systems’ vulnerabilities to a multitude of possible attack mechanisms, inter alia, data manipulation, malware cyber-attacks, ‘false-flag cyber operations,’ 29 social media flooding, or spoofing decision-makers with disinformation and misinformation. Minuteman missile silos are, for example, considered to be particularly vulnerable to cyberattacks. 30 Nuclear-powered ballistic missile submarines (SSBNs) once believed to be air-gapped – not connected to the internet and considered ‘hack-proof’ – are, however, connected via various electromagnetic signals that create potential vulnerabilities to cyber-attacks. A committed non-state or third-party actor may, for example, disrupt (digital jamming), deny (denial of service attacks), and distort or destroy information (spoofing or malware attacks) used by SSBN’s command and control networks to sow miscalculation and misperceptions, fan the waves of a crisis, or trigger an accidental nuclear launch.31 \*\*\*FOOTNOTE BEGINS\*\*\* While SSBN’s are not connected to the internet in any meaningful sense, the submarine’s missiles, warheads (i.e., launch controls and targeting systems), and the various support systems rely on networked computers and software. Submarines are particularly vulnerable to malware introduced to the network during the procurement phase while the submarine and its missiles and warheads are being built, or when the submarine is in port for maintenance, refurbishment and software updates. Andrew Futter, ‘Is Trident safe from cyber-attack?’ European Leadership Network, February 5 2016, <https://www.europeanleadershipnetwork.org/report/is-trident-safe-from-cyber-attack/> \*\*\*FOOTNOTE ENDS\*\*\* In extremis, third-party hackers (or ‘cyber terrorists’) during a crisis might use AI-augmented false flag cyber operation to mislead submarine commanders (or political decision-makers) that an SSBN was – or expected to be in the case of a ‘launch on warning’ policy – under-attack. 32 Echoing these concerns, a 2009 study commissioned by the International Commission on Nuclear Non-proliferation and Disarmament (ICNND) warned that non-state actors might penetrate command and control (C2) systems – and even launch an unauthorized nuclear attack – an easier and more plausible ‘alternative for terrorist groups than building or acquiring a nuclear weapon or dirty bomb themselves.’ 33

Recent developments in AI-enabling technology have exacerbated these vulnerabilities and introduced additional threat vectors non-state actors might leverage, which may precipitate a catalytic nuclear war that manipulates the information landscape in which decisions about atomic weapons occur. In particular, social media manipulation and the spreading of misinformation, false memes, and fake news. For example, in 2016, a false news story appeared on the AWD News site that claimed that Israel had threatened to attack Pakistan with nuclear weapons if Islamabad interfered in Syria. The report consequently caused a tit-for-tat incendiary rhetorical exchange on Twitter – the Pakistani defense minister Khawaja Muhammad Asif warned that Israel should remember that Pakistan is also a nuclear-armed state debunked as fictitious by the Israeli Defense Ministry. 34 This incident puts a modern spin on the Cold War concept of catalytic nuclear war – in which third party actions provoke a nuclear war between the two nuclear-armed powers – and demonstrates the potentially severe damage caused by the misinformation and manipulation of information by non-state actors.

During a crisis involving a competitive strategic dyad – such as the conflict-prone South Asia or Northeast Asia – when communication is compromised, nuclear arsenals are on high-alert, decision-making timeframes are compressed, or launch authority is pre-delegated (e.g., to nuclear-armed submarine commanders), the consequences could be catastrophic. 35 Moreover, in a high pressured crisis environment with confusion and paranoia running high the risk of misperceptions of an adversary’s intentions and behavior (e.g., putting nuclear arsenals on high-alert status) non-routine troop movement), the temptations for pre-emptive action increases. 36 That is, the catalyzing non-state actor produces the effect of an imminent attack on one or both of two nuclear-armed states, for which pre-emption is considered the most advantageous strategy. 37 What factors might aggravate these escalation pathways during a crisis?

Pathways to catalytic nuclear war and catalyzing aggravators

This section examines four aggravating variables – information complexity, greater automation of NC3, disinformation, and nuclear multipolarity – that coalesce in the synthesis between emerging technology and the nuclear weapon systems. In particular, how and why AI and autonomy might compound these dynamics and cause unintentional escalation between nuclear-armed powers are more likely to occur. Early warning systems are the main focus of this study because ‘missiles cannot be recalled; submarine commanders may be out of touch but able to act on their own; missiles may go off accidentally.’ 38 These variables do not, however, constitute mutually exclusive risk scenarios. Instead, the interplay between these conditions might allow them to feed into one another with uncertain and potentially self-reinforcing effects – or a function of the confusion and uncertainty created by the sociotechnical complexity generated in the digital age.

Cognitive psychology is relevant to all four aggravating factors described below. Humans exhibit a range of biases that can influence how they observe, collect, and process information, making them less aware of the reality of a particular situation and thus more inclined to interpret events through the lens of existing desires, preferences, and beliefs. 39 Psychological research has shown that people tend to interpret ambiguous information as consistent with their pre-existing beliefs and values – dismissing information that contradicts these views – and accept information that allows them to avoid unpleasant choices. 40 Human psychology studies also tell us that people are predisposed to making fast, intuitive, reflexive, and heuristic judgments – known by cognitive psychologists as ‘System I’ thinking – rather than slower, more deliberative, conceptual, and analytical – known as ‘System II’ thinking. 41 Fast and reflexive (‘System I’) thinking during a nuclear crisis would be inherently problematic if, for example, the potentially catastrophic risks and second-order effects of nuclear war (i.e., loss of human life and environmental destruction) are actively or unconsciously deprioritized in discussions dominated by national defense heuristic imperatives. 42

Cognitive biases can also be exacerbated when information overload and unfamiliar technologies are a more prominent feature of decision-making. The exponential rise and speed data emerge from today’s information ecosystem will create novel attack vectors to manipulate and propagate misinformation and disinformation during crisis times. While human cognitive biases can be intensified by information complexity in crisis decision-making, over- confirmation bias, anchoring, heuristic thinking, and confidence bias are particularly pertinent in this context.43 \*\*\*FOOTNOTE BEGINS\*\*\* Psychologists have demonstrated that in the case of ‘anchoring, ‘people tend to rely too much on the initial piece of information they receive or learn from while discounting later information. See Daniel Kahneman, Thinking, Fast and Slow\*\*\*FOOTNOTE ENDS\*\*\* In the case of ‘anchoring,’ perceptions of historical lessons from past conflict and crises with minimal relevance may have an outsized influence on decision-makers who seek to ground decisions in precedent and lessons from experience. 44 Humans are also considered poorly equipped to intuitively understand probability – which is essential for ranking preferences rationally for crisis decision-making. 45 People tend to misinterpret (or not recognize) randomness and non-linearity and consider the occurrence of unlikely events as virtually impossible. 46

Three distinct – but not always separate – mechanisms can lead to nuclear escalation, namely, deliberate (or intentional), inadvertent, and accidental escalation (encompassing mistaken or unauthorized usage). 47 These distinctions are not, however, binary or mutually exclusive. An escalation mechanism that leads from a crisis or conflict to its outcome can involve one or more of these categories. For example, if an accidental or inadvertent escalation signal or event is triggered by a non-state actor’s nefarious actions – such as a false flag cyber operation against a state’s NC3 systems – which in turn leads to a deliberate escalatory response. 48 Moreover, the deliberate use of nuclear weapons that originates from a false, manipulated, or distorted assessment of a situation, or in response to an early-warning system false alarm, can quickly muddy the lines of intentionality. 49

Accidental nuclear war – a nuclear confrontation without a deliberate and properly informed decision to use nuclear weapons on the part of the nuclear-armed state(s) involved – could be caused by a variety of accidents, most often encompassing a combination of human – and human-machine interaction failure – system errors, and procedural or organizational factors. 50 This definition of accidental escalation will be used in this article to conceptualize ‘catalytic nuclear war’ – triggered by the deliberate actions of a non-state or third-party actor that is not part of the adversarial nuclear dyad – with developments in AI and autonomy. Therefore, a crucial distinction is between the risk of unintentional (i.e., accidental or inadvertent) escalation and intentional escalation; the fear of deliberate escalation is generally more destabilizing. 51 Despite paying lip-service to Machiavelli’s Fortuna – the role of uncertainty in international affairs – decision-makers often underestimate the importance and frequency of accidents and randomness in these interactions. 52 Ultimately, whether the impact of unintended escalation risk is stabilizing or destabilizing depends on the destabilizing force’s relative strengths and the fear it instills. 53 Similar to historical cases human-machine interactions caused (or compounded) accidents with complex autonomous weapon systems, AI-enhanced systems operating at higher speeds, sophistication, and compressed decision-making timeframes will likely reduce the scope for de-escalating and contribute to future accidents. 54

Information complexity

In contrast to previous eras of military revolution – when technologies diffused and improved specific capabilities and domains of military power – the coalescence of emerging technologies today (especially AI machine-learning) can enhance and enable a diverse range of capabilities and missions. 55 The complex interactions within the tightly enmeshed (or dual-use) and co-mingled systems that control or inform nuclear weapons systems (e.g., early-warning satellites, ISR, electronic data networks, and missile defenses), has become a critical risk vector in the digital age. Thus, making accidents, short of a nuclear detonation, almost par for the course. 56 Further, the risks of technical and human errors that arise from this complexity and interdependency in modern nuclear systems are compounded by the prospect of cyber-attacks against early warning and C2 systems – discussed below.57 \*\*\*FOOTNOTE BEGINS\*\*\* Because of the interdependencies between the various components that comprise NC3 systems, it is impossible to calculate the probability of an accidental nuclear confrontation from the risk of the failure of a particular component or system; in isolation from the system and network as a whole. Intriligator and Brito, ‘Minimizing the Risks of Accidental Nuclear War: An Agenda for Action’, p.230.\*\*\*FOOTNOTE ENDS\*\*\*

A key characteristic of operating NC3 systems infused with advanced technology – AI machine-learning, big data analytics, and cyber – is the vast quantities of data and information collected to inform decision-making. 58 While AI-machine learning data-mining augmented cyber-surveillance – together with AI-enabled pattern recognition technology – could significantly enhance states’ ISR capabilities, the introduction of multiple data streams with varying levels of confidence could overwhelm the ability of decision-makers to determine the credibility of data, especially if the provenance and validity of the information cannot be easily verified.59 \*\*\*FOOTNOTE BEGINS\*\*\* Robotics miniaturization (e.g., CubeSats and swarmed unmanned vehicles) and improvements in networking are enabling the wide deployment of formerly limited capabilities, such as aerial full-motion video, and the harvesting of open-sources (e.g., crowdsourcing, commercial satellite imagery, and geographic information systems (GIS) data), all of which adds to the information burden in the decision-making process. Shane P. Hamilton and Michael P. Kreuzer, ‘The Big Data Imperative: Air Force Intelligence for the Information Age’, Air and Space Power Journal 32, no. 1 (Spring 2018).\*\*\*FOOTNOTE ENDS\*\*\* The U.S. Air Force, for example, has characterized this phenomenon as four ‘V’s’ – higher volume (collection of magnitudes more data points), velocity (the volume of data is acquired at rapid speed), variety (numerous formats of information from diverse sources), and veracity (the volume, velocity, and variety of data includes a substantial amount of noise and redundant data). 60 Similarly, the U.S. Navy has reported being overwhelmed by the floods of data generated from its existing information-gathering systems. 61

The quantity and quality of information generated by the advanced technology that supports NC3 systems can increase escalation risks, inter alia, in three ways. First, human decision-makers’ dependence on the information produced by complex and enmeshed NC3 systems can exacerbate the degradation of the quality and reliably of decision-making if these systems are compromised, especially cyber-attacks. The literature on the risks of a breakdown in NC3 systems and the limitations of human cognitive processing capacity – particularly situations that combine information overload, confusion, and compressed decision-making timeframes – focuses on the accidental escalation risks associated with the organizational reliability of complex information architectures 62 \*\*\*FOOTNOTE BEGINS\*\*\* Recent studies have identified a range of cognitive and psychological effects whereby subjects tend to discard complex or conflicting information, settle for suboptimal conclusions to save time, and experience high-stress levels and other adverse psychological effects. David Bawden and Lyn Robinson, ‘The Dark Side of Information: Overload, Anxiety and Other Paradoxes and Pathologies’, Journal of Information Science 35, no. 2 (April 2009), pp.180–91.\*\*\*FOOTNOTE ENDS\*\*\* general agreement exists that these risks cannot be eliminated. 63

Second, while information dominance does not ensure stability; juxtaposed, information inadequacy (or ‘information asymmetry’) can prompt decision-makers during a crisis to eschew traditional caution and the acute fear of escalation for pre-emption; thereby, increasing inadvertent escalation risks. 64 For instance, the information asymmetries by clandestine cyber operations against NC3 systems can narrow or close the crisis bargaining window, producing a trade-off between possessing counterforce capabilities to blunt an adversary’s nuclear deterrent and increasing the risks of provoking nuclear warfare in the first place. In short, any new capability that increases (or is perceived to do so) information asymmetry about the balance of power and resolve can sow the seed of bargaining and deterrence failure, and ultimately war. 65 Misperception of another’s capabilities, intentions, and assumptions about what information an adversary possesses (or lacks), and in turn, how it perceives a situation, is an established cause of deterrence failure in international relations. 66

The Cold War experience demonstrated that the fear that an action or signal misinterpreted by an adversary, in the context of uncertainty and incomplete information associated with modern warfare might spark nuclear pre-emption, is a useful point of departure to consider the potential effects of AI and autonomy. 67 Moreover, the increasing use and development of advanced weapon technology such as hypersonic glide vehicles, dual-use (nuclear and conventional) missile delivery systems, anti-satellite weapons, and dual-use NC3 systems that blur the distinction between nuclear and conventional (and sub-conventional) warfare can heighten strategic ambiguity during crises. Thereby creating first-mover advantage incentives, leading states to overestimate an adversary’s capabilities and strike preemptively. 68 In sum, the likelihood of escalatory crises originating in cyberspace will continue to rise because of the inherent speed, scope, and opacity surrounding cyber capabilities, coupled with the existential fear of escalatory conflict in cyberspace, the positive feedback loops associated with states’ accumulation of offensive cyber capabilities, and the insensitivity of others’ perceptions and intentions. 69

A cyber-attack – dependent on deception, speed, and covertness – that undermines effective information and communication flow can, therefore, increase the rational incentives for escalation. 70 Besides, irregular or opaque communication flow between adversaries may also increase the risk of misperception and miscalculation and assume the worst of others’ intentions. 71 Paradoxically, therefore, new technologies designed to enhance information (e.g., modern NC3 systems supported by 5G networks, AI machine learning, cyber, big-data analytics, and quantum computing) can also erode reliable information flow and communication, which is critical for effective deterrence. 72 Greater volumes of information emerging from the global information ecosystem, rather than reducing the likelihood of misperceptions arising between adversaries, offer motivated third-party actors unprecedented – low-cost, scalable, and fast – opportunities to manipulate decision-makers perceptions and shape public opinion about others’ intentions, capabilities, and the consequences of responding to an attack that originated in the cyber domain – but might rapidly and inadvertently escalate.

Third, advanced technologies have the potential to qualitatively improve the ‘always-never’ criteria that NC3 systems must meet (i.e., complex failure modes, greater redundancies, and a larger attack surface) 73 the complexity and uncertainties introduced by sophisticated NC3 mechanisms – especially early-warning satellites and radars – can also cause errors, unexpected interactions, and unintended consequences, eroding deterrence and creating rational (or sub-rational) incentives) to escalate a situation.74 \*\*\*FOOTNOTE BEGINS\*\*\* The historical record has shown that most international relations situations involve some sort of ‘sub-rational’ thinking or error, which includes misperception, confusion, and ‘bounded rationality.’ These scenarios also incorporate a degree of deviation from the logic of rational utility maximization. See, James M. Goldgeier and Philip E. Tetlock, ‘Psychology and International Relations Theory’, Annual Review of Political Science 4, no. 1 (2001), pp.67–92; and Janice Gross Stein, ‘The Micro-Foundations of International Relations Theory: Psychology and Behavioral Economics’, International Organization 71, no. S1 (April 2017), pp.249–63.\*\*\*FOOTNOTE ENDS\*\*\* The notion that sophisticated technologies, designed to improve safety, ultimately become a source of accidents and errors is a documented phenomenon. 75 This trade-off is a product of the organizational and strategic-cultural variables in the human decision-making process, creating pressures to escalate a situation, rather than viewing technology as an independent variable per se. 76 The assumption of rationality in a nuclear-armed adversary, or that the adversary has more information than might be the case (or ‘asymmetric information’), inter alia, may stem from misperceptions about the nature of an opponent’s technological capabilities, the nature of a crisis, or an opponent’s intentions. As a result, these factors could exacerbate escalation pressures on states with less robust NC3 systems and safeguards or view its survival at stake – North Korea, Pakistan, or India. Q Furthermore, the normal (or peacetime) perception of events can shift during crises or geopolitical tension, when decision-makers are more prone to harbor worst-case scenario expectations and see things they expect or want to see – known as ‘cognitive consistency.’ 77 This logic – the way people interpret situations under pressure due to anxiety – can also become a self-reinforcing process that directly impacts the number of false alarms that occur in early warning systems. In particular, the probability of Type II errors – or ‘false negatives.’78 \*\*\*FOOTNOTE BEGINS\*\*\* For example, during the 1956 Suez Crisis, misinterpretations and the tendency to view unrelated and even unconfirmed events as part of a pattern of an adversary’s behavior may have compounded the anxiety and high level of tension contributed to the misinterpretation of detection data from early warnings systems, and in turn, created a crisis with a momentum of its own. Paul Bracken, The Command and Control of Nuclear Forces (New Haven: Yale University Press, 1983).\*\*\*FOOTNOTE ENDS\*\*\* Moreover, as the volume of information received by NC3 systems increases during a period of tension, so do the chances of perceiving a pattern of adversarial behavior where under typical situations, no pattern would be detected.

Technological-deterministic schools of thought that conceptualize technology as the sole driver of strategic stability and the conduct of warfare, therefore, oversimplifies this complicated human endeavor – which can mean that rational decisions entail worse consequences than less rational alternatives. For example, if a new state-of-the-art NC3 capability such as AI provides a first-mover advantage (or perception of one) for one or both sides striking preemptively during a crisis, or irreparable damage is suffered by one side from a first strike, the risks of inadvertent nuclear war increases. 79 Besides, problems have often arisen because states tended to place ‘new weapons in old bottles.’ That is, regardless of how sophisticated or capable a system appears to be, these technologies will invariably be assimilated into military organizations with entrenched norms, cultures, and institutional patterns.80 A complete understanding of the relationship between advanced technology and strategic stability requires a deeper understanding of human tendencies, not merely technical capabilities per se.

Greater automation of NC3 systems

Increasing automation levels in modern NC3 systems – particularly those augmented and supported by AI technology – together with false warnings and other forms of nefarious interference in cyberspace, will likely increase the risk of accidental nuclear war.81 Legacy vulnerabilities in C2 systems to computer malfunctions, human error (both Type I and Type II). 82 Furthermore, especially human-machine interfaces will be compounded as AI is infused into the NC3 ecosystem. 83 Moreover, a declared or de facto launch-on-warning posture held by either side during a crisis involving a Type II error (or ‘false positive’) caused by a false signal increases the accidental escalation risks a result of ‘use-them-or-lose-them’ pressures. Thus, it degrades nuclear forces’ usability or reduces the damage limitation window to attack enemy nuclear forces if needed. 84 This skewed assessment in the context of nuclear weapons ready to launch nuclear weapons at a moment’s notice could precipitate worst-case scenario thinking and trigger inadvertent escalation. 85

The historical record demonstrates the vulnerabilities of NC3 systems to frequent false alarms, accidents, ‘close calls,’ and other risks associated with increasingly complex, porous, and interconnected systems, which despite their alleged ‘closed’ nature, may offer non-state actors multiple pathways to cause harm. 86 Because of the inherent problems attribution in cyberspace, a non-state actor might plausibly make both states the target of its attack, convincing each side that the other party is responsible – or a ‘double-sided catalytic attack.’ 87 This problem-set is compounded by the shortened response timeframes available to decision-makers, particularly where a ‘launch on warning’ posture is present.

According to open sources, operators at the North American Aerospace Defense Command (NORAD) have less than three minutes to assess and confirm initial indications from early-warning systems of an incoming attack and decide whether or not to authorize a nuclear response. 88 This compressed decision-making timeframe – for data-collection, assessment, and decision-making – could put political leaders under intense pressure to decide to escalate during a crisis, with incomplete (and possibly false) information of a situation. In the context of advanced technologies, response systems like NORAD raise particular concerns; missiles cannot be recalled, submarines on deterrence patrols may be out of touch for extended times with a high degree of C2 autonomy, and nuclear weapons may be launched accidentally. 89

As Thomas Schelling presciently warned during the Cold War, ‘when speed is critical, the victim of an accident or a false alarm is under terrible pressure.’ 90 This pressure would likely be more intense for nuclear powers nearby (e.g., India and Pakistan, or China and North Korea), or where one side’s NC3 systems are asymmetrically more vulnerable or less sophisticated, for example, North Korea, India, or Pakistan. 91 Further, the increasingly interdependent and commingled (or entangled) nature of states’ conventional and nuclear C2 systems might exacerbate the incentives to escalation a situation to a nuclear-level once a conventional crisis or conflict begins. 92

The decision to automate nuclear assets may also be influenced by the political stability and the threat perceptions of a nuclear-armed state. A regime that fears either a domestic-political challenge to its rule or foreign interference may elect to automate its nuclear forces, ensuring only a small number of agents are involved in the nuclear enterprise. 93 For example, China maintains strict controls on its nuclear command and control structures (i.e., separating nuclear warhead and delivery systems). Open-source evidence does not suggest Beijing has pre-delegated launch authority down the chain of command if a first strike decapitates the leadership. In short, as a means to retain centralized command and control structures and strict supervision over the use of nuclear weapons, AI-enabled automation might become an increasingly amenable and intoxicating option to authoritarian regimes such as China.

In the context of AI and autonomy, particularly information complexity, misinformation, and manipulation, rationality-based deterrence logic appears an increasingly untenable proposition. In sum, the combination of increased speed, compressed decision-making timeframes, complex and interdependent command and control mechanisms, and increasing levels of AI-enabled NC3 automation and human-machine interactions increases the possibility of sparking a cascading set of errors (human or machine), reinforcing feedback-loops that could ultimately lead to an accidental nuclear exchange.

Furthermore, because there is so much redundancy built into modern NC3 systems, scenarios involving accidental nuclear war as a result of a single technical error or malfunction is less threatening, compared to the simultaneous coalescence of multiple failures in a rapid and unpredictable and reverberating fashion – where malfunctions in once system are prone to cause alarms in others.94 In particular, if they are compounded by organizational failures, ambiguous information, misperceptions, or excessive trust in technology, which may lead human operators cognitively offloading judgment to AI algorithms without fully understanding its limitations – also known as ‘automation bias.’ 95 Such automation bias – especially in human-machine interactions – could also mean that both false negatives and false positives go unnoticed (or are discarded) because the operators are overconfident in systems augmented with advanced technology such as AI. 96 This problem-set is compounded during a crisis when stress, fatigue, information overload, and commingled (nuclear and conventional) systems encounter a priori situations between asymmetric nuclear rivals, thickening the ‘fog of war’ – the inevitable uncertainties, misinformation, or even breakdown of organized units, which influences warfare – resulting in irrevocable actions, when use-or-lose-them becomes the only option.97 \*\*\*FOOTNOTE BEGINS\*\*\* Militaries today have already begun developing AI solutions to substitute human prediction to deal with information overload – or the so-called ‘ISR revolution.’ See, Keith Dear, ‘Artificial Intelligence and Decision-Making’, The RUSI Journal, 164:5–6, (2019), pp.18–25; and Yang Feilong and Li Shijiang ‘Cognitive Warfare: Dominating the Era of Intelligence’, PLA Daily, 19 March 2020.\*\*\*FOOTNOTE ENDS\*\*\*

Nuclear multipolarity

In a multipolar world nuclear order with competing and contested strategic dyads – India-Pakistan, U.S.-Russia, U.S.-North Korea, U.S.-China, and perhaps India-China – with weak mechanisms for de-escalation, doctrinal opacity, and questionable attitudes towards nuclear restraint, the potential risk of nuclear catalysis increases. 98 The emergence of nuclear multipolarity in the Second Nuclear Age has created multifaceted escalation pathways to a nuclear confrontation involving an expanding number of nuclear-armed poles, compared with bipolarity during the Cold War. 99 Kenneth Waltz, the founder of structural realism, argued that while nuclear weapons served as a stabilizing force during the Cold War-era, however, ‘increased numbers of actors increase levels of systemic uncertainty … rising uncertainty heightens potential miscommunication and conflict. Bipolarity [compared to multipolarity] is, therefore, the most stable form of international power distribution.’ 100 This multipolarity is essential because each state will choose a different response to the new choices emerging in the digital age. 101 Competing states making decisions under the nuclear shadow will be more inclined to assume the worst of others’ intentions, especially in situations where the legitimacy of the status quo is contested (i.e., maritime Asia).

Against the backdrop of existing tensions – especially a limited or proxy conflict or other crisis – between nuclear-armed adversaries (U.S.-China; U.S.-Russia; India-Pakistan; or U.S.-North Korea), therefore, an act of terrorism or other nefarious non-state action would create additional incentives for political leaders to assume the worst of the other’s intentions. Besides, the victim of a non-state or terrorist attack (e.g., cyber, disinformation, or drone swarm attack 102 ) would likely be under intense domestic political pressure to attribute blame swiftly and retaliate against the perpetrator – or aiders and abettors in case of a proxy actor. 103 During a tense situation, when prudent and careful planning can run aground against the fog and friction of reality, misperception and miscalculation may generate temptations for pre-emption with potentially catalytic effects. 104 According to the offensive realist scholar John Mearsheimer, ‘as long as the system remains anarchic, states will be tempted to use force to alter an unacceptable status quo.’ 105 The other side could easily perceive one state’s efforts to enhance its strategic forces’ survivability with state-of-the-art dual-use technology like AI as a potential threat to its ability to survive and respond to a nuclear first strike – or second-strike capability. 106

Authoritarian states may perceive an adversary’s intentions very differently from a democratic one. 107 The belief that a regime’s political survival or legitimacy is threatened might cause leaders to consider worst-case scenario judgments and behave in a manner predicted by offensive realist scholars. 108 Conversely, non-democratic leaders operating in closed political systems such as China, Russia, or North Korea may exhibit a higher degree of confidence (or overconfidence) in their ability to respond to perceived threats in world politics. 109 Bias assessments from a non-democratic regime’s (or ‘Stasi’ type) intelligence services might reinforce a leader’s faith – or a false sense of security – in their diplomatic skill and maneuverability. 110

Without institutionalized structures (or general staff system) connecting the intelligence services with the military and broader political context, decisions will likely be made in vacuums, with minimal checks and balances on the political leadership (or supreme leader), and a reduction in ‘bottom-up’ (or a ‘fact searching’ organizational culture) information flow – because of the fear of contradicting the leadership. 111 This situation can reinforce a distorted (or false) sense of reality, thereby compounding the cognitive misperceptions of events that are already present. This situation can reinforce a distorted (or false) sense of reality, thus compounding the cognitive misperceptions of events that are already present. Social media – and other AI-enhanced information tools – that supply decision-makers with a continuous flow of near-real-time information might also complicate the practice of deterrence and escalation management before and during future crises. 112 It is politics and the breakdown of human bargaining, therefore, that ultimately leads to conflict; AI and other kinds of advanced technologies – drones, deepfakes, and cyber capabilities – can be viewed as the tools (or dependent variables) that complicate and exacerbate the escalation dynamics determined by human choices, biases, and interactions. 113 The amplification of false alarms or the creation of false signals by social media (i.e., false positives and false negatives) might also disrupt critical communication channels between commanders and their political leadership and between allies and adversaries during crisis or conflict. 114

Authoritarian regimes whose political legitimacy and regime stability are conditioned or legitimized by the general acceptance of official narratives and dogma tend to become empowered when people’s trust in truth (i.e., faith in what they see and hear) is undermined. The vacuum is filled by the opinions of authoritarian regimes and leaders with authoritarian inclinations.115 \*\*\*FOOTNOTE BEGINS\*\*\* In contested information environments, errors in early warning systems and decision-making processes are characterized by a lack of data, ambiguous indicators, mixed signals, and conflicting sensor data inputs. Amidst this complexity and ambiguity, false signals frequently occur (and are even expected), not least because sensor systems may not be cross calibrated to provide cross-checking confirmation.\*\*\*FOOTNOTE ENDS\*\*\* Though authoritarian regimes might follow a rational logic and pattern of behavior in strategic decision-making, this ‘logic’ will reflect the myriad factors that influence a leader’s threat perceptions – including, inter alia, leaders personalities, beliefs, experiences, and the importance attached to reputation and status – tethered to its (possibly distorted or misinformed) version of events. 116 Thereby confounding the expectations and calculations – notions of deterrence and escalation thresholds – of adversaries and increasing accidental escalation risk. 117 The relative importance of these factors upon states’ resolve under crisis conditions in context-bound situations is difficult to answer with any certainty. 118

Furthermore, a regime that views its second-strike capabilities – especially its NC3 systems – as vulnerable or insecure (North Korea, Pakistan, or perhaps China) may be more inclined to automate its nuclear forces and launch postures. In short, non-democratic nuclear states with relatively centralized C2 structures, less confident in the survivability of their nuclear arsenal, and whose political legitimacy and regime stability is conditioned by the general acceptance of official narratives and dogma, would likely be more persuaded by the merits of automation, and less concerned about the potential risks – least of all the ethical, human cognitive, or moral challenges – associated with this decision. Despite official Chinese statements supporting the regulation of military AI by global militaries, much of China’s AI-related initiatives (e.g., the use of data for social surveillance to distill a social-credit scoring system and ubiquitous facial recognition policies) focus on the impact on social stability, and in particular, efforts to insulate the legitimacy of the regime against potential internal threats. 119

By contrast, the political processes, accountability (especially elected leaders and head of state vis-à-vis public opinion), nuclear-launch protocols, nuclear strategy and doctrine, mature civil-military relations, and shared values between allies (i.e., U.S. and its NATO allies), in democratic societies should make them less predisposed – or at least more reticent and encumbered – in use of AI in the nuclear domain. 120 In sum, while technological factors involved in NC3 systems are of great importance, political, psychological, strategic cultural, doctrinal, and organizational considerations are also central to understanding the nature and key to the mitigation – of accidental escalation risk. How might AI-augmented cyber capabilities create new pathways for accidental or inadvertent escalation?

Disinformation, misinformation, and information manipulation

One rapidly developing and increasingly prominent field of AI-augmented technology that can complement and force multiply existing malicious social manipulation behavior and generate campaigns of manipulation – most notably the spread of misinformation or disinformation – is the ability to generate audio and video images that fabricate events, create fictitious situations and propagate falsehoods. 121 Experts expect that it will be possible for non-state actors (or amateurs more generally) to generate photorealistic high definition video, audio, and document forgeries using machine-learning tools – in particular, generative adversarial networks (GANs) – at a low-cost and on a large scale. 122 In combination with other tools, 123 GANs have already demonstrated that producing realistic images is possible and will likely improve significantly in the next few years. 124 Examples of disinformation and manipulation, among other things, include distributed audio of private statements and conversations between political or military leaders (both domestically or with allies and adversaries); video of crises or conflict (see below) designed to incite public outrage and prompt pressure for retribution; or audio or video material calibrated to deflect, deceive, or otherwise distract attention from, an actor’s culpability of an aggressor by producing false alternative versions of events. 125

As AI technology advances, the quality, cost, and availability of GANs and other tools – especially AI-enhanced audio software will make it increasingly difficult to discern what is real from what is not, eroding public trust in hitherto trust-worthy information sources. 126 In 2014, for example, thousands of residents at St. Mary Parish in Louisiana received a fake text message alert via a bogus Twitter account warning of a ‘toxic fume hazard’ in the area. Further fanning the flames, a fake YouTube video was also posted showing a masked ISIS fighter standing next to looping footage of an explosion. 127 Thus, it is not difficult to imagine how these AI-enhanced technologies in the hands of non-state actors with nefarious goals (or ‘apocalyptic’ world view) might have dangerous consequences or for nuclear security and strategic stability. Deliberate malevolent information manipulation by non-state actors (terrorists, criminals, or state proxies) could destabilize implications on effective deterrence and military planning, both during peace and war. GANs generated deepfakes might also exacerbate the escalation risks by manipulating the digital information landscape, where decisions about nuclear weapons are made. It is easy to imagine unprovoked escalation caused by a malicious third-party (or state-proxy) clandestine false-flag operation in the competitive strategic environment. 128 During a crisis, a state’s inability to determine an attacker’s intent may lead an actor to conclude that an attack – threatened or actual – was intended to undermine its nuclear deterrent. 129

AI systems will likely come under inexorable stress from nefarious attacks using counter-AI techniques (e.g., data pollution, spoofing, false alarms, or tricking a system in order to reverse engineering algorithms), which might undermine the confidence in a network, creating new vulnerabilities, errors, and unintentional escalation risks. In the emerging deepfakes arms-race – much like cybersecurity more broadly – detection software will likely lag behind advances in offensive enabling solutions – or offense-dominant ones. 130 According to computer science expert Hany Farid, there are probably 100 to 1,000 times ‘more people developing the technology to manipulate content than there is to detect [it].’ 131 Efforts to counter these technologies and regain the upper-hand in the war on digital fakery have been underway for several years (e.g., automated anti-virus software, encryption, and other tools to call-out manipulated images and videos). Today, more sophisticated AI-enhanced techniques coupled with research that suggests pre-existing cognitive schemes, beliefs, and attitudes rather than credulity or gullibility determines whether the public believes particular fakery is real or not – meaning fake images and videos can achieve accepted even though they can be easily debunked. 132

AI-enhanced fake news, deepfakes, bots, and other malevolent social media campaigns could also influence public opinion – creating false narratives or amplifying false alarms – with destabilizing effects on a mass scale, especially in times of geopolitical tension and internal strife. 133 In 2017, for example, a deepfake video was circulated on Russian social media, alleging a U.S. B-52 bomber had accidentally dropped a ‘dummy nuclear bomb’ on a Lithuanian building. 134 A state or non-state actor could, for instance, generate an image or recording of a military commander obtained from open-sources to generate and disseminate a deepfake containing false orders, intelligence, or geospatial imagery that at best generates confusion that, in the worst-case scenario, aggravates a tense situation or crisis between rival nuclear powers – this idea is examined below. For example, in the world’s first reported AI-enabled theft in 2019, non-state actors used AI voice mimicking software to generate a fake recording of a British energy executive. 135 In short, AI-augmented technology is rapidly becoming another capability in non-state actors’ toolkit to wage campaigns of disinformation and deception – one that both sides may have used against them. 136

The democratization of ever more sophisticated technology will likely amplify documented human pathologies, 137 explaining people’s attraction to novel and negative information, memes, falsehoods, and filter bubbles – the so-called ‘information cascade’ phenomenon – which deepfakes are adapt to perpetuate. 138 In the case of cognitive availability heuristics, people tend to skew their judgments to more recent (or memorable) information, situations, or experiences, thus making new or novel opinions biased toward those that can be more easily recalled. 139 During times of high-pressure crises, decision-makers tend to interpret unusual circumstances as threatening, even if an adversary’s behavior has not changed. Routine activities (e.g., troop movements) scrutinized in the context of an early-warning alert may be considered as more menacing than they might otherwise be. 140

In 2017, for example, South Korean counterintelligence officials received fake mobile and social media alerts with orders for U.S. military and DoD personnel to evacuate the Korean Peninsula. 141 Information attacks such as this suggest that non-state actors, state proxy actors – and perhaps state actors – will inevitably attempt to use social media as a tool of war to provoke nuclear confrontation for political-ideological, religious, or other malevolent goals; and with increasing levels of sophistication, stratagem, and AI-enhanced subterfuge. 142 AI might also enable non-state actors to automate, accelerate, and scale synthetic social media accounts and content to support malevolent disinformation operations. 143

These potentially catalytic dynamics will likely be compounded by human cognitive bias. A motivated non-state actor would be well-positioned to use AI-augmented tools (e.g., ‘fake news’ or deepfake generated propaganda) to exploit this psychological weakness, ensuring control of the dissemination of false narratives and opinions. Threat assessments of catalytic escalation must, therefore, include both the likelihood that a third-party can execute a particular attack and the probability that the falsehoods or fakery that transpires leads to escalation. 144 Strategic decisions made by isolated nuclear-armed authoritarian regimes under these circumstances – especially regimes that believed their survival was threatened – could trigger dangerous accidental nuclear escalation dynamics.

Fictional scenarios

The following section includes four fictional scenarios – cyber ‘false flag’ operation, cyber-attack on nuclear early-warning systems, drone swarming targeting ISR systems, and deepfake disinformation – to illustrated how AI-augmented capabilities in the hands of non-state actors might accidentally or inadvertently drag a competitive nuclear dyad into conflict. 145 These fictional scenarios are premised on three assumptions: (1) the involvement of a nuclear-armed adversarial dyad adversary during a crisis or period of tension; (2) the existence of information asymmetry; and (3) the technical feasibility of the operations described – either currently in existence or considered technically viable shortly. Why these capabilities and not others? These capabilities are of particular interest because they play an increasing role in how non-state actors leverage the asymmetric and low-cost benefits of AI technologies to realize their malevolent objectives. Although multiple pathways may be activated during an actual conflict or crisis – either simultaneously or sequentially – assessing each of these potential escalatory pathways offers insight into the interplay of strategic AI technologies and stability risks. One caveat, though: in the real-world, the aggravating factors described above, would interact with each other. The participating actors’ relative capabilities would vary, thus producing a potentially much larger potential universe of possible scenarios than outlined here.

Scenario (1) Cyber ‘false-flag operation’ 146

Party A (a non-state actor) launches a false flag cyber operation – data manipulation, social media flooding, a spoofing attack, or other deception – against State B and C, which is not traced to Party A and appears to both State B and C to come from the opposing side. 147 Convinced that the other side is responsible and about to be attacked by the opposing side of the nuclear-dyad, State B retaliates against State C in a pre-emptive attack that C views as unprovoked aggression – sparking a catalytic war. During a crisis between two states, leaders would likely be predisposed to assume the worst about the other’s intentions, thus making them less likely to exercise rigorous due diligence to establish high confidence attributions (or false positives) due to a cyber-attack. 148

Scenario (2) Cyber-terrorism vs. early warning systems

During a period of heightened tension or crisis between State A and State B, a third-party actor or terrorist floods social media outlets and open-source crowdsourcing platforms with false information (e.g., satellite imagery, 3D models, or geospatial data) about the suspicious movement of State A’s nuclear road-mobile transporter erectors-launchers (TELs). 149 Because of State B’s inability to determine with confidence the veracity of this information, and with mounting public pressures to respond, State B escalates a situation on the falsehood (or false positive) it is the target of an unprovoked attack. 150 Asymmetries between adversaries NC3 systems and military capabilities would likely exacerbate the fictional scenario’s escalation mechanisms. 151 Taken together, increasingly sophisticated and accessibility of deepfake technology, the inherently dual-use nature of AI, the problem of attribution in cyberspace, the increasingly complex and interdependent nature of NC3 systems, and a compressed timeframe for strategic decision-making associated with hyper-speed warfare, will continue to lower the threshold for false-flag operations. 152

Scenario (3) Drone swarming vs. ISR systems

An insurgent proxy of State A uses a swarm of autonomous micro-drones over an adversary’s territory as part of a clandestine ISR mission. 153 Because this type of sophisticated technology is considered beyond the reach of a lone wolf or unsponsored terrorist group, 154 State B attributes to its militarily superior adversary, and thus, views this proxy as a precursor for an attack planned by A. The use of autonomous swarms, especially during periods of tension or insensitive anti-access/area denial (A2/AD) environments, might generate incentives for pre-emption. Further, the sophistication of A2/AD capabilities such as drone swarms – and advanced non-nuclear strategic weapons including hypersonic weapons, cyber, and anti-ship ballistic missiles (ASBMs) – complicates Herman Kahn’s notion of ‘ladders of escalation’ to achieve a superior position vis-a-vis an adversary across the range of escalation rungs – or ‘escalation dominance.’ 155 Where on the escalation ladder is a swarm attack against the United States’ nuclear ISR? Would a Chinese cyber-attack targeting a U.S. water supply facility be more or less escalatory than an ASBM attack on a U.S. aircraft carrier in the West Pacific? 156

Conversely, the discovery of information by State A (e.g., suspicious troop movement or missiles leaving their garrison) could prompt A to escalate a situation, motivated by the desire to capture the perceived strategic upper hand. Moreover, State A might consider the first-mover advantages of using low-cost and relatively dispensable drones as controllable at a conventional level, which would likely increase their appeal, at least in the opening stages of a conflict. In the event State A’s unarmed proxy drone swarm was attacked by B in a counterterrorist or counterinsurgent strike, 157 State A would be forced to either accept this vulnerable asset’s loss or escalate a situation – through its surrogate proxy or more directly. 158

Scenario (4) Deepfake disinformation

To incite conflict between two nuclear-armed rival states, State A hires proxy hackers to launch a deepfake video, depicting senior military commanders of State B conspiring to launch a pre-emptive strike on State C. 159 This footage is then deliberately leaked into C’s AI-augmented intelligence collection and analysis systems, provoking C to escalate the situation with strategic consequences. 160 B, fearful of a decapitating strike and losing the first mover’s advantage, swiftly escalates the situation. 161 The current underdeveloped state of ‘counter-AI’ capabilities and other fail-safe mechanisms (e.g., circuit breakers) to de-escalate escalation in cyberspace will make the unprovoked and unintentional escalation dynamics depicted in this scenario very challenging to anticipate and thus mitigate. 162

Conclusion

How can militaries maintain effective command and control of nuclear forces in a rapidly evolving, uncertain, and complex conflict environment? While no amount or combination of controls, procedures, or technical enhancements can eliminate the possibility of catalytic nuclear escalation – and accidental escalation more broadly – specific measures that focus on reducing the possibility of accidental nuclear war may help to reduce some of the risks highlighted in the scenarios in this article – especially human and technical errors that occur in cyberspace. 163 Because accidental (and inadvertent) escalation dynamics are not the result of decision-makers electing to escalate, it cannot be deterred in the traditional sense. 164 Deterrence by denial measures by decision-makers, in advance of a non-state actor’s attack, might contribute to escalation management, however. 165

#### Bioterror spreads rapidly---extinction.

Bryan Walsh 20, Future Correspondent for Axios, Editor of the Science and Technology Publication OneZero, Former Senior and International Editor at Time Magazine, BA from Princeton University, End Times: A Brief Guide to the End of the World, Orion Publishing Group, Limited Edition, p. 204-206

I’ve lived through disease outbreaks, and in the previous chapter I showed just how unprepared we are to face a widespread pandemic of flu or another new pathogen like SARS. But a deliberate outbreak caused by an engineered pathogen would be far worse. We would face the same agonizing decisions that must be made during a natural pandemic: whether to ban travel from affected regions, how to keep overburdened hospitals working as the rolls of the sick grew, how to accelerate the development and distribution of vaccines and drugs. To that dire list add the terror that would spread once it became clear that the death and disease in our midst was not the random work of nature, but a deliberate act of malice. We’re scared of disease outbreaks and we’re scared of terrorism—put them together and you have a formula for chaos.

As deadly and as disruptive as a conventional bioterror incident would be, an attack that employed existing pathogens could only spread so far, limited by the same laws of evolution that circumscribe natural disease outbreaks. But a virus engineered in a lab to break those laws could spread faster and kill quicker than anything that would emerge out of nature. It can be designed to evade medical countermeasures, frustrating doctors’ attempts to diagnose cases and treat patients. If health officials manage to stamp out the outbreak, it could be reintroduced into the public again and again. It could, with the right mix of genetic traits, even wipe us off the planet, making engineered viruses a genuine existential threat.

And such an attack may not even be that difficult to carry out. Thanks to advances in biotechnology that have rapidly reduced the skill level and funding needed to perform gene editing and engineering, what might have once required the work of an army of virologists employed by a nation-state could soon be done by a handful of talented and trained individuals. Or maybe just one.

When Melinda Gates was asked at the South by Southwest conference in 2018 to identify what she saw as the biggest threat facing the world over the next decade, she didn’t hesitate: “A bioterrorism event. Definitely.”2

She’s far from alone. In 2016, President Obama’s director of national intelligence James Clapper identified CRISPR as a “weapon of mass destruction,” a category usually reserved for known nightmares like nuclear bombs and chemical weapons. A 2018 report from the National Academies of Sciences concluded that biotechnology had rewritten what was possible in creating new weapons, while also increasing the range of people capable of carrying out such attacks.3 That’s a fatal combination, one that plausibly threatens the future of humanity like nothing else.

“The existential threat that would be most available for someone, if they felt like doing something, would be a bioweapon,” said Eric Klien, founder of the Lifeboat Foundation, a nonprofit dedicated to helping humanity survive existential risks. “It would not be hard for a small group of people, maybe even just two or three people, to kill a hundred million people using a bioweapon. There are probably a million people currently on the planet who would have the technical knowledge to pull this off. It’s actually surprising that it hasn’t happened yet.”

#### Second, hybrid war---the ‘fog of war’ obstructs effective response to Russian hybrid tactics---only US lead demonstrates resolve via alignment.

Dr. Peter Braun 19, Head of the Armed Forces Development Branch within the Swiss Armed Forces Staff, "Fighting ‘Men in Jeans’ in the Grey Zone between Peace and War," NATO Defense College, Policy Brief, No. 8, pg. 2-6, August 2019, JSTOR. error edited.

Whereas NATO’s 2010 Strategic Concept did not refer to “hybrid warfare” at all, the term has been used in all NATO Summit Declarations since 2014. In 2016, hybrid warfare was described as “a broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary, and civilian measures employed in a highly integrated design by state and non-state actors to achieve their objectives”.9 When waging hybrid warfare, an adversary does not primarily seek to destroy opposing forces on the battlefield or occupy territory. The aim is rather to affect and influence the functioning of state institutions and society as a whole – at best, without using overt military force. Since actors who resort to hybrid warfare are normally too weak to confront modern, highly developed armed forces directly, their main objective is to exploit the adversary’s weaknesses and target its underlying vulnerabilities systematically.

In such a scenario of hybrid warfare, non-conventional forces and irregular actors play an essential role, they include armed groups, proxies, Special Forces, terrorists or private security and military companies. Actors like these would complement non-military means such as economic pressure, political blackmail or propaganda. Conventional armed forces would typically be engaged only after all other means have been exhausted without achieving the aggressor’s objectives. One measure could be to deploy conventional military units beyond the borders as an element of deterrence or an (offensive) show of force, ready to intervene immediately if necessary.10

Even if conceived of, instigated and controlled from abroad, terrorist and hybrid threats usually emerge within a state. In conventional military operations, the crossing of geographical borders clearly indicates the origin of such an attack. In contrast, in a hybrid environment, it is difficult to attribute responsibility for the use of force with equal clarity. As a consequence, the distinction between civil unrest, non-international and international armed conflicts, as well as between combatants and non-combatants (as defined in international law) is inevitably blurred in a hybrid environment. The result is a grey zone between the two poles traditionally denoting peace and war.11

Acts of terror as a component of hybrid threats

The main objective of terrorist activity in a hybrid environment is to spread fear and terror, to intimidate populations and degrade the will of an adversary. When multiple terrorist activities follow a central strategy, they can destabilise a state or a society to a considerable degree, even if an individual acting alone may cause relatively little harm. Furthermore, nation states may empower terrorists by making heavy weapons (e.g. anti-tank weapons or drones) available to them. Such support would allow terrorists to unleash significant violence. The traditional means and assets of civilian police forces, which are primarily responsible for counter-terrorism in most Western states, would not suffice to cope with such actors.

At times, state actors too can adopt terror-based tactics. One example is their use by Special Forces, which Collin Gray called “guerrillas in uniform or, in a more pejorative way, […] terrorists in uniform”.12 Nevertheless, it is at least questionable if and how a state actor resorting to hybrid warfare would deploy uniformed Special Forces in the way Russia did successfully during the occupation of Crimea. It seems possible that an aggressor would prefer using “men in jeans” over “little green men”.13 Special Forces acting in such a non-identifiable and non-descriptive mode could operate in a way that would normally qualify as terrorism.

As a component of hybrid warfare, terrorism threatens NATO in multiple ways. Currently, a hybrid approach to warfare is primarily associated with Russia, making NATO’s eastern member states and their neighbourhood seem particularly exposed. However, terrorism as part of a hybrid campaign could also spill over from the South or South East to the Euro-Atlantic region. In addition, home-grown terrorism must be kept in mind too.14 A significant threat to the internal security of NATO members are the thousands of foreign fighters who have return ed home from the conflicts in Northern Africa and the Near and Middle East. These fighters often bring with them military training as well as a broad warfighting experience, and they are used to extreme violence.15 For instance, ex-Jihadists trained in weapons, explosives and tactics could cause considerable damage, especially if operating in groups. Such activities – launched as a coordinated terror campaign – could have similar effects to a hybrid attack launched from outside Alliance territory.

Counter-terrorism and hybrid threats

Despite the potential of terrorist violence as part of hybrid warfare, counter-terrorism as a response or preventive measure has an unexpectedly low profile in NATO’s policy on hybrid threats. For example, in its Countering Hybrid Warfare Strategy issued in 2015, terrorism only appears marginally. The same is true for the documents examined on counter-terrorism: in the 2012 Counter-Terrorism Policy Guidelines, hybrid threats are completely missing, while the 2015 Military Committee Concept for Counter-Terrorism mentions them at least once, albeit more as an aside, i.e. as part of a short list of “CT-related capabilities […] and operating environments”.16 In short, and as far as the strategic documents are concerned, the two interconnected threats coexist side by side or independently.17

Nevertheless, these threats are a particular challenge to the Alliance. As outlined in the 2012 Policy Guidelines, “individual NATO members have primary responsibility for the protection of their populations and territories against terrorism”.18 The same goes for hybrid threats: “The primary responsibility to respond to hybrid threats or attacks rests with the targeted nation”.19 However, when violence reaches a level that overwhelms the civilian security authorities and armed forces of the targeted member(s), NATO is affected as well. In this regard, the Policy Guidelines highlight that “Cooperation through NATO can enhance allies’ efforts to prevent, mitigate, respond to, and recover from acts of terrorism. NATO, upon request, may support these efforts”.20 And the Alliance’s Countering Hybrid Warfare Strategy underlines: “NATO is prepared to assist any ally against hybrid threats as part of collective defence”.21

Article 5 in the grey zone between peace and war

Through covert, non-linear and possibly terrorist action, an aggressor resorting to hybrid warfare aims to stay below the traditional threshold of war in which [they] he must expect an overt collective reaction from the international community. Irregular warfighting methods, however, including terrorist violence, are legally and politically difficult to isolate and focus on. That undermines not least the order of international law, in particular the prohibition on the use of force by states and the right to individual or collective self-defence according to the UN Charter.22 The ambiguity created by irregular action seeks to disguise the responsibilities for acts of war, to confuse adversaries and to slow down their decision-making process. In regards to NATO, the main purpose of such an approach could be to impede a rapid and coherent response under Article 5 of the Washington Treaty.23

One requirement for the collective defence clause to be invoked is an “armed attack”, a term, however, that is not defined in the UN Charter. In its original meaning, Article 5 referred to a conventional military threat from outside the territory of a member state. According to customary international law, a prerequisite for an armed attack is at least a massive use of force, whereas the International Court of Justice has stated that such an attack can also include “the sending by or on behalf of a state of armed bands, groups, irregulars or mercenaries, which carry out acts of armed forces against another state in such gravity as to amount to an actual armed attack conducted by regular forces or its substantial involvement therein”.24 This description can – at least in certain cases – also apply to terrorism as an operational procedure of hybrid warfare.

To invoke Article 5, it is essential that not only a high degree of violence occurs, but that an attack originates from outside the Alliance’s territory. Since, in a hybrid scenario, violence may occur solely within the borders of a state, attribution of responsibility is a major challenge.25 This would be especially true if a state actor waging hybrid warfare were to disguise its terrorist actions through propaganda or if a proper terrorist campaign was not (as were the 9/11 attacks) at least directed from abroad, but emerged exclusively within a country. In such a case, in the light of NATO’s consensus-based decision-making, the likelihood that the Alliance would react too late or not at all is rather high. Should it prove impossible to identify the origin of an attack, a (temporary) division of NATO could ensue. As a recent public survey showed, even if faced with a conventional attack, solidarity between the Alliance’s members seems to be quite humble.26 Cohesion could even be lower if attribution of responsibility were not possible at all. Furthermore, with regard to Article 5, NATO’s 2012 Policy Guidelines are rather ambiguous, stating only that “collective defence remains subject to decision by the North Atlantic Council”.27 Although important, the statement lacks clarity.

Despite these shortfalls, it must be underscored that a massive terrorist threat against one of its member nations would not only provoke discussions regarding the collective defence clause but also directly trigger Article 4 of the Washington Treaty, which refers to member states’ consultation.28 This would allow the Alliance to act resolutely even though the aggression would not necessarily fall under Article 5.29 In addition, it must be kept in mind that NATO members can also act without consensus, either individually or in a “coalition of the willing”. In such a case, American support would be crucial. Given this, SACEUR could – in his double-hatted function as Commander of US European Command (EUCOM) – initiate a rapid military response using at least US assets in favour of the member state under terrorist threat, even without a decision by the North Atlantic Council.30

#### Hybrid war goes nuclear---extinction.

Łukasz Kulesa 18, Research Director at the European Leadership Network, “Envisioning a Russia-NATO Conflict: Implications for Deterrence Stability,” EURO-ATLANTIC SECURITY REPORT, February 2018, https://www.jstor.org/stable/pdf/resrep17437.pdf

“Hybrid” scenarios: trigger for conflict?

One can envisage a number of “hybrid” scenarios of Russia-NATO conflict where operations which started in the cyber, economic, criminal, or “active measure” domains, below the threshold of conflict, trigger a military response or are followed by the physical use of force. As noted in the discussion on the definitions of a conflict, the threshold between crisis and military conflict may not be explicitly stated or otherwise clear to all sides; and it may also be ignored during a crisis. This aspect is especially relevant in the current period of increased interference in the internal affairs of NATO countries attributed to Russia and of the high volume of information ‘warfare’ between Russia and NATO countries.

Russia remains vigilant about foreign interference in its internal affairs and the threat of subversion leading to a severe destabilization of the regime. In the past, Moscow has made accusations about foreign sponsorship of Chechen and radical Islamic terrorists targeting Russia, and has alleged the existence of training camps on the territories of NATO states for activists planning colour revolutions in Ukraine and Belarus. In the extreme circumstances of a crisis, if the Russian leadership became convinced that a non-military campaign against it (which might also involve cyber activities and what Russia calls attempts to instigate colour revolutions) had intensified, this could lead to a military response.

With regards to NATO, some of its members’ views mirror the Russian assessment that we are already in a state of conflict, in which the boundary between peace and war is blurred, and that their defences are being actively attacked through nonmilitary means. They are thus concerned about a scenario in which Russia initiates an attack that moves swiftly from non-military to military means. This scenario should be not dismissed. At the same time, one needs to be wary of interpreting all disturbing developments as part of a grand Russian plan culminating in a provocation or use of force. So there should be prudence before any country presses the “panic button” at the national or NATO / European Union level. There should also be close analysis of early warning indicators related to the gravity, intensity and diversity of incidents and to connections between them. The overall political context and state of the RussiaNATO relationship would also be important: what would be the political and strategic reasons for Russia to move from sub-threshold to abovethreshold activities?

Escalation: Can a NATO - Russia conflict be managed?

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

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

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

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

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

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

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

Conflict termination

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

With regards to Russia, Moscow would most likely be approaching the conflict with a clearer concept of its war aims and thus develop better-formed views on conflict termination. It would seek to establish escalation dominance and confront NATO with a binary choice of either accepting defeat or further intensification of fighting. Such intensification might involve a move to the nuclear level, but Russia would also have conventional escalation options, such as conventional deep strikes.

At the same time, it should be highlighted that Russia is unlikely to start a conflict which involves a high degree of uncertainty about its final outcome and carries a risk of military defeat. Russia cannot safely assume that US-led NATO would act with restraint, nor could it be sure that the Alliance would be ready to surrender and terminate a conflict early. For internal reasons Russia cannot afford to lose a “big war”, so the most prudent option would generally be not to initiate such a conflict in the first place. Such logic could, however, get lost in some of the hybrid scenarios and scenarios of an inadvertent outbreak of a conflict.

#### Third, EU-NATO harmonization---fractures over CT undermine efforts to stabilize MENA.

Lt. Col. Fernando D. Puebla 18, International affairs section analyst, General Staff Plans Division, "Projecting Stability on NATO’s Southern Flank. How can NATO and the EU ensure Efficient Cooperation?" Instituto Español de Estudios Estratégicos, 11/13/2018, pg. 2-14.

The crisis in Ukraine and the aftermath of the Arab Spring with the terrorism of Daesh in the Middle East and North Africa (MENA), provoked important decisions in both NATO´s Summits of Wales 2014 and Warsaw 2016 to adapt the Alliance to the new strategic environment. During the Wales Summit, NATO addressed for the first time the need to reinforce the capabilities to project stability in its eastern and southern neighbourhoods, in order to improve their resilience and their capacity to ensure stability and security by themselves. The idea of ‘projecting stability’ represents the second main vector of NATO adaptation to the new strategic context, together with the new deterrence and defence posture1. During the Warsaw Summit, a ‘framework for the South’ was established to improve regional situational awareness, anticipation and projecting stability through partnership and capacity building2. Secretary General Jens Stoltenberg summarised NATO’s broad objective for the South: ‘to protect our territory, we must be willing to project stability beyond our borders. If our neighbours are more stable, we are more secure’3. As it is appreciated, this term has been widely used in NATO´s declarations and statements; however, there is not an official definition of this concept. Within academics realm, definitions have been provided on the term, such as ‘a spectrum of engagement, running from partnerships with key states, including capacity building, to crisis management measures relying on military capabilities’4. Also, it is important to note the controversy originated with the term of ‘projecting stability’, considered by many partners and developing countries as ‘aggressive’, representing the term ‘projecting’ as an intrusion in partner governments´ rules5.

Taking into account the abovementioned definition, NATO’s projecting stability is unable to address the root causes, mainly related to the demographic pressure that drives instability to the South. Unemployment, food insecurity, environmental issues and water scarcity, lead to large population groups vulnerable to radicalization by terrorists and displacement due to migration6.

NATO has actively engaged its partners for military contributions to enhance stability in the South, but, at the same time, must acknowledge the importance of political and socioeconomic elements that can only be delivered by local governments with a help from organisations like the United Nations (UN) and the European Union (EU). While working with organisations like the African Union (AU) to achieve a regional approach is important, success begins with a key partner, the EU7. Both organisations share a common neighbourhood, a common commitment to their neighbours´ resilience and common security challenges. NATO and the EU developed their respective strategies witnessing initiatives to underpin their cooperation, starting by their Joint Declaration at the Warsaw Summit.

This paper will develop the way to ensure the most efficient cooperation between NATO and the EU, in order to achieve stability in the South. An analysis on strengths, weaknesses, opportunities and threats of NATO and the EU toolboxes will lead to recommendations and conclusions on the issue

NATO Toolbox. Partnership and Defence Capacity Building

At the Warsaw Summit, projecting stability was conceived in the framework of the 360- degree approach8, but the concept has been increasingly associated to the Southern Flank9. The Alliance does not rely on suitable tools to address the challenging situation in MENA and an effective NATO strategy towards Southern Flank still looks indefinite. However, NATO has definitely made a difference as part of the global international community´s efforts10, by enhancing the Mediterranean Dialogue (MD) and Istanbul Cooperation Initiative (ICI) partnerships, fostering Defence Capacity Building (DCB), and making a significant effort in counterterrorism with Operation ‘Sea Guardian’ in the Mediterranean and with AWACS support to the Global Coalition to counter the Islamic State (ISIL).

NATO has deep experience with partnerships. Its greatest contribution to the South is not military, but the partnership pillars: political dialogue and practical cooperation through the full use of NATO´s cooperative security toolkit11. In Operation ‘Unified Protector’ in Libya, the participation of four Arab NATO partners provided an unprecedented Arab League´s support, increasing the legitimacy of the operation. However, NATO´s efforts to project its influence in the South through its partners are likely constrained by issues such as internal political changes in partners, geopolitical rivalries (Russia, China…) and its negative reputation among locals in the MENA region. Therefore, NATO needs to make itself more attractive to its partners12 . At the Wales Summit, NATO adopted the DCB Initiative to fulfil the partners´ primary need of developing and enhancing their defence skills13. NATO´s Capacity Building is focused on priority areas related to current challenges in the South (counterterrorism, border security, counter-Improvised Explosive Device (C-IED), Cyber-Defence, Chemical, Biological, Radiological and Nuclear (CBRN), Intelligence). Their activities are tailored for the specific partner´s needs, enabling them to voluntary participate in other DCBs projects (i.e.: Jordan in Iraq), which could be applied for Tunisia or other partners in future DCBs with Libya. This has generated great acceptance with an increasing number of requests among Southern partners. Another important step to enhance NATO’s regional approach to the South has been the cooperation with regional organizations like AU in areas of mutual interest14.

NATO´s functions in counterterrorism in the South are restricted to assessment and interpretation, unless NATO forces are deployed (Op. ‘Sea Guardian’). A viable way forward for NATO is to enhance intelligence sharing with partners, mainly with the EU, so that its shortfalls are compensated15.

The activities related to projecting stability to the South, requires command and control structures at operational and strategic levels that provides an effective common operating picture. The Hub-South in JFC Naples allows enhanced and coordinated intelligence sharing, counterterrorism and DCB in the South. At the strategic level, the Comprehensive Crisis and Operations Management Centre (CCOMC) facilitates to NATO coordination with civilian and military bodies and organizations.

Still, it is important to stress the different threat perceptions between the Allies, which could hamper consensus for the strategy for the South. This is due to the perception that devoting resources to the South is detrimental to the East. This issue could seriously affect to NATO’s Centre of Gravity: its cohesion.

EU Toolbox. The Integrated Approach

The EU High Representative, Federica Mogherini stated in 2015: ‘Complex threats call for coordinated response, using military and civilian tools, as well as longer term financial and development instruments in a comprehensive way. Responding to emergencies is crucial, but we also need to think strategically, prevent rather than simply react to crises, work on their root causes’16. This statement represents the essence of the Integrated Approach to Conflicts and Crises, a core part of the 2016 EU Global Strategy, which also recognises that none of the conflicts can be solved by the EU alone17 .

The Integrated Approach is a consequence of expanding the Comprehensive Approach (defined in the 2003 EU Security Strategy), with its three pillars (Diplomacy, Development/Economy/Trade and Defence/Security), to the ways to act in Conflicts: multi-phased (all stages of the conflict cycle), multi-level (from local to global) and multilateral (engaging all the players in a conflict)18 . A key aspect is the strategic coherence between Integrated Approach and the EU instruments available. The diversity of political, economic and security instruments has enabled the EU to respond in a multi-faceted manner to situations where other crisis management actors are less prepared19.

[Chart omitted]

The South is vital for the EU, most Common Security and Defence Policy (CSDP) missions are deployed in this area.

The ‘porous’ Sahel is where the EU Integrated Approach is being tested, in order to address the root causes of the challenges and building resilience Diplomacy (EU Delegations), Development (technical and financing instruments of the EU Commission) and CSDP (civilian-military missions) represent the approach to priority domains where EU has particular strengths (governance, democracy, rule of law, human rights, youth, migration, border managing, agriculture, food security, education, infrastructure or climate change)20.

[Chart omitted]

The main CSDP strength in the South is Capacity Building in essential areas such as counterterrorism, migration, border control, rule of law, human trafficking or enhancing domestic security. CSDP missions are adaptable to new security needs (i.e: Operation ‘Sophia’ is also performing capacity building with the Libyan Coast Guard). Also, partnerships with AU and support and finance of the G5-Sahel Joint Force to fight against jihadists in Sahel, have increased the leverage and effectiveness of the CSDP action in the South.

Yet, the EU has the core challenge to ensure coherence between the broad range of instruments of the EU Commission (Development pillar) and those of the European External Action Service (EEAS) (Diplomacy and CSDP pillars)21. Likewise, the experience reveals some deficiencies in the EU Integrated Approach. Its imbalance towards migration is not perceived by partners as the most adequate response for local needs, leaving counterterrorism as a more important factor to address. Also, coordination needs strengthening between CSDP civil and military missions and with other main actors in Southern Flank (France, Italy, and the US)22. The EU Military Planning and Conduct Capability (MPCC) is the first step to get the necessary coordination between civilian mission and non-executive military missions (EUTMs) at the strategic level23.

The insufficient political support of many CSDP missions, impacts in the level of their ambition. Member states with different threat perceptions (East-South), insist on short mandates as many missions by design (i.e: Security Sector Reform) require long-term presence24. Finally, the EU has a broad variety of crisis management tools but, at this moment a modest military capability, having their tools focused on the lower end of crisis spectrum or crisis prevention.

Opportunities and Threats in NATO - EU Approaches

Based on the analysis of both NATO and the EU toolboxes, a number of opportunities for cooperation in different domains and the threats that could jeopardize this cooperation have been identified.

Defence Capability Building is paramount for both NATO and the EU, as they share common commitment to resilience of the South and it represents one of the seven areas for deeper cooperation identified in the Warsaw Joint Declaration in 2016. One concern might arise about the potential competition between both organizations in the South in this realm; therefore, coordination is essential. ‘Leveraging the expertise and financial resources of both NATO and the EU in support of joint projects in partner countries would be a significant way of strengthening a networked approach to projecting stability’25. Tunisia is one of the three pilot countries for NATO - EU cooperation in DCB areas26. Another significant step in the networked approach is the financing decision adopted by the EU in July 2017, allocating $2 million as a contribution to the NATO Building Integrity Programme27 . This programme, launched in 2007, provides practical tools to help participating countries strengthen integrity, transparency and accountability, reduce the risk of corruption in the defence and security sector and promotes good governance28 . Three partners in the South are participating in the Programme (Tunisia, Mauritania and Jordan).

Counterrorism is an area where the cooperation between both organizations is limited mainly due to the difficulties in sharing and coordinating Intelligence, Surveillance and Reconnaissance (ISR) efforts. The EU lacks sufficient ISR assets and presents deficiencies in situational awareness29 . However, there are potential opportunities to achieve a more effective NATO - EU cooperation, as both rely on powerful hubs for intelligence sharing (the EU European Counterterrorism Centre and the NATO HubSouth). Also, important ISR NATO assets (Allied Ground Surveillance System, AWACS) could support the EU missions in the Mediterranean and in the South.

NATO and the EU maritime operations in the Mediterranean are cooperating effectively and mutually complementary. NATO Sea Guardian operation has a mandate covering both Article 5 and non-Article 5 missions, while also supporting the EU mission Sophia, and is available to be tasked to counter the smuggling of migrants across the Mediterranean. This successful support opens opportunities for further cooperation in the maritime domain.

The Hub-South entails an effective tool for coordination with the EU in missions, at the operational level. Also, SHAPE CCOMC would enable efficient coordination with MPCC at the strategic level, initially limited for CSDP non-executive missions (EUTM).

The pre-existing negative perceptions of the Arab world vis-à-vis NATO and the West and related sensitivities to Israeli-Arab relations inhibit NATO´s regional role in the Southern Flank30. However, it is not so negative for the EU, due to its particular insight on the Israeli-Arab conflict, backed by two EU missions in Palestinian territories and its economic effort in development in the MENA.

NATO - EU Cooperation is hampered by some member states prioritising their national interests. Turkey (NATO) and Cyprus (EU) set mutual impediments on operational and intelligence sharing issues because of the unresolved conflict on Cyprus31 . The influence developed by some member states in specific areas (i.e.: the US in Middle East and France in North Africa), makes them enablers for NATO or the EU, in the area, but at the same time, are reluctant to grant them a wider political / military scope32.

Recommendations

NATO allies must change their mindset of prioritizing their threat perceptions to the East or to the South. The approach must support the defence of the Eastern Flank towards the Russian threat while, simultaneously, addressing terrorism and migration challenges in the South. Projecting stability needs a transversal 360-degree approach to avoid the risk of ‘regionalization’ and eroding NATO’s cohesion. One proposal could be the creation / identification of tailored training/mentoring units assigned to existing NATO Force Structure (NFS) HQs with projecting stability tasks (specifically DCB), on a voluntary and rotating basis, and similar to the rotation plan format for NRFs. This would involve a significant number of allies, providing a similar perception of cohesion to the Enhanced Forward Presence initiative.

Capacity building is identified as a major element of partnership for both NATO and the EU, and a key tool to increase stability in the South without deploying large military forces33. It is one core area identified in the NATO - EU Joint Declaration and a scope where joint projects are conceivable. It is paramount to deepen cooperation in this realm by aligning financing, expertise and NATO’s well developed network of national education, training and research centres, avoiding duplicities and competitions, and adapting the terms of cooperation to the specificities of the host nation in order to achieve synergies and cost effectiveness.

NATO has much less leverage than the EU in the Southern Flank34. To increase its approach effectively, NATO must lean on its partners, becoming more proactive and offering them tailored assistance rather than waiting to be approached35. Likewise, NATO should promote public diplomacy activities in the South, by reaching out to opinion shapers in all NATO regional partners to relieve anti-Western prejudices regarding NATO’s ‘real’ intentions36 . In this effort, the EU could support NATO with its diplomatic strengths, particularly in areas where the EU is a key actor (North-Africa, Sahel).

Libya constitutes a ‘black hole’ that threatens to ‘swallow’ its close actors in the area, with the added risk of ‘somalisation’37. At the Warsaw Summit, Allied leaders agreed to support Libya upon request from their authorities. Taking into account that many Libyan security interlocutors have argued that a gendarmerie type structure is more suited to Libya’s security challenges (policing, border control, counter-narcotics) than a conventional, national-level army38, NATO - EU Cooperation would be desirable and should constitute a long-term project39 based on complementarity. Apart from a diplomatic and development approach, the EU could contribute complementarily in Security Sector Reform (SSR) and good governance (this support exists practically in all EU missions), as it relies on a significant expertise regarding reforming police, law enforcement agencies, civil institutions and the establishment of border and gendarmerie-like forces. On the other hand, NATO could lead to support the rebuilding of the Libyan Armed Forces and the reintegration of armed militias into the country’s defence and security structures, roles already played in Kosovo and Afghanistan40, with the potential support of MD partners (i.e. Tunisia), taking the example of Jordan´s participation in DCB in Iraq. The approach would be bottom-up, starting at municipal level, except on the east of Libya, due to the strength of the Libyan National Army41. If needed, NATO would provide military forces to achieve a safe and secure environment.

NATO - EU maritime cooperation in the Mediterranean is another successful example of complementarity and mutual support. Further cooperation could take place in the maritime security task, by protecting the vital Sea Lines of Communication (SLOCs) which access the European Southern neighbourhood (i.e.: The Gulf of Guinea).

NATO and the EU should enhance the cooperation in counterterrorism, assuming the security principle of the continuum between internal and external security and the impossibility of their categorical distinction42. NATO is very experienced in external counterterrorism and the EU relies on powerful internal antiterrorist and coordination instruments. So, it is crucial a fluent and reliable intelligence sharing to make effective the internal-external security nexus and provide an efficient answer to one of the foremost threats from the South.

NATO - EU cooperation should be across all levels of command. By starting with top-down political guidelines by member states and working through concrete measures to implement it, as is currently the case of NATO - EU partnership43. The establishment of NATO Hub-South and the EU MPCC are unequivocal signs of enhancing the opportunities for an efficient multi-level structure of cooperation.

Conclusions

Achieving stability in the South requires a comprehensive approach that would go far beyond simple military responses. The root causes of instability are mainly socioeconomic (Arab Spring is an example), which require government´s reform, economic development, individual freedom, and addressing inequality issues, that outreach NATO’s capabilities to address them44. Even, the term of ‘projecting stability’ should be reconsidered or, at least, renamed, because of the controversy created in partner countries and the wideness that the concept implies.

At the Warsaw Summit, it seems to be admitted implicitly that NATO would not aspire to the role of first responder for the South (the term ‘contribute’ appears very often along the Warsaw Summit Declaration). However, NATO brings a unique added value of defence capacity building, demonstrating that one paramount ingredient to ensure security and stability is the strength of local forces and institutions45. In turn, the EU plays a key role by addressing the root causes of instability, in helping the South with political and socioeconomic reforms, building strong institutions, fighting corruption and focusing on civilian and non-executive military missions. However, as a successful EU Integrated Approach in the South needs security and stabilization providers, particularly in less secure areas and in low-medium intensity conflicts, the EU missions would need the protection of NATO assets. The sense of more robust cooperation between NATO and the EU is more convincing than ever before46.

NATO – EU relationship is strategic, given their complementarity in facing security challenges. Shared values as well as overlapping membership and resources, would make it unlikely for NATO and the EU to be competitors. On the contrary, they should play complementary and mutually reinforcing roles in Projecting Stability, taking into account that neither NATO nor the EU could provide by themselves the full range of the approach in the Southern Flank.

#### MENA is a tinderbox that goes global.

Chloé Berger 20, Researcher and Faculty Adviser at the NATO Defense College, "Projecting Stability to the South: NATO’s Other Challenge," NATO Defense College, Policy Brief, No. 9, pg. 1-4. May 2020, JSTOR.

In this “broader MENA” region, whose confines and internal cohesion are unstable, the challenges are ever more complex. Despite the relative consensus between NATO and its Mediterranean Dialogue (MD) and Istanbul Cooperation Initiative (ICI) partners on the deep-rooted causes of the structural instability, the potential solutions are much debated. NATO’s “Projecting Stability” concept raises as many questions with the partners, as it does within the Alliance, since a desired end-state has yet to be defined. While all efforts contributing to an increase in stability are a priori welcome, the Alliance and its partners must agree on the conditions of stability in order to identify and implement effective means suited to the local context.

Multiple challenges, increasing complexity

The “broader MENA” region has likely never known such instability since the creation of the state of Israel in 1948; all the states in the region are, to a greater or lesser extent, involved in a conflict, or challenged by grave domestic difficulties. From Sudan to Iraq, via Algeria, Lebanon or Iran, popular uprisings have sprung up, placing the very future of the states in the region into question.

Structural instability: a symptom of a state in crisis

The regimes which survived the first wave of the Arab spring seem not to have learned the lessons arising from the chaos in neighbouring Syria or Libya, and continue to use force to contain social tensions. Ageing, they no longer have the ability to respond to the basic socio-economic demands of their populations, and even less so to the aspirations of their people. In a region where half of the population is under the age of 25, demographic growth has acted as a catalyst and exacerbates the pressure put on systems which are already broken, further weakening the infrastructure and resources of the state. Whether inspired by socialism or liberal capitalism, the economies of the region are all struggling to create jobs for young people whose level of education has greatly increased since the 1970s. The State remains a major economic player, relying on revenue from hydrocarbons and tourism to support national industrial and/ or agricultural production. The scale of imports combined with the weakness of domestic production – not to mention the corruption and nepotism which undermine most of the states in the region – hamper the development of private enterprise and discourage foreign investment. And yet the region, as a whole, is in dire need of investment, particularly in the areas of health, education, transport and energy. The credibility and legitimacy of the States’ ability to meet the basic needs of the people directly depend on it, as witnessed by the slogans branded in the demonstrations in Baghdad, Tehran and Beirut, which clamour for greater integrity from their leaders, and decent living conditions. How the regimes of these countries might reform their economies to provide a future for their youth, who have gained in self-awareness as a political class, remains a central issue.

Since the mid-2000s, the region as a whole has entered into a multidimensional process of transition. The regional system, in which the first cracks appeared after the Camp David agreements (1973), no longer exists and a new order is struggling to emerge. The escalation of tensions in the Gulf at the beginning of 2020 seems to signal that red lines could easily be crossed, thereby casting doubt on the reliability of the guarantees afforded by the great powers to their allies in the region.

In addition, the construct of the nation state, resulting from decolonization, is at stake. Preserving their political and ideological heritage has been the main source of legitimacy for the regimes in place, as brought sharply into focus by the political events shaking the region since the beginning of 2019. In Algiers, Beirut, Tehran, and Baghdad, we have seen the extent to which the renewal of the political class, and a gradual opening-up to pluralism, or political change, became an existential issue for these regimes. In this context, secular forces remain largely divided when faced by a well-organized opposition able to mobilize its grass roots with the use of religious ideology. A situation characterized by disunity and violence – where states are seen as shackling individual aspirations, when they are not simply perceived as a force of oppression – is fertile ground for the development of behaviour which goes against the system, as well as for forms of political, religious, and/or sectarian radicalism, which can easily morph into violence.

Renegotiating the social contract: a costly challenge

All the states in the region must now question the fundamental issues on which their social contracts rest. Who is re-defining the forces that shape the political arena and make up the State apparatus? Who are the players powerful enough and/or legitimate enough to redefine what the national interests are, which do not always coincide with the interests of the State? The same holds true for national borders, which often leave some of their constituent communities outside their national perimeter. Implicitly, these questions relate to non-state actors in these societies and to the capacity of states to integrate them and to allow them to play a positive role. Civil society in the MENA region has been relatively resilient and has demonstrated an ability to occupy the public space by creating new forms of political expression which continue to confuse the authorities in place.

All of these examples highlight the challenges faced in (re-)defining social contracts; with the repercussions on governance, and in particular on the distribution of power between civilians and the military within government institutions. The “strong” states which had the upper hand in the 1960s and 70s continue to prioritize security over socio-economic development and individual freedoms. In states which are fragmented, the steady erosion of the state’s ability to govern hints to a redefining of governance, even to the risk of “cantonization” around large urban centres, or “city-provinces” like Cairo. What consequences will the “re-localization” of power have on traditional state responsibilities? One can easily imagine the disastrous results of a general privatization of state responsibilities – already visible in some states – and its impact on social redistribution, border control or the flows of illegal migration and organized crime. Finally, the exponential growth of demographics in the countries of the South, exacerbated by the consequences of climate change and unrestrained urban drift, inform as to the longer-term stability of these countries. The COVID-19 crisis, of which we are witnessing only the preliminary effects, demonstrates the magnitude of the challenges facing these countries in terms of human security2 . Sooner or later, the region will be forced to start transitioning its energy policies, with obvious consequences on energy security in the West. What impact will the diversification of MENA’s oil-based economies then have on their economic partners?

NATO in the South: a clearer vision and revisited approaches

While many of these issues are not new, their accumulation and entanglement constitute a challenge of unprecedented magnitude that cannot be ignored by the Alliance, given the direct and indirect repercussions on the stability of NATO members. Together with the more obvious deterrence and defence mandate, Projecting Stability has therefore become the other priority for NATO. The consequences of the conflicts in Syria and Libya in terms of migration have shown the direct impact that these forces of violence could have on maritime security in the Mediterranean, and on the capacity of European countries to host migrants. Moreover, the weakening of some states on the southern periphery of the Alliance has provided fertile ground for the rise in violent non-state actors who have demonstrated their ability to benefit from new technology. So far, we are witnessing only the first signs; in the longer term, there will undoubtedly be major health and social repercussions for which Alliance countries must be prepared.

What kind of stability for what kind of South?

Disengaging is clearly not an option and NATO must continue to closely monitor what is happening with its neighbours on the other side of the Mediterranean, in order to better anticipate developments and try as much as possible to support the processes of transition in MENA states. Denial strategies to protect our borders or delegating our security responsibilities to our partners cannot be a sustainable strategy. The complexity of the task requires a partial rethinking of our instruments, or at the very least, a questioning of NATO’s ability to tackle the issues previously described. Developing and intensifying our partnerships with other international organizations is certainly one of the best options available.

NATO’s approach to the South is the result of a collection of missions and instruments developed over the past three decades but is no longer sufficiently well structured. A more coherent vision would be useful to deconstruct a number of myths about the Alliance’s “hidden” agenda in the South, and could prove instrumental in building trust between NATO and its partners. A sense of trust which will be critical if we want to see partners taking real ownership of cooperation activities on the ground. To achieve this, and in view of the lack of consensus on the desired end-state of the projecting stability agenda, a clearer vision backed by pragmatic action and well-defined priorities would improve communication between the Alliance and its partners. Providing some public diplomacy in Arabic and engaging our partners in 1.5 track-type discussions would broaden the visibility of the Alliance among influential civil society players in the MENA region. Credibility and legitimacy remain fundamental concerns here, given the growing aspirations of the local population to take part in the decision-making process at both national and regional levels.

In addition to the issue of partners’ ownership of cooperation activities, also at stake are the legitimacy that our partner institutions enjoy in their own countries, as well as our ability to sustain these cooperative activities over time. Recent developments in Iraq should encourage us to reflect on this and question our understanding of military cooperation, especially in terms of Defence Capacity Building, and to ask whether these activities really contribute to the stability and strengthening of local institutions. Is there not a risk – through these programmes – of encouraging political authoritarianism or skewing the balance between civilians and the military? In this context, counter-terrorism operations can often be likened to counter-insurgency missions. This underscores the fact that violent extremist movements such as the Libyan and ISIS militias, and the number of Al Qaida affiliates in the Sahel, or even Hezbollah and other groups connected to Iran, are the product of a specific social context from which they draw support and can find the necessary recruits for their operations.

Interoperability as a lever of stability

These remarks underline the importance of using the appropriate terms and concepts, and more importantly, the need to agree on them. The development of a common culture of defence and security is one of the Alliance’s major achievements in terms of cooperative security with southern partners. Given the complexity of the problems plaguing the South, solutions can only be found collectively. For this reason, interoperability is the key to any effort to stabilize the MENA region. The Alliance must, therefore, continue to invest in professional military education to help partners improve the standardization of equipment and procedures, particularly in the areas of anti-missile defence, maritime security and border control. Conversely, in other areas such as drones, cyber security, energy infrastructure protection or counter-insurrection, the experience and expertise of certain partners, such as Israel, Algeria, and Mauritania, would be valued assets for the Alliance. Engaging with partners who have an intimate knowledge of the territories and local populations is fundamental to better understanding the dynamics of the underlying structural instability we face. In the mid-term, these efforts should benefit from increased activity in the NATO-ICI Regional Centre in Kuwait and from the Hub for the South in Naples.

Beyond, the Alliance would be well advised to support the development of cooperation between partners, by identifying expertise to encourage a South-South trans fer of good practices. Sharing feedback and expertise would be a first step to building trust between southern partners, and thus help them to settle a number of political disputes that currently block the construction of any kind of regional security architecture. The blockages that undermine the proper functioning of the G5 Sahel or the African Union (AU) are well known. Indeed, revising the partnership formats (MD and ICI) on a more “domain-based approach”, rather than its present geographic footing, would help to improve dialogue between partners. These initiatives could be accompanied by the opening of training and education opportunities for military offi cers and civilians from the Sahel and/or sub-Saharan nations. Instead of enlarging its efforts further to the South, the Alliance could contribute to developing local human interoperability, promoting expertise and a culture of defence common to the whole region. These opportunities should of course be coordinated with NATO members already present in these regions: formats of preferred cooperation involving nations volunteering for Mobile Training Teams (MTT) deployment there could be envisaged and could respond, in part, to the recurrent problem of resources experienced by these countries.

Normative work and cooperation with partners

A large part of the woes suffered by the South are political, socio-economic, connected to health or the environment; they are all issues for which the Alliance has only very limited answers. However, constraints linked to the nature of the responses do not condemn the Alliance to powerlessness. On the contrary, by way of example, with regard to climate change, NATO could usefully engage in some collective reflection, involving members but also partners in defining standards for equipment and procedures for the deployment of forces in hot and humid areas, or areas at high risk of natural disasters. Responses to natural disasters or pandemics3 should also be the subject of collective reflection and normative work at Alliance level.

Deepening cooperation with the European Union (EU), the United Nations, the African Union, and even with the Gulf Cooperation Council (GCC), is also a priority. Coordinating NATO and EU Trust Funds would improve the desired end effects on the ground. More generally, in post-confl ict environments, security constraints represent one of the fi rst obstacles to the deployment of personnel from civilian agencies responsible for development and reconstruction. NATO could play a useful role by providing the security conditions necessary for the deployment of these personnel or, at least, by providing them with some pre-deployment training. Deploying gendarmerie/carabinieri forces and switching progressively from a NATO to an EU format, could also enable better coordination between the various actors on the ground, allowing for a quicker restart of civilian institutions and the implementation of Disarmament, Demobilization and Reintegration (DDR) programmes. If deploying the necessary personnel proves impossible, at least gendarmerie-type training missions for local security forces could enable defence as well as policing missions to take place.

Projecting Stability, an essential vector of influence

Projecting stability to the South must remain one of the priorities of the Alliance. The challenges there are becoming increasingly complex and require collective responses, involving NATO members as well as partners in the MENA region. In a constrained budgetary period and politically sensitive context, disengagement is tempting. However, looking away would only increase the vulnerability of Alliance countries to the direct and indirect consequences of instability. Beyond the political will, the solution requires a renewed, more structured and detailed approach, focusing on cooperative actions in areas which can produce a multiplier effect and where the expertise of the Alliance can truly make a difference.

### 1AC---Plan

#### Plan: The United States federal government should reduce its alliance commitments with North Atlantic Treaty Organization member states by restricting the activation of Article V of the North Atlantic Treaty in response to attacks by non-state actors.

### 1AC---UF ADV

#### Contention 2 is Use of Force:

#### The possibility of activation of Article 5 in response to non-state actors has eroded international restraints on self-defense:

#### First, preventive war---activation muddled interpretations, lowering the threshold for use.

Vasja Badalič 20, Senior researcher at the Institute of Criminology at the Faculty of Law in Ljubljana, "The War Against Vague Threats: The Redefinitions of Imminent Threat and Anticipatory Use of Force," Security Dialogue, 07/13/2020, SAGE.

In order to redefine the concept of anticipatory armed attacks, the Bush and Obama administrations dismantled the strict criteria determining when, where and how such use of force was legitimate. In the pre-9/11 era, legal scholars and commentators relied on Webster’s formula to devise a narrow concept of imminent threat and put clear limits to the anticipatory use of force. After 9/11, however, the Bush and Obama administrations advanced a new, too-broad concept of anticipatory self-defence based on a definition of imminent threat that represented a radical departure from Webster’s formula. Both administrations ignored the traditional normative restraints to the anticipatory use of force in order to relax the rules governing the use of military force in drone warfare and ground combat operations.

This shift to a new version of anticipatory use of force created two major problems. The first problem is that the redefinition of preventive use of force in jus ad bellum provided cover for the expansion of US state power through the use of military force. By redefining the preventive use of force in jus ad bellum, the US granted itself the right to use military force against uncorroborated threats, and thus eased the restrictions for the use of force against other states. With the new definition, there is a danger that the US and other powerful states could use vague, unsubstantiated threats as a pretext to launch preventive attacks not to defend themselves but to pursue their narrow national interests (Švarc, 2006: 187–188).

The second major problem is the increased risk for civilians living in war zones. The too-broad definition of imminent threat in ground combat operations enabled US troops to be more flexible in deciding when to pull the trigger in ‘self-defence’ engagements, which led to civilians being more often put in danger of getting killed or injured (Gaston, 2017b: 7). While it is true that imminent threat determinations were always, to a certain extent, subjective, the new concept of imminent threat allowed excessive subjectivity that undermined civilian protection (IHRC, 2016: 18–21). According to Montalvo (2013: 26), the difficulties in assessing imminent threat, which was the result of the unclear meaning of the term, became a primary contributor to civilian casualties.

The redefinition of imminent threat in ground combat operations and the subsequent practices of targeting civilians provided new insights into the reasons behind violence against civilians in armed conflicts.7 Some authors – for example, Kahl (2007: 26) – observed that civilian casualties in anticipatory ‘self-defence’ incidents could be partly attributed to mistakes made by US troops due to the ‘fog of war’ (e.g. the difficulty in distinguishing civilians and combatants) and the constant stress under which the troops operated. While that was true in many cases, it is also important to acknowledge what was a more systemic source of civilian harm. As we have seen above, civilian casualties can be attributed, to a large extent, to the new concept of imminent threat that was part of a risk management strategy the goal of which was to reduce the risk for soldiers by increasing risk for civilians. Risk management strategies usually consist of force protection rules that lower the threshold for the use of military force, and, consequently, transfer the risk from soldiers to civilians (Smith, 2008: 144–145). That is what happened with the introduction of the new definition of imminent threat – killings of civilians were the result of a policy that aimed at minimizing casualties among US troops by using force protection rules that came at the expense of civilians.

Moreover, by lowering the threshold of proof to justify the preventive use of force, its redefinition in ground combat operations allowed US troops to operate with greater impunity, as, based on mere assumptions about future threats, they shot at and killed innocent civilians.

#### Second, sovereignty---the threat of intervention erodes the perception of state control.

Milena Sterio 11, Assistant Professor of Law, Cleveland-Marshall College of Law, "A Grotian Moment: Changes in the Legal Theory of Statehood," Denver Journal of International Law and Policy, Vol. 39, No. 2, 2011 pg. 222-223.

Additionally, some have advocated other forms of intervention. Richard Haass, a senior member of the George H.W. Bush administration, advocated the idea of the so-called involuntary sovereignty waiver.87 According to this theory, states waive their sovereignty in an involuntary manner, thereby inviting intervention by external actors, if they engage in three different types of reprehensible behavior. These three behaviors justifying a waiver of sovereignty on behalf of the offending state include harboring terrorism, hiding weapons of mass destruction, and abusing human rights.88 The United States-led interventions in Iraq, and more recently, Afghanistan, can certainly be explained under the first two reasons for the waiver of sovereignty: Iraq had been accused of harboring weapons of mass destruction, whereas Afghanistan has been accused of harboring terrorists.8 9 The third reason for waived sovereignty, the abuse of human rights, fits within the already existing paradigm of humanitarian intervention.

The involuntary sovereignty waiver theory represents a significant change in the traditional perception of state sovereignty and equality. According to Haass, it is up to the super powers - those super sovereign states described above - to determine when an offending state has done something egregious to involuntarily waive its sovereignty and to invite outside intervention. 90 Haass is perfectly comfortable with the idea that a country like the United States, a super power, can unilaterally decide to engage in an intervention in Afghanistan. 91 Moreover, Haass does not see the need to involve international organizations, such as the United Nations or NATO, in the decision-making process. Haass recognizes the fact that some states are more sovereign than others, but simply sees nothing wrong with it.92 To the extent that this theory prevails in international relations, it represents a true Grotian moment. Through this theory, state equality and sovereignty may have been replaced by a system of unequal power and a rule of the Great Powers. While the Great Powers have always had more clout on the world scene de facto, the Grotian Moment arising from Haass' theory is in the fact that this theory legitimizes the Great Powers rule, turning it into a serious international relations theory.

The legal theory of statehood has changed, and notions of state sovereignty and intervention on our globalized planet are vastly different today. In a Grotian Moment-like manner, globalization has chipped away at state sovereignty, and intervention has become an accepted exception to the absolute ban on the use of force against states. Statehood no longer implies that states may engage in any kind of behavior within their border without repercussions. On the contrary, it seems that certain kinds of offensive behaviors produce direct sanctions by other states.

#### Only scaling back U.S. application of Article 5 to non-state actors reverses the precedent.

Broderick C. Grady 02, J.D. University of Georgia School of Law, "Article 5 of the North Atlantic Treaty: Past, Present, and Uncertain Future," Georgia Journal of International & Comparative Law, Vol. 31, Issue 1, 2002, pg. 197-198.

At heart, Article 5 of the North Atlantic Treaty was designed to serve as a deterrent to any large-scale Soviet invasion of Western Europe. Arguably, given the breakup of the former Soviet Union, and the emergence of the United States as the world's lone superpower, Article 5 and NATO have successfully served the purpose for which they were created. Over 50 years after the drafting of the Washington Treaty, however, a new threat has emerged-the threat of terrorist attack. Although Article 5 has now been invoked in response to terrorist attack, the problems created by this invocation are many. Instead of using the powers in Article 5 directly to create a coordinated NATO response to the terrorist attacks, the United States and Great Britain have conducted a military campaign in Afghanistan largely without direct NATO assistance, and certainly without direct NATO control. The invocation of Article 5 in this case, therefore, has given an international and 'official' feeling to an essentially unilateral American-British military action. This process has revealed a deep flaw in the function of Article 5; namely, that the Article can be invoked in such a way that it places little or no added scrutiny or responsibility on a NATO member state acting in self-defense under Article 51 of the UN Charter. Indeed, the invocation seems to have been nothing more than an attempt to add an extra measure of legality or legitimacy to self-defense action under UN Article 51.

The problems associated with the invocation of Article 5 following the September 11 attacks suggest that a better solution to the terrorist problem must exist. Given the various solutions offered by the OAS"5 7 and by NATO itself, ' perhaps even those who invoked Article 5 in the wake of September11 realize that the powers given under the Article are ill-suited to military campaigns against terrorist organizations. Certainly the NATO Member States, like many other countries throughout the world, must face the reality of the terrorist threat and meet this threat in the most effective manner. Given the design and purpose of Article 5, as well as its effects, or lack thereof, following September 11, NATO should realize that Article 5 is simply not an effective tool for countering terrorism. Invocation of Article 5 should therefore be reserved for use in response to a large-scale military attack on NATO.

Certainly, the breakup of the former Soviet Union suggests that Western Europe may not face any credible large-scale military threat, which brings into focus the question of whether Article 5 has outlived its usefulness. Even if this is the case, it does not suggest that Article 5 should now be used in a manner inconsistent with its purpose and language. Leaving Article 5 intact does not harm the effectiveness of the Treaty or of the Organization. In fact, Article 5 could be looked upon as an "article of last resort," available in the unlikely event of large-scale attack, but unused and largely forgotten when the only significant threats are from terrorist groups. With any luck, NATO would never have to invoke Article 5 again.

#### An erratic, expansive justification ignites numerous hotspots, including between great powers---the threat alone is sufficient.

Stefano Recchia 16, Lecturer, International Relations, University of Cambridge, "Authorising humanitarian intervention: a five-point defence of existing multilateral procedures," Review of International Studies, Vol. 43, 08/31/2016, pg. 56-66. error edited.

In what ways, then, do existing multilateral procedures limit the negative consequences of intervention and help achieve desirable outcomes? Specifically, I ask, what impact can compliance with these procedures be expected to have on the protection of physical integrity rights? I also address two related questions: how might physical integrity rights be affected by greater consensus among policymakers, scholars, and the general public that: (a) multilateral approval is always required for humanitarian intervention or, conversely; (b) states may bypass multilateral bodies whenever they identify a situation of ‘humanitarian necessity’? Lest our answers be entirely speculative, they should rely, fundamentally, on what we know about state behaviour and foreign policy decision-making; in other words, they should be informed by the best empirical research available.

I. Reduced risk of conflict spirals among powerful states

All-out war among major powers, such as the Thirty Years’ War, the Napoleonic Wars, and the two World Wars, has dramatic and probably unparalleled implications in terms of physical integrity rights violations. Today, if a military dispute between nuclear great powers such as the United States and China, or China and Russia, spiralled out of control, it might end human civilisation. All-out war between regional rivals, such as Iran and Saudi Arabia, or Malaysia and Indonesia, could also cause unfathomable suffering and destruction.

Therefore, to the extent that multilateral rules and procedures regulating the use of force help manage international rivalries and reduce the risk of accidental war among powerful states, they can be said to have a beneficial impact on physical integrity rights. Similar arguments have been made by pluralist theorists of international society, who emphasise the importance of a strong international rule of non-intervention and of multilateral authorisation for the use of force as foundations for international order.31 They point out that over time, a procedural consensus has emerged among states about the rules that ought to govern their external behaviour, including in matters of military intervention; these rules create stable expectations among states and should not be forsaken lightly. ‘Unilateral intervention’, as Hedley Bull wrote, whether by individual states or ad hoc coalitions, ‘threatens the harmony and concord of the society of states’. 32

From a rational-choice perspective, as well, multilateral rules and decision-making procedures can function as ‘focal points’ that reduce coordination problems among powerful states. The formal institutions that embody these rules also offer a platform for states to communicate their concerns, thus increasing transparency and reducing the risk of accidental escalation.33 Allowing states to intervene without multilateral approval, when such approval is not readily forthcoming and they determine on their own that a foreign crisis has reached the threshold of ‘humanitarian necessity’, could have destabilising consequences: while state leaders tend to believe that others will share their own benign view of their state’s policy, foreigners (especially foreign adversaries) usually interpret such policies based on their pre-existing (and often hostile) images and assumptions.34 Consequently, absent multilateral validation, what appears as a humanitarian mission to some may be interpreted as an imperial war of aggression by others, fuelling security dilemmas and spirals of misperception that could heighten regional tensions and, eventually, result in major-power war.35

Compliance with the rules of positive international law, and thus approval of humanitarian interventions by the UNSC, is most likely to prevent conflict spirals and accidental escalation among powerful states. But approval by regional organisations, too, may signal benign intentions and thus help manage international tensions, especially in the following circumstances: first, when the regional organisation includes among its members dyads of potentially antagonistic states that might otherwise see their relationship deteriorate due to one state’s participation in the intervention, such as for Greece and Turkey in the case of NATO’s interventions in the Balkans (Greece had strong reservations about the US-led Bosnia and Kosovo interventions, while Turkey contributed militarily); and second, when the organisation approves a military intervention by outside powers against one of its own members, thus providing a potentially powerful counter to accusations of neo-imperialism, as in the case of Arab League-endorsed interventions by Western powers in the Arab world.

One important caveat is that to effectively signal benign intentions, intervening states not only have to secure multilateral approval; they also have to abide by the terms of the authorising resolution. If interveners blatantly exceed the available mandate, as they arguably did during the 2011 Libya intervention, this may exacerbate broader international tensions. Security Council Resolution (SCR) 1973 on Libya, adopted on 17 March 2011, provided a narrowly tailored authorisation of the use of force to ‘protect civilians and civilian populated areas under threat of attack’ and to enforce a no-fly zone over Libya. However, Washington and its allies soon shifted to a more ambitious policy of regime change, arguing that this was essential to achieve peace and secure longer-term improvements in human rights.36 Russian authorities, who had abstained on SCR 1973, felt strongly that as a result, the intervention exceeded the available UN mandate, which led to significant tensions between Moscow and the West.37

II. Reduced likelihood of self-serving interventions

Scholars and political authorities from the developing world, in particular, worry that humanitarian intervention has the ‘potential of becoming a tool for the interference by the strong in the affairs of the weak, with humanitarian considerations providing a veneer to justify such intervention’. 38 A strong case can be made that existing multilateral rules and procedures make it more difficult for powerful states to use humanitarianism as a pretext when the real purpose is something else.39

As noted, a genuine humanitarian intervention has as its primary purpose the protection of foreign nationals from manmade violence. This purpose plays a key role in making the intervention legitimate.40 The intervener’s purpose needs to be distinguished from his or her underlying motives. The purpose is what one aims at, whereas the motive is why one aims at it. Traditional Catholic just war theory was fundamentally concerned with an intervener’s inner motives, as the ultimate goal was the salvation of the soul; however, from a secular perspective, ‘pure’ or altruistic motives are not essential for legitimate humanitarian intervention. What matters is that the motives are compatible with and support the pursuit of a humanitarian objective.41

Thus, the United States might intervene in Haiti with the aim (purpose) of ending a humanitarian crisis there, and France and the United Kingdom might intervene in Libya with the same aim, but their motives for doing so could be self-interested – for example, stopping refugee flows or a desire for international prestige. Indeed, ‘mixed motives’ involving a degree of self-interest may be desirable, as they make it more likely that an intervener will marshal the resources and have the commitment necessary to bring about a positive humanitarian outcome.42

When the purpose of an intervention is entirely self-serving, the intervention cannot be called ‘humanitarian’. States might nevertheless use humanitarian rhetoric fraudulently: for example, a state might declare that its purpose is to save an ethnic or religious minority abroad, but its actual goal is to overthrow a troublesome foreign government regardless of human rights considerations, annex a particular territory, or exploit that territory’s natural resources. For instance, Russia claimed in 2008 that its military intervention in Georgia, motivated largely by neo-imperial ambitions, was justified under the Responsibility to Protect doctrine in response to an imminent threat of mass atrocities against South Ossetians.43 Similarly, in 1983, President Ronald Reagan sought to justify the US invasion of Grenada, whose main purpose was to overthrow that country’s communist government, as a new type of pro-democracy humanitarian intervention.44

To argue persuasively that contemporary multilateral rules and procedures make it more difficult for powerful states to use humanitarianism as a pretext, one would need to be able to show the following: first, these procedures are reasonably successful at exposing the fraudulent use of humanitarianism; and second, prospective interveners generally seek to comply with multilateral procedures because they expect that non-compliance can be costly.

Existing multilateral institutions and procedures can help bring to light a state’s true purpose – or, at a minimum, expose the state’s justification as unsound – in various ways. Multilateral bodies can dispatch impartial fact-finding missions and observers to the territory in question to establish whether there is evidence of massive human rights violations that might warrant a humanitarian intervention. When a prospective intervener seeks multilateral approval, it may also be required to disclose its own intelligence assessments to other member states, which will then be able to closely scrutinise the methodologies employed and related findings. Should the available evidence indicate that conditions on the ground might warrant a humanitarian intervention in principle, the prospective intervener will then need to persuade other member states that a good faith effort has been made to resolve the crisis peacefully and that it has both the capabilities and the political will to achieve a positive humanitarian outcome. When a state simply refuses to subject its policy to multilateral vetting and authorisation, this inherently raises questions about its purpose.

Political realists have traditionally doubted the ability of multilateral institutions to meaningfully influence and constrain the behaviour of powerful states. Recent research, however, indicates that even powerful states value multilateral approval for their interventions. Democracies – including most Western countries – crave multilateral approval for domestic political reasons, to satisfy groups of their own citizens that mobilise around international norms45 and to reassure sceptical legislators that the operational burden will be shared internationally.46 Even non-democracies for the most part desire multilateral approval as a way of signalling benign intentions to other states and averting potentially costly retaliation across issue areas.47

Most states most of the time cherish the international status quo and are not threatened in their survival; consequently, they are likely to intervene militarily only if they anticipate that the costs to them will be relatively low. Multilateral institutions have the ability to constrain powerful states by threatening to delegitimise, and thus increase the cost, of interventions that are not clearly in self defence and are carried out without those institutions’ approval. Because multilateral bodies are unlikely to authorise self-serving interventions and even powerful states desire multilateral approval, it seems fair to conclude that existing multilateral procedures make self-serving interventions less likely. The suggestion from some quarters that the presumption against unauthorised humanitarian warfare should be relaxed, if widely accepted, probably would make it easier for powerful states to engage in self-serving interventions masked as humanitarianism.

III. Reduced epistemic uncertainty and lower risk of accidental abuse

A related but different problem arises when a prospective intervener genuinely has a humanitarian purpose, aiming to save foreign nationals from manmade violence, but is mistaken in its judgement. For instance, the state wishing to intervene might be mistaken in its assessment of the situation on the ground, its estimate of the costs of intervention, and/or its evaluation of the likelihood of success. Such mistaken judgements can be expected to result in accidental abuse, whereby the human rights situation of the target population is unintentionally made worse.48 International deliberations aimed at securing multilateral approval, as Jürgen Habermas affirms, can limit the risk of such accidental abuse, for instance, by helping well-meaning interveners distinguish their own partial viewpoint from the ‘universalisable interests that all the other nations could share’. 49 But why should we expect that deliberation within inter-national, as opposed to merely national, fora will result in less biased assessments?

Decision-makers operating within the bureaucracies and public sphere of a particular country are especially prone to motivated biases – that is, they are likely to misjudge a situation because of powerful psychological and political forces. Research in cognitive psychology has identified a tendency for individuals and tightly integrated organisations such as national governments to reach ‘premature cognitive closure’, coming to images, beliefs, and conclusions on the basis of limited and fragmentary information, and then to interpret ambiguous or even discrepant information as confirming these beliefs.50 National bureaucracies are also prone to ‘groupthink’, which occurs when decision-making in highly cohesive groups produces a psychological drive for consensus. This inhibits the expression of internal dissent and the consideration of alternative viewpoints – reinforcing the propensity to reach decisions prematurely, based on limited evidence and preconceived notions.51

Political pressures often reinforce these psychological tendencies.52 Thus, a national leadership subject to intense domestic political pressure to ‘do something’ about a foreign humanitarian crisis may conclude after a quick review of the evidence and brief internal debate that military intervention not only would be politically advantageous but also is warranted on human rights grounds and that a positive outcome can be achieved at little cost. Once a decision has been taken to follow such a course of action, discrepant opinions within the national bureaucracy, emphasising that the distinction between local victims and aggressors may not be as clear-cut as initially thought and that the costs of intervention could be much higher, are likely to be silenced – because politically, it is disadvantageous to express public doubts about one’s favoured policy.

The requirement to seek external validation, or approval, of one’s national perspective through multilateral procedures can break through such motivated biases. First, it helps reduce epistemic uncertainty related to the existence of a just cause for intervention; second, it may result in a more accurate assessment of the likely costs of humanitarian warfare and its chances of success. Multilateral organisations provide an institutionalised platform for sharing intelligence and military assessments: when a crisis situation arises, established routines make it easier for member governments to compare and contrast the information generated by their respective national bureaucracies. In addition, multilateral bodies can gather their own information about alleged human rights violations by dispatching fact-finding missions, deploying international monitors, or setting up commissions of inquiry.53

In the case of Bosnia, for instance, the presence of UN personnel on the ground was essential in 1995 to ascertain Serb responsibility for mass atrocities in the town of Srebrenica and in the capital, Sarajevo, triggering US-led airstrikes that facilitated an end to the Bosnian war.54 In the Kosovo case in late 1998 and early 1999, the presence of international monitors was again central to determining that Serb forces had employed indiscriminate violence, this time against ethnic Albanians, thereby strengthening the hand of those who were calling for military intervention.55

For both Bosnia and Kosovo, if President Bill Clinton had not been committed to securing NATO’s approval for air strikes, the United States might have intervened much sooner, with only an ad hoc coalition of allies and under much greater uncertainty as to whether one of the parties on the ground reasonably could be termed the aggressor. On Bosnia, from the spring of 1993 onward, US ambassador to the United Nations Madeleine Albright, as well as Vice President Al Gore, National Security Adviser Tony Lake, and other senior US officials, relied on fragmentary information to advocate coercive air strikes against the Bosnian Serbs.56 Albright, in particular, dismissed evidence that the Bosnian Muslims were responsible for their own share of war crimes and insisted from early on that the United States had a moral obligation ‘to resist evil’. 57 In a secret April 1993 memo, Albright argued that given the hesitations of America’s Western European allies, the United States might have to use air power ‘unilateral[ly] … to demonstrate the commitment and will of the U.S. to prevent “ethnic cleansing”’. 58 Likewise on Kosovo, from the spring of 1998 onward, Albright (then secretary of state) and other senior US officials pushed for unilateral air strikes against Belgrade – at a time when many international observers still had doubts as to whether Serb security forces had exceeded the bounds of legitimate counterinsurgency.59

In both the Bosnia and Kosovo cases, President Clinton long held out against the entreaties of his hawkish advisers. Mindful of keeping the Atlantic alliance together and securing international legitimacy for the use of force, Clinton worked hard to forge a NATO consensus behind coercive air strikes.60 Washington’s continental European allies were reluctant to go to war against the Serbs; the Europeans were also sceptical about the ability of air power alone to achieve sustainable improvements in human rights; therefore, it seems likely that the need to bring NATO on board raised: (a) the evidentiary threshold for establishing the Serbs’ primary responsibility for violations of international humanitarian law; and (b) ensured that when NATO intervened, its members were committed to contributing the necessary resources for long-term success – including armed peacekeepers on the ground.

There are nevertheless circumstances in which multilateral procedures may fail to reduce epistemic uncertainty and thus the risk of accidental abuse. The 2011 Libya intervention, for instance, was justified (and swiftly authorised by multilateral bodies) on the basis of claims of an impending humanitarian disaster, but it is unclear whether the intervention met the jus ad bellum proportionality requirement (saving more civilians than are killed or injured as a consequence of the intervention).

After a rebel uprising in Libya in early 2011, by mid-March, forces loyal to the country’s president, Muammar Qaddafi, seemed poised to crush the anti-government forces. Qaddafi’s threat to show the rebels holding out in Benghazi, their last stronghold, ‘no mercy or compassion’, was seized upon by advocates of humanitarian intervention as evidence of the regime’s intent to commit mass atrocities – resulting in the adoption of SCR 1973.61 However, as Alan Kuperman has shown, ‘although the [Libyan] government did respond forcefully to the rebels, it never targeted civilians or resorted to “indiscriminate” force’. 62 In his warning to Benghazi’s residents, Qaddafi promised amnesty for those ‘who throw their weapons away’. 63

US defence officials have since conceded that the decision to intervene in Libya was ‘an intelligence light decision’ based on speculative claims about what might happen to civilians rather than on facts reported from the ground.64 The main advocates of military intervention in the Barack Obama administration – US ambassador to the United Nations Susan Rice, National Security Council staffer Samantha Power, and Secretary of State Hillary Clinton – may have fallen prey to motivated bias: they made up their minds quickly, relying on fragmentary evidence and extrapolating from previous experiences in Bosnia and Rwanda.65

Why did the multilateral authorisation process not help break through such bias in the Libya case? The most likely reason is that by early March, there was considerable international support for military intervention; hence the United States did not have to meet a high evidentiary threshold for proving large-scale violations of international humanitarian law. Washington’s principal European allies – notably, France and Britain – had been calling for military action for weeks; Qaddafi was unloved in the Arab world, which encouraged two regional organisations, the Gulf Cooperation Council and the Arab League, to endorse the imposition of a no-fly zone over Libya; and Russia, though sceptical, did not consider its national interests sufficiently threatened to veto the UNSC resolution.66 This suggests that, perhaps unsurprisingly, multilateral authorisation procedures are less likely to help overcome motivated bias (and thus reduce the risk of accidental abuse) when securing multilateral approval is relatively easy.

IV. Reduced moral hazard

Advocates of humanitarian intervention believe that a credible threat of international military action will often deter states from committing atrocities. If deterrence fails, actual intervention can then compel an abusive government to stop its atrocity crimes and facilitate a political solution.67 Others, however, contend that a low threshold for intervention ‘creates moral hazard that unintentionally fosters rebellion’ by encouraging armed opposition groups to deliberately provoke state atrocities in the expectation that this will trigger intervention on their behalf.68 According to a weaker form of this argument, expectations of humanitarian intervention may prolong civil wars, making rebels less prone to accept negotiated solutions because they have incentives to hold out for a better deal in the future.69 In short, the prospect of military intervention in support of anti-government opposition groups may operate much like an insurance policy, which creates moral hazard by encouraging greater risk taking on the part of its intended beneficiaries.70

The ‘moral hazard of humanitarian intervention’ argument remains contested. Two studies, in particular, find little evidence that expectations of humanitarian intervention cause substate groups to initiate violence against government forces.71 However, critics have not been able to disprove the moral hazard argument in its weaker form – namely, that the prospect of humanitarian intervention fosters escalation (rather than initiation) of rebel violence and prolongs violent rebellions by making negotiated settlements more difficult.72

In the Kosovo case, for example, in October 1998, US envoy Richard Holbrooke persuaded the Serbdominated government of Yugoslavia to end its crackdown on Kosovar Albanian civilians. Soon thereafter, as revealed by declassified documents, senior US officials determined that ‘there exists very substantial FRY [Federal Republic of Yugoslavia] compliance’ with international demands.73 But the Kosovo Liberation Army (KLA), the region’s main rebel group, had by then little interest in a negotiated compromise solution, given that earlier in the fall the Americans had explicitly threatened military action against Serb targets. Indeed, there is considerable evidence that the KLA took advantage of Serb restraint to reorganise itself, and by mid-November, it had dramatically stepped up its attacks against Serb authorities in Kosovo. According to Wolfgang Petritsch, the European Union’s envoy to Kosovo at the time, these increased attacks were clearly intended to bring about Serb retaliation, with the goal of triggering a US-led military intervention.74

Others have found that in the case of Darfur, rebels similarly prolonged the fighting in 2003–4, ‘either to take advantage of the possibility that the international community would intervene in their defence, or to obtain better peace terms under international sponsorship’. 75 Likewise, there is some indication that in the case of Libya in the spring of 2011, the prospect of international intervention emboldened antigovernment rebels to keep on fighting despite of their inferior firepower rather than seeking a negotiated settlement. In early March of that year, Qaddafi reportedly accepted international offers of mediation, yet the rebel leadership flatly rejected any possibility of negotiations.76 Kuperman concludes that the early and significant signals of support for the Libyan rebels from Britain, France, and the United States, and those countries’ growing talk of military intervention, are important factors that ‘help explain why the otherwise feeble rebels continued fighting’ at great cost to the civilian population.77

In short, one ought to take seriously the possibility that a high ex ante likelihood of military intervention in support of anti-government rebels may embolden the rebels to step up their violent activities and adopt a more intransigent stance, at the cost of increased human rights violations. How can this moral hazard be reduced without leaving civilian populations exposed to the threat of government-sponsored mass atrocities? Kuperman identifies several strategies for mitigating moral hazard: first, randomisation, which consists in ‘add[ing] uncertainty about insurance payouts, thereby lowering the insured’s incentive to take excessive risks’; 78 second, insulation from lobbying by adopting various measures to reduce the insurance provider’s exposure and vulnerability to political pressures aimed at generating a payout; and third, better regulation aimed at increasing the likelihood that payouts will be made only to those who behave responsibly.79

Current norms placing value on multilateral approval for humanitarian intervention are likely to have already reduced the problem of moral hazard. A strong argument can be made that greater consensus among scholars, pundits and policymakers that multilateral approval is always required for humanitarian intervention would help further mitigate moral hazard through all of the aforementioned mechanisms.

To begin with, the presumption in favour of requiring multilateral approval, reaffirmed by UN member states in the 2005 World Summit outcome document,80 introduces an element of ambiguity into the rules for insurance protection. It thereby contributes to randomisation, as even the most optimistic among rebels cannot expect a payout in the form of intervention to occur automatically once a certain threshold of violence has been crossed. In addition, and related to this, delegating the authorisation to multilateral bodies insulates intervention from lobbying, as persuading a single powerful government that may be easily swayed by advocacy is no longer sufficient. Finally, the presumption in favour of requiring multilateral approval results in better regulation, reducing the likelihood that payouts will be made to opposition groups that behave irresponsibly. For instance, the fact-finding missions and observers dispatched by multilateral organisations can, in theory, delegitimise a rebel group if they find that it has used anti-government violence as a deliberate instrument of provocation and/or has engaged in large-scale human rights violations of its own.

#### Each is a unique vector for nuclear escalation.

Rajesh Basrur 18, Professor of International Relations at the S. Rajaratnam School of International Studies, Nanyang Technological University, "Avoiding Nuclear Crises in Asia," RSIS Commentaries, No. 11, 2018, pg. 1-3. language edited.

Though a serious crisis has not yet occurred, the confrontations conform to patterns of events leading up to past crises between nuclear powers. These include US-Soviet crises in Berlin (1961) and Cuba (1962), Sino-Soviet border clashes in 1969, US-China fighting during the Vietnam War (1964-69), the Kargil conflict between India and Pakistan in 1999, and a second crisis between the two in 2001-02.

All of these have featured tussles over territory, differences in political systems setting democracies against authoritarian polities (including a military-dominated hybrid regime in Pakistan); hostile image construction; and the pronounced use of rhetoric and threats aimed at each other but also at reinforcing domestic support. In each case, though, the prospect of a nuclear conflagration has induced a measure of caution – avoidance of major military thrusts (notable in the considerable fighting that took place in the 1969 and 1999 crises), the opening of negotiations between the two sides, and, sometimes, explicit stabilisation agreements.

The current episodes of [brinkship] ~~brinkmanship~~ and verbal duels exhibit the same pattern. In each case, as tensions have risen, a line of communication has been opened. North Korea has expressed a willingness to talk, while – despite hesitations – the United States has done the same; and North and South Korea have attempted to build bridges by coming together at the 2018 PyeongChang Winter Olympics.

Chinese and Indian forces wound down their confrontation and their Special Representatives met in December 2017 to defuse border tensions. And the Indian and Pakistani National Security Advisers met secretly at least four times in third countries to work toward stability. These are encouraging developments, but we cannot be sanguine about their stabilizing effects.

Potential To Spin Out of Control

None of the three issues has approached resolution. North Korea and the US remain at loggerheads: the US announced on 16 January 2018 that it had deployed nuclearcapable B-52 and B-2 bombers in Guam and was preparing conventional forces for military action. Tensions remain high on the India-China border: Indian troops ejected a Chinese civilian road construction crew at Tuting in the Indian state of Arunachal Pradesh, which is claimed by China, in December 2017; and reports have come in that Chinese forces have built up their presence in Doklam.

Cross-border firing between Indian and Pakistani forces continues to exact its human toll on the LoC. In each instance, notwithstanding moves to seek stability, the political differences that raised tensions remain in place.

There are additional problems that could cause any of them to spin out of control. First, local military commanders may take initiatives, causing clashes that will be difficult to reverse. This applies not only to South Asia’s tension-ridden land borders, but also to the Northeast Asian seas. Second, a local skirmish can quickly escalate owing to uncertainty about the adversary’s capability and the element of surprise.

On land borders, the presence of radar-evading capabilities such as cruise missiles is a factor; the short distances separating India’s forces from those of China and Pakistan place serious constraints with respect to response times. At sea (and above it for air forces), the absence of clear red lines is problematic in Northeast Asia.

Third, in the event that localised conflict does break out, it may quickly morph into nuclear conflict amidst rising tensions if conventional attacks accidentally target nuclear forces or command and control systems. Finally, since all complex systems are subject to what sociologist Charles Perrow calls “normal accidents,” a false alarm of impending nuclear attack during a crisis might set off a nuclear response.

The erroneous missile alert in Hawaii on 13 January is a warning that is hardly exceptional – such incidents have occurred regularly in the past. A similar error during a crisis could conceivably set in motion a series of escalatory reactions culminating in nuclear conflict.

#### Intensified civil wars go nuclear---extinction.

Aditya Ramanathan 19, Research Analyst with the Takshashila Institution, works on issues relating strategic affairs and foreign policy focusing on nuclear weapons policy and India’s evolving posture towards to the Arctic region; Shibani Mehta is a Programme Associate with the Strategic Studies Programme, post-graduate of the S. Rajaratnam School of International Studies (RSIS, NTU); Kunaal Kini is an intern with the Takshashila Institution, “Nuclear First Use: A Critique,” Takshashila Discussion Document, 06/21/19, https://takshashila.org.in/wp-content/uploads/2019/06/TDD-Global-Nuclear-First-Use-GPM-AR-KK-2019-03.pdf

6. Climate Devastation: Even if a disarming strike was to somehow completely achieve its objectives, success could be as deadly as deadly failure. The extreme temperatures of nuclear explosions cause long-lasting and widespread fires around the blast areas. In the early 1980s, some scientists pointed out that once the black soot from these fires rises into the upper atmosphere, it blocks solar radiation, causing a “nuclear winter” resulting in catastrophic crop failures and mass starvation.14

Recent studies have estimated that even a “limited” nuclear war between India and Pakistan involving fission bombs could deplete the ozone layer and have a devastating impact on global climate.15 Indeed, the irony is that the climatic impact of limited nuclear use could far exceed the damage caused by the initial blasts and pose an existential threat to states and societies.

While some of these estimates of climatic impact are still being debated16 , it is clear that any attempt at a large-scale disarming strikes using nuclear weapons risks plunging the planet into a climate disaster. A smaller-scale nuclear war between India and Pakistan would pose an existential threat to both countries. A larger nuclear war would threaten humanity itself. These realities make bolt-from-blue strikes much less likely and in turn, reduce the imperative for pre-emptive strikes.

Deterring Conventional Forces

States can use nuclear weapons to hold at risk the conventional forces or population centres of an adversary when under military attack.

The use of nuclear weapons against conventional forces has two effects. One, the blast, heat, and radiation will damage and disrupt the adversary’s forces. Two, the use of nuclear weapons will provide a political signal to the adversary to cease military operations or risk further nuclear war. For the signal to be credible, the deterring state must retain enough nuclear forces to be able to absorb a retaliatory strike from its adversary and then hit back at the adversary’s strategic targets.

The challenges of deterring conventional forces:

1. The Threat is not credible: States seeking to deter the conventional forces of an adversary are, as Thomas Schelling put it, “manipulating the shared risk of war”.17 The deterring state may attempt to create a plausible pathway from conventional warfighting to nuclear use in the hope that this will deter the attacker. The challenge is that the deterrer has to wield the incredible threat of using nuclear weapons first.

A state deterring non-nuclear attacker has a relatively easy task since the use of nuclear weapons will primarily make the attacker worse off. If Israel’s neighbours threaten to overrun it, Israel can threaten Arab cities without fear of nuclear reprisals.

However, it is harder to deter a conventional attack carried out by a nuclear-armed attacker since the mutual rain of nuclear fire would leave both the deterrer and attacker worse off. For the deterring state, carrying out its nuclear threat would be the equivalent of an outlaw pulling the pin on a grenade when a lawman apprehends him. To make this threat seem credible, deterring states have to display a marked preference for death over subjugation.

Furthermore, when the choice at hand involves limited damage rather than subjugation or extinction, nuclear threats lose credibility. Adversaries will remain unconvinced that deterring states are going to risk nuclear escalation in a conflict fought for limited ends.

2. Assuming Intra-War Deterrence: Instead of threatening suicide by murder, states may choose to wield battlefield or theatre nuclear weapons against their adversaries. To make the use of these weapons more credible, states treat them like tools of warfighting, targeting them at the adversary’s military forces. These so-called ‘sub-strategic’ weapons are supposed to provide an intermediate rung on an escalation ladder. They promise to deliver crippling blows to the attacker’s war plans while leaving enough nuclear weapons in reserve to deter further escalation.

The problem is that such “asymmetric escalation” assumes intra-war deterrence even though the presence of nuclear weapons has already failed to prevent conflict. In reality, deterrence will be difficult to maintain once nuclear weapons have been used. Even as the mushroom clouds from the initial nuclear strikes dissipate, the attacking state’s original interests would not only remain, they could potentially expand if casualties are horrific.18 In other words, instead of killing the attacker’s risk appetite, nuclear first use may only whet it further with the desires to wreak vengeance and win back honour.

3. False Economies: Deterring powers sometimes believe they can trade in expensive manpower and materiel for nuclear weapons, especially battlefield nuclear weapons. However, deploying nuclear weapons in a war zone adds complications of its own. For one, special arrangements need to be made to safely store and transport the weapons during peacetime. Two, additional command and control systems need to be set up. Three, and most importantly, deterring states need to devote substantial conventional forces to protect battlefield nuclear weapons since they’re likely to be priority targets for an adversary.19

CASE STUDY III A.

The Problem with Using Nuclear Weapons to Deter Conventional Attacks: The Case of North Korea

While North Korea does not have a publicly articulated nuclear policy, its theory of victory is well understood.20 In the event of a major conventional war, the country’s leader Kim Jong-un would likely launch nuclear strikes against US bases in Guam and Japan while holding the US mainland at risk with his ICBM force. Kim would hope his initial strikes severely degrade American forces while the threat of an all-out nuclear exchange forces the US to de-escalate.

Unfortunately for Kim, his actions are likely to have the opposite effect by providing US decision-makers with the political cover they need to escalate. As the 2019 US Nuclear Posture Review makes clear: “There is no scenario in which the Kim regime could employ nuclear weapons and survive.”21 It is in such circumstances - after nuclear weapons have already been used - that the US will launch a devastating retaliation.

CASE STUDY III B.

The Problem with Using Nuclear Weapons to Deter Limited Threats: The Case of the United States

The latest American Nuclear Posture Review retains the option of using nuclear weapons against “non-nuclear strategic attacks”. This is widely interpreted to include large-scale cyberattacks on nuclear command and control facilities. While cyberattacks on a country’s deterrent force is serious matter, the threat of nuclear retaliation is not one the attackers are likely to believe. Besides the challenge of reliably identifying the perpetrators, nuclear retaliation against another nuclear power will cause obvious escalation problems, while using nuclear weapons against a non-nuclear power will be grossly disproportionate and may not achieve the desired goals.

Extended Deterrence

A guarantor state may choose to implicitly or explicitly extend its nuclear umbrella to the ally, enabling it to share some of the strategic benefits of a nuclear arsenal. The great question with extended deterrence is whether the guarantor state will risk its own cities to protect those of an ally.

While extended deterrence does not automatically lend itself to first use, the NATO allies of the United States – the sole country that offers a nuclear umbrella – generally believe “first use of nuclear weapons must remain in the quiver of escalation”.22

The challenges of extended deterrence:

1. Attempts to Establish Credibility Creates More Problems: Extended deterrence demands that the deterring state persuade two distinct audiences -adversaries and allies - of its willingness to defend the allies like it would defend its own people. This is a difficult task and it is natural for the deterring state to over-compensate in its attempts to persuade sceptics from both audiences.

Proposals for the United States to adopt a no first use policy are commonly countered by those who say it will achieve “the worst of all strategic worlds” because allies will believe the pledge and adversaries won’t.23

However, the same could be said about option of first use: America’s allies might believe it, but its adversaries - especially Russia and China - won’t.

To make matters worse, while the option of striking first is not credible enough to deter conventional attacks from an adversary with a secondstrike capability, it is enough to generate further tension once a crisis has begun.

2. First Use Makes the Ally a Nuclear Target: Advocates of first use argue that in extended deterrence relationships, nuclear weapons offer an alternative to painful conventional war.24 In any such conflict, the guarantor state would have two nuclear options. One, a limited nuclear strike on the adversary’s conventional forces. Two, a large-scale disarming strike that attempts to destroy the adversary’s nuclear forces. The fundamental problem with both options is that they risk nuclear retaliation against the guarantor’s allies.

The tragic reality is that once fighting breaks out, the allies of a guarantor state have to choose between conventional conflict and the risk of nuclear devastation. The choice of painless nuclear victory does not exist. Therefore, any ally that does not want to be become a sponge for nuclear strikes would do well to urge its guarantor to adopt abandon the first use option.

Advocates of nuclear first use also cite the threat of biological or chemical weapons. But it is possible to retain the nuclear option to counter the threat of large-scale biological or chemical attacks – India’s own no first use doctrine carves out such an exception.25

Similarly, if a no first use policy is interpreted as a symptom of a deteriorating alliance commitment, the guarantor state can take simple steps to reassure allies. These will include clear and consistent messaging to both allies and adversaries that reiterate the commitment to common defence, strengthening wider bilateral ties with allies, conducting regular joint military exercises, and bolstering ballistic missile defences.

CASE STUDY IV A.

Massive Retaliation, Flexible Response, and Nervous Allies

The US policy of massive retaliation, first announced in 1954, threatened nuclear responses to Soviet or Chinese attacks on American allies. However, with Soviet nuclear capabilities rising, the policy made little sense by the early 1960s. It after all, strained credulity that the US would rather be dead than see Europe turn red.

The Kennedy administration’s solution was ‘flexible response’, a policy that would provide decision makers more conventional and nuclear options including the use of tactical nuclear weapons. While the declared policy undoubtedly got Soviet attention, historical scholarship shows US leaders also used flexible response to manage politics within the NATO alliance. Tactical nuclear weapons in particular “served a fundamental political purpose” by reassuring nervous allies.26

Nervous allies made a comeback in 2016. When the Obama administration considered adopting a no first use pledge, the governments of South Korea, Japan, the UK, and France quietly voiced their opposition and helped kill the idea.27 While the objections of America’s allies appear to stem from a general concern about the credibility of the US nuclear umbrella rather than specifics of doctrine28, extended deterrence has forced the US into a more aggressive nuclear posture than it needs to secure its global interests.

Compellence

Unlike deterrence, which seeks to prevent an adversary from taking action, compellence is the use of a threat to force an adversary to change the status quo.

Nuclear compellence threatens the use of nuclear weapons. It may be used by a nuclear power against a non-nuclear power or even by one nuclear power against another.

The challenges of compellence:

1. Compellence is Harder than Deterrence: While deterrence asks adversaries to forgo something, compellence requires adversaries give up something they already possess. However, as studies have shown, “measures of willingness to accept greatly exceed measures of willingness to pay”.29 This makes compellence more difficult to achieve than deterrence in both nuclear and non-nuclear contexts.

2. Establishing Credibility & Resolve: A wide-ranging study from 2017 found nuclear compellence to be rarely successful and “uniquely difficult” whether against nuclear or non-nuclear adversaries.30 This lack of success was primarily an issue of credibility and resolve. The states seeking to compel usually had less resolve than the subjects of their compellence. Furthermore, the political, diplomatic and military costs of using nuclear weapons was so high that the threats weren’t credible.

The compelling state may choose to establish credibility and resolve through acts of nuclear violence. The sole historical case of this was the atomic bombing of Hiroshima and Nagasaki in 1945 which came with the implicit threat that many more cities would face “prompt and utter destruction” if Tokyo did not surrender. 31 While this is evidence compellence might work in rare cases, we should note that some dissenters argue that Tokyo’s decision to surrender may have been equally driven by the Soviet declaration of war on Japan, which occurred at the same time.32

In summary, the trouble with nuclear compellence is that it is only credible for a narrow band of contingencies where the target state is unable to carry out nuclear retaliation and the stakes for the compelling state are high enough to risk the political (and literal) fallout of nuclear use.

CASE STUDY V A.

Why Compellence will Remain Difficult in the Future

In the future, states seeking to compel may use a demonstrative nuclear strike to establish their credibility early on. The political scientist Paul Bracken imagines an intense conflict between Israel and Iranian proxies. To compel Iran to cease support for the fighters, Israel detonates a nuclear weapon 30,000 metres over Tehran. The resulting explosion “would shatter windows in downtown Tehran,” but cause few casualties.33

Some also see the combatants in a conflict using nuclear depth charges to target submarines. Underwater explosions far from civilians would make it easier to break the nuclear taboo while delivering a compellent signal to an adversary.34

While such actions may offer more credible nuclear threats, they suffer problems of their own. One, detonating a nuclear device is an extreme measure with unpredictable consequences (including radiation fallout from high altitude explosions). Two, when used against other nuclear powers, it would run the same risks of uncontrolled escalation as the strategies of North Korea and Pakistan. (Indeed, the risks would be greater if the adversary did not anticipate such actions as part of a deterrence posture.) Three, when used against a non-nuclear adversary, it will likely entail high diplomatic costs.

Preventive Strikes

A nuclear power may seek to deny another state nuclear weapons capability by striking those facilities with its own nuclear weapons. In such a preventive nuclear strike, nuclear weapons would be used to destroy infrastructure related to a state’s nuclear programme.

The challenges of preventive strikes:

The key problem with using nuclear weapons against another country’s nuclear facilities is that it offers few military benefits while carrying high diplomatic costs.

The extensive infrastructure needed to make nuclear weapons is vulnerable to conventional military action. Military saboteurs destroyed the Norwegian heavy water plant in 1944, Israeli jets knocked out an Iraqi nuclear reactor in 1981, and later, one in Syria in 2007.35

In the early 1960s, the US considered attacks on China’s nuclear weapons programme largely using conventional means. While American planners also looked the possibilities of using tactical nuclear weapons, this was primarily because they lacked the precision guided conventional munitions of today. 36

Recognising this vulnerability to conventional weapons, states like Iran have buried their uranium enrichment facilities deep underground.37 In turn, the US has considered with the idea of a ‘robust nuclear earth penetrator’ to take them out.

However, the case for nuclear bunker busters suffers from the same problems of low military utility and high diplomatic costs. Conventional weapons like the Massive Ordnance Penetrator can do the much the same job as nuclear weapons, while the radioactive fallout from a ground bursting nuclear bunker buster will be large, inflicting international opprobrium on the US.38

Finally, using nuclear weapons to destroy another country’s nuclear programme could also make the problem more intractable in the long run. Any nuclear destruction is only likely to convince the populace and elites of the target country they need nuclear weapons of their own at any cost.

Civil War and Conquest

The world is fortunate to have not yet seen an “Atomic Hitler” willing to unleash nuclear weapons to conquer territory, target the population concentrations of specific ethnic groups, or suppress internal rebellion. Future despots may see utility in detonating a nuclear device over a rebellious city as a deterrent to others. Warlords in a failed nuclear state might decide to use nuclear weapons against enemy factions. And state leaders could decide a few nuclear detonations would aid the conquest of another state.

#### Pseudo-offensive doctrine causes a return to global gunboat diplomacy, especially by Russia, Turkey, and Columbia.

Patrick C. R. Terry 19, Dean of the faculty of law at the University of Public Administration in Kehl, Germany, "The Return of Gunboat Diplomacy: How the West Has Undermined the Ban on the Use of Force," Harvard National Security Journal, Vol. 10, No. 1, pg. 78-80, 2019, HeinOnline. error edited.

This article explores how the "West," the main creator of modem international law after WWII, is now, nevertheless, steadily undermining it. While purporting to be reemphasizing each state's right to defend itself and elevating the protection of human rights, the West is, in truth, rendering the far-reaching ban on the use of force envisaged in the U.N. Charter ineffective, thereby paving the ground for a return to 19th century gunboat diplomacy.1 This new age of international law is marked by the use of force no longer being governed by the rule of law, but rather almost exclusively by the raw power of states-a fact western politicians attempt to conceal by issuing dubious, often hypocritical, but well-sounding statements. These states have abandoned the-perhaps utopian-goal of realizing the principle of sovereign equality and are increasingly replacing it with an aggressively hierarchical order of states reminiscent of the colonial era of the 19th century.

Seemingly disparate western forces are eroding the ban on the use of force: right-wing interventionists-predominantly, but not exclusively-to be found in the United States, and so-called liberals spread across the West. Common to both approaches is the argument that international law is steadily and necessarily evolving to adapt to developments in the modem world.

There are supposedly stark differences between right wing and liberal approaches to international law. Right-wing interventionists tend to be quite open about their disdain for international law, sometimes even claiming that law does not and/or has never governed international relations and that outcomes are ultimately the result of the involved states' relative power.2 Others, such as Michael Glennon, do accept that international law has a role to play in foreign affairs, but argue that its rules should flexibly adjust to the major powers' relative strength.3 Furthermore, right-wing interventionists tend to focus their arguments on the rules governing the use of force while the liberals' reforming zeal is generally broader.

The liberal approach tends to emphasize its strict adherence to the rule of law in international affairs. Liberals, however, often argue that international law, especially customary international law, is evolving under the influence of international human rights law. It is no longer the state, but the individual human being that is becoming and should become the focus of international law.4 This has allegedly led to the emergence of a right to intervene abroad on humanitarian grounds. More extreme advocates of the liberal strand of thought have even justified interventions in order to install/reinstate a "democratic" government. At this point, some liberal and right-wing scholars have in fact found limited common ground, as this argument can readily serve to justify the right-wing interventionists' general "regime change" agenda in "rogue states."

This article will show both strands of thought to be similarly harmful to the international rule of law. Both necessarily require the acceptance of a hierarchy of states, based on their relative power, and both rely on the United States' alleged exceptionalism as leader of the Free World and the West's unparalleled strength following the Eastern Bloc's collapse in the early 1990s. Since then, the widespread assumption has been that only the United States and its close allies could retain the capabilities to rely on more generous rules permitting the use of force.

As we near the end of the second decade of the 21st century, this blase attitude towards the rest of the world has turned out to be misplaced. Rather, countries as diverse as Russia, Saudi Arabia, Colombia, and Turkey have increasingly come to rely on ever-expanding exceptions to the ban on the use of force first advocated by the West. Consequently, we are witnessing a return to gunboat diplomacy: states that feel powerful enough to intervene forcefully in another state's internal affairs will do so and claim justification based on the often ill-defined and ill-advised rules that right-wing interventionists and liberals have tried to impose. The rule of law is thus again being replaced by the Darwinian principle of the "survival of the fittest." Meanwhile, we are steadily approaching the point Glennon claims we have already passed,5 whereby the jus ad bellum has become indeterminate, meaning that few, if any, constraining rules on the use of force remain.

Recent developments illustrate this: the United States did not even bother to put forward a serious legal argument to justify its attacks on Syrian forces in 2017 and 2018 in retaliation for their alleged use of chemical weapons. The frequent recourse to force irrespective of international law, as practiced by western and, increasingly, other states has led to a widespread increase in spending on defensive and offensive capabilities. States wish to protect both their sovereignty and standing in the new hierarchy of states, and many of them have presumably come to the same conclusion as India already had in 2003, following the United States' and the U.K.'s unlawful attack on Iraq: disagreement with the United States requires the possession of nuclear weapons.6

The article will focus on the two areas of the law on the use of force where the effect of western thought has contributed to the serious weakening of legal structures. First, I will examine the erosion of the law on self-defense in some detail, before subsequently turning to the attempts to justify the use of force in other cases, notably during humanitarian crises. I will first outline the arguments in support of an expansive view of the right to resort to force before assessing them according to the U.N. Charter, the jurisprudence of the International Court of Justice (hereinafter ICJ) and traditional customary international law. This will be followed by an expose of state practice and opinio juris. Finally, a brief conclusion will summarize the current state of affairs.

This analysis will demonstrate that successive attempts at "modernizing" international law are in danger of dismantling the safeguards against war and of recreating a world in which a few privileged states can attempt to impose their will on the rest. The logic of an ever-expanding concept of justified military action self-evidently reveals a hierarchal view of the international community: only the wealthy and privileged western states and their close allies should benefit from such generous rules. It was never in the West's interest that other states, such as Russia, China, or India should invoke an expansive view of the right to use force. However, as recent developments illustrate, the West has miscalculated; its power is no longer sufficient to stop other states from exploiting its dubious precedents.

#### Nagorno-Karabakh goes nuclear

Alexander Zhelenin & Pavel Felgenhauer 20, Александр Желенин, Zhelenin is a reporter for Rosbalt; Павел Фельгенгауэр, Felgenhauer is a military expert specializing in Russian military policy in the Caucasus, “Если придется, Россия спасет Армению ядерным ударом,” or, “Russia will defend Armenia with a nuclear strike, if necessary,” Rosbalt, 7/29/20, <https://www.rosbalt.ru/world/2020/07/29/1856219.html> , Translated by Truf & Yandex

\*\*\*ORIGINAL\*\*\*

Турция фактически ввела войска на территорию Нахичеванской автономной республики — это эксклав Азербайджана, который от основной территории страны отделяют Армения и непризнанный Нагорный Карабах. Официально это сделано под предлогом совместных турецко-азербайджанских военных учений, который начались 29 июля.

Однако учитывая, что эти маневры пройдут в момент обострения армяно-азербайджанского конфликта, что Турция в нем традиционно на стороне Азербайджана, а Ереван — член Организации договора о коллективной безопасности (ОДКБ), основным звеном которой является Россия, уже звучат опасения, что все это может закончится очередным, на этот раз гораздо более масштабным, российско-турецким столкновением.

Военный эксперт Павел Фельгенгауэр, с которым обозреватель «Росбалта» обсудил эту тему, не исключает втягивания в такую войну НАТО с дальнейшим катастрофическим развитием событий.

— На ваш взгляд, проведение в нынешней накаленной обстановке совместных военных учений турецкой и азербайджанской армий на территории Нахичевани, это демонстрация моральной поддержки Баку в армяно-азербайджанском конфликте или президент Турции Реджеп Эрдоган всерьез готов выступить в нем на стороне Баку?

 — Ничего себе моральная поддержка! И Эрдоган, и его министр обороны говорят о том, что будут драться на стороне Азербайджана, если что. Таким образом они обозначают свою позицию, которая, впрочем, всегда была такой. Тут возникает ряд проблем, в том числе, касающихся статуса Нахичевани, обозначенного Московским договором 1921 года между Турецкой республикой и Советской Россией. Сейчас турки говорят, что если у Азербайджана начнутся проблемы, то они могут вмешаться и это вмешательство может быть очень серьезным.

— Что в случае такого вмешательства Турции будет делать Россия?

 — Конечно, такое развитие событий грозит войной с Москвой — в этом случае Россия будет защищать Армению от турок. Для этого в Гюмри и находится наша военная база.

— Да, ведь если Москва в подобном случае не будет защищать Армению, то тогда встает вопрос, а зачем вообще существует ОДКБ, членом которого является, в том числе, и Ереван…

— Нет, речь идет не конкретно об ОДКБ — это все фикция, потому что ни Киргизия, ни Казахстан, ни Таджикистан или Белоруссия, входящие в эту организацию, воевать в Закавказье не будут ни при каких обстоятельствах. ОДКБ — это ведь не НАТО, где даже Черногория посылала несколько своих солдат на последние большие учения Альянса Trident Juncture («Единый трезубец»). Белорусская конституция, например, запрещает воевать армии этой страны за пределами ее территории. Среднеазиатские республики, состоящие в ОДКБ, тоже не собираются воевать в Закавказье. Иначе говоря, это дело касается только Армении и России, а другие участники ОДКБ в случае чего будут оказывать им главным образом моральную поддержку.

При этом российские войска, которые находятся в Армении, не совсем российские — процентов на 90 по личному составу они армянские. Старая имперская традиция — нанимать для службы местных. Это просто дешевле выходит, чем возить самолетами из России контрактников.

В любом случае, там всего одна мотострелковая бригада, около четырех тысяч человек. Помимо этого, там есть еще наш авиационный отряд с МиГ-29, зенитно-ракетные комплексы. Но в целом это достаточно символическая боевая сила по сравнению с находящейся на другой стороне границы 3-й полевой армией Турции.

Возможности усиления нашей группировки там достаточно ограничены, потому что в случае чего придется пробиваться через Грузию. А грузины могут не пустить, и тогда придется с боями проходить их территорию… Можно, конечно, подвозить подкрепления по воздуху. Но воздушным путем танковые и мотострелковые бригады перебрасывать сложно. Кроме того, у турок тоже очень мощная современная авиация.

В общем, при развертывании там военных действий, турки снесут и армянские, и российские силы, находящиеся в Армении. Но это будет означать войну с Россией, которая в таких условиях может прибегнуть к силам ядерного сдерживания — в соответствии с нашей оборонной доктриной.

— Пойдет ли Москва на такой рискованный шаг?

— Может и пойти. Нанесет, например, демонстрационный удар по горной местности, где никого нет, или по какой-нибудь базе в Анатолии, чтобы показать, что мы к этому готовы. Но, с другой стороны, это уже будет война со всем НАТО.

Ситуация достаточно серьезная, и обостриться она может в один момент. Переход турецко-азербайджанской границы турецкими войсками для участия в этих маневрах — это очень серьезная эскалация, которая в худшем варианте потенциально в довольно сжатые сроки может привести к ядерной войне. Впрочем, если полномасштабной войны между Азербайджаном и Арменией не случится, то и Турция в нее вмешиваться не будет. Всегда можно отыграть назад.

\*\*\*TRANSLATION\*\*\*

Turkey has actually sent troops to the territory of the Nakhchivan Autonomous Republic-an exclave of Azerbaijan, which is separated from the main territory of the country by Armenia and the unrecognized Nagorno-Karabakh. This was officially done under the pretext of joint Turkish-Azerbaijani military exercises, which began on July 29.

However, given that these maneuvers will take place at a time of aggravation of the Armenian-Azerbaijani conflict, that Turkey is traditionally on the side of Azerbaijan in it, and that Yerevan is a member of the collective security Treaty Organization (CSTO), of which Russia is the main link. There are already concerns that all this may end in another, much larger Russian-Turkish clash.

Military expert Pavel Felgenhauer, with whom the Rosbalta columnist discussed this topic, does not rule out drawing NATO into such a war with a further catastrophic development of events.

— In your opinion, holding joint military exercises of the Turkish and Azerbaijani armies on the territory of Nakhichevan in the current tense situation is a demonstration of moral support for Baku in the Armenian-Azerbaijani conflict, or is Turkish President Recep Erdogan seriously ready to take Baku's side in it?

You call that moral support! Both Erdogan and his defense Minister say that they will fight on the side of Azerbaijan if anything happens. This is their way of publicly clarifying their position, which remains unchanged. This raises a number of problems, including as it relates to the status of Nakhichevan, which was defined by the Moscow Treaty of 1921 between the Republic of Turkey and Soviet Russia. Now the Turks say that if Azerbaijan starts having problems, they can intervene and this intervention can be very serious.

— What will Russia do if Turkey intervenes in this way?

Such a development would, of course, threaten war with Moscow — in this case, Russia will protect Armenia from the Turks. This is why our military base is located in Gyumri.

— Yes, because if Moscow does not protect Armenia in such a case, then the question arises, why does the CSTO exist at all, of which Yerevan is also a member…

No, we are not talking specifically about the CSTO — this is all a fiction, because neither Kyrgyzstan, nor Kazakhstan, Tajikistan or Belarus, which are all members of this organization, will fight in Transcaucasia under any circumstances. The CSTO is not NATO, where even Montenegro sent several of its soldiers to the last major exercises of the Trident Juncture Alliance. The Belarusian Constitution, for example, prohibits its army from fighting outside its territory. Central Asian republics that are members of the CSTO are also not going to fight in Transcaucasia. In other words, this case concerns only Armenia and Russia, and the other CSTO members will mainly provide them with moral support.

At the same time, the Russian troops that are in Armenia are not exactly Russian — they are 90% Armenian in terms of personnel. It's an old Imperial tradition to hire locals for service. It's just cheaper than flying contract workers from Russia.

In any case, there is only one motorized rifle brigade, about four thousand people. In addition, there is also our aviation detachment with MiG-29 anti-aircraft missile systems. But in general, this is a symbolic fighting force compared to Turkey’s 3rd field army located on the other side of the border.

The options for strengthening our troops there are quite limited, because if something happens, we will have to fight our way through Georgia. The Georgians may not grant us passage, in which case we will have to fight through their territory… we can, of course, bring reinforcements by air, but it is difficult to transfer tank and motorized rifle brigades by air. In addition, the Turks also have a very powerful and modern air force.

In general, if military operations are initiated, the Turks will demolish both Armenian and Russian forces located in Armenia. But this would mean a war with Russia, which in such circumstances can result in nuclear use, in accordance with defense doctrine.

— Will Moscow take such a risky step?

It might. For example, it could launch a demonstration missile at a mountainous area where no one lives, or at some base in Anatolia, to show that we are ready for this. On the other hand, such a move would result in a war involving all of NATO.

The situation is quite serious and can escalate instantaneously. The crossing of the Turkish-Azerbaijani border by Turkish troops to participate in these maneuvers is a very serious escalation, which in the worst-case scenario could potentially lead to a nuclear war within a fairly short time frame. However, if a full-scale war between Azerbaijan and Armenia does not happen, then Turkey will not interfere. Any losses can always be recouped.

#### Columbian attacks spark deadly LA instability.

Francisco Toro 19, Political commentator and contributing columnist for Global Opinions, "Armed conflict between Venezuela and Colombia is now a real, and terrifying, possibility," Washington Post, 09/12/2019, ProQuest.

BOGOTA, Colombia — Thinking up ways our all-encompassing crisis could get even worse has become a grimly popular parlor game for Venezuelans. For years, the go-to worst-case scenario was civil war between the political factions in our country. These days, an even scarier prospect has begun to displace that in the pantheon of Venezuelan nightmares: armed conflict with Colombia.

The reason? Venezuela's increasingly tight alliance with the drug-running guerrilla armies waging war on the Colombian state, which has rattled Bogota so hard it's now seeking a hemispheric response.

On Wednesday, Colombia, the United States and nine other countries invoked the Inter-American Treaty of Reciprocal Assistance (TIAR), signed in Rio de Janeiro in 1947, which commits the countries of the Western Hemisphere to respond to military aggression against any one of them. The move came after Nicolás Maduro said he would deploy 150,000 troops to the border with Colombia. Invoking TIAR is an extreme measure in the region and an unmistakable sign that armed conflict is now a real possibility.

For some time, security analysts in Bogota have been alarmed by Caracas's embrace of ELN — the Cuban-backed National Liberation Army that for decades played second fiddle to the Soviet-inspired Revolutionary Armed Forces of Colombia, or FARC. But the recent announcement by top FARC leaders that they are returning to war made a tense situation much worse, creating the prospect of multiple forces within Colombia acting as Venezuelan proxies.

For more than a decade, Venezuela has served as a friendly safe space for Colombia's various leftist rebel guerrillas. Colombian rebels used Venezuela as a rear-guard, a place where their soldiers could go for R & R, for medical treatment or for training. Gradually, they expanded their operations in the country, using it as a conduit for drugs for export and running extortion rackets in Venezuelan territory.

But the depth of cooperation between Venezuela and Colombian rebels seems to have ballooned this year, as the Venezuelan state shifts from tolerating them to treating them as allies in a common fight.

Venezuelan intelligence documents leaked to Colombian newsweekly Semana recently paint the most troubling picture yet, portraying Venezuela's relationship to Colombian "red groups" as something close to Iran's relationship with Hezbollah. Colombia's rebels aren't just tolerated in Venezuela; they're actively trained and armed there, including in the use of enormously dangerous weapons such as high-tech Russian shoulder-mounted antiaircraft missiles.

The documents leaked to Semana imply Venezuela is mainstreaming ELN and the resurgent FARC into its intelligence systems, relying on the groups to help identify high-value military targets inside Colombia. Pointedly, Colombia said FARC's video announcing a return to violence was shot inside Venezuela.

For a Venezuelan leadership that's increasingly paranoid about outside threats, this alliance with Colombia's rebels offers obvious benefits, strengthening its negotiating hand by enabling it to make credible threats to destabilize Colombia. For the rebel groups themselves, the benefits are just as obvious. Venezuela provides everything they need to become impossible for Colombia to defeat: territory, extortion opportunities, drug routes, training, weapons.

For Colombia, this state of affairs threatens to become simply intolerable. Some of the grimmest scenarios hardly stretch the imagination. Say, for instance, Colombia's intelligence learns of a guerrilla cell in Venezuela training for a major attack in Bogota: The case for a preemptive strike could quickly prove overwhelming. To be sure, it wouldn't be the first time Colombia has struck guerrillas in a neighbor's territory.

For years, Venezuela watchers have been muttering that the country's collapse was bound to destabilize the region one way or another. Now, the shape that destabilization is likely to take is beginning to come into focus.

To be sure, no sane Venezuelan leader could want an armed conflict that pits Venezuela's shambolic, underfed recruits against Colombia's much-better-armed, trained and battle-hardened fighters. It's not a winnable proposition.

But the presence of the guerrillas complicate any calculation: Venezuela wouldn't have to launch an invasion to get its forces into Colombia — its guerrilla allies are already there. Those same guerrillas multiply the potential for mistakes, miscalculations and accidents that could easily set off an escalation none of the players can bring under control.

Latin America isn't prepared for the dynamic taking shape along the Venezuela-Colombia border. The region hasn't witnessed serious interstate conflict since the 1930s. Venezuela's wholehearted embrace of Colombia's narco-revolutionaries is creating conditions for a kind of clash the region has no memory of.

#### Goes nuclear.

Eric Lindsey & Andrew F. Krepinevich 14. Krepinevich, Jr. is the President of the Center for Strategic and Budgetary Assessments; Lindsey is an analyst at the Center for Strategic and Budgetary Assessments (CSBA). 01-09-14. “Hemispheric Defense in the 21st Century.” CSBA. https://csbaonline.org/research/publications/hemispheric-defense-in-the-21st-century

As the previous chapter demonstrates, for the past two hundred years the principal cause of concern for U.S. defense policymakers and planners thinking about Latin America has been the prospect that great powers outside the Western Hemisphere could exploit the military weakness and internal security challenges of the states within it to threaten U.S. security. While there is reason for optimism about the future of Latin America,58 there is also cause for concern. The region faces enduring obstacles to economic59 and political development60 as well as signi􀂿cant internal security challenges. As General John Kelly, the commander of U.S. Southern Command (SOUTHCOM)61 noted in his March 2013 posture statement before Congress, Latin America: 􀀾I􀁀s a region of enormous promise and exciting opportunities, but it is also one of persistent challenges and complex threats. It is a region of relative peace, low likelihood of interstate con􀃀icts, and overall economic growth, yet is also home to corrosive criminal violence, permissive environments for illicit activities, and episodic political and social protests.62 The instability and non-traditional security challenges that General Kelly cites provide potential opportunities for the United States’ major rivals to (borrowing a term from Monroe’s declaration) “interpose” themselves into the region and, by so doing, threaten regional stability and U.S. security. Two discernible trends suggest that current and prospective Eurasian rivals could seek to exploit regional conditions and dynamics in ways that could impose immense costs on the United States and divert its attention from more distant theaters overseas. The first trend is a return to a heightened level of competition among the “great powers” following two decades of U.S. dominance. The second trend concerns the growing cost of projecting power by traditional military means due to the proliferation of “anti-access/area-denial” (A2/AD) capabilities in general, and precision-guided munitions (PGMs) in particular. These trends suggest that, despite a possible decline in relative U.S. power, external forces will continue to 􀂿nd it beyond their means to threaten the hemisphere through traditional forms of power projection. Far more likely is a return of a competition similar to that which the United States engaged in with the Soviet Union during the Cold War. During that period both powers sought to avoid direct con􀃀ict with the other, given the risks of escalation to nuclear con􀃀ict. Instead each focused primarily on gaining an advantage over the other through the employment of client states and non-state groups as proxies. Proxies were employed for reasons other than avoiding a direct clash, such as gaining positional advantage (e.g., enabling the sponsor to establish bases in its country, as the Soviets did in Cuba). Proxies were also employed as a means of diverting a rival’s attention from what was considered the key region of the competition and to impose disproportionate costs on a rival (e.g., Moscow’s support of 􀀱orth Vietnam as a means of drawing o􀌆 U.S. resources from Europe). This chapter outlines trends in the Western Hemisphere security environment that outside powers may seek to exploit to advance their objectives in ways that threaten regional stability and U.S. security. This is followed by a discussion of how these external powers might proceed to do so. Seeds of Instability Crime, Illicit Networks, and Under-Governed Areas Latin America has a long history of banditry, smuggling, and organized crime. As in the case of Pancho Villa and the 1916-1917 Punitive Expedition, these activities have occasionally risen to a level at which they in􀃀uence U.S. national security calculations. Rarely, however, have these activities been as pervasive and destabilizing as they are today. Although a wide variety of illicit activity occurs in Latin America, criminal organizations conducting drug tra􀌇cking are the dominant forces in the Latin American underworld today, accounting for roughly 􀀇􀀗0 billion per year63 of an estimated 􀀇100 billion in annual illicit trade.6􀀗 Since the Colombian cartels were dismantled in the 1990s, this lucrative trade has been dominated by powerful Mexican cartels whose operations extend across the length and breadth of Mexico, as well as up the supply chain into the cocaine-producing regions of the Andean Ridge and through their wholesale and retail drug distribution networks across the United States.65 The cartels, along with countless smaller criminal organizations, comprise what the head of SOUTHCOM has described as, 􀀾a􀁀n interconnected system of arteries that traverse the entire Western Hemisphere, stretching across the Atlantic and Paci􀂿c, through the Caribbean, and up and down 􀀱orth, South, and Central America . . . 􀀾a􀁀 vast system of illicit pathways 􀀾that is used􀁀 to move tons of drugs, thousands of people, and countless weapons into and out of the United States, Europe, and Africa with an e􀌇ciency, payload, and gross pro􀂿t any global transportation company would envy.66 That being said, the drug tra􀌇cking underworld is by no means a monolithic entity or cooperative alliance. Rather, it is a fractious and brutally competitive business in which rival entities are constantly and literally 􀂿ghting to maximize their share of the drug trade and for control of the critical transshipment points, or plazas, through which it 􀃀ows. To attack their competitor’s operations and protect their own operations from rivals and the Mexican government’s crackdown that began in 2006, the cartels have built up larger, better armed, and more ruthless forces of hired gunmen known as sicarios. Using the billions of dollars generated by their illicit activities, they have acquired weapons and equipment formerly reserved for state armies or state-sponsored insurgent groups, including body armor, assault ri􀃀es, machine guns, grenades, landmines, anti-tank rockets, mortars, car bombs, armored vehicles, helicopters, transport planes, and—perhaps most remarkably—long-range submersibles.67 The cartels’ pro􀂿ts have also enabled them to hire former police and military personnel, including members of several countries’ elite special operations units68 and, in several cases, active and former members of the U.S. military.69 These personnel bring with them—and can provide to the cartels—a level of training and tactical pro􀂿ciency that can be equal or superior to those of the government forces they face. As a result of this pro􀂿ciency and the military-grade weapons possessed by the cartels, more than 2,500 Mexican police o􀌇cers and 200 military personnel were killed in confrontations with organized crime forces between 2008 and 2012 along with tens of thousands of civilians.70 In the poorer states of Central America, state security forces operate at an even greater disadvantage.71 While their paramilitary forces enable the cartels to dominate entire cities and large remote areas through force and intimidation, they are not the only tool available. The cartels also leverage their immense wealth to buy the silence or support of police and government o􀌇cials who are often presented with a choice between plata o plomo—“silver or lead.” According to the head of the Mexican Federal Police, around 2010 the cartels were spending an estimated 􀀇100 million each month on bribes to police.72 By buying o􀌆 o􀌇cials—and torturing or killing those who cannot be corrupted—the cartels have greatly undermined the e􀌆ectiveness of national government forces in general and local police in particular. This, in turn, has undermined the con􀂿dence of the population in their government’s willingness and ability to protect them. Through these means and methods the cartels have gained a substantial degree of de facto control over many urban and rural areas across Mexico, including major cities and large swathes of territory along the U.S.-Mexico border. In many of these crime-ridden areas the loss of con􀂿dence in the government and police has prompted the formation of vigilante militias, presenting an additional challenge to government control.73 Meanwhile, in the “northern triangle” of Central America (the area comprising Guatemala, Honduras, and El Salvador through which the cartels transship almost all cocaine bound for Mexico and the United States) the situation is even more dire. Approximately 90 percent of crimes in this area go unpunished, while in Guatemala roughly half the country’s territory is e􀌆ectively under drug tra􀌇ckers’ control.7􀀗 Further south, similar pockets of lawlessness exist in coca-growing areas in Colombia, Venezuela, Ecuador, Peru, and Bolivia. In Colombia and along its borders with Venezuela, Ecuador, and Peru, much of the coca-growing territory remains under the control of the Revolutionary Armed Forces of Colombia, or FARC. A guerrilla organization founded in the 1960s as a Marxist-Leninist revolutionary movement dedicated to the overthrow of the Colombian government, the FARC embraced coca growing in the 1990s as a means of funding its operations and has subsequently evolved into a hybrid mix of left-wing insurgent group and pro􀂿t-driven cartel.76 This hybrid nature has facilitated cooperation between the FARC and ideological sympathizers like the Bolivarian Alliance, Hezbollah, Al Qaeda in the Islamic Maghreb, and other extremist groups77 as well as with purely criminal organizations like the Mexican cartels. Although the FARC has been greatly weakened over the past decade and no longer poses the existential threat to the Colombian government that it once did, it remains 􀂿rmly in control of large tracts of coca-producing jungle, mostly straddling the borders between Colombia and FARC supporters Venezuela and Ecuador. In summary, organized crime elements have exploited under-governed areas to establish zones under their de facto control. In so doing they pose a signi􀂿cant and growing threat to regional security in general and U.S. interests in particular. As SOUTHCOM commander General Kelly recently observed: 􀀾T􀁀he proximity of the U.S. homeland to criminally governed spaces is a vulnerability with direct implications for U.S. national security. I am also troubled by the signi􀂿cant criminal capabilities that are available 􀀾within them􀁀 to anyone—for a price. Transnational criminal organizations have access to key facilitators who specialize in document forgery, trade-based money laundering, weapons procurement, and human smuggling, including the smuggling of special interest aliens. This criminal expertise and the ability to move people, products, and funds are skills that can be exploited by a variety of malign actors, including terrorists.78 Hezbollah and the Bolivarian Alliance Hezbollah in Latin America 􀀱on-state entities recognized by the U.S. as terrorist organizations also operate in the region, most notably Lebanon-based Hezbollah, an Iranian client group. Hezbollah maintains an active presence in the tri-border area (TBA) of South America— the nexus of Argentina, Brazil, and Paraguay—stretching back to the 1980s. The TBA has traditionally been under-governed and is known by some as “the United 􀀱ations of crime.”79 Eight syndicate groups facilitate this activity in South America’s so-called “Southern Cone,” overseeing legitimate businesses along with a wide range of illegal activities to include money laundering, drug and arms traf- 􀂿cking, identity theft and false identi􀂿cation documents, counterfeiting currency and intellectual property, and smuggling. 􀀱ot surprisingly they are linked to organized crime and to non-state insurgent and terrorist groups, such as the FARC.80 Estimates are that over 􀀇12 billion in illicit transactions are conducted per year, a sum exceeding Paraguay’s entire GDP by a substantial amount.81 Hezbollah achieved notoriety in the region in 1992 when it bombed the Israeli embassy in Argentina. This was followed with the bombing of the AMIA Jewish community center in Buenos Aires two years later. Like many other terrorist organizations, as Hezbollah expanded it established relationships with drug cartels82 that it supports in a variety of ways. For example, the cartels have enlisted Hezbollah, known for its tunnel construction along the Israeli border, for help in improving their tunnels along the U.S.-Mexican border. In 2008, Hezbollah helped broker a deal in which one of Mexico’s major drug cartels, Sinaloa, sent members to Iran for weapons and explosives training via Venezuela using Venezuelan travel documents. 83 As the locus of the drug trade and other illegal cartel activities moved north into Central America and Mexico, Hezbollah has sought to move with it with mixed success. In October 2011, Hezbollah was linked to the e􀌆orts of an Iranian-American to conspire with Iranian agents to assassinate the Saudi ambassador to the United States. The plot involved members of the Los Zetas Mexican drug cartel.8􀀗 The would-be assassin, Mansour Arbabsiar, had established contact with his cousin, a Quds Force85 handler, Gen. Gholam Shakuri. The plot is believed by some to be part of a wider campaign by the Quds Force and Hezbollah to embark on a campaign of violence extending beyond the Middle East to other Western targets, including those in the United States.86 In early September 2012, Mexican authorities arrested three men suspected of operating a Hezbollah cell in the Yucatan area and Central America, including a dual U.S.-Lebanese citizen linked to a U.S.-based Hezbollah money laundering operation. 87A few months later, in December 2012, Wassim el Abd Fadel, a suspected Hezbollah member with Paraguayan citizenship, was arrested in Paraguay. Fadel was charged with human and drug tra􀌇cking and money laundering. Fadel reportedly deposited the proceeds of his criminal activities—ranging from 􀀇50-200,000 per transaction—into Turkish and Syrian bank accounts linked to Hezbollah. In summary, Hezbollah has become a 􀂿xture in Central and Latin America, expanding both its activities and in􀃀uence over time. It has developed links with the increasingly powerful organized crime groups in the region, particularly the narco cartels, along with radical insurgent groups such as the FARC and states like Venezuela who are hostile to the United States and its regional partners. Hezbollah’s principal objectives appear to be undermining U.S. in􀃀uence in the region, imposing costs on the United States, and generating revenue to sustain its operations in Latin America and elsewhere in the world. These objectives are shared by Iran, Hezbollah’s main state sponsor. The Bolivarian Alliance As noted above, geographic, economic, and cultural factors have traditionally helped to prevent the emergence in Latin America of any real military rival to the United States. Although there are no traditional military threats in the region, there are indigenous states whose actions, policies, and rhetoric challenge regional stability and U.S. security. Over the past decade, several states have come together to form the Bolivarian Alliance of the Americas (ALBA), an organization of left-leaning Latin American regimes whose overarching purpose is to promote radical populism and socialism, foster regional integration, and reduce what they perceive as Washington’s “imperialist” influence in the region.89 Since its founding by Hugo Chavez of Venezuela and Fidel Castro of Cuba in December 200􀀗, the Bolivarian Alliance has expanded to include Antigua and Barbuda, Bolivia, Dominica, Ecuador, 􀀱icaragua, and Saint Vincent and the Grenadines. Although the members of the Bolivarian Alliance are militarily weak and pose almost no traditional military threat to the United States or its allies in the region,90 they challenge American interests in the region in other ways. First, they espouse an anti-American narrative that finds substantial support in the region and consistently oppose U.S. efforts to foster cooperation and regional economic integration.91 Second, in their efforts to undermine the government of Colombia, which they consider to be a U.S. puppet, ALBA states provide support and sanctuaries within their borders to coca growers, drug traffickers, other criminal organizations, and the FARC.92 Links to Hezbollah have also been detected.93 Perhaps of greatest concern, they have aligned themselves closely with Iran, inviting it and Syria to participate as “observer states” in the alliance. Other worrisome ALBA activities involve lifting visa requirements for Iranian citizens and hosting large numbers of Iranian diplomats and commercial exchange members that some observers believe to be Iranian intelligence and paramilitary Quds Force operatives.9􀀗 By hosting and cooperating with both foreign agents and violent non-state actors, the ALBA states have come to function as critical nodes in a network of groups hostile to the United States. A Coming Era of Proxy Wars in the Western Hemisphere? History shows that Washington has often emphasized an indirect approach to meeting challenges to its security in Latin America. Yet the United States has not shied away from more direct, traditional uses of force when interests and circumstances dictated, as demonstrated over the past half century by U.S. invasions of the Dominican Republic (1965), Grenada (1983), and Panama (1989) and the occupation of Haiti (199􀀗).Yet several trends seem likely to raise the cost of such operations, perhaps to prohibitive levels. Foremost among these trends is the diffusion of precision-guided weaponry to state and non-state entities. 92 The Second Lebanon War as “Precursor” War A precursor of this trend can be seen in the Second Lebanon War between Israel and Hezbollah.95 During the con􀃀ict, which lasted less than 􀂿ve weeks, irregular Hezbollah forces held their own against the highly regarded Israeli Defense Force (IDF), demonstrating what is now possible for non-state entities to accomplish given the proliferation of militarily-relevant advanced technologies. Hezbollah’s militia engaged IDF armor columns with salvos of advanced, man-portable, antitank guided missiles and other e􀌆ective anti-armor weapons (e.g. rocket-propelled grenades (RPGs) with anti-armor warheads) in great numbers. When the IDF employed its ground forces in southern Lebanon, its armored forces su􀌆ered severe losses; out of the four hundred tanks involved in the 􀂿ghting in southern Lebanon, forty-eight were hit and forty damaged.96 Hezbollah’s defensive line was also well equipped with latest-generation thermal and low-/ no-light enhanced illumination imaging systems, while frontline units were connected to each other and higher command elements via a proprietary, 􀂿ber-optic based communications network, making collection of communications tra􀌇c by Israeli intelligence extremely di􀌇cult. Perhaps most important, Hezbollah possessed thousands of short- and medium- range rockets, often skillfully hidden below ground or in bunkers that made detection from overhead surveillance platforms nearly impossible. During the brief con􀃀ict Hezbollah’s forces 􀂿red some four thousand unguided rockets of various types that hit Israel. Hezbollah’s rocket inventory enabled its forces to attack targets throughout the northern half of Israel. Over nine hundred rockets hit near or on buildings, civilian infrastructure, and industrial plants. Some two thousand homes were destroyed, and over 􀂿fty Israelis died with several thousand more injured. The casualties would undoubtedly been greater if between 100,000 and 250,000 Israeli civilians had not 􀃀ed their homes. Haifa, Israel’s major seaport had to be shut down, as did its oil re􀂿nery.97 Hezbollah also employed several unmanned aerial vehicles for surveillance of Israel, as well as C-802 anti-ship cruise missiles used to attack and damage an Israeli corvette. 98 The G-RAMM Battlefield The brief war between Israel and Hezbollah suggests that future irregular forces may be well-equipped with enhanced communications, extended-range surveillance capabilities, and precision-guided rockets, artillery, mortars and missiles (G-RAMM) 99 able to hit targets with high accuracy at ranges measured from the tens of kilometers perhaps up to a hundred kilometers or more. In projecting power against enemies equipped in this manner and employing these kinds of tactics U.S. forces—as well as other conventional forces— will find themselves operating in a far more lethal battlefield than those in either of the Gulf wars or in stability operations in Afghanistan and Iraq. Moreover, currently constituted conventional forces typically depend on large fixed infrastructure (e.g., military bases, logistics depots, ports, airfields, railheads, bridges) to deploy themselves and sustain combat operations. These transportation and support hubs also serve as the nodes through which internal commerce and foreign trade moves within a country. This key, fixed infrastructure will almost certainly prove far more difficult to defend against irregular forces armed with G-RAMM weaponry. Indeed, had Hezbollah’s “RAMM” inventory had only a small fraction of G-RAMM munitions, say 10-20 percent, it would have been able to in􀃀ict far greater damage than it did historically to Israeli population centers, key government facilities, military installations, and essential commercial assets such as ports, air􀂿elds, and industrial complexes. An irregular enemy force armed with G-RAMM capabilities in substantial numbers could seriously threaten Latin American governments as well as any U.S. (or external great power) forces and support elements attempting a traditional intervention operation. Implications for the U.S. and Other Major Powers The preceding narrative suggests that the combat potential of irregular forces is likely to increase dramatically in the coming years. As this occurs, the cost of operating conventional forces—especially ground forces—and defending key military support infrastructure is likely to rise substantially. Given these considerations the United States and other major powers external to the Western Hemisphere will have strong incentives to avoid the use of conventional forms of military power, particularly large ground forces, in favor of employing irregular proxy forces to advance their interests. Moreover, the high cost and questionable bene􀂿t of the campaigns in Afghanistan and Iraq are likely to create strong domestic opposition in the United States to such operations for some time to come. This must be added to the United States’ greatly diminished 􀂿scal standing that has led to large cuts in planned investments in defense. These factors suggest that Washington will be much less likely to engage in direct military action in Latin America in the coming years than historically has been the case. At the same time, rivals of the United States like China and Russia may be incentivized by these trends, as well as the United States’ overwhelming military dominance in the Western Hemisphere, to avoid the direct use of force to expand their in􀃀uence in Latin America. Instead, like some of the Bolivarian Alliance members, they appear likely to follow the path taken by the Soviet Union during the Cold War and Iran today: supporting non-state proxies to impose disproportionate costs on the United States and to distract Washington’s resources and attention from other parts of the world. This is not to say that Beijing, Moscow, and Tehran would eschew future opportunities to establish bases in Latin America. As in the past, such bases can support efforts to accomplish several important objectives. They can, for example, further insulate a Latin American regime from the threat of direct U.S. military intervention, since Washington would have to account for the possibility that the conflict would lead to a direct confrontation with a more capable and potentially nuclear-armed power .100 Bases in the hemisphere can also enable external powers to conduct military assistance activities, such as training, more easily. Electronic surveillance of the United States and Latin American states could be accomplished more cheaply and e􀌆ectively from forward positions. Finally, certain kinds of military capabilities, such as long-range ballistic missiles and attack submarines, could be pro􀂿tably stationed in Latin America by powers external to that region, particularly if they intended to create the option of initiating con􀃀ict at some future date. These reasons, among others, have made preventing an extra-hemispheric power from establishing bases in Latin America an enduring U.S. priority. Players in a Latin American Great Game Given current trends, several powers external to the region may, either now or over the coming decade, have both the motive and the means to employ both state and non-state proxies in Latin American to achieve their interests. Principal among them is Iran, which is already engaged in supporting proxies against the United States and its partners in the Middle East and has long been developing proxies in Latin America. Additionally, there are reasons to think that China and Russia may be interested in cultivating and supporting Latin American proxies as well.

#### Introducing doctrinal clarity rebalances use AND generates global compliance.

Jana Hözel 17, MA, Department of Public Law, University of Cape Town, "The Paris attack – A case for the right to self-defence?" OpenUCT, 02/15/2017, pg. 44-46.

The doctrine’s major shortcoming and the main reason why it is criticised, is its high level of generality.282 As I have already mentioned, there is no established definition of the criteria ‘unwilling’ or ‘unable’.283 What factors must a state consider when it evaluates the host state’s unwillingness or inability? The doctrine therefore suffers from ‘substantive indeterminacy’ since the parameters are not clear.284 Although many aspects in the use of force area are unclear, for example, what constitutes an armed attack, because of this lack of clarity, the doctrine is not able to provide guidance for states as well as it could do. This is demonstrated very well by the inconsistent and disrupted state practice after 9/11. This dissertation will try to provide some parameters in order to make the doctrine more precise.

Another reason why some commentators view the doctrine with scepticism is the risk of abuse that the doctrine entails. It is argued that the weak host states are more or less entirely at the mercy of the powerful attacked states.285

Against this, there are mainly two arguments. Firstly, state practice has shown that it is not always powerful states like the US, Russia or Israel that invade in other states but also states that are not necessarily considered superpowers like Kenya, Colombia or Ethiopia. Secondly, it is true that the unwilling or unable-doctrine can be abused by states but this alone is not a good reason for not having a rule at all. States have always violated and still constantly violate international law, in every filed. Rosalyn Higgins has argued, in the context of humanitarian intervention, that:

Many writers argue against the lawfulness of humanitarian intervention today. They make much of the fact that in the past the right has been abused. It undoubtedly has. But then so have there been countless abusive claims to the right to self-defence. That does not lead us to say that there should be no right of self-defence today. We must face the reality that we live in a decentralized international legal order, where claims may be made either in good faith or abusively. We delude ourselves if we think that the role of norms is to remove the possibility of abusive claims ever being made.286

Hence, the best way to avoid abuse is to make the doctrine more accurate and to give states in this way clear guidance for determining when a state is unwilling or unable.

In theory, the Unwilling or Unable-Doctrine should function as an useful control on the defensive use of force by an attacked state outside of its own territory, but only with a clear legal content will it be able to fulfil this function. This dissertation tries to provide that content.

2. A new approach: a clarified Unwilling or Unable-Doctrine

This section of the dissertation introduces a new standard of attribution in the form of a clarified Unwilling or Unable-Doctrine.

A clarification of the doctrine will bring several advantages. First of all, it will provide guidelines for the attacked state as well as the host state. A clearer doctrine with transparent parameters ensures that both states know what to do and how to assess the respectively other state’s behaviour. But above that, it will help states in general to deal with attacks of terrorist organisations, to assess the attacked state’s and the host state’s behaviour and to react to such attacks appropriately and lawfully. And finally, a clarification of the doctrine would make it more legitimate in the eyes of states.287 The clearer or the more determined a norm is, the more, states are willing to comply with it.288 As reported by Franck:

Determinacy seems the most important [aspect of legitimacy], being that quality of a norm that generates an ascertainable understanding of what it permits and what it prohibits. When that line becomes unascertainable, states are unlikely to defer opportunities for self-gratification. The rule’s compliance pull evaporates.289

In the current situation in which no one really knows what the legal situation is and what the requirements are it is very difficult for states to act lawfully even though they want it.

### IF TIME

#### Back to Counterterror.

#### Chemical terror causes extinction.

Shigeo Atsuji 14, Professor at the Kansai University Faculty of Informatics, et al., “Our Stolen Sustainability: Unsafe Eden Contaminated by Environmental Hormones”, p. 6-7

Figure 4 shows levels of PCB and DDT in skipjack tuna liver. Measurements are from the Pacific, Indian, and Southwest Atlantic oceans and do not cover the North Atlantic. There can be no such thing as locally limited environmental contamination. Convection through the water and air that make up the global ecosphere and interactions due to the movements of animal species such as migratory birds and fish that move with sea currents have the effect of disseminating contamination, so that environmental destruction spreads throughout the ecosphere. This may initially involve contamination at low concentration, but chemical compounding with other substances and reactions with various chemical elements lead to the secondary development of toxicity and bio-accumulation in a ‘domino effect’ of environmental destruction. Environmental contamination can no longer be a distant concern but is casting an unmistakeable shadow on the lives of modern humans. Environmental hormones have a multiple presence in our lives, not only in synthetic preservatives, colorants, and flavorings, herbicides and agricultural chemicals, but also for instance in dioxins emitted through waste incineration, and these substances have left residues in the bodies of nearly every human being. The threat from environmental hormones highlighted by Colborn was that, mediated through the interaction between living organisms that takes place in the food chain, contaminants would undergo bio-accumulation and collect in high concentrations in the bodies of modern humans. This would mean damage to DNA, which is a ‘blueprint for preservation of the species.’ The contamination of animal wombs with environmental hormones amounts to the contamination of the global ecosphere, which is the amniotic fluid of all life on earth, in other words contamination of Gaia. This is because contamination of any one group of individuals, such as waterfowl, poses a danger to all living organisms, all intelligent life forms with a nervous system dependent on water and carbons. Waterfowl contamination leads ultimately to ‘Gaia contamination’, or contamination of the whole of the global ecosphere, which threatens human survival.

#### Action now is critical to achieve allied buy-in.

A. Wess Mitchell 21, Vice chairman of the board of the Center for European Policy Analysis, "Use the Honeymoon with U.S. Allies to Frontload NATO Reform," in Key Republican Lessons for Biden’s Global Agenda, Foreign Policy, 02/03/2021, https://foreignpolicy.com/2021/02/03/republicans-biden-foreign-policy-national-security-agenda/.

The new administration should push for an overhaul of NATO that prepares the alliance for an era of geopolitical rivalry with Russia and China. The need for this adaptation was laid out in a November report by a group of experts commissioned by NATO Secretary General Jens Stoltenberg, which I co-chaired with former German Minister of Defense Thomas de Maizière. Many of the recommended changes are long overdue and urgently needed in order to clarify priorities, improve cohesion, and streamline decision-making.

The administration should frontload the more difficult reforms that may become harder once its honeymoon period with U.S. allies wears off. A good starting point would be to update NATO’s Strategic Concept, which is now more than a decade old, to reflect new geopolitical realities facing the alliance. Washington should push for the creation of a consultative body encompassing the North Atlantic Council—NATO’s main decision-making body—and European Council to coordinate the West’s approach on China, and to ramp up cooperation with Indo-Pacific partners and India. It should encourage NATO to build a North Atlantic counterpart to the U.S. Defense Advanced Research Projects Agency to fund intra-alliance innovation and spur shared research and development.

The administration should also band with like-minded allies to discourage the European Union from pursuing what it calls “strategic autonomy” and channel European defense aspirations toward enhancing NATO capabilities. It should encourage NATO to build a center for democratic resilience to rebuff external influence in NATO democracies. This should go hand in hand with stricter barriers against military-technological relationships between NATO members and the alliance’s rivals. Finally, it should push for reform in NATO’s decision-making processes—for example, by making it harder for individual allies to use their veto power to paralyze the alliance, allowing sub-groups of allies to act under the North Atlantic Council’s authority, and limiting deliberations in a crisis to 24 hours.

This is an ambitious but urgent agenda to boost the strength and effectiveness of the alliance. The timing is auspicious, coming at the start of a new U.S. administration’s term, the completion of NATO’s own review process, and the conclusion of Brexit but before the elections this year in Germany and France. Goodwill for the Biden administration will be high, and allies will be looking for new direction in the transatlantic relationship. Moments like this are perishable and should not be wasted.