# Aff – OCOs 3 – BFHR

### notes

Thanks a ton to Sam Gordon and Paul Wallace for their work this wave! Please email [khirn10@gmail.com](mailto:khirn10@gmail.com) with any comments or concerns.

Many cyber affs---including OCOs and space---clearly have interactions with the ‘Article 5’ debate. I figured that 1acs should have the option of explicitly designing their plan to include an attempt at pressuring NATO to agree on appropriate Article 5 thresholds for what constitutes an armed attack with regards to cybersecurity. The aff/neg file is thus designed as a supplement, with defensible and distinct impact mods both for and against changing the threshold.

The DAs in this file are essentially deterrence and assurance, the links assuming the aff attempts to establish some cyberattacks as falling short of meeting the threshold of ‘armed attack’. The “Lower A5 Threshold” DA is meant for a hypothetical aff that **lowered** the Article 5 threshold, functionally saying “all cyberattacks are armed attacks and we will respond accordingly.” The aff material in “OCOs 3” doesn’t support this angle, but I could envision somewhat putting it together.

## 1AC/Core A5 Advantages

### PMC’s Adv---1AC

#### Clarifying Article 5’s application to cyberspace is necessary to establish NATO’s ‘armed attack’ thresholds and rules for engagement in gray zone warfare---spills over to other issues

Hill ’21 [Steven Hill (Ex Chief Legal Counsel, NATO; Member, Executive Council of the American Society of International Law; Associate Senior Policy Fellow, Institute of Security and Global Affairs, Leiden University); “NATO and the international law of cyber defence;” *Research Handbook on International Law and Cyberspace*, Chapter 24; 2021; Edward Elgar Publishing]

4. INTERNATIONAL LAW AND NATO CYBER DEFENCE POLICY

What role has international law played in the evolution of NATO’s cyber defence policy? And what influence might NATO’s cyber policy decisions have on the international law applicable to cyberspace?

(a) Applicability of International Law to Cyberspace

Perhaps the most straightforward way in which international law has played a role in NATO’s cyber policy evolution has been in the Alliance’s constant affirmations of the applicability of international law in cyberspace. As explained above, at the NATO Summit in Wales in 2014, Allies recognised that international law, including international humanitarian law and the UN Charter, applies in cyberspace. More recently, at the Brussels Summit in July 2018, allies re-affirmed their commitment to act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law, as applicable.

These statements were part of a broader movement of cyber diplomacy conducted by States, international organisations, and non-governmental organisations. That effort had some notable successes at the international level, including the 2013 and 2015 reports of the UN Group of Governmental Experts.56 However, this consensus proved to be tenuous. Currently some States, among them China and Russia, are pushing back on the very notion of the applicability of international law principles, including the applicability of international humanitarian law, in cyberspace.57 Many NATO Allies are attempting to counter these attempts to dismantle previous consensus. Their techniques include detailed legal statements of a series of how international law applies in cyberspace.58 However, while the number of States making such statements is slowly growing, it still remains a small number that of course does not include all NATO allies. In this context, language like that adopted at NATO can be useful as evidence of where all NATO allies and likeminded States currently stand.59 These and similar statements in other international organizations may help with ongoing cyber diplomacy.

(b) Article 5 and Armed Attack

International law considerations have also factored into NATO’s cyber policy in relation to Article 5 of the North Atlantic Treaty. As mentioned above, the 2014 Wales Summit contained the basic policy decision regarding the interplay between cyber attacks and the international law concept of armed attack: ‘We affirm therefore that cyber defence is part of NATO’s core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis’. Article 5 is the self-defence provision at the core of the North Atlantic Treaty.60 It refers back to Article 51 of the UN Charter, which itself reflects the ‘inherent’ right of self-defence under customary international law. In NATO’s practice to date, Article 5 has been treated as coterminous with the customary right reflected in Article 51.61 All of these formulations revolve around the notion of armed attack.

From an international law perspective, NATO’s policy illustrates at a minimum that a cyber attack could constitute an armed attack giving rise to the right of individual or collective self-defence under international law. It clearly does not say that all cyber attacks would rise to this level. Nor does it provide any further guidance on important international law questions, such as the threshold for an armed attack. For example, the policy does not refer to the well-known analysis that an armed attack must attain a certain level of scale and effect. That analysis features prominently in a range of judicial decisions62 and in scholarly commentary.63 Nor does it seek to address some of the debated questions. These include whether an attack ‘having severe albeit neither injurious nor physically destructive effects could ever constitute an armed attack and, if so, under what circumstances’.64

From a policy perspective, the primary reason for this lack of detail about what would constitute an armed attack is straightforward. It is seen as strengthening the deterrence value of NATO’s posture. The NATO Secretary General has said: ‘I am often asked, “under what circumstances would NATO trigger Article 5 in the case of a cyber-attack?” My answer is: we will see. The level of cyber-attack that would provoke a response must remain purposefully vague’.65 In any event, as the policy makes clear, the decision to invoke Article 5 would be taken on a case-by-case basis. This decision would be taken by the North Atlantic Council on the basis of consensus of all Allies. Whether or not an armed attack has occurred is a question of fact and law. NATO does not prejudge the threshold for an Article 5 decision. This would be a political decision in which a wide range of factors, including but not limited to legal advice, would be considered by the North Atlantic Council.”

If Article 5 were invoked in response to a cyber attack, the Alliance’s collective response would also be decided on a case-by-case basis by the North Atlantic Council. The legal obligation on Allies under Article 5 is set forth in the North Atlantic Treaty:

each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.66

This is an obligation of assistance to the State or States that are the victim of the armed attack. The Treaty does not specify what actions the attacked State’s Allies are under an obligation to take. Rather, it requires each Ally to take ‘such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area’. The text specifies that this is actions for all each ally to take both on its own and together with (‘in concert with’) other Allies.

It is impossible to predict what might happen if NATO Allies were to decide that a future cyber attack crosses the armed attack threshold in Article 5. The exact collective response would be decided on a case-by-case basis by the North Atlantic Council. This could include the use of force in exercise of the right of individual or collective self-defence. Such a use of force would not necessarily be limited to the cyber domain and could include action in other domains. As Secretary General Stoltenberg put it, NATO’s response under Article 5 ‘could include diplomatic and economic sanctions, cyber-responses, or even conventional forces, depending on the nature and consequences of the attack’.67 Finally, given the text of Article 5, it is possible that in addition to the collective response agreed by consensus, individual States would take action that they deem appropriate.

(c) ‘Below the Threshold’ Incidents

Since the vast majority of cyber incidents occurs below the armed attack threshold, international lawyers have had to think about the peacetime legal framework for responses to such malicious cyber activity. NATO’s recent work has included ‘a NATO guide that sets out a number of tools to further strengthen NATO’s ability to respond to significant malicious cyber activities’.68 However, this is document is not publicly available, so it is difficult to assess what its contents may indicate on some of the key questions that arise in responding to internationally wrongful acts against the Alliance or individual Allies.

In response to future incidents, Allies may wish to use NATO as a forum to coordinate multilateral responses to such responses, or as a means of requesting assistance with their own responses. In the case of a serious incident, one option would be to request consultations under Article 4 of the North Atlantic Treaty. Article 4 provides that ‘[t]he Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened’. Article 4 has only been explicitly been called upon in a handful of situations during NATO’s history, none of which has been focused on cyber.69 It is certainly possible that future malicious cyber activity could constitute the kind of threat to territorial integrity, political independence or security envisioned by Article 4. However, it is not necessary to use Article 4 in order for NATO to take action to deal with any given incident.

Close attention to NATO’s future responses to ‘below the threshold’ cyber incidents may yield some insight on a range of international law questions. For example, given NATO’s collective defence mandate, one question is whether States will be willing to consider NATO as a means to conduct collective countermeasures. At the time of writing, some Allies appear to have different views on whether collective countermeasures are a legally available option under international law.70

Finally, some NATO allies have developed a practice of using public identification of the perpetrators of malicious cyber activity as a means of countering that activity. This practice is referred to as attribution. As the Brussels Summit declaration put it in 2018, ‘[i]ndividual Allies may consider, when appropriate, attributing malicious cyber activity and responding in a coordinated manner, recognising attribution is a sovereign national prerogative’.71 There is an increased trend of States making attributions, either unilaterally or in concert with others.72

(d) Providing a Forum for Expressing Legal Views

As an international organisation, NATO does not create international law or other norms that regulate State behaviour. While NATO’s cyber practice to date may help shed light on some questions of international law (or at least help stimulate thinking on these questions), there would be little appetite among Allies and in the broader international community for NATO to take a lead role in driving such debates forward.73 Put another way, NATO does not see itself as a norm-creating institution. At the same time, as a well-established multinational intergovernmental organisation with a considerable amount of practical experience on cyber defence issues, NATO can often provide a good vantage point not just for emerging State practice, but for encouraging it to be expressed.

More and more States have been making public statements of their views of how international law applies in cyber space. This process should be encouraged. One of the advantages of NATO is that it provides a forum for daily multilateral discussions and exchanges of views on cyber defence. NATO is also a way for Allies that have not yet taken a view on a subject can express support or alignment with positions of other Allies. Regular meetings at the ministerial and even Head of State and Government level provide an opportunity for Allies to make clear public statements. In addition, NATO has the convening power to host regular high-level interaction between government cyber policy experts, lawyers, academics and industry representatives. Sometimes sponsored and led by individual Allies, these are initiatives that can take a holistic approach by bridging the legal, political, and military domains. Finally, NATO also conducts regular multilateral cyber exercises, often with a legal component or designed so as to raise legal questions. Properly designed, multilateral cyber defence exercises that engage the highest level of government decision makers could help clarify State practice. Leveraging all of these advantages may help generate more clarity on the international legal framework.

5. CONCLUSION: FUTURE CHALLENGES FOR NATO CYBER DEFENCE POLICY

NATO’s cyber policy evolution over more than two decades has been a prime example of how the Alliance has adapted to new threats. What challenges can NATO expect in future cyber policy? And how can NATO’s traditional approach to legal issues pertaining to cyberspace help the alliance address these challenges? In the future, the trajectory for NATO’s cyber defence policy work will continue to be shaped by the threat environment as it evolves and will likely follow the direction indicated by existing work as the alliance seeks to further strengthen the cyber defences of the alliance itself and those of individual allies, deter cyber activities directed against NATO and its allies, and respond to future incidents.

The future cyber threat environment will be equally if not more intense than NATO sees today. For example, cyber defence will need to become increasingly powered by artificial intelligence in order to respond to AI-powered attacks.74 Especially as technology evolves, the cyber domain of operations will become more central to – and more integrated with – other domains. For example, in December 2019, NATO Heads of State and Government declared outer space as NATO’s newest domain of operations.75 There is a strong link between outer space and cyber.76 If the intensity of attacks and their potential impact on all domains continues to increase, one future outcome would be for Allies to be interested in stronger responses to them. Whether Allies prefer to do this individually or on a bilateral or ‘small group’ basis, or whether they will seek out stronger collective tools for the alliance is an open question.

Given Allies’ commitment to the rule of law, compliance with international law will continue to be a cornerstone of NATO’s cyber policies in the future. The challenge will be how to ensure that other actors in the international system, both State and non-State, comply as well and whether the broad cooperation among like-minded States that has been developing in numerous venues can be sustained in the long term.77 Pressure for more collective action against cyber attacks and malicious cyber activities may well raise the stakes on some of the open legal questions that have been on NATO’s agenda. One recommendation would be for allies to continue their ongoing legal dialogue on questions such as the armed attack threshold for Article 5, the types of response measures available for malicious cyber activity below the armed attack threshold, whether techniques like countermeasures are available not just for use by an individual victim State but also for collective use, and others. Technological developments may also lead to more calls for legal dialogue. For example, since applications of artificial intelligence and machine learning for use in cyber defence have already made their way onto NATO’s agenda, there will likely be demand for multilateral ways of responding to them. Another recommendation would be for more dialogue on the legal framework for the use of such technologies.78 Legal dialogue on these forward-looking issues might help bring allies closer together, not only in the legal area but in broader cyber policy terms.

#### Specifically, it enables NATO to establish norms for PMCs---solves global misalc

Morten **Fogt 20** - Lieutenant Colonel of the Danish Army and Chief Legal Advisor at the NATO Multinational Division North (MNDN)in Latvia/Denmark. Associated Professor in Civil and International Law at Aarhus University. (“LEGAL CHALLENGES OR “GAPS” BY COUNTERING HYBRID WARFARE – BUILDING RESILIENCE IN JUS ANTE BELLUM,” SOUTHWESTERN JOURNAL OF INTERNATIONAL LAW, 2020, <https://www.swlaw.edu/sites/default/files/2021-03/2.%20Fogt%20%5B28-100%5D%20V2.pdf> ) PJW

Second, the distinction between an IAC and a NIAC in a hybrid warfare setting will depend on evidence of state attribution, which will be a difficult and highly political issue. State denial policy and covert operations by provocateurs, Private Military Contractors (**PMC**) or Private Military Security Contractors (PMSC) like the Wagner Group, mercenaries in terms of non-state conventional forces and state special forces (SOF) provoking the uprising of the civilian population is a **central part of the hybrid warfare**. If one adds to this evidential legal uncertainty, the ICJ and ICTY dispute about whether one should apply a high degree of "effective control" or a lesser degree of "overall control," the legal picture of a possible perfect hybrid scenario becomes visible. The strict ICJ requirement of "effective control" in the Nicaragua case seems less convincing as it legally allows states to use non-state actors in the gray zone where these strict conditions and proof thereof cannot be met. The arguments presented by the ICTY in the Tadi? Appeal case against the view of the ICJ seem persuasive, if alleged "lawful" interventions by third states and hybrid campaigns through private non-state actors should be reduced and prevented:

A first ground on which the Nicaragua test as such may be held to be unconvincing is based on the very logic of the entire system of international law on State responsibility.

The principles of international law concerning the attribution to States of acts performed by private individuals are not based on rigid and uniform criteria ... The rationale behind this rule is to prevent States from escaping international responsibility by having private individuals carry out tasks that may not or should not be performed by State officials, or by claiming that individuals actually participating in governmental authority are not classified as State organs under national legislation and therefore do not engage State responsibility. In other words, States are not allowed on the one hand to act de facto through individuals and on the other to disassociate themselves from such conduct when these individuals breach international law. The requirement of international law for the attribution to States of acts performed by private individuals is that the State exercises control over the individuals. The degree of control may, however, vary according to the factual circumstances of each case. The Appeals Chamber fails to see why in each and every circumstance international law should require a high threshold for the test of control. Rather, various situations may be distinguished. 114

The disagreement between the ICJ and ICTY on the attribution of acts by non-state actors to a state was reinforced by the subsequent ICJ judgement in Genocide case 2007, where for the purpose of deciding state responsibility, the ICJ confirmed the Nicaragua "effective control" test and, moreover, expressis verbis, rejected the ICTY jurisprudence. 115With the ICJ jurisprudence, the attribution test for the purpose of conflict classification may well be the ICTY "overall control" test, which according to the ICJ could be applicable and suitable. However, this test does not persuade for the purpose of state responsibility. This introduces two different quality tests, which adds another legal layer of complexity: a state can instigate an IAC by having "overall control" of acts of non-state actors, but simultaneously avoid state responsibility for the acts of those non-state actors as the "effective control" test is not met. The ICJ logic of the possible application of difference attribution tests for conflict classification and state responsibility seems questionable and critical, at least from a hybrid warfare perspective. Moreover, from a general perspective, it seems unconvincing and, thus, questionable that the "overall control" test is unsuitable and in the view of the ICJ stretches too far, almost to a breaking point, the connection which must exist between the conduct of a State's organs and its international responsibility. The restrictive perception of the ICJ on state responsibility seems out of tune with the factual needs and the "requirements of international life" to be able to legally counter strategically willful and unlawful hybrid threats and warfare.

The experience in East Ukraine speaks for itself. The threshold ('trigger') for an international, armed conflict (IAC) involving more than one state, and the threshold for state responsibility are not only difficult to demonstrate with reliable evidence, but also covered with legal uncertainty. In addition, there may exist a lack of appetite to declare an IAC at the strategic political level and thereby risk an escalation and a possible ad hoc activation of collective self-defense.

C. Specific Legal Challenges or "Gaps" in jus ante bellum by Hybrid Threats and Warfare

A hybrid threat or warfare kept under the threshold of an "armed attack" and below the intensity or organizational requirement for an internal "armed conflict" (NIAC) will pose critical challenges to a peacetime law enforcement regime, as it will be conducted by inter alia indirectly employed non-state actors and covert state agents, by provoked opposition from own and foreign citizens, by cyber-attacks, and by the use of information campaigns utilizing fabricated or switched fake news.

Such a hybrid threat or warfare is often coupled with a firm denial policy of any immutability and attribution of such activities to a state initiating and de facto controlling the hybrid campaign. The integrated hybrid information campaign merely portrays a public picture of civilian movements consisting of "normal" people being dissatisfied with the current political regime in power and the society conditions in general. With the legal requirement of attribution in the sense of the "effective control" test or the relaxed "overall control" test being disputed, and clear evidence thereof likely either ignored without legal effect or covered by hybrid information campaign, a continued hybrid threat and warfare with both kinetic and non-kinetic means is possible without high, or much, political or legal risks. 116

The emerging problems with the principle of distinction just add to this. Military clothing has become popular and trendy among civilians, as paramilitary uniforms are seen more often in the streets. Regular armies have been seen to disrespect traditional uniform codes and permit self-equipment of soldiers in combat zones, missions or on exercises. Moreover, uniforms, accessories and insignia of different states are becoming more similar and hard to distinguish, even at a close distance. 117 The possible and recommendable remedy is, on the one hand, that military forces consider distinction by choice of design and uniforms and, on the other hand, that military discipline of wearing those regular uniforms when on duty is re-enforced.

If all these circumstances come together in a law enforcement scenario in peacetime or crisis, there will be several legal constraints and restraints in the jus ante bellum, which will **create legal vulnerabilities** for both the victim states (host nations) and states sending armed forces for assistance, deterrence purpose, and countermeasures. Some of these will be addressed below.

a. Limits set by the national domestic law enforcement regime and HRL

1. Respect of Receiving State (Host Nation) Law and Political System

The deployment and presence of foreign military forces are conditioned on the consent by the host nation as the territorial law of the host nation decides whether foreign military units may enter the state territory ( jus ad praesentiam) and on what conditions ( jus in praesentia). This consent can be given ad hoc prior to each individual deployment, or in general, as part of a defense agreement and standard status of force agreements. The NATO SOFA applies to the "force" and "civilian component" accompanying a force in the territory of another NATO alliance state, whether stationed or in transit. 118 Under the NATO SOFA and usually under any other standard or ad hoc agreed SOFA, the foreign forces and civilian component thereof have an obligation under treaty law "to respect the law of the receiving state and to abstain from any activity inconsistent with the spirit of" the standard or ad hoc agreed SOFA. 119 Moreover, the forces of the sending state (also termed "Troop-Contributing Nation," TCN) shall not interfere with the internal political affairs of the receiving state and, in particular, take necessary measures to avoid "any political activity." 120 As will be discussed subsequently, the latter will be of relevance by measures to counter informational hybrid activities as any such activity by foreign forces to promote a certain political view and NATO policy may be held to constitute "political activity," infra V.A(d).

Hence, the host nation's political governance and law enforcement remain intact. Foreign forces are stationed in the country only for the purpose of military exercises, planning, and deterrence measures with, as a starting point, little or no legal competence to conduct counter hybrid operations in peace time and crisis.

2. Possession and carrying of arms by foreign forces and contractors

For any conduct of military exercises, deterrence measures, hybrid counter operations, clarity on the laws and directives for the handling of weapons and ammunition is vital. In this regard, military forces are well-educated and trained to be particularly careful and observant.

According to the NATO SOFA, members of a "force may possess and carry arms" if so authorized by orders whereby "sympathetic consideration to request" from the host nation shall be made. 121Arguably, although the wording for the NATO SOFA only mentions "arms" and, hence, strictly speaking "weapons," an interpretation in accordance with the context and object and purpose of the provision would include both weapons and ammunition. 122The possession and carrying of weapons/ammunition will be governed by the sending states' (TCN's) law, military regulations on weapons and ammunition, and the specific directives and orders given to their forces, but still, due regard shall be had to the host nation regulations as well. 123

By multi-national forces stationed in a host nation, different military regulations regarding weapons and ammunition may apply. Moreover, the national requests may differ in the various host nations concerned, such as in the Baltic states, Poland, Germany and Denmark. For a multi-national Headquarters, such as the MNDN, with a distributed "Headquarters East" in Denmark and a "Headquarters West" in Latvia and ongoing duty travel between the two permanent locations, the host nation's legal framework would differ and change constantly. The varying regulations on weapons and ammunition will create legal complexity and administrative obstacles and, thus, may hamper timely and effective reactions to a hybrid campaign. There are good legal and operational reasons to conclude separate multi-national SOFAs on the question of arms and ammunition in peacetime and crisis and align the legal framework of both sending and receiving nations. 124 The "gap" in the NATO SOFA regarding specific directives for handling arms and ammunition would thereby be closed.

Under Article II of the NATO SOFA, there are two important limitations on the right which state that members of a "force may possess and carry arms" if so authorized by orders.

Firstly, the granted right under the NATO SOFA that a "force may possess and carry arms" is thus exempted from the host nation's public law regulations on weapons and ammunition as it only applies to the forces in their performance of military duties in accordance with the authorization by orders, 125where the sending states (TCNs), in principle, maintain primary jurisdiction under the NATO SOFA. 126 When not acting on duty, restrictive public rules on weapons and ammunition in the host nation may apply, such as the Danish prohibition to import, produce, collect, purchase, possess, carry and use any kinds of weapons, including specific knives, without authorization. 127 More flexible and relaxed weapon regulation for possessing and carrying arms off duty are usually enforced in other NATO alliance countries, inter alia, the Baltic states and in particular in the U.S. This is a practical and legal concern in the jus ante bellum that military personnel in peacetime and crisis will be temporarily off duty, or on leave, and in that timespan be subject to perhaps unknown, strict weapons regulation in the host nation, and in principle punishable for any violation thereof under the receiving state's (host nation) law and jurisdiction. For foreign troops present in other NATO states, the determination of when a person is "on duty" or "off duty" may not always be easy. In any case, members of foreign forces will have to be educated and trained in legal compliance with the host nation's law and regulations. 128 In a hybrid campaign, foreign troops are a more vulnerable target for provocation, threats, attacks, and media exposure while "off duty," and acts in violation of the host nation's law may be exploited by a hybrid propaganda campaign.

Secondly, the right under the NATO SOFA to "possess and carry arms" only applies to members of a force and **not to civilian components**, family members or sending state contractors, **including PMSCs.** Again, host nation law applies, and the host nation maintains primary or exclusive jurisdiction. If sending states employ civilian components and contractors to perform security and other military tasks requiring them to carry weapons and potential use of force, this should be regulated in a bilateral or multi-lateral SOFA, 129or in the host nation's applicable law. 130 Moreover, the status of state contractors is **not governed by the NATO SOFA**, and a specific permission for entry and stay must be granted. In this connection, the jurisdiction issue regarding state contractors should be considered. 131

3. Use of force and self-defense by foreign forces

AA) THE SOFA "GAP" ON THE USE OF FORCE

Neither the NATO SOFA nor the UN Model SOFA address the question of the source, scope and application of the use of force in self-defense by foreign forces present on foreign territory. This is a significant "gap" in the standard SOFA regulation.

Rarely do specific bilateral SOFAs deal with this vital question. The detailed US/Poland SOFA 2009 and the SOFAs between the U.S. and the Baltic states concluded in 2017, do not address this issue. Additionally, separate multi-lateral or bilateral SOFAs for major exercises are normally silent on the issue of use of force and definition of self-defense. 132 An exception to this silent feature of SOFA regulations is found in the NATO/German SOFA 1954 concluded after the end of the occupation regime following the Second World War, where the permanent stationing of troops in the former West Germany was regulated. The NATO/German SOFA 1954 (now Revised Supplementary NATO/German SOFA 1993) requires that the sending state may authorize "civilian component and other persons employed in the service of the force" to possess and carry arms. However, regarding the use of arms it must "issue regulations, which shall conform to the German law on self-defense ( Notwehr) on the use of arms." 133

BB) THE DISTINCTION BETWEEN PERSONAL AND STATE (UNIT) SELF-DEFENSE

The most restricted legal basis for the use of force is self-defense, which constitutes a generally recognized inherent right of all persons and, in addition, of all states, their organs and armed forces pursuant to Article 51 of the UN Charter and customary international law. However alike, the two forms of self-defense must be strictly distinguished.

The right to personal self-defense derives from the national law applicable and HRL. It is codified in most national laws and constitutes a necessary corollary to the right to life under HRL. However, regarding the source, scope and application the right differs decisively under various national laws.

The right to state individual or collective self-defense derives from public international law and is, pending differences in interpretation, in principle uniform. It is a right vested in a state, its organs and armed forces, and, thus, includes self-defense of the state armed force (force self-defense), the so-called "unit self-defense" or the defense of a single soldier in service and performing military duties. 134The exercise of force, unit or soldier self-defense will follow military orders and directives, including ROE, where a unit and soldiers can be ordered not to open fire, cease-fire or withdraw even if the conditions for state (unit) self-defense under international law are fulfilled. Moreover, force self-defense is usually a standing order in terms of an obligation (military duty) and not just an "inherent" right. On the contrary, the right to personal self-defense is generally seen as an inherent right of a person, which cannot be limited by military orders or directives. 135

Hence, in any discussion of "self-defense," this divide between personal self-defense under national law and HRL, and force (unit) self-defense as part of the right to state self-defense under international law must be kept in mind.

Regarding the use of force and self-defense by foreign forces, the inherent right to personal self-defense is, on the one hand, assumed to be governed by territorial law of the receiving state (host nation) albeit special agreements between the states concerned. As part of the right of state self-defense, the right of force/unit self-defense is governed by international law. The exercise of it depends on how de facto this is implemented in the law and policy of the sending state and its military orders and directives. In principle, it does not make any difference whether this right is exercised on foreign territory. 136Illustrative in this regard is the Danish Royal Standing Order 1952 (still in force) to all Danish armed forces and personnel that in case of an armed attack on the territory of Denmark or on Danish military units, including Danish forces present outside Danish territory, Danish forces must engage in combat without delay and without awaiting or requesting an order, even when there is no knowledge of a declaration or state of war. 137It is expressly stated that false orders and information not to mobilize, resist and interrupt fighting are expected, and as such may not be followed before there is necessary proof of these being issued by competent authorities. 138

CC) RIGHT TO POLICE AND TO ENSURE ORDER AND SECURITY

In the limited regulation on the use of force in the NATO SOFA, "the right to police" and to "take appropriate measures to ensure the maintenance of order and security on such premises" is accorded to foreign military units and formations inside camps, establishments or other premises occupied by foreign forces. 139It is not defined what exactly is covered by a right to police and to maintain order and security and what kind of use of force is permitted to that end. The SOFAs between the U.S. and the Baltic states further extend the right and authority of the U.S. as a sending state and authorize the U.S. on host nation territory to exercise all necessary rights and authorities for the use, operation, defense, or control of premises, including taking appropriate measures to maintain or restore order. Hence, by these SOFAs, the U.S. is entitled to exercise all rights and authorities necessary in defense of premises and take appropriate measures to protect U.S. forces, U.S. contractors, and dependents. 140However, it is not addressed whether the use of force in exercising all rights in defense and taking appropriate measures to protect U.S. forces, U.S. contractors, and dependents are governed by host nation law or U.S. law, including a presumably more extensive right to personal self-defense under U.S. law.

Outside such premises, according to the NATO SOFA, any employment of foreign military police or force is subject to arrangements with the receiving state (host nation) and only in so far as such employment "is necessary to maintain discipline and order among the members of the force." 141For other purposes, the maintenance of internal law and order is entirely the host nation's competence and task. Nevertheless, the receiving state has the obligation to seek such legislation as it is deemed necessary to ensure the adequate security and protection of the foreign forces. 142

DD) THE DILEMMA OF PERSONAL AND STATE SELF-DEFENSE IN MULTINATIONAL OPERATIONS

When the use of force is not regulated in the NATO SOFA or a separate supplementary SOFA, the territorial host nation law will apply and determine the extent to which personal self-defense may be used by members of foreign military forces, civilian components, dependents, and contractors. The inherent right to personal self-defense is universally recognized, but the threshold for an attack or imminent threat of attack to life or causing of serious personal injury varies, just as the possibility to use force in self-defense of others and for the protection of property differs, and the proportionality and necessity requirement can be very strict or to a wide degree relaxed. 143

If based on an agreement the law of the sending states applies, the multi-national forces and Headquarters will face a multiplicity of personal self-defense concepts, and the host nation may have to accept the use of force in self-defense on its territory beyond what its own national law permits. Conversely, if the law of the receiving states (host nation states) applies, there will also be more concepts by cross-border operations and distributed Headquarters and, rather critical, some sending states such as the U.S. will see their national definition of personal self-defense narrowed down -- perhaps to an unacceptable degree.

This constitutes the dilemma of personal self-defense in multi-national operations, which, in principle, is unsolvable. There is no expectation that a law harmonizing the personal right to self-defense will see the daylight in a near or foreseeable future at a global or even regional level. One will have to choose between one of the two options of applying either the law of the sending states (TCNs) or the law of the receiving states (host nations). In NATO, the first path of referring to the sending nation law regarding personal self-defense has been chosen. Here, the ROE do not limit the inherent right to self-defense under national law by forces under NATO command and control of foreign territory. 144This approach may be adopted at a national level in the ROE issued for peacetime and crisis by a host nation or agreed upon by separate SOFAs, which then allows foreign forces to use force in accordance with their own national concept of personal self-defense. 145

Until unity of allied command is established by a Transfer of Authority (TOA) from each nation to a common military command such as NATO, the national formations and units will operate under national command and directives regarding the use of force. This means that various national ROEs and policies of state (force/unit) self-defense will apply in a low threshold hybrid warfare theater. The example of the NATO enhanced Forward Presence (eFP) in the Baltic states and Poland is illustrative; as of October 2019, the four multinational battalions consist of rotating troops and staff members from twenty-one countries and four host nations with consequently multiple policies and interpretations of force/unit (state) self-defense being applied. 146

This constitutes the dilemma of state (force/unit) self-defense in multi-national operations and will be the status of the jus ante bellum and jus in bello until there is a TOA to NATO by all nations involved. When the allied headquarters is in command, it can and likely will authorize and issue common ROE, which depending on the situation can have a defensive or (perhaps dormant) offensive character. 147 By such ROE, the differences in the national concepts of personal and force (unit) self-defense can be leveled out by, inter alia, the use of ROE requiring hostile act and hostile intent for the use of minimum but up to lethal force. The use of force against persons, units or groups showing hostile act and hostile intent (perhaps including "hot pursuit') will be in line with the concept of personal and force (unit) state self-defense of some states and clearly excessive when compared to national law and directives of others.

The TOA decision is a critical national political matter and the TOA over national armed forces may come under conditions and, thus, include reservations and caveats. It is only likely to be granted by states just prior to or immediately after activation of individual and collective state self-defense. In a national crisis and in cases of small-scale armed hostilities with non-state actors and armed groups in parts of the territory of an alliance state only, the territorial states concerned may wish to retain command and control of national armed forces and, thus, for the time being refuse TOA. This disregarding whether the armed hostilities fall below or exceed the threshold for a NIAC, where in the latter NIAC scenario, according to the prevailing and convincing view, the LOAC applicable for a NIAC extends to the entire territory of the states concerned.

Another and recommendable option -- even though presumably politically difficult -- would be for all states concerned, to agree on common ROE applicable in peacetime and crisis when taking part in NATO reassurance measures, either by ad hoc agreements or a supplementary SOFA, and thereby filling the decisive "gap" in the NATO SOFA in the time prior to TOA to NATO command.

4. Military Assistance and Support to Law Enforcement and Crisis Control

The receiving state (host nation) has the sole responsibility and competence regarding internal security and law enforcement. However, the host nation can permit, and upon consent receive support from law enforcement in peacetime and crisis from the military forces and civilian component of another state present on its territory. The military forces of the sending states have limited authority, which is confined to maintaining law and discipline in designated military facilities, areas, and among members of their forces. Further authority is not granted under the NATO SOFA and only exceptionally given in separate bilateral SOFAs. In Article 29(2), the US/Poland SOFA 2009 authorizes exclusively U.S. operations outside such designated areas for the purpose of protecting U.S. forces and dependents:

Upon request of either Party and with the consent of the appropriate authorities of the Republic of Poland, United States military authorities may operate outside of the agreed facilities and areas in order to ensure security of United States forces and dependents. During such operations, United States military authorities shall use clear identification of their special status, and they shall immediately contact the appropriate authorities of the Republic of Poland and shall act consistent with their instructions. 148

The legal framework in the host nation, including the applicable HRL constraints and restraints, and the limits for military support to civil law enforcement must be clarified. In addition, the sending states' (TCN's) possible reservations and caveats regarding supporting operations must be adhered to as well. In any event, such foreign military support requires, not only specific military and police training, including legal training, but in particular mutual trust regarding the performance of law enforcement (police) tasks. The host nation and TCNs' caveats may concern the possible military support in the first place and, if allowed, the specific conditions regarding, inter alia, police command and control, detention, and use of force in personal or unit self-defense, in defense of others (civilians), military equipment, and facilities. Each nation will presumably have adopted its own legal regime for the military support to police and law enforcement in peacetime and crisis, which will be designed and shaped by the national tradition and culture and, thus, constitute a sui generis regime for each nation. Consequently, an intensive legal training of incoming foreign forces regarding the host nation's peacetime or emergency law, including the impact of TCN's reservations and caveats, should be made. With the constant routine of in- and outgoing foreign multi-national forces every third to sixth month in the territories of the NATO states, placed geographically at the hybrid threat or warfare frontline, this will be a demanding, time-consuming and complex task.

In summary, while the NATO SOFA permits alliance state forces to be present and carry arms on the territory of the receiving host nation, any assistance and support to a host nation's law enforcement by other states military forces, including the use of force, must be in accordance with the host nation's peacetime and human rights law. While in times of unrest and crisis, national military force may be empowered to perform law enforcement tasks under police and/or military command, foreign forces must be especially authorized by both the sending nation and the host nation to do so.

A practicable solution -- but also a rather radical and politically sensitive one -- would be to accord to foreign NATO forces the same authorization to use force in support of police law enforcement as given to national forces at any point in time. This is the stage of Latvian law and, thus, the host nation policy at the East Headquarters of MNDN. As a general statement, the Latvian national rules on the use of force, including rules on escalation of the use of force, apply to foreign NATO forces present in Latvia. 149Thus, Latvian law permits foreign NATO forces to wear uniforms, carry and use weapons in the same way as Latvian National Armed Forces, and accord them with the relevant rights of the Latvian National Armed Forces. This includes the right to individual self-defense under Latvian law, defense of other persons and to avert an attempt to violently obtain a service firearm. When foreign forces take part in military guard duties or perform other official tasks such as support to the police law enforcement in times of emergency or crisis, they will be authorized to use force in the same manner as Latvian armed forces. If the sending states approve such a support by their armed forces, there will be alignment in the peacetime and crisis Standing Rules for the Use of Force (SRUF). 150Compared with the law of other states, the use of force permitted by the armed forces according to Latvian law could be viewed as excessive in peacetime. However, it signals a necessity to employ military force against certain hostile and armed activities on the frontline of hybrid threats and warfare already in peacetime and crisis. The same result in terms of alignment of the ROE is reached under Lithuanian law by the application of the peacetime Lithuanian Force Protection ROE 2017 by virtue of separately agreed MOUs with the sending states of eFP forces, however, with respect of the application of the personal self-defense according to national law of the foreign armed forces. 151

Turning from the East Headquarters of MNDN in Riga, Latvia, to the MNDN West Headquarters in Denmark, the use of force in peacetime and crisis is entirely a national police task with a possible exclusive supporting role by Danish armed forces. The possibility for the police to request military support from Danish armed forces (but not foreign armed forces) was extended in 2018, but it is still quite limited. It can be provided regarding a wide range of specific tasks only under the strict conditions that the resources and capabilities of the police are insufficient, that supporting operations are under police command and control, and that the rules governing the competence and the use of minimum force by the police are followed. 152With the amendment of the Police Act in 2018, it was made possible to designate specific military areas for, inter alia, NATO re-enforcement forces, the outer security of which are secured and guarded by Danish military forces only, and not by foreign forces. 153

In case of an escalation of a crisis in terms of increasing unrest, riots and armed hostilities below or even above the "armed conflict" threshold for a NIAC, deviation from the normal peacetime law enforcement regime may follow a step-by-step or at once enacted national emergency (martial) law and/or escalation steps taken collectively by the defense alliance concerned.

b. Different National Emergency (Martial) Law Regime and Possible Derogation from HRL

The Baltic states and Poland have been on the frontline of the Russian hybrid threat and warfare for years and have adapted their national legislation and planning on emergency, mobilization, re-organization of governance, civilian support, preparedness and resistance to meet the hybrid challenges. 154In addition, Poland and the three Baltic states have entered into bilateral SOFAs with the U.S. in 2009 and 2017, which supplements the NATO SOFA, and facilitates the presence of U.S. forces. 155Other NATO or PfP states without specific bilateral SOFAs or MOUs are left with the standard NATO SOFA and its "gaps".

Some of the most important issues to be dealt with in the various national emergency (martial) laws or ad hoc emergency regulations regarding national and foreign forces are the following: First, the conditions for possession and carrying of weapons and ammunition. When on duty, temporally on leave or "off duty', military personnel may need to possess and carry weapons and ammunition as the security situation may require military personnel and civilian components to be able to defend themselves at all times. Second, the use of force beyond mere personal self-defense or unit self-defense when encountering hostile hybrid activities until TOA and common NATO ROE will apply. Here, the Latvian regulation aligning the use of force by national and foreign forces seems to represent a model to follow. 156 Third, the conditions for own national, bilateral or NATO military support to law enforcement (the assist/support role). Fourth, the need for legal education and training of all personnel on exercise in peacetime and crisis scenarios. This should be prioritized as military forces will have to operate under a certain national law enforcement regime and apply the peace time and emergency law of the respective host nations.

The national regulatory approach to a state of emergency or a state of exception vary from state to state. Here again, a comparison with the legal state of affairs in Denmark and the Baltic states show a striking difference, although the countries apply the concept of total state defense.

Under Danish law, the maintenance of law and order, including law enforcement, in peacetime and crisis is exclusively the competence of the civil police with possible support by the Danish armed forces. This is where civilian and military efforts will be coordinated by local authorities and the National Operative Staff (' Den Nationale Operative Stab', the so-called NOST) on an ad hoc basis. 157The entire joint operation will be conducted under the police law enforcement regime and the use of force applicable in this context. 158There is no national regulation or law on emergency (martial law) which governs and regulates the emergency and crisis situations as such. For an international military staff and its legal advisors in Headquarters such as the MNDN in Denmark/Latvia, this creates legal challenges as the exact content of the a d hoc legal regulations and directives in emergency situations to some extent is uncertain.

Under Latvian law, as well as under Lithuanian and Estonian law, the state of emergency and state of exception is expressly regulated in a specific emergency or martial law, which provides clarity and allows for prior planning accordingly. 159The "State of Exception" in Latvia as a special legal regime can be declared if: 1) the State is endangered by an external enemy; 2) internal disturbances which endanger the democratic structure of the State have arisen or are in danger of arising in the State or any part thereof.' 160The latter situation includes civilian unrest, riots and internal conflicts even though this may fall below the threshold of an internal "armed conflict" (NIAC). 161Upon a declaration of a "State of Exception', the reasons, time, territory, set of measures, restrictions and additional duties of civilians, the tasks of state and local authorities and information to and recommendations for actions of inhabitants must be stated. 162

As HRL still plays an important role in case of national emergency and crisis, the possible derogations of applicable human rights law regimes in times of national emergency and war is a viable and necessary option for states, in order to ensure compliance with constitutional rights and HRL treaty law. 163However, this may result in different national derogations and, thus, an even wider discrepancy of the content of the host nation's emergency (martial) laws and more legal complexity. 164Hence, member States of defense alliances such as NATO should seek to align their possible derogation from the HRL regime applicable, in particular regarding those states which are bound to the same regional HRL treaties. According to the "derogation clause" contained in HRL treaties, a derogation from most provisions is possible:

In time of war or other public emergency threatening the life of the nation ... may take measures derogating from its obligations under the Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law. 165

Not permissive under any circumstances is a derogation from the provision concerning the right to life (Article 2 of the ECHR), except in respect of deaths resulting from lawful acts of war, the prohibition of torture and other forms of ill-treatment (Article 3 of the ECHR), the prohibition of slavery or servitude (Article 4(1) of the ECHR) and no punishment without law (Article 7 of the ECHR). 166When the threshold of an "armed conflict" has been exceeded and the LOAC applies, the special LOAC regime will determine whether lethal use of force is lawful. 167

This is not the place for a detailed analysis of the conditions and validity of possible derogations from, inter alia, the ECHR in time of "war and other public emergency'. Nevertheless, from the military legal advisor's point of view, both the de facto declared and possible future derogations, their content and validity should, if possible, be considered in planning and executing military operations in a hybrid crisis and potential armed conflict. Here, it suffices to allude to some of the legal "gray zones" by the interpretation of the HRL "derogation clauses."

First, the term "war" in Article 15(1) of the ECHR has not been subject to interpretation by the European Court of Human Rights, but should be held to equal the definition of an "armed conflict" in the meaning of the LOAC, whether a NIAC or an IAC. For the purpose of a HRL derogation, a "conflict" below the threshold of an "armed conflict" will mostly constitute a situation of "other public emergency threatening the life of the nation," where the European Court of Human Rights has deferred to the national authorities' prima facie assessment as to whether such an exceptional situation exists with subsequent judicial appreciation. 168 Second, a HRL derogation can be made for a part of the state, where the "armed conflict" or an actual or imminent crisis in terms of "other public emergency threatening the life of the nation" exists. 169 Third, and most importantly, it is up to each individual Contracting State, responsible for the life of its nation, to determine whether the life of the nation is threatened by a "public emergency." Thus, it is presumably the individual, receiving state (host nation) which for its territory or a part thereof will have to declare a HRL derogation. 170

c. The Dilemma Regarding Use of Private Contractors and Civilian Resistance

The use of state contractors (PMC or PMSC) and the use of civilians for the support of military operations is a delicate legal matter for various reasons.

The employment of state contractors raises the issues of lack of **c**ommand a**n**d **c**ontrol, lack of disciplinary competence, insurance of compliance with national peacetime laws and, when applicable, the **LOAC**, operational security and jurisdiction issues. Some states are reluctant regarding the use of PMSC, others require compliance with specific vetting procedures, and others may have a general state policy of not using private companies for any military and security tasks in peacetime and crisis, 171and involving direct participation in hostilities in case of an armed conflict. 172Hence, there may be requirements from sending states (TCNs) for the use of their own PMCs or PMSCs such as U.S. contractors as well as host nation caveats in this regard. An important "gap" in the NATO SOFA is present regarding this issue. It may be dealt with differently in various specific bilateral SOFAs. When an opponent in a hybrid information campaign is systematically exploiting mistakes, the possible misconduct and illegal acts of PMC and PMSC employed to be a sending state and positioned out of reach of the military chain of command **poses an even larger risk** and a legal challenge of ensuring law compliance in host allied nations.

The voluntary use of civilians to support an armed defense of a state or the spontaneous appearance and/or encouragement of civilian resistance (a sort of modern levée en masse) likewise raises legal issues. The civilian support can constitute acts harmful to the adversary and, thus, constitute taking direct part in hostilities that lead to loss of civilian protection. If this is not the case, civilians supporting armed forces may risk being part of lawful collateral damage. Overall, the civilian population as such may be endangered as the vital distinction between civilians and armed resistance (NIAC) or civilians and combatants (IAC) will be blurred. Moreover, the population in Estonia and Lithuania may refer to their constitutional duty and right to defend their state independence and country against armed attack and invasion, as either a last resort ("[i]f no other means are available") 173or an unconditioned duty and right. 174

This "duty" and/or "right" to conduct civilian resistance depends on the means available such as weapons (also improvised), ammunition, cyber/media capabilities among the civilian population, and the lawfulness of such acts by " levée en masse" movements under the LOAC, which will not be further analyzed here.

d. Specific Legal Challenges by countering Informational Campaign and Psychological Operations

A hybrid information campaign, psychological operation, or any other hostile informational activity regarding fake news will not reach the threshold of an armed conflict in the sense of an armed attack or equivalent acts of aggression, but may still constitute an unlawful threat of attack or other unlawful acts under international law such as interfering in the internal affairs of other states. If the hybrid information campaign includes encouragements of the commission of acts contrary to general principles of humanitarian law and illegal advice in a distributed manual on psychological operations this would constitute a violation of LOAC, including the Common Article 3 of the GCs in a NIAC. 175In addition, national law usually limits, prohibits or even criminalizes certain forms of propaganda for unrest, riots, terror or other acts of hostilities and war. 176

The means and methods to counter hybrid information campaigns and psychological operations in peacetime and crisis are limited firstly by SOFA restrictions such as the general prohibition under the NATO SOFA to engage in any "political activity" in the receiving state, secondly by HRL restraints, and most importantly, thirdly by the limited extent of suitable and capable law enforcement measures applicable in peacetime and crisis. For the most part, counter information measures will have to be strictly based on facts and truth and will, thus, come too late to prevent the effect of the hybrid campaign - the countermeasures will only mitigate the damages. The effective measure against a hybrid information campaign is a rule of law-based counter and preemptive information about an existing hybrid threat and warfare, knowledge of which can build civilian, political and legal resilience.

VI. CONCLUSION AND THE WAY FORWARD: BUILDING LEGAL RESILIENCE IN JUS ANTE BELLUM

A defense alliance can undertake various tasks, and the core tasks for NATO are three: cooperative security, crisis management under Article 3-4 of the NATO treaty, and collective defense under Article 5 of the NATO treaty. The raison d'être of NATO is maintaining member state's commitment and support, where legal legitimacy, adherence to legal values, and member states "rule of law" policies are essential parts.

The legal interoperability and legal resilience are, however, decisively challenged by a hybrid threat and warfare mostly conducted just below, or in the "gray-zone" of the threshold for armed conflict and, thus, apparently in a peacetime or crisis legal setting. Here, the framework for a response by individual states and NATO, as such, is to some degree uncertain, different from nation to nation and imposing legal constraints, making it difficult and complex to respond effectively. These legal challenges and "gaps" within the jus ante bellum and additional gray-zones in the jus ad bellum and jus in bello - some of which are analyzed above - will have to be considered more thoroughly by defense alliances, such as NATO, and its member states with the purpose of building and increasing legal resilience. 177

On the one hand, the legal framework of the jus in bello applicable in case of an armed conflict and the activation of individual and collective self-defense according to Article 5 of the NATO Treaty is well-codified at the international level and/or supplemented by customary international law, although a number of key issues remain unregulated and/or disputed. The critical issue is not the content of the law governing the conduct of hostilities but rather the conditions for the applicability of the jus in bello. This grayzone area of the threshold for a NIAC (organization, intensity and territorial control) and an IAC (attribution of hostile activities to states in terms of "effective control" or "overall control") gives ample options for the conduct of hybrid campaigns.

On the other hand, the jus ad bellum is covered by several gray zones and uncertainties, which in a hybrid threat and warfare setting create significant legal "gaps" to be exploited by, in particular, non-law-abiding states and non-state actors. The unclear and disputed "gravity" requirement and the unsettled issue of a possible use of force under the disguise of a "humanitarian intervention" are symbolic in this regard.

Apparently, the case law of the ICJ is based on a ratio of restricting the right to use force (the jus ad bellum regime) by setting a gravity requirement for the jus ad bellum, a formalistic approach to (collective self-defense) and a highly effective control test for state attribution, which all seem out of tune with the realities of hybrid threats and warfare. Such a restrictive and formalistic view of international law may turn out to achieve the exact opposite; it opens several windows of opportunity for an asymmetric hybrid warfare below the critical threshold for the right to war ( jus ad bellum) and narrows down the possibility to create effective deterrence policies and apply effective countermeasures.

Most importantly, the legal regime applicable before a situation of state self-defense and an armed conflict is, to a large extent, national and not international and uniform. Thus, the content of jus ante bellum applicable in each state differs significantly and is only in some areas, such as HRL, aligned. The supporting treaty framework for NATO operations mainly focuses on whether and on what conditions foreign forces, Headquarters, and NATO as an organization, national representatives to NATO and international staff to NATO can be present in alliance or partner states (questions of entry, status and jurisdiction). However, these agreements and **bilateral SOFAs do not address how and to what extent foreign forces can act, use force, support security** and crisis management under Articles 3-4 of the NATO treaty and be used in supporting law enforcement in a state of emergency or martial law. This is a decisive regulative and an alignment "gap" in the existing the SOFA regime. The national emergency (martial) law and the applicable HRL with possible national derogations in times of crisis provoked by a hybrid warfare differ decisively, which reduces the important legal resilience in jus ante bellum.

The possible way forward is to build more legal resilience in the jus ante bellum and align the current views and interpretations of international law, including the jus ad bellum, jus in bello and jus post bellum in order to meet the legal challenges of hybrid threats and warfare. If a defense alliance, such as NATO, wants to effectively counter the ongoing and future hybrid threats and warfare, the aspects of legal resilience and robustness must be an integrated part. Therefore, it is recommended that a NATO Center of Excellence on Legal Resilience (Legal Resilience CoE) is set up with this main task. Research should inter alia be conducted on: (i) the various gray zones and "gaps" in international law, the LOAC and HRL; (ii) the different national peacetime and emergency regulations and how these could be improved, aligned and model laws drafted; and (iii) a possible reform of existing SOFAs by drafting new model SOFAs, which address the significant "gaps" in the current SOFA regulation.

#### US leadership over PMC regulation encourages international follow-on

Michael Scheimer 9, 2009, “Separating Private Military Companies From Illegal Mercenaries in International Law: Proposing an International Convention for Legitimate Military and Security Support the Reflects Customary International Law”, American University International Law Review, Article 6, Vol. 24, Issue 3,

2. The Convention Should Specifically Require PMCs to Adhere to the Laws of War The convention should explicitly require PMCs to adhere to the rules of the laws of war, humanitarian law, and international criminal law.151 Furthermore, the convention should require that PMCs only work for recognized governments or internationally accepted movements for self determination.152 Only association with a state or emerging state through contract marks a PMC as a legitimate actor.153 A PMC that fails to obey the provisions of the convention should lose its approved PMC operator license. 3. The PMC Convention Should Require Registration and Licensing for PMCs to Establish Legitimacy The licensing process should clearly distinguish the legitimate PMC from the lone mercenary in the eyes of the international community, by vetting the backgrounds of the PMC’s employees.154 The international community should shun any PMC that does not go through the licensing process,155 although some countries may chose to ignore the requirements of international registration and hire non- accredited PMCs at their peril.156 But those states run the risk of becoming tainted by the actions of PMCs on their behalf that may reflect poorly on the state.157 It is also in a PMC’s interest to become internationally licensed so the PMC may present the license as a clear, international approval of the PMC, distinguishing it from the illegal operator.158 Furthermore, if PMCs choose not to seek a license, the stigma of being an unaccredited PMC could have an impact on their global business.159 It is also in the interest of the PMCs themselves to have a uniform, international standard rather than risk the uneven application of laws to their employees in different countries.160 4. The U.S. Must Champion the Initiative to Draft a PMC Convention The absence of U.S. support for the 1977 and 1989 definitions of mercenaries has only weakened the impact of the resulting international conventions.161 Since the flood of private military firms is a result of the build up of Cold War forces, and the consequent draw down of military forces during the 1990s, it is vital that the United States, its allies, and the former Soviet Bloc states take the forefront of revising international law.162 The U.S. failure to implement a strict domestic licensing and oversight regime regulating the PMCs accompanying military forces weakens the effect of any U.S. law.163 In particular, the United States should take the lead in an international solution because of the highly visible problems in Iraq with private military firms that are working for U.S. government agencies.164 Furthermore, the support of major state powers like the United States and its allies will ensure the new convention is speedily implemented, and does not sit idle for decades like the U.N. Convention.165

#### Russian PMC’s cause World War Three

Steve **Bird 19** - Senior Reporter at TELEGRAPH MEDIA GROUP. (“Rash Russia could start world war, says defence chief,” the Sunday Telegraph, 09/10/2019, accessed thru Lexis ) PJW

RUSSIA'S imprudent behaviour and lack of respect for **i**nternational **law** risk an "**inadvertent miscalculation**" that could **escalate into world war**, the Chief of Defence Staff warns today.

Drawing comparisons with the series of catastrophic events in 1914 that triggered the First World War, General Sir Nick Carter writes in an article for The Sunday Telegraph that peace is under threat from "new types" of "alternative weapons" that no longer need to "go bang" to destabilise international security.

In a Remembrance Sunday message, he highlights how a "grey zone" has emerged where new techniques, including cyber attacks, assassination, fake news, corrupt business practices and the use of **private security companies, are creating a world "less stable than at any time since World War Two".**

After outlining how Russia has been accused of testing "disinformation tactics" through Facebook, Sir Nick writes: "I am not suggesting that our opponents want to go to war in the traditional definition of the term, but **reckless behaviour** and the lack of respect for international law relating to these new types of 'weapons', **risks escalation** that could easily lead to inadvertent miscalculation.

"The July crisis of 1914 instigated by the assassination of Archduke Ferdinand escalated into war as a result of a complex web of alliances and a series of miscalculations by European leaders."

Sir Nick, 60, also calls for a "global response to modernise and protect" the multilateral alliances that have secured stability since 1945.

He explains how "ambitious" foreign powers, including Russia, China and Iran, are trying to assert themselves both regionally and globally.

Meanwhile, terrorist organisations such as Isil are determined to undermine Western democracies, a threat "complicated by mass migration and compounded by populism", he claims.

#### China models US PMC policy – Chinese PMC prolif imperils global stability

Dr. Christopher **Spearin 20** – Professor in the Department of Defence Studies at Canadian Forces College. holds a BASc from McMaster University and an MA in International Affairs from Carleton University. He conducted his doctoral work in political science, with a speciality in security studies, at the University of British Columbia. He joined the College as an Assistant Professor in 2003, was promoted to the rank of Associate Professor in 2007 and to Professor in 2017. During his time at the College, Dr Spearin has held a number of administrative and curriculum development posts and has taught in all of the College’s major on-site programmes. (“China’s Private Military And Security Companies: ‘Chinese Muscle’ And Reasons For US Engagement – Analysis,” Eurasia Review, 07/07/2020, <https://www.eurasiareview.com/07072020-chinas-private-military-and-security-companies-chinese-muscle-and-reasons-for-us-engagement-analysis/> ) PJW

On 7 February 2019, General Thomas Waldhauser, then-Commander of United States Africa Command, stated the following during a hearing of the U.S. Senate Armed Services Committee: "The Chinese bring the money and the Russians bring the muscle."1 "Chinese money" is evident in the fact that since 2009, China has been Africa's largest trading partner. Building upon this robust relationship, President Xi Jinping announced in September 2018, that USD 60 billion in assistance, loans, and investments would be forthcoming to African recipients.2 "Russian muscle" in Africa is increasingly evident through Moscow's reliance upon private military and security companies (PMSCs)—such as the Wagner Group— to do its bidding in countries like Libya, Sudan, and Central African Republic.

This article does not dispute the Commander's wide-ranging assertions about the United States' two appointed great power rivals, but it does contend that U.S. policymakers should also consider Chinese PMSCs, the "Chinese muscle" often found alongside "Chinese money." Moreover, one should contemplate the Chinese PMSC presence beyond Africa. As China develops a global footprint, for example through geoeconomic and geostrategic efforts such as the Belt and Road Initiative (BRI), its dependence upon PMSCs too will expand.

To make its case, this article has two parts. First, it presents the rationale for why **China is increasingly relying upon PMSCs.** The article identifies the growing vulnerabilities that have accompanied China's advancing global presence and the merits of a Chinese PMSC solution. Second, the article suggests the need for U.S. engagement vis-à-vis the Chinese PMSC issue despite its potential implications for China's expansionism. Indeed, the BRI, Chinese interactions with Africa, and Beijing's endeavors elsewhere will continue, thus maintaining its reliance on PMSCs. Additionally, the Chinese PMSC industry is in the midst of flux. Its eventual orientation is a matter of concern given that the United States has been the **global champion of a defensively oriented and transparent PMSC industry**. The United States assuredly wishes to dissuade China from following the assertive, offensive, and deniable route taken by Russia and its reliance upon firms. As such, the article contends that U.S. policymakers should strive, with some sensitivity, to **bring China and its PMSCs more into the regulatory fold** developed over the past 20 years.

Chinese Global Expansion and Security Privatization

While China has engaged in development assistance, resource extraction activities, and infrastructure projects with African partners since the 1990s, the BRI is of a newer vintage and on a transcontinental scale. Announced by President Xi in 2013, China is working in more than 80 countries in Central, South, and Southeast Asia, the Middle East, and the Horn of Africa to construct energy, land and maritime transportation, and communications networks with and through them, ending at the European Union. At its planned fruition, the BRI will connect 70 percent of the earth's population and be linked to countries generating 55 percent of the world's gross domestic product, and locales of 75 percent of global energy reserves.3 With the level of investment reaching perhaps as high as USD 4 trillion, the BRI is nothing less than "a Marshall Plan with Chinese characteristics."4

Taking the mature China-Africa relationship and the upstart BRI together, Chinese interests are now considerably exposed to security upheaval well beyond China's borders. Wang Duanyong and Zhao Pei categorize these overseas challenges as "extraneous risks" and "endogenous risks."5 Extraneous risks are those that Chinese actors confront in the often weak state, conflicted environments in which they invest, extract, and work. Criminality, **extremism, terrorism**, ethnic strife, and separatism frequently blight the countries in which China pursues its interests. Moreover, non-state actors may target the Chinese presence because of its perceived assistance to host government authorities. For example, in recent years, Chinese interests have been so targeted in South Sudan and Pakistan.

In contrast, endogenous risks are those of Chinese origin. Anti-Chinese sentiment may arise due to poor working conditions, the upset caused to the local economic status quo, a disregard for environmental degradations, a failure to engage fulsomely with local populations, and cultural insensitivity.6 In some instances, resentment can surface because the hiring of locals is in fact limited given a Chinese penchant for "whole chain industry export."7 Extraneous and endogenous risks can combine when the Chinese presence becomes embroiled in a host country's political dynamics. In Kenya, Zambia, South Sudan, the Maldives, Malaysia, and elsewhere, governing and opposition politicians in the midst of their politicking have decried the Chinese presence and the corruption that has allegedly occurred, leading to increased antipathy and heightened tensions.8

Though Beijing would like to rely upon local forces to provide security, host government authorities may be unable or unwilling to provide Chinese workers and businesses with adequate protection. The very weakness of many states in which China invests means that military and police bodies are often underpaid, overstretched, poorly trained, and riven by the same tensions affecting the state writ large. For instance, Chinese personnel working in the Democratic Republic of Congo report of routinely being subject to "legitimate harm" at the hands of soldiers and police officers.9 In Iraq, one Chinese business called upon the local police in response to looting only to see the responding officers join in the fray.10

Private security contractor DeWei Group has more than 8,000 employees operating in 37 countries. (Handout)

The dangers Chinese citizens and operations confront overseas and the varying responses of local forces have caught the attention of Chinese officialdom. In 2012, thePeople's Daily, the official newspaper of the Central Committee of the Communist Party of China, printed the following: "China should deeply study the diplomatic protection issue… China should also discuss how China strengthens its diplomatic influence… so that China can safeguard its national interests and protect its citizens to the maximum extent."11In terms of hard measures, note now the training offered by Chinese peacekeepers and other military personnel. Consider also that China is presently the second largest arms exporter to Africa. In terms of soft measures, the Chinese leadership hopes that economic improvements catalyzed by Chinese engagement will improve security outcomes overall. In 2014, President Xi promoted sustainable development as the way forward for security: "We need to focus on development, actively improve people's lives and narrow down the wealth gap so as to cement the foundation of security."12Nevertheless, only certain weapons are appropriate for protecting Chinese workers and worksites, embedding the lessons from training takes time, and reforming political, economic, and cultural issues takes even longer.

Yet reliance instead upon the People's Liberation Army (**PLA**) in a consistent and substantial way **is also problematic**. As the RAND Corporation's Timothy Heath identifies, the overseas protection of China's rights and interests is not fundamentally conceived as a military problem. True, Heath does recognize a Chinese capability to transport and operate military forces abroad, but this is a nascent and limited capability.13 Moreover, other obstacles confronting greater PLA engagement include the following: complications concerning China's official non-interference policy; the symbolism of a PLA presence on land; potential concerns of escalation and a related tentativeness due to a lack of combat experience; the financial implications of funding such operations; and concerns that a robust PLA presence could unduly confound Beijing's regional diplomatic relationships.14 One former PLA officer captures the limitations thus: "The need for security protection overseas is quite significant and the army is clearly not suitable for this job due to the potential problems it might cause for foreign relations."15

With the security demand not readily satisfied, the regulatory and political milieus have become increasingly supportive of a Chinese PMSC presence overseas. On 28 September 2009, the Executive Meeting of the State Council adopted the "Regulation on the Administration of Security and Guarding Services" which came into force 1 January 2010. This regulation provides some guidance on the requirements for registration and operations domestically and abroad. Lest there be concerns that Chinese PMSCs might work against the state, Article 78 of China's 2015 National Security Law draws all non-state actors to the cause of China's national security: "State organs, mass organizations, enterprises, public institutions, and other social organizations shall cooperate with relevant departments in employing relevant security measures as required by national security efforts."16 Finally, top level sanction came in the wake of attacks against the Chinese presence in South Sudan in 2016. President Xi embraced the sorts of activities performed by PMSCs by identifying a requirement for "improved safety risk evaluation, monitoring and pre-warning, and the handling of emergencies."17

The result has been a burgeoning private security industry. Domestically, 2017 statistics reveal an industry 5,800 firms strong that employs approximately five million personnel.18 China's domestic private security industry is now one of the largest in the world with a growth rate of approximately 20 percent annually.19

Internationally, the Chinese PMSC footprint, while smaller than some others, is growing in size and importance. Consider these examples. Dewei Security Group Limited protects both the China Road and Bridge Corporation's efforts to construct the Nairobi-Mombasa railway and the China National Petroleum Corporation's work in Sudan and South Sudan. It also provides security services to Chinese Poly-GCL Petroleum Group Holdings' Liquefied Natural Gas undertakings in Ethiopia. Huaxin China Security performs counter-piracy work on Chinese flagged ships operating off the Horn of Africa and in Southeast Asian waters. Guanan Security & Technology guards ZhenHua Oil's activities in Iraq. Other firms are active in Afghanistan, Cambodia, Iraq, Libya, Malaysia, Mongolia, Mozambique, Pakistan, Thailand, Turkey, and elsewhere working mostly for state-owned enterprises (SOEs). In total, approximately 30 Chinese firms offer their services overseas.20

Several factors capture the appeal of utilizing Chinese PMSCs specifically. Given the largely Chinese clientele, Chinese PMSCs can offer a common working language and respect cultural affinities.21 As one Dewei official put it, "For Chinese firms, especially with security work, they… want to speak with another Chinese person. We can also one hundred percent reflect their thinking when we work."22 Another factor is cost. Whereas foreign PMSCs often have more experience, it comes at a cost Chinese clients are unwilling to bear. Some calculations suggest that 12 Chinese guards equate to the cost of one U.S. or British guard.23 Lastly, and related to this, Chinese personnel are preferred over foreigners given sensitivity to protecting the confidential information of SOEs. Chinese PMSC personnel with former military, police, or government experience seemingly pass an implicit higher loyalty test.24 Therefore, it is not surprising that many Chinese PMSCs working abroad have their Beijing offices near SOE headquarters and the Chinese Ministry of Foreign Affairs.25

Looking to the future, opportunities seemingly abound for Chinese PMSCs. A managing director of the Chinese Overseas Security Group assessed in 2017 that "In eight years' time, we want to run a business that can cover 50–60 countries, which fits with the One Belt One Road coverage."26 Given that 2016 assessments found that Chinese PMSC personnel working abroad outnumbered PLA personnel on United Nations duty—3,200 to 2,600—**Chinese PMSCs are an important element of China's international posture.**27 In fact, for one industry watcher, China's swelling global presence and the quantitative expansion of Chinese PMSCs operating internationally taken together mean that the role Chinese firms play in "the security arena is going to affect not only the security actors but also the security stage as a whole."28

U.S. Engagement: Reasons and Response

On the one hand, the Chinese presence in Africa and a successful implementation of the BRI inherently challenge U.S. interests and standing in many parts of the world. Though the United States has implemented countering initiatives such as the Build Act, they do not match the scale of Chinese financing and infrastructure efforts.29 These activities will likely open up new markets that will help China and others to wean themselves from their reliance on the U.S. market and the U.S. dollar.30 Coupled with its material gains, China's endeavors will ideationally **advance authoritarian capitalism**, rather than free market capitalism championed by the United States, as a way of doing business globally. Absolutely and relatively to the United States, China will garner more sway abroad either through its welcomed largesse or through foreign governments now being economically indebted to Beijing.31In short, these developments easily fall into the 2017 National Security Strategy's worries that China wants "to **shape a world antithetical to U.S. values and interests**."32

On the other hand, U.S. policymakers might also benefit from a degree of perspective—the BRI's fulsome success is no sure thing and Beijing has already encountered challenges in Africa. True, speaking about the BRI specifically in May 2017, President Xi asserted that the initiative "should focus on the fundamental issue of development, release the growth potential of various countries and achieve economic integration and interconnected development and deliver benefits to all."33The Chinese narrative for the BRI and elsewhere is that China works to develop "win-win" relationships. Nevertheless, according to one China observer, "win-win cooperation is perceived as 'China is going to win twice.'"34As indicated earlier, such a dynamic increases political tensions among the governments, political parties, and populations of target countries.

Regarding China's specific reliance upon PMSCs in this milieu, this author's contention is that the United States should not look away. This is counterintuitive because, at first glance, the above might suggest that the United States should not concern itself. From one angle, China's usage of PMSCs may help to make secure various Chinese economic and political initiatives that will negatively affect the United States in a zero-sum fashion. Why should the United States help this relationship to flourish? From another angle, China faces considerable problems abroad and Beijing's usage of PMSCs speaks, in part, to this generated resistance. Why should U.S. policymakers expend limited diplomatic resources to ameliorate China's sometimes fraught relationships?

To contextualize the reasons for a U.S. response, one should recognize that **the U**nited **S**tates **is the global champion of a defensively oriented and transparent PMSC industry**. This was made plain during the military activities in Afghanistan, Iraq, and elsewhere in this century that set the United States as the world's largest consumer of PMSC services. Certainly, U.S. officials have not denied their reliance upon PMSCs. If anything, government officials promote contractors writ large as part of the "Total Force Concept." As a regulator it is important to note the U.S. **D**epartment **o**f **D**efense's 2012 decision to contract ASIS International and the American National Standards Institute to create the PSC.1 Standard. This standard buttresses the industry's defensive credentials that U.S. hiring decisions in turn reinforce. Moreover, **other states now use the standard** in their PMSC procurement efforts.35

One can also applaud the United States as a **setter of international norms** for a variety of actors. The United States is an initial signatory to the 2008 Montreux Document on PMSCs.36In the Document, "Military and security services include, in particular,armed guarding and protection of persons and objects, such as convoys, buildings and other places; maintenance and operation of weapons systems; prisoner detention; and advice to or training of local forces and security personnel" (italics added).37The document also recommends various procedures that publicly set relationships between states and firms. This document has 56 state signatories as of June 2019.

Building on this, the United States, along with only six other countries, is a member of the International Code of Conduct Association (ICoCA). This association concerns, in many ways, Montreux Document-related matters. This is through its advancement of the 2010 International Code of Conduct for Private Security Service Providers (ICoC), the industry's response to the Montreux Document. Like the Montreux Document, the ICoC has a defensive focus: firms are not to "use firearms against persons except in self-defence or defence of others against the imminent threat of death or serious injury, or to prevent the perpetration of a particularly serious crime involving grave threat to life."38

In addition, predating the Montreux Document, the United States has been attentive to PMSC usage by non-state actors such as resource extraction companies. For instance, the 2000 Voluntary Principles on Security and Human Rights is a multi-stakeholder initiative involving states and non-governmental organizations, oil, gas, and mining companies that espouses a defensive focus: "Consistent with their function, private security should provide only preventative and defensive services and should not engage in activities exclusively the responsibility of state military or law enforcement authorities."39In short, PMSCs are not to use offensive violence on behalf of their commercial clients.

It follows that there are three reasons why the United States should engage on the Chinese PMSC issue. First, Chinese economic and political dynamics that are not going to disappear drive China's reliance on PMSCs. Chinese economic growth, a key element for domestic calm, has slowed, catalyzing Beijing to look to Africa and Asia particularly in order to export its excess capacity and to find new markets for consumer goods.40 The fact that President Xi, unburdened by term limits since 2018, has linked himself closely to the BRI further extends the horizon. Indeed, Beijing has invested so much in the BRI that, for one Chinese analyst, it is "the essence of the realisation of the Chinese dream and the rejuvenation of our nation… It is the framework for foreign policy in the decades to come."41Overall, China's international outreach towards multiple continents, and the associated PMSC usage, will continue.

The second reason for U.S. engagement is that in the midst of China's continued reliance, **there is great potential for change in the orientation of Chinese PMSCs.** To explain, most Chinese PMSCs presently lack substantial capabilities to inflict lethal violence. Though the aforementioned 2010 regulation loosened restrictions on China's private security industry, rules remain in place regarding firearm possession. With the exception of firms conducting counter-piracy work at sea, the government does not permit Chinese PMSCs to use firearms abroad. Instead, Chinese PMSCs have focused on security within compounds and have generally relied upon non-lethal weaponry, martial arts, negotiation skills, local intelligence collection, and crisis management and evacuation procedures. In challenging environments, Chinese PMSCs are to rely either upon locally contracted security firms who can carry arms or upon Chinese embassy and consular officials for assistance.

This approach has its limits and there is evidence of some workarounds given the dangers involved. Non-lethal measures may not provide the necessary deterrence. Local private security may not have the requisite capabilities, skillsets, or professionalism. Chinese government officials are often at great distance from the threatened worksite or living quarters and they have to count on their relationships with a sometimes shaky host security sector described above. As such, media reports indicate a persistent dilemma that confronts PMSCs: stay unarmed or delve into the local black market for weaponry.42 Others indicate that firms have borrowed firearms from the local security firms.43 Underscoring the need to arm their personnel, some firms have made arrangements abroad for firearms training.44

Additional change, going beyond a more robust defensive posture through firearms usage, might arrive through Chinese concepts and an experiential record concerning non-state actors that could frame an offensive use of PMSCs. Conceptually, since 2003, the Communist Party and China's Central Military Commission have embraced the so-called "Three Warfares" concept. While one can find an in-depth consideration of this approach elsewhere, it is important to stress for this article that it places less emphasis on violence delivered by state armed forces.45 Instead, "Three Warfares" pays greater attention to a wider variety of tools, including state and non-state actors, which are neither as costly nor imbued with the same degree of symbolism. As Laura Jackson suggests, this stance is "a significant shift away from current understandings of war as defined primarily by the kinetic and tangible, and towards one focused more on thought processes, mental impressions, and the will to act."46 Yet the concept's tools can be coercive in their own way and are the means to achieve strategic objectives. To explain further, these tools, used alone or in combination, are not as likely to spark a considerable response from adversaries prohibiting China's task achievement. In fact, their **usage may be ambiguous**, thus further hindering the reactions of others. Moreover, utilization of the "Three Warfares" is constant, thus **blurring the boundaries between war and peace.** As asserted by Elsa Kania: "the application of the three warfares is intended to control the prevailing discourse and influence perceptions in a way that advances China's interests, while compromising the capability of opponents to respond."47

The realization of this concept is evident through Chinese practices at the country's peripheries. As Lora Saalman contends, China relies upon "'little green men' (nomads and paramilitaries at land borders) and 'little blue men' (fishermen and coastguard vessels at maritime borders)" to expand its influence.48 Reliance on these actors keeps the Chinese military in the background while the status quo is nevertheless upended in China's favor by means of incremental moves, coercion, and ambiguity. James Kraska asserts that such an approach augments "operational, legal and political challenges for any opponent ... [it] complicates the battlespace, degrades any opponent's decision-making process and exposes adversaries to political dilemmas that will make them more cautious to act against China."49

Though China uses this approach in areas of proximity to the mainland, one can argue that it might be employed further away. Indeed, China's approach towards the South China Sea is arguably a testing ground for future activism.50In this vein, the successful spread of the BRI might recast what is deemed as China's periphery, at least in a strategic sense.

In sum, one should not shy away from considering the future trajectory of Chinese PMSCs given these ideas and evolving practices. Without a doubt, they would stand contrary to the U.S. experience and how the U.S. approach has framed the defensive and predictable character of the international PMSC industry.

The third reason for U.S. engagement is to dissuade China from mimicking the route taken by Russia in its usage of PMSCs. Not only has Russia relied upon companies in a generally offensive manner, as a non-signatory to the Voluntary Principles on Security and Human Rights, it has advocated a particularly aggressive posture vis-à-vis resource producing areas. For instance, a Syrian-Russian agreement permits Russian extractive companies to accrue 25 percent of the proceeds produced from regions external to Damascus' control. To capture these regions, PMSC reliance is required. On the one hand, Moscow has put this development in the context of countering international terrorism. President Putin commented that "members of these firms are risking their lives in the fight against terrorism by retaking oil wells and infrastructure that had been controlled by the Islamic State."51On the other hand, one should recall the February 2018 clash in Syria between U.S. forces and the Russian firm Wagner. This is because near the battle site was the Coneco oil processing facility under non-ISIS and non-regime control.52 Due to the aggressive bent of some Chinese non-state actors, the resource-centric elements of China's relationship with Africa and the BRI, and the fact that China also is not a signatory to the Voluntary Principles on Security and Human Rights, one could envision a more provocative and assertive China following a similar path.

Furthermore, there are potential similarities between Russia and China regarding transparency. For Russia, a non-signatory to the Montreux Document, despite high-level recognition that firms like Wagner are working abroad, Moscow denies official control and responsibility. Again, to quote President Putin, companies "are indeed present there [Syria]… However, they are related to neither the Russian government, nor the Armed Forces; therefore, we have no comment."53Nevertheless, according to analyst Mark Galeotti, connections with the state are plain: firms are "'hybrid businesses,' technically private, but essentially acting as the arms of the Russian state."54 For China, PMSC usage is a prospective tool to avoid negative outcomes that might be associated with a PLA mission abroad and an official disruption of the aforementioned non-interference policy. Because former members of China's state security sector populate firms, they are possibly "a parallel security strategy" upon which the Chinese state can rely.55 Also, similar to Russian firms being both celebrated and denied, analysts from Merics and the International Institute for Strategic Studies contend that firms permit China "plausible deniability in worst-case scenarios whilst reaping the PR benefits of successful missions in the best-case scenarios."56 For the United States then, Russian deniability vis-à-vis PMSCs has already proven problematic in the context of **gray zone conflict**.57 Diverting China from considering a similar path would no doubt be optimal from the U.S. perspective.

#### China-led global order causes nuclear war

Hass 17, senior fellow and the Michael H. Armacost Chair in the Foreign Policy program at Brookings, where he holds a joint appointment to the John L. Thornton China Center and the Center for East Asia Policy Studies. (Ryan, 12-29-2017, "The case for continued American leadership in Asia", *Brookings*, https://www.brookings.edu/opinions/the-case-for-continued-american-leadership-in-asia/)

While I support focusing on getting our house in order at home, I fear that it would be dangerously shortsighted for the U.S. to retreat from its 70-plus-year status as the leading power and agenda-setter in the Asia-Pacific region.

We have to be able to walk and chew gum at the same time. Here’s why:

First, the Asia-Pacific region is rapidly becoming the most important area in the world for the U.S. It accounts for nearly 60 percent of global economic growth, and U.S. exports to the region create more jobs (3.4 million) than any other part of the world. It is home to five U.S. treaty allies, many of the world’s most capable militaries and the most proximate threat to America’s national security: North Korea’s nuclear and missile programs.

When America has been active in the region, it has spurred Asian countries to share the burden in responding to humanitarian disasters, dealing with climate change, increasing pressure on North Korea and agreeing on trade rules for nearly 40 percent of the global economy. At the same time, the U.S. has led efforts to push China to emerge as a constructive — and not a coercive — actor. If the U.S. withdraws from these roles, there is no other country capable of pulling the region together in common purpose to address shared challenges.

Second, America’s long and steady presence in the region has helped deter aggression, cool historical rivalries, and support the spread of market-based democracies. While the people of the region deserve credit, the U.S.-provided security umbrella also enabled progress.

Up to now, the U.S. has served as a buffer in regional disputes, and a check against China or others seeking to use their military to move borders or seize resources. If confidence in U.S. resolve to protect the peace recedes, the risk of interstate conflict will rise. Countries will confront a choice between becoming more deferential to Beijing’s interests in exchange for hoped-for security and economic benefits, or developing military capabilities — including nuclear weapons — to guard against coercion by China or North Korea. If Japan goes nuclear, for example, South Korea and Taiwan could follow. A pattern of nuclear dominoes would elevate risk of a catastrophic conflict that could crater the global economy and create unimaginable destruction.

Third, sustained U.S. support for rule of law and human rights has helped generate a more just and predictable environment for American businesses and travelers. For decades, the U.S. has promoted freedoms of speech, worship and peaceful assembly; the ability to choose leaders democratically; and the right to due process and equal administration of justice. These efforts have garnered goodwill for the U.S. by aligning U.S. power with aspirations of ordinary people.

If the U.S. pulls back from promoting human rights, China will step up its efforts to influence domestic politics throughout the region — pressuring politicians, entrapping special interests, and filtering what information reaches the public. Beijing would like to normalize its model of privileging internal security over individual liberties. There also could be heightened risk of democratic backsliding, as leaders feel less inhibited from resorting to strongman governance.

Fourth, a diminished U.S. role would embolden China to seek to hasten the return of a Sino-centric regional order. Broadly speaking, Beijing would like to maximize its influence and minimize Washington’s throughout the region. In instances where interests clash, such as over trade and maritime disputes and America’s alliance relationships, Beijing would like regional governments to side with it. Beijing also would like to lock in trade agreements and investment patterns that place China at the center and the U.S. on the outside. This would put U.S. firms at a disadvantage. Beijing does not seek to conquer new territories, but rather hopes to gain regional acceptance of the notion that China sits atop a hierarchical regional structure. Beijing views such a distribution of power as a restoration of a natural order.

So, why does it matter if the U.S. remains the agenda-setter in the Asia-Pacific? Because American leadership still holds the most promise of protecting the peace, preserving respect for rule of law and human rights, unlocking opportunities for American businesses, and increasing burden-sharing for dealing with transnational challenges. And if the U.S. withdraws, Beijing will seek to fill the vacuum. That outcome would raise the risk of democratic backsliding, nuclear proliferation, disadvantaging U.S. companies and intensifying great power competition. Given the growing importance of Asia to America’s national security and economic well-being, this is an outcome the U.S. can ill-afford.

Morten Fogt 20 - Lieutenant Colonel of the Danish Army and Chief Legal Advisor at the NATO Multinational Division North (MNDN)in Latvia/Denmark. Associated Professor in Civil and International Law at Aarhus University. (“LEGAL CHALLENGES OR “GAPS” BY COUNTERING HYBRID WARFARE – BUILDING RESILIENCE IN JUS ANTE BELLUM,” SOUTHWESTERN JOURNAL OF INTERNATIONAL LAW, 2020, <https://www.swlaw.edu/sites/default/files/2021-03/2.%20Fogt%20%5B28-100%5D%20V2.pdf> ) PJW

Second, the distinction between an IAC and a NIAC in a hybrid warfare setting will depend on evidence of state attribution, which will be a difficult and highly political issue. State denial policy and covert operations by provocateurs, Private Military Contractors (PMC) or Private Military Security Contractors (PMSC) like the Wagner Group, mercenaries in terms of non-state conventional forces and state special forces (SOF) provoking the uprising of the civilian population is a central part of the hybrid war**fare**. If one adds to this evidential legal uncertainty, the ICJ and ICTY dispute about whether one should apply a high degree of "effective control" or a lesser degree of "overall control," the legal picture of a possible perfect hybrid scenario becomes visible. The strict ICJ requirement of "effective control" in the Nicaragua case seems less convincing as it legally allows states to use non-state actors in the gray zone where these strict conditions and proof thereof cannot be met. The arguments presented by the ICTY in the Tadi? Appeal case against the view of the ICJ seem persuasive, if alleged "lawful" interventions by third states and hybrid campaigns through private non-state actors should be reduced and prevented:

A first ground on which the Nicaragua test as such may be held to be unconvincing is based on the very logic of the entire system of international law on State responsibility.

The principles of international law concerning the attribution to States of acts performed by private individuals are not based on rigid and uniform criteria ... The rationale behind this rule is to prevent States from escaping international responsibility by having private individuals carry out tasks that may not or should not be performed by State officials, or by claiming that individuals actually participating in governmental authority are not classified as State organs under national legislation and therefore do not engage State responsibility. In other words, States are not allowed on the one hand to act de facto through individuals and on the other to disassociate themselves from such conduct when these individuals breach international law. The requirement of international law for the attribution to States of acts performed by private individuals is that the State exercises control over the individuals. The degree of control may, however, vary according to the factual circumstances of each case. The Appeals Chamber fails to see why in each and every circumstance international law should require a high threshold for the test of control. Rather, various situations may be distinguished. 114

The disagreement between the ICJ and ICTY on the attribution of acts by non-state actors to a state was reinforced by the subsequent ICJ judgement in Genocide case 2007, where for the purpose of deciding state responsibility, the ICJ confirmed the Nicaragua "effective control" test and, moreover, expressis verbis, rejected the ICTY jurisprudence. 115With the ICJ jurisprudence, the attribution test for the purpose of conflict classification may well be the ICTY "overall control" test, which according to the ICJ could be applicable and suitable. However, this test does not persuade for the purpose of state responsibility. This introduces two different quality tests, which adds another legal layer of complexity: a state can instigate an IAC by having "overall control" of acts of non-state actors, but simultaneously avoid state responsibility for the acts of those non-state actors as the "effective control" test is not met. The ICJ logic of the possible application of difference attribution tests for conflict classification and state responsibility seems questionable and critical, at least from a hybrid warfare perspective. Moreover, from a general perspective, it seems unconvincing and, thus, questionable that the "overall control" test is unsuitable and in the view of the ICJ stretches too far, almost to a breaking point, the connection which must exist between the conduct of a State's organs and its international responsibility. The restrictive perception of the ICJ on state responsibility seems out of tune with the factual needs and the "requirements of international life" to be able to legally counter strategically willful and unlawful hybrid threats and warfare.

The experience in East Ukraine speaks for itself. The threshold ('trigger') for an international, armed conflict (IAC) involving more than one state, and the threshold for state responsibility are not only difficult to demonstrate with reliable evidence, but also covered with legal uncertainty. In addition, there may exist a lack of appetite to declare an IAC at the strategic political level and thereby risk an escalation and a possible ad hoc activation of collective self-defense.

C. Specific Legal Challenges or "Gaps" in jus ante bellum by Hybrid Threats and Warfare

A hybrid threat or warfare kept under the threshold of an "armed attack" and below the intensity or organizational requirement for an internal "armed conflict" (NIAC) will pose critical challenges to a peacetime law enforcement regime, as it will be conducted by inter alia indirectly employed non-state actors and covert state agents, by provoked opposition from own and foreign citizens, by cyber-attacks, and by the use of information campaigns utilizing fabricated or switched fake news.

Such a hybrid threat or warfare is often coupled with a firm denial policy of any immutability and attribution of such activities to a state initiating and de facto controlling the hybrid campaign. The integrated hybrid information campaign merely portrays a public picture of civilian movements consisting of "normal" people being dissatisfied with the current political regime in power and the society conditions in general. With the legal requirement of attribution in the sense of the "effective control" test or the relaxed "overall control" test being disputed, and clear evidence thereof likely either ignored without legal effect or covered by hybrid information campaign, a continued hybrid threat and warfare with both kinetic and non-kinetic means is possible without high, or much, political or legal risks. 116

The emerging problems with the principle of distinction just add to this. Military clothing has become popular and trendy among civilians, as paramilitary uniforms are seen more often in the streets. Regular armies have been seen to disrespect traditional uniform codes and permit self-equipment of soldiers in combat zones, missions or on exercises. Moreover, uniforms, accessories and insignia of different states are becoming more similar and hard to distinguish, even at a close distance. 117 The possible and recommendable remedy is, on the one hand, that military forces consider distinction by choice of design and uniforms and, on the other hand, that military discipline of wearing those regular uniforms when on duty is re-enforced.

If all these circumstances come together in a law enforcement scenario in peacetime or crisis, there will be several legal constraints and restraints in the jus ante bellum, which will **create legal vulnerabilities** for both the victim states (host nations) and states sending armed forces for assistance, deterrence purpose, and countermeasures. Some of these will be addressed below.

a. Limits set by the national domestic law enforcement regime and HRL

1. Respect of Receiving State (Host Nation) Law and Political System

The deployment and presence of foreign military forces are conditioned on the consent by the host nation as the territorial law of the host nation decides whether foreign military units may enter the state territory ( jus ad praesentiam) and on what conditions ( jus in praesentia). This consent can be given ad hoc prior to each individual deployment, or in general, as part of a defense agreement and standard status of force agreements. The NATO SOFA applies to the "force" and "civilian component" accompanying a force in the territory of another NATO alliance state, whether stationed or in transit. 118 Under the NATO SOFA and usually under any other standard or ad hoc agreed SOFA, the foreign forces and civilian component thereof have an obligation under treaty law "to respect the law of the receiving state and to abstain from any activity inconsistent with the spirit of" the standard or ad hoc agreed SOFA. 119 Moreover, the forces of the sending state (also termed "Troop-Contributing Nation," TCN) shall not interfere with the internal political affairs of the receiving state and, in particular, take necessary measures to avoid "any political activity." 120 As will be discussed subsequently, the latter will be of relevance by measures to counter informational hybrid activities as any such activity by foreign forces to promote a certain political view and NATO policy may be held to constitute "political activity," infra V.A(d).

Hence, the host nation's political governance and law enforcement remain intact. Foreign forces are stationed in the country only for the purpose of military exercises, planning, and deterrence measures with, as a starting point, little or no legal competence to conduct counter hybrid operations in peace time and crisis.

2. Possession and carrying of arms by foreign forces and contractors

For any conduct of military exercises, deterrence measures, hybrid counter operations, clarity on the laws and directives for the handling of weapons and ammunition is vital. In this regard, military forces are well-educated and trained to be particularly careful and observant.

According to the NATO SOFA, members of a "force may possess and carry arms" if so authorized by orders whereby "sympathetic consideration to request" from the host nation shall be made. 121Arguably, although the wording for the NATO SOFA only mentions "arms" and, hence, strictly speaking "weapons," an interpretation in accordance with the context and object and purpose of the provision would include both weapons and ammunition. 122The possession and carrying of weapons/ammunition will be governed by the sending states' (TCN's) law, military regulations on weapons and ammunition, and the specific directives and orders given to their forces, but still, due regard shall be had to the host nation regulations as well. 123

By multi-national forces stationed in a host nation, different military regulations regarding weapons and ammunition may apply. Moreover, the national requests may differ in the various host nations concerned, such as in the Baltic states, Poland, Germany and Denmark. For a multi-national Headquarters, such as the MNDN, with a distributed "Headquarters East" in Denmark and a "Headquarters West" in Latvia and ongoing duty travel between the two permanent locations, the host nation's legal framework would differ and change constantly. The varying regulations on weapons and ammunition will create legal complexity and administrative obstacles and, thus, may hamper timely and effective reactions to a hybrid campaign. There are good legal and operational reasons to conclude separate multi-national SOFAs on the question of arms and ammunition in peacetime and crisis and align the legal framework of both sending and receiving nations. 124 The "gap" in the NATO SOFA regarding specific directives for handling arms and ammunition would thereby be closed.

Under Article II of the NATO SOFA, there are two important limitations on the right which state that members of a "force may possess and carry arms" if so authorized by orders.

Firstly, the granted right under the NATO SOFA that a "force may possess and carry arms" is thus exempted from the host nation's public law regulations on weapons and ammunition as it only applies to the forces in their performance of military duties in accordance with the authorization by orders, 125where the sending states (TCNs), in principle, maintain primary jurisdiction under the NATO SOFA. 126 When not acting on duty, restrictive public rules on weapons and ammunition in the host nation may apply, such as the Danish prohibition to import, produce, collect, purchase, possess, carry and use any kinds of weapons, including specific knives, without authorization. 127 More flexible and relaxed weapon regulation for possessing and carrying arms off duty are usually enforced in other NATO alliance countries, inter alia, the Baltic states and in particular in the U.S. This is a practical and legal concern in the jus ante bellum that military personnel in peacetime and crisis will be temporarily off duty, or on leave, and in that timespan be subject to perhaps unknown, strict weapons regulation in the host nation, and in principle punishable for any violation thereof under the receiving state's (host nation) law and jurisdiction. For foreign troops present in other NATO states, the determination of when a person is "on duty" or "off duty" may not always be easy. In any case, members of foreign forces will have to be educated and trained in legal compliance with the host nation's law and regulations. 128 In a hybrid campaign, foreign troops are a more vulnerable target for provocation, threats, attacks, and media exposure while "off duty," and acts in violation of the host nation's law may be exploited by a hybrid propaganda campaign.

Secondly, the right under the NATO SOFA to "possess and carry arms" only applies to members of a force and **not to civilian components**, family members or sending state contractors, **including PMSCs.** Again, host nation law applies, and the host nation maintains primary or exclusive jurisdiction. If sending states employ civilian components and contractors to perform security and other military tasks requiring them to carry weapons and potential use of force, this should be regulated in a bilateral or multi-lateral SOFA, 129or in the host nation's applicable law. 130 Moreover, the status of state contractors is not governed by the NATO SOFA, and a specific permission for entry and stay must be granted. In this connection, the jurisdiction issue regarding state contractors should be considered. 131

3. Use of force and self-defense by foreign forces

AA) THE SOFA "GAP" ON THE USE OF FORCE

Neither the NATO SOFA nor the UN Model SOFA address the question of the source, scope and application of the use of force in self-defense by foreign forces present on foreign territory. This is a significant "gap" in the standard SOFA regulation.

Rarely do specific bilateral SOFAs deal with this vital question. The detailed US/Poland SOFA 2009 and the SOFAs between the U.S. and the Baltic states concluded in 2017, do not address this issue. Additionally, separate multi-lateral or bilateral SOFAs for major exercises are normally silent on the issue of use of force and definition of self-defense. 132 An exception to this silent feature of SOFA regulations is found in the NATO/German SOFA 1954 concluded after the end of the occupation regime following the Second World War, where the permanent stationing of troops in the former West Germany was regulated. The NATO/German SOFA 1954 (now Revised Supplementary NATO/German SOFA 1993) requires that the sending state may authorize "civilian component and other persons employed in the service of the force" to possess and carry arms. However, regarding the use of arms it must "issue regulations, which shall conform to the German law on self-defense ( Notwehr) on the use of arms." 133

BB) THE DISTINCTION BETWEEN PERSONAL AND STATE (UNIT) SELF-DEFENSE

The most restricted legal basis for the use of force is self-defense, which constitutes a generally recognized inherent right of all persons and, in addition, of all states, their organs and armed forces pursuant to Article 51 of the UN Charter and customary international law. However alike, the two forms of self-defense must be strictly distinguished.

The right to personal self-defense derives from the national law applicable and HRL. It is codified in most national laws and constitutes a necessary corollary to the right to life under HRL. However, regarding the source, scope and application the right differs decisively under various national laws.

The right to state individual or collective self-defense derives from public international law and is, pending differences in interpretation, in principle uniform. It is a right vested in a state, its organs and armed forces, and, thus, includes self-defense of the state armed force (force self-defense), the so-called "unit self-defense" or the defense of a single soldier in service and performing military duties. 134The exercise of force, unit or soldier self-defense will follow military orders and directives, including ROE, where a unit and soldiers can be ordered not to open fire, cease-fire or withdraw even if the conditions for state (unit) self-defense under international law are fulfilled. Moreover, force self-defense is usually a standing order in terms of an obligation (military duty) and not just an "inherent" right. On the contrary, the right to personal self-defense is generally seen as an inherent right of a person, which cannot be limited by military orders or directives. 135

Hence, in any discussion of "self-defense," this divide between personal self-defense under national law and HRL, and force (unit) self-defense as part of the right to state self-defense under international law must be kept in mind.

Regarding the use of force and self-defense by foreign forces, the inherent right to personal self-defense is, on the one hand, assumed to be governed by territorial law of the receiving state (host nation) albeit special agreements between the states concerned. As part of the right of state self-defense, the right of force/unit self-defense is governed by international law. The exercise of it depends on how de facto this is implemented in the law and policy of the sending state and its military orders and directives. In principle, it does not make any difference whether this right is exercised on foreign territory. 136Illustrative in this regard is the Danish Royal Standing Order 1952 (still in force) to all Danish armed forces and personnel that in case of an armed attack on the territory of Denmark or on Danish military units, including Danish forces present outside Danish territory, Danish forces must engage in combat without delay and without awaiting or requesting an order, even when there is no knowledge of a declaration or state of war. 137It is expressly stated that false orders and information not to mobilize, resist and interrupt fighting are expected, and as such may not be followed before there is necessary proof of these being issued by competent authorities. 138

CC) RIGHT TO POLICE AND TO ENSURE ORDER AND SECURITY

In the limited regulation on the use of force in the NATO SOFA, "the right to police" and to "take appropriate measures to ensure the maintenance of order and security on such premises" is accorded to foreign military units and formations inside camps, establishments or other premises occupied by foreign forces. 139It is not defined what exactly is covered by a right to police and to maintain order and security and what kind of use of force is permitted to that end. The SOFAs between the U.S. and the Baltic states further extend the right and authority of the U.S. as a sending state and authorize the U.S. on host nation territory to exercise all necessary rights and authorities for the use, operation, defense, or control of premises, including taking appropriate measures to maintain or restore order. Hence, by these SOFAs, the U.S. is entitled to exercise all rights and authorities necessary in defense of premises and take appropriate measures to protect U.S. forces, U.S. contractors, and dependents. 140However, it is not addressed whether the use of force in exercising all rights in defense and taking appropriate measures to protect U.S. forces, U.S. contractors, and dependents are governed by host nation law or U.S. law, including a presumably more extensive right to personal self-defense under U.S. law.

Outside such premises, according to the NATO SOFA, any employment of foreign military police or force is subject to arrangements with the receiving state (host nation) and only in so far as such employment "is necessary to maintain discipline and order among the members of the force." 141For other purposes, the maintenance of internal law and order is entirely the host nation's competence and task. Nevertheless, the receiving state has the obligation to seek such legislation as it is deemed necessary to ensure the adequate security and protection of the foreign forces. 142

DD) THE DILEMMA OF PERSONAL AND STATE SELF-DEFENSE IN MULTINATIONAL OPERATIONS

When the use of force is not regulated in the NATO SOFA or a separate supplementary SOFA, the territorial host nation law will apply and determine the extent to which personal self-defense may be used by members of foreign military forces, civilian components, dependents, and contractors. The inherent right to personal self-defense is universally recognized, but the threshold for an attack or imminent threat of attack to life or causing of serious personal injury varies, just as the possibility to use force in self-defense of others and for the protection of property differs, and the proportionality and necessity requirement can be very strict or to a wide degree relaxed. 143

If based on an agreement the law of the sending states applies, the multi-national forces and Headquarters will face a multiplicity of personal self-defense concepts, and the host nation may have to accept the use of force in self-defense on its territory beyond what its own national law permits. Conversely, if the law of the receiving states (host nation states) applies, there will also be more concepts by cross-border operations and distributed Headquarters and, rather critical, some sending states such as the U.S. will see their national definition of personal self-defense narrowed down -- perhaps to an unacceptable degree.

This constitutes the dilemma of personal self-defense in multi-national operations, which, in principle, is unsolvable. There is no expectation that a law harmonizing the personal right to self-defense will see the daylight in a near or foreseeable future at a global or even regional level. One will have to choose between one of the two options of applying either the law of the sending states (TCNs) or the law of the receiving states (host nations). In NATO, the first path of referring to the sending nation law regarding personal self-defense has been chosen. Here, the ROE do not limit the inherent right to self-defense under national law by forces under NATO command and control of foreign territory. 144This approach may be adopted at a national level in the ROE issued for peacetime and crisis by a host nation or agreed upon by separate SOFAs, which then allows foreign forces to use force in accordance with their own national concept of personal self-defense. 145

Until unity of allied command is established by a Transfer of Authority (TOA) from each nation to a common military command such as NATO, the national formations and units will operate under national command and directives regarding the use of force. This means that various national ROEs and policies of state (force/unit) self-defense will apply in a low threshold hybrid warfare theater. The example of the NATO enhanced Forward Presence (eFP) in the Baltic states and Poland is illustrative; as of October 2019, the four multinational battalions consist of rotating troops and staff members from twenty-one countries and four host nations with consequently multiple policies and interpretations of force/unit (state) self-defense being applied. 146

This constitutes the dilemma of state (force/unit) self-defense in multi-national operations and will be the status of the jus ante bellum and jus in bello until there is a TOA to NATO by all nations involved. When the allied headquarters is in command, it can and likely will authorize and issue common ROE, which depending on the situation can have a defensive or (perhaps dormant) offensive character. 147 By such ROE, the differences in the national concepts of personal and force (unit) self-defense can be leveled out by, inter alia, the use of ROE requiring hostile act and hostile intent for the use of minimum but up to lethal force. The use of force against persons, units or groups showing hostile act and hostile intent (perhaps including "hot pursuit') will be in line with the concept of personal and force (unit) state self-defense of some states and clearly excessive when compared to national law and directives of others.

The TOA decision is a critical national political matter and the TOA over national armed forces may come under conditions and, thus, include reservations and caveats. It is only likely to be granted by states just prior to or immediately after activation of individual and collective state self-defense. In a national crisis and in cases of small-scale armed hostilities with non-state actors and armed groups in parts of the territory of an alliance state only, the territorial states concerned may wish to retain command and control of national armed forces and, thus, for the time being refuse TOA. This disregarding whether the armed hostilities fall below or exceed the threshold for a NIAC, where in the latter NIAC scenario, according to the prevailing and convincing view, the LOAC applicable for a NIAC extends to the entire territory of the states concerned.

Another and recommendable option -- even though presumably politically difficult -- would be for all states concerned, to agree on common ROE applicable in peacetime and crisis when taking part in NATO reassurance measures, either by ad hoc agreements or a supplementary SOFA, and thereby filling the decisive "gap" in the NATO SOFA in the time prior to TOA to NATO command.

4. Military Assistance and Support to Law Enforcement and Crisis Control

The receiving state (host nation) has the sole responsibility and competence regarding internal security and law enforcement. However, the host nation can permit, and upon consent receive support from law enforcement in peacetime and crisis from the military forces and civilian component of another state present on its territory. The military forces of the sending states have limited authority, which is confined to maintaining law and discipline in designated military facilities, areas, and among members of their forces. Further authority is not granted under the NATO SOFA and only exceptionally given in separate bilateral SOFAs. In Article 29(2), the US/Poland SOFA 2009 authorizes exclusively U.S. operations outside such designated areas for the purpose of protecting U.S. forces and dependents:

Upon request of either Party and with the consent of the appropriate authorities of the Republic of Poland, United States military authorities may operate outside of the agreed facilities and areas in order to ensure security of United States forces and dependents. During such operations, United States military authorities shall use clear identification of their special status, and they shall immediately contact the appropriate authorities of the Republic of Poland and shall act consistent with their instructions. 148

The legal framework in the host nation, including the applicable HRL constraints and restraints, and the limits for military support to civil law enforcement must be clarified. In addition, the sending states' (TCN's) possible reservations and caveats regarding supporting operations must be adhered to as well. In any event, such foreign military support requires, not only specific military and police training, including legal training, but in particular mutual trust regarding the performance of law enforcement (police) tasks. The host nation and TCNs' caveats may concern the possible military support in the first place and, if allowed, the specific conditions regarding, inter alia, police command and control, detention, and use of force in personal or unit self-defense, in defense of others (civilians), military equipment, and facilities. Each nation will presumably have adopted its own legal regime for the military support to police and law enforcement in peacetime and crisis, which will be designed and shaped by the national tradition and culture and, thus, constitute a sui generis regime for each nation. Consequently, an intensive legal training of incoming foreign forces regarding the host nation's peacetime or emergency law, including the impact of TCN's reservations and caveats, should be made. With the constant routine of in- and outgoing foreign multi-national forces every third to sixth month in the territories of the NATO states, placed geographically at the hybrid threat or warfare frontline, this will be a demanding, time-consuming and complex task.

In summary, while the NATO SOFA permits alliance state forces to be present and carry arms on the territory of the receiving host nation, any assistance and support to a host nation's law enforcement by other states military forces, including the use of force, must be in accordance with the host nation's peacetime and human rights law. While in times of unrest and crisis, national military force may be empowered to perform law enforcement tasks under police and/or military command, foreign forces must be especially authorized by both the sending nation and the host nation to do so.

A practicable solution -- but also a rather radical and politically sensitive one -- would be to accord to foreign NATO forces the same authorization to use force in support of police law enforcement as given to national forces at any point in time. This is the stage of Latvian law and, thus, the host nation policy at the East Headquarters of MNDN. As a general statement, the Latvian national rules on the use of force, including rules on escalation of the use of force, apply to foreign NATO forces present in Latvia. 149Thus, Latvian law permits foreign NATO forces to wear uniforms, carry and use weapons in the same way as Latvian National Armed Forces, and accord them with the relevant rights of the Latvian National Armed Forces. This includes the right to individual self-defense under Latvian law, defense of other persons and to avert an attempt to violently obtain a service firearm. When foreign forces take part in military guard duties or perform other official tasks such as support to the police law enforcement in times of emergency or crisis, they will be authorized to use force in the same manner as Latvian armed forces. If the sending states approve such a support by their armed forces, there will be alignment in the peacetime and crisis Standing Rules for the Use of Force (SRUF). 150Compared with the law of other states, the use of force permitted by the armed forces according to Latvian law could be viewed as excessive in peacetime. However, it signals a necessity to employ military force against certain hostile and armed activities on the frontline of hybrid threats and warfare already in peacetime and crisis. The same result in terms of alignment of the ROE is reached under Lithuanian law by the application of the peacetime Lithuanian Force Protection ROE 2017 by virtue of separately agreed MOUs with the sending states of eFP forces, however, with respect of the application of the personal self-defense according to national law of the foreign armed forces. 151

Turning from the East Headquarters of MNDN in Riga, Latvia, to the MNDN West Headquarters in Denmark, the use of force in peacetime and crisis is entirely a national police task with a possible exclusive supporting role by Danish armed forces. The possibility for the police to request military support from Danish armed forces (but not foreign armed forces) was extended in 2018, but it is still quite limited. It can be provided regarding a wide range of specific tasks only under the strict conditions that the resources and capabilities of the police are insufficient, that supporting operations are under police command and control, and that the rules governing the competence and the use of minimum force by the police are followed. 152With the amendment of the Police Act in 2018, it was made possible to designate specific military areas for, inter alia, NATO re-enforcement forces, the outer security of which are secured and guarded by Danish military forces only, and not by foreign forces. 153

In case of an escalation of a crisis in terms of increasing unrest, riots and armed hostilities below or even above the "armed conflict" threshold for a NIAC, deviation from the normal peacetime law enforcement regime may follow a step-by-step or at once enacted national emergency (martial) law and/or escalation steps taken collectively by the defense alliance concerned.

b. Different National Emergency (Martial) Law Regime and Possible Derogation from HRL

The Baltic states and Poland have been on the frontline of the Russian hybrid threat and warfare for years and have adapted their national legislation and planning on emergency, mobilization, re-organization of governance, civilian support, preparedness and resistance to meet the hybrid challenges. 154In addition, Poland and the three Baltic states have entered into bilateral SOFAs with the U.S. in 2009 and 2017, which supplements the NATO SOFA, and facilitates the presence of U.S. forces. 155Other NATO or PfP states without specific bilateral SOFAs or MOUs are left with the standard NATO SOFA and its "gaps".

Some of the most important issues to be dealt with in the various national emergency (martial) laws or ad hoc emergency regulations regarding national and foreign forces are the following: First, the conditions for possession and carrying of weapons and ammunition. When on duty, temporally on leave or "off duty', military personnel may need to possess and carry weapons and ammunition as the security situation may require military personnel and civilian components to be able to defend themselves at all times. Second, the use of force beyond mere personal self-defense or unit self-defense when encountering hostile hybrid activities until TOA and common NATO ROE will apply. Here, the Latvian regulation aligning the use of force by national and foreign forces seems to represent a model to follow. 156 Third, the conditions for own national, bilateral or NATO military support to law enforcement (the assist/support role). Fourth, the need for legal education and training of all personnel on exercise in peacetime and crisis scenarios. This should be prioritized as military forces will have to operate under a certain national law enforcement regime and apply the peace time and emergency law of the respective host nations.

The national regulatory approach to a state of emergency or a state of exception vary from state to state. Here again, a comparison with the legal state of affairs in Denmark and the Baltic states show a striking difference, although the countries apply the concept of total state defense.

Under Danish law, the maintenance of law and order, including law enforcement, in peacetime and crisis is exclusively the competence of the civil police with possible support by the Danish armed forces. This is where civilian and military efforts will be coordinated by local authorities and the National Operative Staff (' Den Nationale Operative Stab', the so-called NOST) on an ad hoc basis. 157The entire joint operation will be conducted under the police law enforcement regime and the use of force applicable in this context. 158There is no national regulation or law on emergency (martial law) which governs and regulates the emergency and crisis situations as such. For an international military staff and its legal advisors in Headquarters such as the MNDN in Denmark/Latvia, this creates legal challenges as the exact content of the a d hoc legal regulations and directives in emergency situations to some extent is uncertain.

Under Latvian law, as well as under Lithuanian and Estonian law, the state of emergency and state of exception is expressly regulated in a specific emergency or martial law, which provides clarity and allows for prior planning accordingly. 159The "State of Exception" in Latvia as a special legal regime can be declared if: 1) the State is endangered by an external enemy; 2) internal disturbances which endanger the democratic structure of the State have arisen or are in danger of arising in the State or any part thereof.' 160The latter situation includes civilian unrest, riots and internal conflicts even though this may fall below the threshold of an internal "armed conflict" (NIAC). 161Upon a declaration of a "State of Exception', the reasons, time, territory, set of measures, restrictions and additional duties of civilians, the tasks of state and local authorities and information to and recommendations for actions of inhabitants must be stated. 162

As HRL still plays an important role in case of national emergency and crisis, the possible derogations of applicable human rights law regimes in times of national emergency and war is a viable and necessary option for states, in order to ensure compliance with constitutional rights and HRL treaty law. 163However, this may result in different national derogations and, thus, an even wider discrepancy of the content of the host nation's emergency (martial) laws and more legal complexity. 164Hence, member States of defense alliances such as NATO should seek to align their possible derogation from the HRL regime applicable, in particular regarding those states which are bound to the same regional HRL treaties. According to the "derogation clause" contained in HRL treaties, a derogation from most provisions is possible:

In time of war or other public emergency threatening the life of the nation ... may take measures derogating from its obligations under the Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law. 165

Not permissive under any circumstances is a derogation from the provision concerning the right to life (Article 2 of the ECHR), except in respect of deaths resulting from lawful acts of war, the prohibition of torture and other forms of ill-treatment (Article 3 of the ECHR), the prohibition of slavery or servitude (Article 4(1) of the ECHR) and no punishment without law (Article 7 of the ECHR). 166When the threshold of an "armed conflict" has been exceeded and the LOAC applies, the special LOAC regime will determine whether lethal use of force is lawful. 167

This is not the place for a detailed analysis of the conditions and validity of possible derogations from, inter alia, the ECHR in time of "war and other public emergency'. Nevertheless, from the military legal advisor's point of view, both the de facto declared and possible future derogations, their content and validity should, if possible, be considered in planning and executing military operations in a hybrid crisis and potential armed conflict. Here, it suffices to allude to some of the legal "gray zones" by the interpretation of the HRL "derogation clauses."

First, the term "war" in Article 15(1) of the ECHR has not been subject to interpretation by the European Court of Human Rights, but should be held to equal the definition of an "armed conflict" in the meaning of the LOAC, whether a NIAC or an IAC. For the purpose of a HRL derogation, a "conflict" below the threshold of an "armed conflict" will mostly constitute a situation of "other public emergency threatening the life of the nation," where the European Court of Human Rights has deferred to the national authorities' prima facie assessment as to whether such an exceptional situation exists with subsequent judicial appreciation. 168 Second, a HRL derogation can be made for a part of the state, where the "armed conflict" or an actual or imminent crisis in terms of "other public emergency threatening the life of the nation" exists. 169 Third, and most importantly, it is up to each individual Contracting State, responsible for the life of its nation, to determine whether the life of the nation is threatened by a "public emergency." Thus, it is presumably the individual, receiving state (host nation) which for its territory or a part thereof will have to declare a HRL derogation. 170

c. The Dilemma Regarding Use of Private Contractors and Civilian Resistance

The use of state contractors (PMC or PMSC) and the use of civilians for the support of military operations is a delicate legal matter for various reasons.

The employment of state contractors raises the issues of lack of **c**ommand a**n**d **c**ontrol, lack of disciplinary competence, insurance of compliance with national peacetime laws and, when applicable, the LOAC, operational security and jurisdiction issues. Some states are reluctant regarding the use of PMSC, others require compliance with specific vetting procedures, and others may have a general state policy of not using private companies for any military and security tasks in peacetime and crisis, 171and involving direct participation in hostilities in case of an armed conflict. 172Hence, there may be requirements from sending states (TCNs) for the use of their own PMCs or PMSCs such as U.S. contractors as well as host nation caveats in this regard. An important "gap" in the NATO SOFA is present regarding this issue. It may be dealt with differently in various specific bilateral SOFAs. When an opponent in a hybrid information campaign is systematically exploiting mistakes, the possible misconduct and illegal acts of PMC and PMSC employed to be a sending state and positioned out of reach of the military chain of command **poses an even larger risk** and a legal challenge of ensuring law compliance in host allied nations.

The voluntary use of civilians to support an armed defense of a state or the spontaneous appearance and/or encouragement of civilian resistance (a sort of modern levée en masse) likewise raises legal issues. The civilian support can constitute acts harmful to the adversary and, thus, constitute taking direct part in hostilities that lead to loss of civilian protection. If this is not the case, civilians supporting armed forces may risk being part of lawful collateral damage. Overall, the civilian population as such may be endangered as the vital distinction between civilians and armed resistance (NIAC) or civilians and combatants (IAC) will be blurred. Moreover, the population in Estonia and Lithuania may refer to their constitutional duty and right to defend their state independence and country against armed attack and invasion, as either a last resort ("[i]f no other means are available") 173or an unconditioned duty and right. 174

This "duty" and/or "right" to conduct civilian resistance depends on the means available such as weapons (also improvised), ammunition, cyber/media capabilities among the civilian population, and the lawfulness of such acts by " levée en masse" movements under the LOAC, which will not be further analyzed here.

d. Specific Legal Challenges by countering Informational Campaign and Psychological Operations

A hybrid information campaign, psychological operation, or any other hostile informational activity regarding fake news will not reach the threshold of an armed conflict in the sense of an armed attack or equivalent acts of aggression, but may still constitute an unlawful threat of attack or other unlawful acts under international law such as interfering in the internal affairs of other states. If the hybrid information campaign includes encouragements of the commission of acts contrary to general principles of humanitarian law and illegal advice in a distributed manual on psychological operations this would constitute a violation of LOAC, including the Common Article 3 of the GCs in a NIAC. 175In addition, national law usually limits, prohibits or even criminalizes certain forms of propaganda for unrest, riots, terror or other acts of hostilities and war. 176

The means and methods to counter hybrid information campaigns and psychological operations in peacetime and crisis are limited firstly by SOFA restrictions such as the general prohibition under the NATO SOFA to engage in any "political activity" in the receiving state, secondly by HRL restraints, and most importantly, thirdly by the limited extent of suitable and capable law enforcement measures applicable in peacetime and crisis. For the most part, counter information measures will have to be strictly based on facts and truth and will, thus, come too late to prevent the effect of the hybrid campaign - the countermeasures will only mitigate the damages. The effective measure against a hybrid information campaign is a rule of law-based counter and preemptive information about an existing hybrid threat and warfare, knowledge of which can build civilian, political and legal resilience.

VI. CONCLUSION AND THE WAY FORWARD: BUILDING LEGAL RESILIENCE IN JUS ANTE BELLUM

A defense alliance can undertake various tasks, and the core tasks for NATO are three: cooperative security, crisis management under Article 3-4 of the NATO treaty, and collective defense under Article 5 of the NATO treaty. The raison d'être of NATO is maintaining member state's commitment and support, where legal legitimacy, adherence to legal values, and member states "rule of law" policies are essential parts.

The legal interoperability and legal resilience are, however, decisively challenged by a hybrid threat and warfare mostly conducted just below, or in the "gray-zone" of the threshold for armed conflict and, thus, apparently in a peacetime or crisis legal setting. Here, the framework for a response by individual states and NATO, as such, is to some degree uncertain, different from nation to nation and imposing legal constraints, making it difficult and complex to respond effectively. These legal challenges and "gaps" within the jus ante bellum and additional gray-zones in the jus ad bellum and jus in bello - some of which are analyzed above - will have to be considered more thoroughly by defense alliances, such as NATO, and its member states with the purpose of building and increasing legal resilience. 177

On the one hand, the legal framework of the jus in bello applicable in case of an armed conflict and the activation of individual and collective self-defense according to Article 5 of the NATO Treaty is well-codified at the international level and/or supplemented by customary international law, although a number of key issues remain unregulated and/or disputed. The critical issue is not the content of the law governing the conduct of hostilities but rather the conditions for the applicability of the jus in bello. This grayzone area of the threshold for a NIAC (organization, intensity and territorial control) and an IAC (attribution of hostile activities to states in terms of "effective control" or "overall control") gives ample options for the conduct of hybrid campaigns.

On the other hand, the jus ad bellum is covered by several gray zones and uncertainties, which in a hybrid threat and warfare setting create significant legal "gaps" to be exploited by, in particular, non-law-abiding states and non-state actors. The unclear and disputed "gravity" requirement and the unsettled issue of a possible use of force under the disguise of a "humanitarian intervention" are symbolic in this regard.

Apparently, the case law of the ICJ is based on a ratio of restricting the right to use force (the jus ad bellum regime) by setting a gravity requirement for the jus ad bellum, a formalistic approach to (collective self-defense) and a highly effective control test for state attribution, which all seem out of tune with the realities of hybrid threats and warfare. Such a restrictive and formalistic view of international law may turn out to achieve the exact opposite; it opens several windows of opportunity for an asymmetric hybrid warfare below the critical threshold for the right to war ( jus ad bellum) and narrows down the possibility to create effective deterrence policies and apply effective countermeasures.

Most importantly, the legal regime applicable before a situation of state self-defense and an armed conflict is, to a large extent, national and not international and uniform. Thus, the content of jus ante bellum applicable in each state differs significantly and is only in some areas, such as HRL, aligned. The supporting treaty framework for NATO operations mainly focuses on whether and on what conditions foreign forces, Headquarters, and NATO as an organization, national representatives to NATO and international staff to NATO can be present in alliance or partner states (questions of entry, status and jurisdiction). However, these agreements and **bilateral SOFAs do not address how and to what extent foreign forces can act, use force, support security** and crisis management under Articles 3-4 of the NATO treaty and be used in supporting law enforcement in a state of emergency or martial law. This is a decisive regulative and an alignment "gap" in the existing the SOFA regime. The national emergency (martial) law and the applicable HRL with possible national derogations in times of crisis provoked by a hybrid warfare differ decisively, which reduces the important legal resilience in jus ante bellum.

The possible way forward is to build more legal resilience in the jus ante bellum and align the current views and interpretations of international law, including the jus ad bellum, jus in bello and jus post bellum in order to meet the legal challenges of hybrid threats and warfare. If a defense alliance, such as NATO, wants to effectively counter the ongoing and future hybrid threats and warfare, the aspects of legal resilience and robustness must be an integrated part. Therefore, it is recommended that a NATO Center of Excellence on Legal Resilience (Legal Resilience CoE) is set up with this main task. Research should inter alia be conducted on: (i) the various gray zones and "gaps" in international law, the LOAC and HRL; (ii) the different national peacetime and emergency regulations and how these could be improved, aligned and model laws drafted; and (iii) a possible reform of existing SOFAs by drafting new model SOFAs, which address the significant "gaps" in the current SOFA regulation.

#### US leadership over PMC regulation encourages international follow-on

Michael Scheimer 9, 2009, “Separating Private Military Companies From Illegal Mercenaries in International Law: Proposing an International Convention for Legitimate Military and Security Support the Reflects Customary International Law”, American University International Law Review, Article 6, Vol. 24, Issue 3,

2. The Convention Should Specifically Require PMCs to Adhere to the Laws of War The convention should explicitly require PMCs to adhere to the rules of the laws of war, humanitarian law, and international criminal law.151 Furthermore, the convention should require that PMCs only work for recognized governments or internationally accepted movements for self determination.152 Only association with a state or emerging state through contract marks a PMC as a legitimate actor.153 A PMC that fails to obey the provisions of the convention should lose its approved PMC operator license. 3. The PMC Convention Should Require Registration and Licensing for PMCs to Establish Legitimacy The licensing process should clearly distinguish the legitimate PMC from the lone mercenary in the eyes of the international community, by vetting the backgrounds of the PMC’s employees.154 The international community should shun any PMC that does not go through the licensing process,155 although some countries may chose to ignore the requirements of international registration and hire non- accredited PMCs at their peril.156 But those states run the risk of becoming tainted by the actions of PMCs on their behalf that may reflect poorly on the state.157 It is also in a PMC’s interest to become internationally licensed so the PMC may present the license as a clear, international approval of the PMC, distinguishing it from the illegal operator.158 Furthermore, if PMCs choose not to seek a license, the stigma of being an unaccredited PMC could have an impact on their global business.159 It is also in the interest of the PMCs themselves to have a uniform, international standard rather than risk the uneven application of laws to their employees in different countries.160 4. The U.S. Must Champion the Initiative to Draft a PMC Convention The absence of U.S. support for the 1977 and 1989 definitions of mercenaries has only weakened the impact of the resulting international conventions.161 Since the flood of private military firms is a result of the build up of Cold War forces, and the consequent draw down of military forces during the 1990s, it is vital that the United States, its allies, and the former Soviet Bloc states take the forefront of revising international law.162 The U.S. failure to implement a strict domestic licensing and oversight regime regulating the PMCs accompanying military forces weakens the effect of any U.S. law.163 In particular, the United States should take the lead in an international solution because of the highly visible problems in Iraq with private military firms that are working for U.S. government agencies.164 Furthermore, the support of major state powers like the United States and its allies will ensure the new convention is speedily implemented, and does not sit idle for decades like the U.N. Convention.165

### Gunboat Diplomacy---1AC

#### NATO will overapply article V to any hybrid threat which unravels the international legal order and expands use of force justifications

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

The legal challenges that hybrid threats present for collective security guarantees have been recognized at the highest political level. At their Warsaw summit held in July 2016, NATO’s member states confirmed their readiness to assist each other at any stage of a hybrid campaign and to counter hybrid warfare as part of collective defense.294 They also underscored that the North Atlantic Council “could decide to invoke Article 5 of the Washington Treaty.”295 They repeated these points at their Brussels summit in July 2018.296 By drawing an express link between hybrid warfare and collective defense, NATO leaders signaled their resolve not to allow Article 5 to be hollowed out.297 Still, their declarations of intent strike a rather conservative note. Whilst they accept that NATO may assist an Ally at any stage of a “hybrid campaign,” it is only in cases of “hybrid warfare” that they foresee a potential role for Article 5. This is not an unreasonable position to take. As we saw earlier, recourse to the use of force to counter hybrid threats falling below the threshold of an armed attack is neither permissible nor necessarily appropriate. A pledge to invoke the mutual defense commitment in response to every type of hybrid threat would be a promise to use the proverbial sledgehammer to crack a nut. It would be unrealistic and therefore lack credibility in the eyes of hybrid adversaries.298 By accepting that the role of Article 5 is confined to situations of hybrid warfare, the Warsaw and Brussels Summit Declarations avoid such empty gestures. However, in the same breath they also concede that the application of Article 5 is contingent on the legal threshold between warfare and peace, and thus vulnerable to subversion along the lines discussed in the preceding sections.

It may be tempting to deal with the problem of legal thresholds by attempting to escape them altogether, but this is not a feasible strategy. Even if the contracting parties were to revise Article 5 NAT and Article 42(7) TEU to avoid references to “armed attack” and “armed aggression,”299 they would remain bound by the rules governing the use of force under the UN Charter and customary international law. Although the member states of NATO and the EU make up an influential part of the international community, it is not within their ability to adjust these general rules of international law unilaterally. In any event, lowering the threshold for the use of force in order to facilitate the application of Article 5 and Article 42(7) would come with significant costs, since it would loosen the legal restrictions for all states, including hostile powers. The applicable thresholds therefore cannot be unilaterally modified at will and without the risk of unraveling key elements of the international legal order as it currently stands.

A more promising approach is to strengthen legal interoperability among NATO and EU nations. One line of effort is to reduce legal gray zones,300 for example by narrowing disagreements over the gap that lies between the definition of force and armed attack. This could prepare the ground for developing a shared understanding of what kind of hybrid threats may trigger the applicability of Article 5 NAT and Article 42(7) TEU. Given that the assessment of any security threat depends heavily on its context, it may prove somewhat sterile to build such a consensus in the abstract. Drawing on war-gaming and exercises may offer a more fruitful way forward. Bearing in mind how attractive the use of proxies is to a hybrid state adversary,301 developing a common approach to attribute their activities to the sponsoring state also merits attention. Although many aspects of the rules governing the attribution of wrongful acts are settled, certain questions could benefit from a joint posture.302 NATO and EU nations should also strengthen their collective mechanisms for unmasking attempts at plausible deniability in order to deny its use as a hybrid instrument,303 as illustrated by their united response to the Skripal incident and to Russian cyber operations.304

#### Otherwise, the status quo legal precedent will be exploited by adversaries to make war more likely in every theater and signals a return to gunboat diplomacy – great power war

Terry ’19 [Patrick; Feb; 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 Volume 10, https://harvardnsj.org/wp-content/uploads/sites/13/2019/02/Return-of-Gunboat-Diplomacy.pdf]

This article explores how the “West,” the main creator of modern 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 wellsounding 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 modern 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 blasé 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 exposé 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 selfevidently 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.

#### War in the Mediterranean is likely now, draws in great powers and destroys NATO

Lesser ’20 [Ian; August 28; Lesser is Vice President and Executive Director, Brussels, “Eastern Mediterranean Brinkmanship Is a Clear and Present Danger,” German Marshall Fund, https://www.gmfus.org/blog/2020/08/28/eastern-mediterranean-brinkmanship-clear-and-present-danger]

The United States and Europe cannot be complacent about the risk of conflict in the Eastern Mediterranean. Alongside the dangerous situation in the South China Sea, the deepening confrontation in the Aegean and in the waters off Cyprus, Crete, and Libya is arguably the most serious and immediate security flashpoint facing transatlantic partners today. The crisis poses key tests for NATO and the European Union. On the face of it, the crisis has been driven by maritime demarcation disputes affecting offshore energy exploration and transport. These differences are longstanding and could be amenable to legal and diplomatic solutions. However, current brinkmanship is not really about energy per se, and it is being shaped by wider strategic developments.

Greek-Turkish relations are at the core. The détente that has prevailed between Athens and Ankara since the late 1990s is on the verge of collapse. This would have profound implications for regional stability and NATO’s ability to function in the face of pressing security demand emanating from the Levant, North Africa, and around the Mediterranean. Even if the immediate threat of conflict can be contained, the alliance could be faced with a return to the tense conditions that prevailed for decades and impeded NATO solidarity and operations.

There have been profound changes on both sides. Turkey has lost its inhibitions regarding power projection. It has become a more independent and assertive actor, encouraged by operational successes in Syria and Libya. The country has also rediscovered its maritime interests and strategy. And at a time of over-heated nationalism, Cyprus and sovereignty concerns in the Aegean and beyond are nationalist issues par excellence across the political spectrum. Ankara has few supporters for its assertive posture in Europe or among NATO allies, who are already deeply troubled by President Erdogan’s rhetoric and authoritarianism, the S-400 deal with Russia, and Ankara’s policy in Syria and Libya.

Greece, for its part, has never been closer to its transatlantic partners. Differences over finances aside, Athens is now fully in the European mainstream on key policy questions. Greek-American security cooperation has expanded significantly over the last decade, spanning changes of administration in Athens and Washington. Support from transatlantic allies and regional actors such Egypt and the UAE has encouraged a tougher stance in Athens where maritime sovereignty issues are central to the national narrative.

Both Greece and Turkey would have much to lose from an actual conflict—a reality acknowledged by all sides. It is enough to note that the tourist economy dwarfs the energy stakes on both sides of the Aegean. The coronavirus pandemic and the economic crisis affecting both countries underscore this reality. A Greek-Turkish clash would impose tremendous costs and would likely result in Turkey’s open-ended estrangement from Western partners. It would pose huge challenges for NATO cohesion and operations. Moscow might be the only beneficiary.

Greece and Turkey are at the center of this maelstrom. But unlike past periods of regional brinkmanship, many more actors are engaged politically and militarily this time. The United States, Russia, France, Egypt, Israel, Cyprus, Italy, and the UAE are among the countries conducting naval and air operations in the Eastern Mediterranean. The potential for accidents, misjudgment, and escalation has increased substantially. Recent incidents between French and Turkish ships and a glancing collision between Greek and Turkish frigates in mid-August illustrate the risk. Things can and do go wrong—and can easily get out of control.

### Cohesion Adv---1AC

#### Russian cyberattacks are inevitable - tying cyber-attacks to Article V prevents meaningful cyber defense

Blessing 22 - Jeane Kirkpatrick Visiting Research Fellow at the American Enterprise Institute, where he focuses on cybersecurity, military cyber forces, military technological transformation and force structure, US cyber defense policy including civilian-military dynamics in cyberspace, and cyber defense agreements (Jason, “The Russian Cyber Threat Is Here to Stay and NATO Needs to Understand It,” AEI, 4-25-2022, <https://www.aei.org/op-eds/the-russian-cyber-threat-is-here-to-stay-and-nato-needs-to-understand-it/>) //nt-sg

Since the Russian invasion of Ukraine, the Biden administration has escalated warnings about likely Russian cyber-attacks on American infrastructure and business. More worrying still, cyber alarmists like Senate Intelligence Committee Chairman Mark Warner, D-Va., have suggested that cyber-attacks from the Kremlin could be acts of war that trigger NATO’s collective defense.

This sky-is-falling **delusion**, particularly from leaders with access to classified intelligence, is at best **counterproductive** and at worst **dangerous**.

Cyber-attacks are **rarely** acts of war, and treating them as if they are **undermines** NATO’s ability to deal with real threats short of cyber war.

NATO has only invoked Article 5 – which triggers a collective response – once and that was after the 9/11 attacks.

Cyber-attacks are unlikely to destroy buildings and kill thousands in an instant. While collective defense extends to cyberspace, few operations could **realistically** be a cause for war.

This would include cyber-attacks resulting in death or damage like traditional military operations or coordinated assaults that take the power grid or entire economic sectors offline. These scenarios are unlikely though: such attacks **require far too much time, funding, manpower, and control**. Instead, most attacks temporarily overwhelm servers with traffic, deny network access, hold computers hostage, and steal or delete data.

Even if allies wanted to trigger Article 5 over cyber operations, **disagreements** about the definitions of threats, origins of attacks, and pain thresholds in cyberspace can **derail the process**.

Collective retaliation requires a unanimous vote across NATO; building unity across these points is **nearly impossible** for most cyber activity. Unlike missile attacks or tanks in the streets, few “red lines” exist to distinguish cybercrime, cyber espionage, and cyber disruption from digital acts of war.

Beyond the bureaucratic and logistical limitations of elevating cyber to a casus belli, focusing on cyber-attacks as acts of war **distracts** from the more likely Russian digital assaults below the level of armed conflict. These include ransomware attacks and supply chain infiltrations that look like criminal activity or espionage.

The Kremlin is particularly adept at the latter. In the SolarWinds compromise, Russia hacked one company’s software product to access networks of Fortune 500 companies and U.S. government agencies.

Spillover from operations in Ukraine poses an **additional risk.** The Russians have already deployed several digital tools to destroy computer data, resulting in corrupted computers for Ukrainian companies with government support roles. The same malicious software has also affected several Latvian and Lithuanian businesses.

The danger is another situation like NotPetya in 2017, where malware self-replicated, spread past Ukrainian targets to cripple networks in over 150 countries, and created $10 billion in damages.

Each of these scenarios are **much more likely** than a “cyber doomsday” that would justify an Article 5 response from NATO members.

To be fair, policymakers’ fears of cyber war have led to some positive developments for the alliance. For instance, over the last several years, NATO has developed its own framework for combining cyber and conventional military capabilities in warfighting. But allies **remain unprepared** to deal with “death by 1000 cuts” in cyberspace.

Concentrating only on acts of war **comes at the expense** of addressing the cumulative costs of low-level cyber threats over time. It leads to an **overreliance** on cyber deterrence or defensive whack-a-mole strategies, **neither of which are sustainable**.

Threats of retaliation **simply don’t deter** most cyber-attacks, and it is unrealistic for defensive measures to stop every hacker.

Policymakers across NATO must acknowledge that security failures are the norm in cyberspace, and that the compounding costs of failure over time are **every bit as dangerous** as the threat of cyber war.

Building cyber resilience is an important step forward. It acknowledges that, in many cases, the Russians will get the best of us in cyberspace. The focus is on controlling failures to limit damage and quickly get networks back online.

Moving from buzzword to actual strategy requires addressing several questions. Which digital assets are most significant? Where is the alliance most exposed to Russian cyber-attacks? Where should NATO reduce operating risks, and in what areas can it assume more? How can allies track long-term trends and adapt to new technologies?

The Russian cyber threat is here to stay. Collective defense is – and should remain – the cornerstone of NATO. But **time is running out** for the alliance to protect itself from scenarios that aren’t all-out cyber war.

#### Absent effective cyber defense high tech weapons are left increasingly vulnerable

Grazier 19 – Senior Defense Policy Fellow @ Project on Government Oversight (Dan, “What Should We Do About a Generation of Weapons Vulnerable to Cyberattacks?” POGO, 1-31-19, <https://www.pogo.org/analysis/2019/01/what-should-we-do-about-a-generation-of-weapons-vulnerable-to-cyberattacks>) //nt-sg

The GAO examined cybersecurity assessment reports from certain programs tested between 2012 and 2017, and found that programs across every service regularly identified “**mission-critical cyber vulnerabilities**.” For legitimate national security concerns, the GAO report does not specify the programs under review, but it does say auditors investigated a variety of weapons, including ships and aircraft, as well as communications systems. “Using relatively **simple tools and techniques**, testers were able to take control of systems and largely operate undetected, due in part to **basic issues** such as poor password management and unencrypted communications.” This echoes a warning from former Pentagon testing director Dr. J. Michael Gilmore, who wrote in 2014 that “the cyber threat has become as real a threat to U.S. military forces as the missile, artillery, aviation, and electronic warfare threats.”

In spite of the danger posed by hackers, the services have **not always been diligent** in ensuring the security of their systems—like in 2015, when the F-35 Joint Program Office canceled a cyber test, citing concerns that the test could damage the troubled fighter jet’s computer system, and in so doing actually confirmed the need for such a test in the first place. Attitudes like this appear to be part of the new normal: the evaluators for this report found “program officials GAO met with **believed their systems were secure** and discounted some test results as unrealistic.”

#### Vulnerabilities guarantee Iran and North Korea will attack NC3s – goes nuclear

Karr 21\* - Analyst for Emerging Tech Policy Laboratory Orem (Hunter, “Nuclear Defense and Control Systems (NC3) Threatened Through Advancing Technology Within Cyber Operations,” The institute of World Politics, <https://cyberintelligence.world/nuclear-defense-and-control-systems-nc3-threatened-through-advancing-technology-within-cyber-operations/)//nt-sg> \*I can’t find a date for the website, but all of the works cited were from 2021\*

Cyberspace is often used to **gain advantage** over enemies, whether it is through cyber espionage campaigns, coordinated cyber-attacks on private industries, or major attacks on critical infrastructure. A weaker state launching a cyber-attack against a stronger state, such as the United States, is certainly within the realm of possibility. If a weaker state were able to deny access to, or take control of, a stronger state’s NC3 systems through a coordinated cyber-attack, there could be devastating results, the worst being **all out nuclear war**. Currently, two weaker states that present this concern to the United States are **Iran and North Korea**.

Within the past decade, the Iranian cyber program has undergone significant improvement. They have been accused of multiple different cyber-attacks against the United States, as well as actors within their own region. These attacks showcased Iran’s cyber capabilities and underscored that Iran is **not afraid** to launch major cyber-attacks against the United States and other powerful entities. Iran recently entered into a **cyber agreement with Russia**, which includes a new emphasis on training and cooperation between these two countries. This agreement, coupled with Iran’s continuous development of its own cyber capabilities, makes Iran a **critical cyber threat** to the United States; this threat is exacerbated by the high tensions between our two states.

There have also been multiple reports stating that North Korean hackers present a **more tangible threat than their nuclear missiles**. The premise is that their hackers are at work **every** **day** infiltrating and stealing information from various systems. North Korean hackers and cyber organizations have been tied to multiple attacks within this past decade. These attacks have demonstrated the expertise of their organizations and a **willingness to attack high-profile targets** such as Sony, Microsoft, and other major establishments. North Korean hackers have been recognized as **some of the best in the world** at finding and exploiting vulnerabilities within a system. The assertions regarding North Korea, in addition to their immense history of cyber-attacks, make North Korea a constant threat in cyberspace. Tensions between our two countries amplifies this threat.

Unfortunately, the cyber threat presented by Iran and North Korea has become **more realistic and tangible** over the past decade. Their capabilities are becoming increasingly complex, and they are emboldened to attack high-profile targets to showcase their abilities. These two countries, although historically considered weak in comparison to the United States, present a **major concern** to U.S. systems, including U.S. NC3 systems, because of their advanced cyber capabilities and their ability to gain major advantages through a coordinated cyber operation against these systems.

#### NoKo escalation likely---they’re exploiting global attention on Ukraine to ramp up nuclear provocations

Terry ’22 [Sue Mi; March 24; Director of the Wilson Center’s Hyundai Motor-Korea Foundation Center for Korean History and Public Policy, former CIA analyst, served on the National Intelligence Council in 2009–10 and the National Security Council in 2008–9; Foreign Affairs, “North Korea’s Nuclear Opportunism,” foreignaffairs.com/articles/united-states/2022-03-24/north-koreas-nuclear-opportunism]

With the entire world focused on Ukraine, North Korea launched its first intercontinental ballistic missile (ICBM) since 2017 on Thursday. The long-range missile, which is designed to carry nuclear weapons, should be seen as a major escalation by North Korea.

U.S. and South Korean officials had warned that such a long-range missile test was coming and the war in Ukraine presented the perfect opportunity for North Korea to make trouble, knowing that the United States and other powers would be distracted. Now that North Korea has resumed its ICBM testing, the Biden administration must be ready for a flare-up on the Korean Peninsula even as Russian President Vladimir Putin causes bloodshed and threatens nuclear war in Ukraine. This could be the sleeper crisis of 2022.

The Russian invasion of Ukraine will only redouble North Korean leader Kim Jong Un’s determination to expand his nuclear arsenal. Kim knows that under the 1994 Budapest Memorandum, Ukraine gave up the nuclear weapons it inherited from the Soviet Union, and he no doubt figures that if Ukraine were still a nuclear power, Russia would not have dared to attack. For Kim, Ukraine’s experience only reinforces the lessons that his fellow dictators in Iraq and Libya learned the hard way: countries that give up their nuclear weapons programs become vulnerable, and their leaders face serious risks of being overthrown and killed.

There are multiple reasons to be concerned that North Korea will continue to carry out missile tests, a nuclear test, or other provocations in the coming year. First, the regime in Pyongyang has a history of greeting incoming South Korean presidents with threats. Yoon Suk-yeol, the conservative candidate who won the South Korean presidential election earlier this month, has already signaled that he will pursue a tougher policy toward North Korea. The last time a conservative president was elected in South Korea—Park Geun-hye—Kim conducted North Korea’s third nuclear test just weeks before her inauguration in February 2013. Progressive presidents have hardly gotten a pass: in 2017, during the first four months of Moon Jae-in’s presidency, North Korea conducted its sixth nuclear weapons test (of a hydrogen bomb) and two intercontinental ballistic missile tests. (A third ICBM, capable of reaching targets in the entire United States, followed later in the year.)

This year also has symbolic resonance in North Korea: it marks Kim’s first decade in power, the 80th anniversary of the birth of his father, Kim Jong Il, and the 110th anniversary of the birth of his grandfather, Kim Il Sung. The latter anniversary, on April 15, could prompt a major weapons test in North Korea. It is highly plausible, even probable, that North Korea is gearing up to test an ICBM or to launch a military satellite utilizing the same missile technology, which is banned by UN Security Council resolutions.

Even before the latest crisis, North Korea’s nuclear program was already in overdrive. Since coming to power, Kim has conducted four nuclear tests and more than 130 missile tests. Pyongyang is estimated to have up to 60 nuclear warheads and is producing enough fissile material to make half a dozen new bombs annually. Kim is now moving to place multiple warheads on a single ICBM. This capability, using what is known as a multiple independent reentry vehicle, would likely stymie limited U.S. missile defenses and enhance North Korea’s ability to strike the U.S. mainland with nuclear missiles—making North Korea one of just three countries in the world able to do so, along with China and Russia.

#### Invoking Article V for a cyber-attack ensures NATO vulnerabilities that Russia will exploit

Lonergan and Moller 22 - Erica D. Lonergan is an assistant professor in the Army Cyber Institute and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University. Sara B. Moller is a former Eisenhower Fellow at the NATO Defense College and will be joining the Center for Security Studies at Georgetown University later this year (Erica and Sarah, “Opinion | NATO’s Credibility Is on the Line with its Cyber Defense Pledge. That’s a Bad Idea,” Politico, 4-27-22, <https://www.politico.com/news/magazine/2022/04/27/nato-credibility-cyber-defense-pledge-russia-ukraine-00027829>) //nt-sg

This equivocation is not surprising, for several reasons. The nature of cyberspace often **confounds** unequivocal deterrence declarations. States tend to operate in cyberspace with **plausible deniability**, which can make it difficult to rapidly ascertain responsibility for cyber incidents. Also, it can be challenging to understand the **intent** behind observed cyber behavior, and there is often a **substantial time lag** between when an initial penetration of a network occurs and when the target even realizes the breach. And the vast majority of cyber operations cause **virtual, not physical, damage**, complicating efforts to assess and evaluate the implications of the costs inflicted. Moreover, it can take time to develop and identify a way to infiltrate a network as well as the computer code that takes advantage of a vulnerability for malicious ends. This means states may **lack a palatable cyber response** option for retaliatory purposes at the desired time.

This creates a **slew of** practical **problems** if Article 5 were to be invoked for a cyberattack. From an implementation perspective, it would trigger deliberations within the North Atlantic Council, NATO’s primary decision-making body. Decisions made within the NAC require **unanimity**, which can be difficult to achieve for many issues but is especially **burdensome** for cyber ones, given all of the ambiguities outlined above. The most likely outcome of this process would be a long, drawn-out deliberation resulting in a **divided alliance** unable to agree on how or whether to respond. Quite simply, some allies are unlikely to want to risk World War III for a cyberattack that disrupts the financial infrastructure, for instance, of another country but doesn’t lead to loss of life or sustained damage.

These challenges have major **strategic implications** for NATO. After years of publicly and repeatedly linking Article 5 to cyberspace and reinforcing that policy in response to the Ukraine conflict, a failure to achieve consensus and respond to a Russian cyberattack against a NATO member could **imperil Article 5** in other areas. The disunity that is likely to be revealed during NAC deliberations would then undermine the broader political cohesion that has, for the most part, been remarkably strong throughout the war in Ukraine. This would make it more **difficult for the alliance to respond** to other forms of Russian behavior. As Biden emphasized at a press conference last month, “the single-most important thing is for us to stay unified … We have to stay fully, totally, thoroughly unified.”

#### Russia will gradually push red-lines – that goes nuclear

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

Escalation: Can a NATO - Russia conflict be managed?

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

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

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

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

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

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

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

Conflict termination

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

#### If Article V was invoked - the US would have no choice but to retaliate with OCOs

Healey 22 – Senior Research Scholar at Columbia University's School for International and Public Affairs specializing in cyber conflict (Jason, “Preventing Cyber Escalation in Ukraine and After,” War on the Rocks, 3-9-22, <https://warontherocks.com/2022/03/preventing-cyber-escalation-in-ukraine-and-after/>) //nt-sg

First, Russian offensive cyber operations might **spark a wider war**. President Vladimir Putin has declared sanctions “are akin to a declaration of war” and may see aggressive cyber attacks as the perfect response, particularly since they are reversible and non-lethal. Russia has been entangled with Western economies for decades, especially in the realms of energy and finance. But now, as ties are being severed quickly and viciously, Russia no longer has to fear the backlash if its cyber forces were to disrupt Western banks or liquified natural gas terminals. If you are dealt out of the game, why not just flip the table?

Russia’s cyber generals may be just as enthusiastic as their Army counterparts. They may assure Putin their forces are ready for battle and can quickly and bloodlessly get the West to back down. Putin could be convinced disruptive attacks against the West are no big deal, a low-cost signal that the West should de-escalate or just the next natural move in a non-escalatory intelligence contest. After all, U.S. research found that in response to cyber attacks, “Americans are less likely to support retaliation with force” compared to a more traditional strike.

This can lead to escalation in two ways. The United States — along with countries like the United Kingdom, France, and the Netherlands — might well decide to **defend forward against such attacks**. Gen. Paul Nakasone, the commander of U.S. Cyber Command, has **insisted** his forces “must take this fight to the enemy, just as we do in other aspects of conflict.” His then-deputy has also argued that the United States **“cannot cede any territory”** to adversaries as the “Russians will keep pushing until we push back on them.”

Worse, Dmitri Alperovitch recently warned that if Russia launches cyber attacks after “[h]aving already **exhausted the power of economic sanctions**, America and its European allies would have **few choices** other than to respond to these attacks with offensive cyber-strikes of their own.” Such dynamics can feed a **spiraling escalation in cyberspace** that might take on a life outside of the control of policymakers.

#### Retal triggers tit-for-tat cyber escalation – nuclear war

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

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

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

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

### Solvency---1AC

#### Internal clarification of Article 5 commitments is key---closes gaps between expectations and capabilities and gives member states a collective framework for understanding and countering threats via coalitions of the willing

Ucko ’10 [David; October 26; Professor and Director of the Combating Terrorism Fellowship Program in the College of International Security Affairs at the National Defense University; World Politics Review, “Resetting Article 5: Toward a New Understanding of NATO's Security Guarantees,” <https://www.worldpoliticsreview.com/articles/6838/resetting-article-5-toward-a-new-understanding-of-natos-security-guarantees>]

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.

Upholding a security regime that is limited, patchy and short on substance is far from ideal, yet it would accurately reflect the alliance's current intentions, capabilities and political will. So long as both those making the promise of collective defense and those hoping to take it up are mutually aware of its true possibilities and very real limitations, it may be the least-bad and most-viable way out of an awkward situation.

### Solvency---Imminence---1AC

#### Limiting Article 5 to be bound by imminence creates a threshold that is non-escalatory

Dominic ’18 [Programme Officer at Centre for Communication Governance at National Law University, Delhi, JD from NYU. Studied at Jindal Global Law School, Studied at Queen's University “NATO: From Defensive to Offensive” Posted on January 12, 2018 by Elizabeth Dominic. <https://ccgdelhi.org/2018/01/12/nato-from-defensive-to-offensive/>]

To keep pace with the rapidly developing landscape of military technologies, the North Atlantic Treaty Organization (NATO) is reportedly changing its approach to cyber warfare. NATO, a primarily defensive alliance so far, is considering the adoption of offensive cyber warfare strategies to confront hacking attacks from its opponents. Member states including United States, Germany, Spain, Britain, Netherlands, and Norway are already actively developing offensive cyber warfare strategies and are hoping to solidify their agreement by 2019. The agreement would enable the alliance to combat cyber attacks that undermine governments and steal their intelligence information and military technologies.[1] This post will briefly examine the prospect of NATO adopting the proposed offensive cyber warfare strategy within the current framework of international law.

NATO’s Current Cyber Strategy

At present, NATO has a strong cyber defense policy in place. It aims to protect its own networks, and provides assistance to its members to develop their own cyber defense capabilities.[2] Following the denial of service (DoS) attacks against Estonia, NATO adopted a new cyber defense policy at the 2008 Bucharest Summit, which then led to the establishment of the Cyber Defense Management Authority. It was subsequently replaced with Cyber Defence Management Board, which is the nodal agency responsible for “technical, political, and information sharing between allies” and for directing and coordinating between existing cyber defence entities.[3]

In the following years, NATO made substantive progress towards integrating cyber defense into its exercises. At the 2014 Wales summit, cyber defense was established as an integral component of NATO’s core mission of collective defense, triggering the application of collective defense under Article 5 of the NATO Treaty. Under Article 5, all member states are required to come together to aid a member state if it is subjected to an armed attack. With the adoption of the cyber defence policy, an armed attack was defined to also include a cyber attack. However the threshold that is to be satisfied by the cyber attack to trigger collective defense was not disclosed so that it would remain as a deterrent for potential attackers.[4] This was followed by an official recognition of cyber as a domain of warfare in 2016.

Should NATO Adopt An Offensive Cyber Warfare Strategy?

The cyber threat landscape is rapidly undergoing dramatic changes; it is becoming increasingly sophisticated and diverse. A war in cyber space is not a distant possibility. In response to these current developments, it might be appropriate for NATO to adopt a more proactive approach to counter the threats posed by the proliferation of cyber weapons by its adversaries and to ensure global security. An offensive cyber warfare strategy, as considered by NATO could be a solution. Embedding offensive cyber operations into NATO’s military operations may serve as a deterrent for potential attackers.[5]

However the use of offensive cyber strategies should be governed by the principles of international law. Even though the UN Charter prohibits the use of force, Article 51 of the Charter recognizes the inherent right of states to act in self-defence. Therefore an offensive cyber strategy should be employed only if it amounts to an act of self-defence. In the cyber context, as per the unanimous opinion of the Group of Experts that prepared the Tallinn Manual, only cyber attacks with kinetic consequences are tantamount to an armed attack, legitimizing the use of force in self-defence. There are limited circumstances in which an act of offensive warfare can be considered an act of self-defence, which is legitimate in international law.

International Law and Offence as Defence

Currently, there are two possible types of self-defence- anticipatory and pre-emptive- that could be claimed by a state if it exercises use of force against another prior to getting attacked. However there is an ongoing debate on their legitimacy under international law. Over the course of time, anticipatory self-defence has gained international consensus with the support of significant state practice[6] and is considered legitimate if an imminent threat of attack clearly exists and the response is proportional to the threat.[7] However pre-emptive self-defence involves preventive action by a state against a non-imminent threat, and is more controversial.

Even though the ICJ has in the past ruled a claim of pre-emptive self-defence invalid in Democratic Republic of the Congo v. Uganda stating that it is not in consonance with the language of the UN Charter, the claim is being increasingly reaffirmed by many countries including Australia, UK, China and the US.[8] But if imminence is not a pre-requisite, where do we draw the line between legitimate and illegitimate pre-emptive self-defence attacks? The international community is yet to establish a criteria for determination of the same.

In light of the profound political consequences attached to an offensive attack, it is ideal for NATO to resort to offensive strategies only if either a member state is subjected to cyber attack or if there is an imminent threat. It is also imperative that the response remains proportional. However in case of cyber attacks, key questions remain in relation to the determination of proportionality and imminence. This confusion is exacerbated by the uncertain nature of law in this field, with a lack of consensus on even basic questions such as what amounts to a cyber attack.

### Hybrid Threats Key---1AC/2AC

#### Hybrid threats are the only challenge Russia will pose to NATO---threats to invoke article V are not deterring

Deni ’19 [John; Nov/Dec; Research Professor of Joint, Interagency, Intergovernmental, and Multinational Security Studies at the US Army War College’s Strategic Studies Institute; “The Paradox at the Heart of NATO’s Return to Article 5,” RUSI Newsbrief, Vol.39 No.10, https://rusi.org/sites/default/files/20191101\_newsbrief\_vol39\_no10\_deni\_web.pdf]

Despite the necessity of exercises like Defender 2020, new purchases of advanced military equipment and the expansion of military manpower (all underway since 2014), these steps together constitute a growing paradox that the Alliance has been slow to recognise and respond to. That is, just as the Alliance is becoming more focused on and more capable of responding to an Article 5 threshold-crossing event, the probability of a conventional manoeuvre warfare scenario is decreasing. Put another way, major improvements in the Alliance’s ability to defend the territory of its member states are necessary, but it is becoming ever more obvious that these steps will not be sufficient for collective defence in NATO’s next decade.

Many European security analysts believe an Article 5 threshold-crossing event is unlikely in the coming years. Russia is a declining state along several measures, especially in economic terms, and over time the acute threat that it represents today should diminish. Certainly, it has made advances recently in limited military capability areas, such as indirect fires and precision munitions. Yet, the Russian playbook evidently continues to eschew frontal attacks on states that are members of a military alliance, at least in the air, sea, land and space domains.

A frontal attack in one of these domains or some other egregious assault compelling NATO to invoke Article 5 would not play to Russia’s strengths – instead, it would actually expose its many weaknesses, ultimately resulting in certain defeat. Moscow’s military and governing elites know this. For this reason, the Kremlin has consistently chosen to emphasise and leverage its comparative advantages to make effective use of its clearly limited resources. The military policy tools that facilitate this do not resemble armoured columns crossing national frontiers. Rather, they include fomenting civil unrest with the goal of creating a justification for Russian military or paramilitary action in unaligned, neighbouring or near-neighbouring states, as seen in Moldova (1992), Georgia (2008) and Ukraine (2014). They also include cyber attacks, such as that unleashed on Estonia in 2007. They include influence peddling and the cultivation of patronage networks. And they include semi-deniable election interference, as occurred in the US in 2016 and 2018 and in Europe in recent years as well. All of these policy tools represent asymmetric responses to US and Western power, especially military capacity and capabilities. They enable Moscow to cost-effectively pursue the disintegration of Western power and the Western alliance, as a way of achieving Russia’s strategic and material ends. Given the current state of the Russian economy and the rather grim outlook for the years to come, Moscow is very likely to continue pursuing these sorts of policies in the coming decade, because it lacks other options.

The fundamental challenge facing NATO between now and the Alliance’s 80th anniversary is figuring out how, where and when it will counter and compete iteratively with Russia – but also China – in the grey zone, the space between war and peace, or between offense and defence. Because grey-zone challenges do not neatly correspond to classical notions of those which fall in the military’s domain and those which do not, they are particularly vexing. This is why adversaries such as Russia and China employ grey-zone tactics and operations – they allow Moscow and Beijing to confront the West on more favourable terrain.

The good news is that NATO’s leaders appear to understand the character of the competition, and have taken several steps to address the challenge. The Alliance has reportedly developed a strategy outlining NATO’s role in responding to grey-zone or hybrid threats. In some cases, grey-zone scenarios are finding their way into NATO and member states’ exercises. And critical infrastructure protection, energy security and societal resilience have become important topics of discussion at Alliance-sponsored events and seminars, and among Alliance-affiliated entities such as centres of excellence.

However, in several important aspects, the Alliance response remains ~~handicapped~~ [weak]. Although NATO declared in 2016 and again in 2018 that it could consider a hybrid attack as grounds to invoke Article 5, the bar seems high – perhaps impossibly so. Achieving consensus – and quickly – in the face of an ambiguous attack or in response to ostensibly unrelated low-level provocations will not be an easy task. Perhaps more importantly, NATO remains in a defensive crouch when it comes to grey-zone challenges – Alliance rhetoric, exercises and actions emphasise response and reaction. It is precisely for this reason that grey-zone challenges against NATO are likely to be effective – actors such as Russia and China are evidently undeterred by the Alliance’s defensive posture, and attacks on Western institutions continue to this day. To be clear, defence is important, but in the current international security environment, offense and the competitive actions in between the two are equally important.

Given the arguably inadequate Alliance response to date, some guideposts may be helpful to illuminate the path ahead as NATO attempts to ensure collective defence remains robust into its eighth decade. First, Article 5 is an imperfect tool for determining when and where the West must spend blood and treasure in defence of its interests and way of life. Despite Alliance rhetoric regarding hybrid warfare as a potential Article 5 trigger, the threshold for Alliance-wide action is too high, and adversaries like Russia and China know it – this is why they pursue grey-zone tactics in the first place. To facilitate the speedy response that will be necessary to meet the needs of Allied defence against grey-zone challenges, greater, routine use can be made of Article 4 and Alliancewide consultations and coordination on issues and topics that go beyond conventional military operations that are NATO’s bread and butter. For instance, the Alliance can and should conduct more vigorous, regular consultations and intensified coordination on topics such as keeping Chinese investment out of sensitive information-technology and logistics sectors, limiting and rolling back Russian broadcast and print media penetration of Western markets, undermining the Kremlin’s and Putin’s trustworthiness within Russia, and exposing Russian and Chinese official corruption at home and abroad, all as mechanisms to compete and thereby strengthen collective defence.

#### Unchecked Russian probes cause global war and instability

Richard Sakwa 20, PhD, Professor, University of Kent, Associate Fellow of the Russia and Eurasia Programme at the Royal Institute of International Affairs, Chatham House, Honorary Senior Research Fellow at the Centre for Russian, European and Eurasian Studies (CREES) at the University of Birmingham, "Stasis and Change: Russia and the Emergence of an Anti-hegemonic World Order", Russia in the Changing International System, https://link.springer.com/chapter/10.1007/978-3-030-21832-4\_2

The Dynamics of Change

The West sees in Russia a heuristic image of itself, when in fact Russia has broken out of the traditional hermeneutics of European international relations. The starkest manifestation of this is the intensification of the continuing “pivot to the East”, and in particular the close alignment with China accompanied by the strengthening of a “post-Western” world order encompassing such bodies as the SCO and BRICS, the heart of what is emerging as an anti-hegemonic alignment. Even Europe is shaken by the new dynamic of change, undermining the stasis in its affairs. The Atlantic enlargement strategy did not represent the resolution of the European security dilemma but the intensification of that problem. Relations between Russia and Europe, and with the West more generally, entered a deep impasse. The resolution of the problem it appeared could not be found from within the hermeneutics of the system itself, in which the liberal international order is faced by a number of rising powers loosely aligned in an anti-hegemonic bloc. There is a clash of orders, but at the same time some profound changes are taking place in international relations. In the framework of my two-level model of the international system, there are changes in the vertical axis— relations between states and orders and the institutions of global governance, above all the UN; and at the horizontal level, where the universalistic ambitions of the liberal international order are challenged by the emergence of the anti-hegemonic alignment as well as by non-systemic forces that seek to destroy the entirety of the international system to create, in particular, a new militant form of the Islamic ummah.

The clash between Russia and the West is only an early version, and ultimately perhaps not the most significant, of the challenges now challenging the long-term stasis in international affairs. International relations are now being reshaped, above all by the putative defection of the US from the core of the liberal international order that it has so assiduously developed over the last 70 years. Many of the themes sounded by Trump were advanced in one form or another by American leaders before him, but none with such intensity or generated by ideas that are so fundamentally at odds with the multilateral normative Atlanticism that took shape after 1945. Trump is the consummate national realist, having little respect for international institutions or multilateral processes. By contrast, Russia’s continuing commitment to international society as expressed in the UN and other “secondary institutions” means that Putin is a “conservative institutionalist”, defending international law and the traditional rules of global governance (the intervention in Ukraine in 2014 was a revisionist act, but not part of a revisionist strategy). By contrast, after 1989 “democratic institutionalists” sought to use international society to “remedy drawbacks of traditional international law and develop new institutions by using the rule of the majority in roughly the same way it works in domestic politics” (Sokov 2018). There has long been a national realist strain in US foreign policy, and it was this tendency which defeated Woodrow Wilson’s attempts to create a multilateral world order in the wake of the First World War, and which kept the US out of the League of Nations. Although Putin’s policy is pragmatic and broadly realist, it is not realist in the strict definition of the term because of its willingness to share sovereignty with international institutions (notably the UN, Council of Europe and World Trade Organization), irrespective of its chequered relations with these bodies.

At the same time, Russia challenges the attempt by democracy promotion activists and others to extend the scope of global governance bodies to disrupt the balance between sharing and maintaining sovereignty. The Responsibility to Protect (R2P) mechanism adopted in 2005 alarmed Russia and other states who considered it as an unwonted increase in the power of an international community dominated by the hegemonic powers, although in practice Russia engaged with R2P, despite the conservatism of its institutionalism (Averre and Davies 2015). In the inter–Cold War years, the main tension between Russia and the US was between the two forms of institutionalism, although both camps evolved under different leaders. Even though Putin pursued a “new realist” policy, this represented an attempt to find some mode of integration and reconciliation with the democratic institutionalist agenda, but in the end this was doomed to fail. Nevertheless, even as neo-revisionism came to predominate in Russian foreign policy, this did not make Putin a realist of the old school. It is for this reason “any cooperation between them [Putin and Trump] can only be temporary and tactical”. For Trump power is the key asset, deployed as finite asset, in a context where the balance of power is perceived to be moving away from the US (Sokov 2018). Hence Trump insists that allies contribute more to their own defence, a long-term stance of US leaders but now couched in terms of a transactional relationship rather than the traditional common commitment to multilateral institutions. It is in this light that Trump while campaigning in 2016 argued that NATO was “obsolete”, and in power he made little effort to hide his distaste for the EU. He appeared to make NATO’s Article 5 security guarantee dependent on whether a state met the 2 per cent defence spending target set in Wales in September 2014. This represents a shift from collective to transactional defence, where security guarantees apply only if the appropriate contribution has been made.

Trump’s approach to Russia is in line with his national realist view of international relations. He consistently stressed the importance of good relations with Russia (provoking the fears of the defenders of the traditional order in Washington), and pushed for the Helsinki summit with Putin in July 2018. However, this did not prevent him from taking numerous measures against Russia, including the sale of lethal arms to Ukraine, ramping up funding for the European Reassurance Initiative and reinforcing the US troop presence in Europe, condemning the building of Nord Stream 2 as making Germany subservient to Russia, imposing harsh sanctions, expelling Russian diplomats and closing down Russian diplomatic facilities in the US. His overall strategy was in the Henry Kissinger mode (and he appears to have been advised by Kissinger), namely to try to recruit Russia to align with the US against what was perceived as the greatest long-term threat, China. In practice, the sum of US actions only reinforced the Russo-Chinese alignment, and there was zero chance of Russia defecting. At the best of times, the two countries saw the US as an unreliable protagonist, and although there are plenty of voices in Moscow warning of the dangers of a too-close embrace with China, their alignment is far more than one built on the truly extraordinary relationship between Putin and Xi Jinping. The two share not only a strong personal relationship but also the conservative institutionalist position. Thus Russia condemned Trump’s withdrawal from the Joint Comprehensive Plan of Action (JCPOA, Iran nuclear deal) in May 2018 while emphasizing the crucial role of the UN, while China emerged as the great defender of open markets and global economic governance.

The struggle for recognition as an equal in the management of international affairs is now a more credible proposition, as evidenced in Russia’s remarkably effective intervention in Syria from September 2015 (even though the end game of the Syrian civil war may entail intensified great power conflict). At the tenth BRICS summit, held in South Africa in July 2018, Putin noted that the group had developed into “a full-scale organization with new spheres of activity and broader common interests”. The main topics discussed were “resistance to unilateral approaches in global affairs, the protection of multilateralism”, and the condemnation of economic sanctions and the use of force in violation of the UN Charter (Kremlin.ru 2018). BRICS established its New Development Bank in July 2014, based in Shanghai but with plans to open regional branches in all the BRICS members. At that time the BRICS accounted for 26.5 per cent of the world’s land area, 42.6 per cent of world population, and according to the IMF in 2015 generated almost a quarter of the world’s GDP and contributed more than half of global economic growth in the previous decade (RT 2018). George Toloraya (2018), executive director of the Russian National Committee on BRICS research, argued that “BRICS is about world order”, creating its own structure of global governance “to create a world order that will be more just and balanced than what we see now”.

Russia and China are not the harbingers of a new nationalism but of a new internationalism. Both insist on the equal status of all countries under international law. Under the flag of this principle, they contested the slide towards democratic majoritarian rule in international politics, and thus opposed humanitarian intervention unless sanctioned by the UN Security Council. They opposed attempts by the West to impose rules through majority decisions or the use of multilateral institutions for political purposes. This was the case when in July 2018 the majority of members of the Organization for the Prevention of Chemical Weapons (OPCW) voted on the right to draw on outside expertise to assign responsibility for the use of chemical weapons, which Russia argued gave it a political role that it feared could be used by the West to pursue broader unrelated political objectives. Moscow’s concern at the perceived politicization of the organization opened up the possibility that Russia could even leave the Chemical Weapons Convention.

Overall, if the twentieth century was the century of ideology, then the twenty-first in its Trumpian version is beginning to look rather more like the nineteenth, that is, nationalistic and mercantilist. For the commentators who in 2014 condemned Russia’s actions in Ukraine as a throwback to the nineteenth century, this would confirm a natural convergence between Putinite Russia and Trumpian America. However, this would be wrong for the reasons outlined earlier. Paradoxically, it is now Russia and China that are defending multilateralism and the governance institutions of international society. Both defend the traditional view of state sovereignty, but as noted this does not represent a simple reversion to Westphalian internationalism. Their conservative institutionalism is ranged as much against the Trumpian sovereignty discourse as it is against the expansive interventionism of the democratic institutionalists.

One of the more striking manifestations of the shift from stasis to change is that the very concept of “the West” is being challenged. It is not that Russia is looking to the East to build alliances with other illiberal states, the way that recent developments are categorized by defenders of the old liberal hegemony, but an expression of the changing realities of global politics. The West is no longer the centre of the world in economic and even normative terms. Values of good governance, defensible property rights, rule of law, free and fair elections remain embedded as the core values of international society, although tempered by developmental and security considerations in countries like Russia and China. In fact, if decoupled from the Western power system and its inexorably hegemonic demands, there is a greater chance for them to be achieved. NATO enlargement effectively militarized the democracy promotion efforts of the West, while unmediated EU enlargement and power projection into the contested “common neighbourhood” reinforced the view of critics in Moscow that “democratic institutionalism” represented a fundamental threat to Russia’s security and national interests (Hahn 2018).

Not surprisingly, some Russian analysts take great glee in describing the travails of the disintegrating West. In their view, Trump’s policy called into question the common interests and common values of some of the fundamental institutions of the old order. The G7 summit in Taormina, Italy, in May 2017 was considered a failure, while the one in La Malbaie, Canada, in June 2018 proved a veritable disaster. Trump’s application of the transactional business model to his allies raised the question of whether the West would survive in its traditional form at all. This would provide an opportunity for the anti-hegemonic alignment to assume a greater share of the burden of global leadership, but only if the end of stasis in international affairs was accompanied by the positive transcendence of immobilism. However, just as after the end of the First Cold War, a negative transcendence is possible, intensifying the conflicts and deepening the Second Cold War. The inertia associated with the post-war stasis has deep roots, but its unravelling can have both positive and negative outcomes.

Conclusion

Is an alternative possible? Some years ago Andrew Hurrell (2006, 1) noted that the four BRIC countries had a certain “capacity to contribute to the production of international order, regionally or globally”. At that time Russia was considered the outlier, since “the reality of the past two decades here has been one of decline and the dissolution of power” (Hurrell 2006, 2; MacFarlane 2006). Hurrell (2006, 2) noted that while a central theme of the twentieth century was the struggle of revisionist states to achieve equal rights, “the recognition of regional spheres of influence, and the drive for equality of status within formal and informal international institutions”, and although in the recent period “the currency of power” may have changed, the issue of recognition “has been sharpened by the growth of the idea that international society should aim to promote shared values and purposes rather than simply underpin coexistence and help to keep conflict to a minimum”. In the second decade of the twenty-first century, Russia re-emerged as an active player in international affairs, and although still only barely in the top dozen countries economically, its impressive military reform and re-equipment since the 2008 Russo-Georgian war allowed it to “punch above its weight”. Stasis and change now balance each other, and although the post-First Cold War order is unravelling, this has given rise to both a Second Cold War and the emergence of an antihegemonic alignment. The question today is whether the latter can help transcend the former.

Although the sinews of a post-Western world are emerging, notably in the form of SCO and BRICS, it remains to be seen whether these bodies and countries behind them will be able to sustain the multilateralism of the past seven decades in the absence of the hegemon that had provided the security and support for such multilateralism to thrive. The post-Western world may well assume the characteristics of the pre-Western international system, dominated by vast competing empires. Nevertheless, Trumpian realism entails partial de-globalization, and it would be the supreme irony if liberal internationalism and open markets were to be saved by the leaders of the anti-hegemonic alignment. This could herald a new age of post-hegemonic internationalism, but it could equally inaugurate a new era of zero-sum conflict, protectionism, a drive to the bottom in regulatory standards and another three-decade-long Cold War.

## AT: Ambiguity Good/Changing A5 Bad

### AT: Assurance DA---2AC

#### Eliminating unsustainable and unenforceable alliance commitments doesn’t signal unreliability

Brad L. LeVeck and Neil Narang 16, associate professor of political science at the University of California Merced, associate professor in the Department of Political Science and director of the Security Hub at the University of California Santa Barbara 2016, How International Reputation Matters: Revisiting Alliance Violations in Context, https://faculty.ucmerced.edu/bleveck/assets/pdfs/how\_international\_reputation\_matters.pdf

In this context, a particularly good indicator of future alliance behavior may be past behavior. If a state violated its agreements in the past, it seems intuitive that it may be more likely to do so in the future. However, Spence (1973) famously showed that past behavior is not always equally informative and that whether past behavior distinguishes one type from another depends crucially on the behavior’s cost. If, for instance, honoring an alliance becomes so difficult that all states are forced to violate their commitments together, then a violation conveys little information about how reliable one state is relative to another. Beyond this extreme example, the general insight is that alliance violations do more to signal that a state is relatively unreliable when many other states appear to be willing and able to honor the same agreement. Of course, whether other states would honor a particular agreement under similar conditions is often difficult to observe (Narang 2014; Narang and Mehta 2015), as each alliance has elements that are somewhat unique. However, there may be times and regions where system-level shocks cause a large number of countries to simultaneously violate alliance commitments together. This may provide relatively clear evidence to a potential partner that the costs of honoring a previous alliance were so great that even reliable states that would normally honor their commitment were unable to do so. This discussion has important implications for empirically studying how violating an alliance affects a state’s reputation. It is likely that the cost of maintaining an alliance varies significantly by region and time and that one can identify shocks across these dimensions. Figure 1, which plots the percentage of states violating their bilateral security alliance in each region and year based on Leeds et al. (2009), supports this supposition.

#### Hybrid threats are the most pressing issue to allies---clarifying Article 5 alleviates abandonment fears

Pugliese ’18 [Giulio; Feb 28; PhD, University of Cambridge, Post-doctoral Fellow, the Nissan Institute of Japanese Studies, Oxford; “Japan-EU Views on the US and Russia in an Age of Hybrid Threats,” IAI Commentaries, Istituto Affari Internazionali, https://www.iai.it/en/pubblicazioni/japan-eu-views-us-and-russia-age-hybrid-threats]

Hybrid threats and warfare represent one of the most pressing security issues in contemporary world politics. Seldom noticed and appreciated, the unravelling of the international order may slowly come about through repeated hybrid blows to US military credibility and its alliance system. In fact, the unconventional nature of coercion, and the confusion and ambiguity central to hybrid warfare have kindled fears of abandonment by security partners. Because such operations fall short of a direct and conventional “armed attack” by one state against another, the stipulated condition for self-defence and retaliation, allies may fear that in such circumstances security commitments will not be upheld.

Japan, for instance, was uncomfortable with the Obama administration’s weak-kneed response to China’s steady encroachment in the South and East China Seas, which began with China’s seizure of the Scarborough Shoal in 2012. In 2015, Abe eventually secured a redefinition of the guidelines governing the US-Japan security alliance to deter China in so-called “grey zone” scenarios also through intelligence sharing, deeper coordination and bilateral planning.[7] Somewhat similar dynamics and reassurances have been at play among NATO partners following Russia’s encroachment in Ukraine, but fears of abandonment persist.

Concerns of potential entrapments, or slippery slopes towards a full-blown military entanglement due to US security commitments, combined with the very nature of hybrid/grey-zone scenarios, is likely to cloud US decision-making in such instances. This will potentially slow retaliatory measures and circumstantial political factors will have more weight than ever on such decisions. For these reasons, Russian and Chinese activities are currently at the centre of NATO summits and security consultations between Japan and the United States.

#### Russian hybrid tactics threatens the unity and credibility of the alliance

Ivana Stradner and Max Frost 2o, Jeane Kirkpatrick fellow at the American Enterprise Institute, senior research associate at the American Enterprise Institute, NATO Has a New Weak Link for Russia to Exploit, https://foreignpolicy.com/2020/04/22/north-macedonia-nato-russia/

In 1938, British Prime Minister Neville Chamberlain made it possible for Adolf Hitler to march into Czechoslovakia despite the overwhelming military superiority of Prague’s Western allies because Chamberlain had decided the issue was “a quarrel in a faraway country, between people of whom we know nothing.” Today, it is similarly difficult to believe that NATO would go to war over its far-flung commitments in Eastern Europe. Nevertheless, on March 27, the Western alliance admitted North Macedonia as its newest—and weakest—member. In so doing, it has given Russian President Vladimir Putin a terrific opportunity to expand his influence, further erode NATO’s unity, and test the bloc’s commitment to defend a member of the alliance.

North Macedonia is the definition of a weak link and easy pickings for an adversary. A landlocked country of 2 million inhabitants, it has weak political institutions and only a short history of independence. As of 2018, it spent only 1 percent of its GDP on defense—short of the 2 percent NATO guideline—and had just 8,000 active-duty soldiers. There is simmering communal tension between a Slavic Orthodox majority and a sizable ethnic Albanian, mainly Muslim minority, making it vulnerable to interference. Within NATO, only neighboring Albania has a lower per capita GDP and a higher level of corruption. The Economist Intelligence Unit’s Democracy Index ranks North Macedonia as having Europe’s least developed political culture.Russia has held massive war games that were only thinly disguised simulations of attacks on NATO members such as Poland and the Baltic States.

Moscow has viewed NATO’s expansion in Eastern Europe with suspicion since the 1990s. Yet it wasn’t until the 2000s, after Russia’s military and economy rebounded from the chaos of the post-Soviet era, that Putin declared NATO’s eastward expansion a “direct threat” and openly confronted the alliance. Russia’s invasion of Georgia in 2008—not coincidentally, the year that NATO declared an interest in Georgia’s eventual accession to the alliance—stopped the bloc’s expansion into former Soviet-controlled areas in its tracks. Putin’s 2014 invasion of Ukraine and subsequent annexation of Crimea, while not a direct assault on a NATO member, further demonstrated Western impotence in the face of Russian aggression. Further north, Russia has held massive war games that military experts say were thinly disguised simulations of attacks on NATO members such as Poland and the Baltic States.

Now that North Macedonia has joined NATO, Putin appears to be relishing his first chance to prove that the alliance is little more than a paper tiger. In 2018, Russia’s ambassador to North Macedonia declared the country a “legitimate target” if tensions between NATO and Russia were to increase. But there was no “if” about it: Even before North Macedonia became a member, Russia had already been working assiduously to ratchet up tensions in the region. Moscow has shipped S-400 anti-aircraft missiles to neighboring Serbia for joint Russian-Serbian military drills, facilitated an attempted coup in Montenegro, and tried to destabilize Bosnia and Herzegovina by stoking sectarian tensions. And in North Macedonia itself, Russia has funded troll factories that, among other things, were used to target the 2016 U.S. presidential campaign with disinformation. Moscow also tried to influence North Macedonia’s September 2018 referendum on NATO membership, is using its embassy and consulates there as bases for intelligence-gathering operations, and has spread propaganda detailing alleged Western plots to break up the country.

That Russia would threaten NATO’s members in Eastern Europe is nothing new, of course. Russia has long attempted to undermine the Baltic countries—Lithuania, Latvia, and Estonia—which joined NATO and the European Union after gaining their independence from the Soviet Union. But today, the Baltic States are well integrated into alliance structures and the European economy and are home to thousands of NATO troops. Whereas the Baltics have become part of NATO’s well-armored front, the Balkans are its soft underbelly.

Whereas the Baltics have become part of NATO’s well-armored front, the Balkans are its soft underbelly.

 NATO’s posture in North Macedonia and its neighborhood is very limited. The Balkan countries are also poorer, more ethnically divided, and less economically integrated with Europe. Their potential instability and the much lower likelihood of a robust response by the West make North Macedonia and its neighbors ripe and easy targets for Russian meddling.

Taking a page from history’s playbook, Putin rightly assumes that most decision-makers in NATO capitals would consider North Macedonia a “faraway country” of “people of whom we know nothing.” U.S. President Donald Trump, whose relationship with Putin continues to attract attention, confirmed a similar suspicion with regard to neighboring Montenegro when he appeared to question NATO’s commitment to defend the Balkan nation during an interview aired on Fox News. And while some may have taken offense at Trump’s statement, the truth is he speaks for many.

According to a February poll by the Pew Research Center, less than half the populations of France, Spain, Turkey, and Greece hold a favorable view of NATO. Pandering to the alliance’s critics, French President Emmanuel Macron last year declared that NATO had “brain death.” The citizens of only three European countries—Britain, the Netherlands, and Lithuania—say their country should respond with military force if Russia were to attack a NATO member in Eastern Europe.

No surprise then that NATO’s posture toward its newest member remains unclear. Though NATO broadened the definition of its joint defense commitment—Article 5 of the alliance’s charter—to include cyberattacks in 2014, it has failed to clarify just what that means. When asked what level of cyberattack on one of its members would trigger a response, NATO Secretary-General Jens Stoltenberg said only, “We will see.” The 2018 Brussels Declaration reaffirmed NATO’s intent to defend member states from nonconventional attacks—but only meekly asserted that in “cases of hybrid warfare, the Council could decide to invoke Article 5.” These Western weasel words will have been duly noted in the Kremlin.

These Western weasel words will have been duly noted in the Kremlin.

The type of meddling Russia has specialized in includes election interference, inflaming ethnic tensions, and provoking violent conflict. These three real possibilities could trigger a NATO response under Article 5. The most pressing issue is securing North Macedonia’s upcoming elections, now postponed until further notice due to the COVID-19 pandemic. Polls last showed VMRO-DPMNE, a pro-Russian nationalist party, in a dead heat with the pro-Western Social Democrats. Russian interference in the election process or outcome not only threatens Macedonian sovereignty but, if successful, could result in a government that tilts North Macedonia toward Moscow.

Russia may also seek to pressure and destabilize North Macedonia in other ways, including through Moscow’s regional client, Serbia. Russian propaganda aimed at North Macedonia includes conspiracy theories about the country’s sizable Albanian minority supposedly colluding with NATO and Albania to fold North Macedonia into a “greater Albania” amid great bloodshed. As any student of Balkan history knows, such rhetoric has led to ethnic violence in the region before. Alternatively, Russia may stoke simmering conflicts in Serbia, whose unstable Presevo region directly borders North Macedonia, or the unresolved Kosovo dispute. Either conflict could easily spill into North Macedonia.

NATO’s next steps to secure its new member could include adapting the successful tactics used when Montenegro joined the alliance in 2017. A NATO-sponsored cyberteam provided the Montenegrin government with technical support to learn to identify and counter hybrid warfare. NATO raised awareness of the benefits of NATO membership by working with officials, civil society, local governments, and media organizations. It also worked to improve governance in Montenegro’s defense sector. Similarly, the European Union, which has just opened accession talks with North Macedonia, could move quickly to signal to the world that the Balkan nations are an integral part of Europe.

More broadly, however, NATO needs a mechanism to respond to Russian aggression in the event that the alliance’s members can’t unanimously agree to do so. Article 5 requires unanimity before invoking collective defense, but NATO’s members differ in their attitudes to Russia.

Article 5 requires unanimity before invoking collective defense, but NATO’s members differ in their attitudes to Russia.

 One solution would be to form, as a backstop in case it is needed, a coalition of the willing comprising NATO members with credible defense capabilities that are willing to confront Russia and prepare a collective response to any attack.

Despite NATO’s overall military superiority, it has a weak hand in the Balkans, and Russia continues to outmaneuver it there. NATO must quickly signal that it remains steadfast and, having decided to admit it, that North Macedonia is an integral member of the alliance. If NATO fails in its support of new members like North Macedonia, the chances have just risen that it will be met with Russian aggression—hybrid or conventional—that may just mean the end of NATO as a credible alliance.

#### No spillover

Brad Stapleton 16, Former visiting fellow in defense and foreign policy at the Cato Institute and former adjunct researcher at the RAND Corporation, "Trump and NATO—Redefining the US Role,” CATO, 11/11/16 https://www.cato.org/blog/trump-nato-redefining-us-role

Some would argue, however, that although Article V does not legally obligate the United States to deploy military forces in defense of its NATO allies, such a response would be essential to preserve American credibility. In other words, if the United States failed to defend its NATO allies against Russian aggression, all of the United States’ other allies around the globe would begin to doubt whether they could really depend upon the United States. Yet U.S. credibility would only suffer if Washington were to maintain an expectation of U.S. intervention and subsequently failed to fulfill that expectation.

If the incoming Trump administration is serious about reducing its commitment to NATO, its first priority should therefore be to eliminate the expectation that the United States would automatically intervene militarily in defense of its NATO allies. For that expectation is the root of the inequitable distribution of the defense burden within NATO. Why should the European allies invest significantly in defense if they can count on the United States to guarantee their security? Rather than maintaining an implicit commitment to spearhead any defense of NATO territory (particularly in Eastern Europe), the Trump administration could make it clear to the allies that the United States will serve as a balancer of last resort in Europe. In other words, the European allies will bear primary responsibility for the defense of Europe; the United States will only intervene in dire circumstances if they are unable to defend themselves (much like during the two world wars).

#### Credibility theory is context specific---allies care about how we treat countries similar to them, not everyone

Henry 20 (Iain D. Henry, Lecturer in the Strategic and Defence Studies Centre at the Australian National University, “What Allies Want: Reconsidering Loyalty, Reliability, and Alliance Interdependence,” April 13th, 2020, https://www.mitpressjournals.org/doi/full/10.1162/isec\_a\_00375)

Leaders believe that if their state abandons one ally during a crisis, then their state's other allies will expect similar disloyalty in the future. Thus, a single instance of disloyalty can damage, or even destroy, alliances with other states. Because of this belief in interdependence—that developments in one alliance will also affect other alliances—the desire to demonstrate loyalty has exercised a tremendous influence on U.S. policy. But is indiscriminate loyalty what allies want? The First Taiwan Strait Crisis (1954–55) case study suggests that allies do not desire U.S. loyalty in all situations. Instead, they want the [US] United States to be a reliable ally, posing no risk of abandonment or entrapment. In the First Taiwan Strait Crisis, several allies worried that U.S. loyalty to the Republic of China increased the risk of unwanted conflict, and as the crisis persisted, these allies sought to restrain the United States and thus reduce the likelihood of war. Although U.S. leaders were reluctant to coerce the Republic of China into backing down during this territorial dispute with the People's Republic of China, other U.S. allies actively encouraged such disloyalty. These findings have significance for theories of alliance politics and international reputation, as well as contemporary alliance management. Introduction Do states judge their ally's behavior toward its other allies? If yes, how? Historically, decisionmakers have instinctively adopted deterrence theory's logic that a state's character is judged through displays of innate loyalty: if a state is disloyal to one ally, then this will create a reputation for disloyalty, which will cause other allies to doubt the state's reliability. Thus, disloyalty can have calamitous consequences: the aggrieved ally will punish the betrayal; other allies will suffer crises of faith; and adversaries will conclude that the state's alliances are cheap talk. The logic is that discrete alliance commitments are interdependent—that what happens in one alliance affects the expectations of other allies—and that this interdependence is underpinned by demonstrations of loyalty. President Lyndon Johnson said that if the United States were “driven from the field in Viet-nam, then no nation can ever again have the same confidence in American promise or in American protection.”1 These convictions regularly animate contemporary debates: Nancy Bernkopf Tucker and Bonnie Glaser argue that if the United States were to abandon Taiwan in a conflict with China, this could deal “a fatal blow to the U.S.-Japan alliance” and might lead to South Korea “renouncing its security alliance with Washington and aligning with Beijing.”2 Aaron Friedberg writes that expecting a U.S. “back down … [and] a Chinese victory over Taiwan … to leave America's Asian alliances unscathed, is to indulge in wishful thinking of the most dangerous kind.”3 Others suggest cross-regional effects, claiming that by “retreating from the Middle East and abandoning Ukraine to Russian aggression,” President Barack Obama left “America's Asian allies … bewildered and alienated.”4 If alliance interdependence exists, and is governed by innate loyalty, then fighting for reputation is crucial, because any single alliance rift could quickly tear asunder other alliance relationships. Some scholars, described as “reputation skeptics,” dispute this common wisdom. Skeptics argue that because “reputation is in the eye of the beholder,” the United States should never regard demonstrating loyalty as sufficient grounds for military action.5 Jonathan Mercer argues that when allies observe the United States demonstrating loyalty, they will attribute this desired behavior to situational causes and thus will not conclude that it will be loyal in future crises. In contrast, he concludes that when the United States is disloyal, this undesired behavior will be attributed to national character, but will not always cause allies to expect similar behavior in the future.6 Reputation skeptics believe that “leaders are tragically mistaken when they commit to the use of force in the expectation of long-term benefits beyond any gains in the immediate dispute.”7

#### No spread NOR prolif impact.

Jonas Schneider 20. Senior researcher at the Center for Security Studies, held post-​doctoral fellowships at the German Institute for International and Security Affairs (SWP) in Berlin and at the CSS and worked as a research associate at the Institute for Security Policy at the University of Kiel, holds a PhD in Political Science from the University of Kiel. 2020. “Chapter 26 Nuclear Proliferation and International Security.” Understanding Global Politics: Actors and Themes in International Affairs, edited by Klaus Larres and Ruth Wittlinger, Routledge, pp. 409–425.

Other analysts have sounded a much less alarmist tone, however. Some scholars even suggested that an Iranian bomb held great potential for stabilising an unbalanced and volatile Middle East (Waltz, 2012). Closer to the mainstream of Western strategic discourse, various experts have argued that despite the risks of proliferation, nuclear weapons, and the deterrent they provide should get (more) credit for contributing, in combination with other factors, to what has been labelled ‘the Long Peace’ among the great powers since 1945 (Gaddis, 1999, p. 268–271; Gavin, 2012a, p. 164; Acton 2010, pp. 16–17). Still others have contended that because nuclear proliferation is such a rare phenomenon, and since robust nonproliferation measures tend to be disruptive, the net destabilising effect of new nuclear countries is quite small and, therefore, manageable (Mueller 2010, pp. 95–99; Hymans 2013, pp. 293–296).

The question of whether nuclear proliferation has stabilising or destabilising effects is not just fascinating for scholars of the nuclear age, but also highly consequential for practical policy issues. For in order to debate the merits of particular policy choices – such as preventive military strikes against nuclear facilities, grand bargains with potential proliferators or complete nuclear disarmament – we need to understand first how the spread of nuclear weapons impacts regional and global security.

The chapter proceeds in three steps. The first section provides the foundation for the other parts by summarising what we know about empirical patterns of proliferation and the utility of nuclear weapons for statecraft. The second section then engages the literature on the consequences of proliferation, focusing in particular on how proliferation has influenced international stability. The final section explores whether some states have been more affected than others, and what measures these states have taken to prevent proliferation, or at least mitigate its negative consequences.

Patterns of nuclear proliferation and the utility of nuclear weapons

Nuclear proliferation is commonly defined as the spread of nuclear weapons to states that did not previously have them. Within a broader conceptual framework that is rarely used by scholars, yet popular in the arms control community, this diffusion of nuclear weapons to additional states is labelled horizontal proliferation. It is conceptually accompanied by the notion of vertical proliferation, which refers to qualitative improvements and increases in the number of nuclear weapons in the stockpiles of existing nuclear weapon states. In accordance with the typical usage of the term in the scholarly debate, this chapter focuses only on how the horizontal proliferation of nuclear weapons affects international stability.

One important empirical pattern that has shaped how nuclear proliferation is understood concerns the way in which nuclear weapons have spread. The word ‘spread’ appears to suggest that the established nuclear powers have provided other interested nations with (at least a few) operational nuclear warheads. Yet such transfers have never been undertaken. Certainly, states that sought nuclear weapons have often received significant assistance from other nations (Schofield, 2014; Fuhrmann, 2012), sometimes in the form of highly sensitive technologies (Kroenig, 2010). Nonetheless, since all these transfers remained well below the weapons threshold, nations seeking nuclear weapons always had to build them indigenously. Hence, in reality, the spread of nuclear weapons has meant that merely the ambition to possess a nuclear arsenal has spread to additional states, each of which then had to pursue that goal primarily through indigenous efforts.

Importantly, since a state’s national efforts to turn its desire for nuclear weapons into reality naturally span several (and sometimes many) years, nuclear proliferation must be conceived of as a process, as opposed to just a single step (Meyer, 1986). This point is reinforced by the fact that 29 out of 39 states that have embarked upon that path (Müller and Schmidt, 2010, p. 157; Mikoyan, 2012; Santoro, 2017) have not acquired a nuclear arsenal. Hence, a lot of nuclear proliferation activity has been undertaken by nations that did not ultimately become nuclear weapon states. Three patterns explain this situation.

First, owing not just to the technological, but also the institutional and managerial challenges of the task, some nations simply failed in their efforts to build the bomb (Hymans, 2012; Braut-Hegghammer, 2016). Second, a few countries have chosen a nuclear ‘hedging’ strategy, intentionally confining their efforts to developing the technological capability to build an arsenal quickly while refraining from exercising that option (Narang, 2016–17, p. 134). Third, several states have undertaken a ‘nuclear reversal’, abandoning their nuclear weapons activities before developing nuclear explosive devices (Müller and Schmidt, 2010).

#### Prolif is harmless.

Dr. John Mueller 18, Professor of Political Science at Ohio State University, “Nuclear Weapons Don’t Matter”, Foreign Affairs, November / December 2018, https://www.cato.org/publications/commentary/nuclear-weapons-dont-matter

That logic might seem plausible at first, but it breaks down on close examination. Not only has the world already survived the acquisition of nuclear weapons by some of the craziest mass murderers in history (Stalin and Mao), but proliferation has slowed down rather than sped up over time. Dozens of technologically sophisticated countries have considered obtaining nuclear arsenals, but very few have done so. This is because nuclear weapons turn out to be difficult and expensive to acquire and strategically provocative to possess.

They have not even proved to enhance status much, as many expected they would. Pakistan and Russia may garner more attention today than they would without nukes, but would Japan's prestige be increased if it became nuclear? Did China's status improve when it went nuclear — or when its economy grew? And would anybody really care (or even notice) if the current British or French nuclear arsenal was doubled or halved?

Alarmists have misjudged not only the pace of proliferation but also its effects. Proliferation is incredibly dangerous and necessary to prevent, we are told, because going nuclear would supposedly empower rogue states and lead them to dominate their region. The details of how this domination would happen are rarely discussed, but the general idea seems to be that once a country has nuclear weapons, it can use them to threaten others and get its way, with nonnuclear countries deferring or paying ransom to the local bully out of fear.

Except, of course, that in three-quarters of a century, the United States has never been able to get anything close to that obedience from anybody, even when it had a nuclear monopoly. So why should it be true for, say, Iran or North Korea? It is far more likely that a nuclear rogue's threats would cause its rivals to join together against the provocateur — just as countries around the Persian Gulf responded to Saddam's invasion of Kuwait by closing ranks to oppose, rather than acquiescing in, his effort at domination.

#### Prolif’s inevitable.

Economist 21, "The World Is Facing an Upsurge of Nuclear Proliferation," The Economist, 01/30/2021, https://www.economist.com/leaders/2021/01/30/the-world-is-facing-an-upsurge-of-nuclear-proliferation.

THIRTY-ONE countries, from Brazil to Sweden, have flirted with nuclear weapons at one time or another. Seventeen launched a formal weapons programme. Just ten produced a deliverable bomb. Today nine states possess nuclear arms, no more than a quarter-century ago. Yet the long struggle to stop the world’s deadliest weapons from spreading is about to get harder.

In the past 20 years most countries with nuclear ambitions have been geopolitical minnows, like Libya and Syria. In the next decade the threat is likely to include economic and diplomatic heavyweights whose ambitions would be harder to restrain. China’s rapidly increasing regional dominance and North Korea’s growing nuclear arsenal haunt South Korea and Japan, two of Asia’s largest powers. Iran’s belligerence and its nuclear programme loom over the likes of Saudi Arabia and Turkey (see article). Proliferation is not a chain reaction, but it is contagious. Once the restraints start to weaken they can fail rapidly.

The nuclear omens are bad. Arms control between America and Russia, which saw cuts of 38,000 warheads—a 79% fall—in 1991-2010, has dwindled. On January 26th Presidents Joe Biden and Vladimir Putin agreed to extend the last remaining pact, the New START treaty, for five years. That is welcome, but prospects for a follow-on are dim. China, India, North Korea and Pakistan are all expanding and modernising their nuclear forces. There is dismal progress towards global disarmament, the ultimate aim of the Non-Proliferation Treaty (NPT), the cornerstone of the nuclear order. A new treaty banning the bomb, which was signed by 86 countries and came into force on January 22nd, channels the frustration among nuclear have-nots. It accomplishes little else.

### AT: Deterrence DA---2AC

#### Zero-tolerance deterrence is not credible---cumulative deterrence is more effective for the grey zone

Whitney L. Cissell 20, MA thesis in Security Studies, Naval Postgraduate School, Army Major, Nuclear Nonproliferation Officer, March 2020, "DETERRENCE IN THE DANGER ZONE: HOW THE UNITED STATES CAN DETER RUSSIAN GRAY ZONE CONFLICT", https://calhoun.nps.edu/handle/10945/64844

2. Applying Deterrence in the Context of Russian Behavior

This section builds on the previous assessments and explores the application of deterrence theory at the sub-conventional level in the specific context of Russia as a state actor and its use of a gray zone strategy. It considers the value of tailoring a deterrent strategy against Russian gray zone conflict by supplementing conventional deterrence with “cumulative deterrence.” Recall that any deterrence strategy relies on sufficient capabilities, solid resolve, and strong communication of a threat, which in turn create credibility.225 Cumulative deterrence, elaborated in the following paragraphs, introduces the idea that credibility can be sustained across multiple encounters even if deterrence fails in certain instances, vis-à-vis classic zero-tolerance nuclear deterrence.

Regarding tailoring deterrence, Bunn writes, “If deterrence is about influencing the perceptions—and ultimately, the decisions and actions—of another party, it is logical that the requirements for deterrence will differ with each party that we might try to deter and may well differ in each circumstance or scenario.”226 Adapting deterrence to the subconventional level requires an understanding of the unique relationship between the states to identify the relative stability and instability that can inform deterrence strategy.

The stability–instability paradox applies to the nuclear and conventional level, and indeed, Russia’s effort to avoid conventional-level warfare with the United States strengthens stability between the states at the conventional level similar to the strategic nuclear level. While U.S.–Russian nuclear stability is based on parity, conventional stability in this relationship is more complex. As shown in Chapter II, Russia has a strong aversion to conflict with the United States and NATO at the conventional level. Russia would be outmatched in military superiority after two to three weeks of conflict and beyond its near abroad and, thus, prefers to operate at the sub-conventional level below the threshold of armed conflict.227 In effect, Russia’s strategy of avoiding any actions that might trigger conventional conflict aims to bolster a sort of “firewall” between conventional warfare and gray zone conflict. NATO, up to now, has effectively obliged this Russian strategy by not brandishing threats of conventional escalation in response to Russian gray zone aggression, let alone undertaking conventional responses. As much as Russia seeks to avoid escalation to conventional warfare it could not win, it is also learning how averse NATO is to threaten such escalation. This aversion is ironic insofar as Cold War–era extended deterrence relied on NATO’s threat of escalatory nuclear responses to conventional attacks.

These respective Russian and NATO postures enhance conventional stability, but at the cost of fueling instability at the gray zone level, reflecting a form of the stability– instability paradox familiar in nuclear strategies. This tailored application of the stability– instability paradox to the specific Russian context yields a tiered relationship of stability between the United States and Russia at each level of warfare, as depicted in Figure 1, and helps explain why the United States and Russia are the most unstable at the subconventional level, on which this research focuses.

Cumulative deterrence may be an option to address the issues created when adapting conventional deterrence to the sub-conventional level including the credibility and communication of the threat. Cumulative deterrence has not been a standard element of U.S. deterrence strategy in the past, and there is limited academic literature and strategic thought about its use in areas outside of cyber and terrorism. However, this new security environment characterized by great power competition at levels below open conflict requires a new way of looking at the deterrence landscape at the sub-conventional level. Subject matter experts for this research confirm that a zero-tolerance deterrence mindset will not work at the sub-conventional level and that the United States might have to choose what portions of the gray zone it wants to deter because it may be difficult to deter everything.229

There is a precedent for applying a cumulative model and mindset of deterrence to limit and shape the sub-conventional level of conflict, and this suggests it may also be applied to the current U.S. need to deter Russia’s gray zone conflict. According to Thomas Rid, cumulative deterrence “consists of a series of acts of force to create—and maintain— general norms of behavior for many political actors over an extended period. Using force, consequently, does not represent a principal failure of deterrence but its maintenance through swift, certain, but measured responses.”230 Cumulative deterrence has been a key part of Israel’s strategy for decades and was developed in the conventional and subconventional level focusing on limiting and shaping ongoing conflicts against both state and non-state actors at the conventional and sub-conventional level.231 In addition, cumulative deterrence has recently been considered for use in deterring terrorism and cyberattacks, as it is designed for long-term sustained conflict, such as competition in the gray zone.232

Doron Almong describes cumulative deterrence as functioning on two levels: the macro, which creates an image of overwhelming military superiority, and the micro, which relies on responses to adversarial actions.233 Almong also explains that cumulative deterrence has three key features.

First, its effectiveness is measured in terms of the number of victories accumulated over the duration of the conflict, which might be envisioned as “assets in a victory bank.” Second, over time, these victories produce increasingly moderate behavior on the part of the adversary and a shift in its strategic, operational, and tactical goals until there is a near-absence of direct conflict. Third, this moderation may eventually result in political negotiations and perhaps even a peace agreement.234 Almong is describing cumulative deterrence as applied to the conventional level of warfare; however, in the context of Russia, the construct can be transposed to the subconventional level. At the sub-conventional level, U.S. responses over time to Russian gray zone aggression could moderate Russian behavior, causing a shift in Russia’s decision calculus and strategic goals, thereby diminishing the conflict.

The advantage of layering a strong conventional deterrence strategy with cumulative deterrence is that it allows the restoration of deterrence over time if conventional threats fail to deter at the sub-conventional level. Over time, cumulative deterrence responses to gray zone actions bolster the credibility of the United States and alter Russia’s decision calculus at the sub-conventional level, therefore strengthening deterrence overall. Successful deterrence at the sub-conventional level requires a reorientation in how the U.S. views deterrence, moving from a zero-tolerance strategy to the long-term attrition of gray zone conflict. This renewed mindset allows for tailored punitive strategies that over time limit the bounds of the gray zone through the reiteration of unacceptable behavior through punishment. Regardless of the level at which a state wishes to conduct warfare, all deterrence strategies rely on three aspects that must work in concert: sufficient capabilities, solid credibility, and strong communication of a threat.235 As Rid explains, confrontations should be “seen as necessary evils that should be kept on as low a level as possible, but that could not be pushed down to zero.”236 This argument assumes escalation control, which is to say that the United States can control escalation at the sub-conventional level on its own terms.

Many authors challenge the notion of escalation control, claiming that it is risky and nearly impossible. Scholars claim that avoiding escalation requires deterring the action and that a policy to deter one action could in fact risk escalation to another. Additionally, scholars claim, “Escalation control or management is an inherently imperfect business. It can be done well or poorly, but it is extremely rare for any set of policies to eliminate the risk of significant escalation altogether.”237 These same scholars agree that the risk of inadvertent escalation can be reduced, but they are concerned that policy makers are incorrectly assuming it can be eliminated altogether.238 The concerns over escalation control are valid; however, it is possible to control escalation and use the threat of escalation to bolster deterrence. Mazarr explains that the gray zone puts the defender in the position to escalate, which is part of the challenge of deterrence.239 Both escalation control and deterrence fundamentally rely on communication and a thorough understanding of the adversary. Proper communication of the capability and the resolve to use the capability to deny or punish an action are just as crucial to escalation control as they are to deterrence. The same scholars who express concerns over escalation control also admit there is a way to control the risk: “Escalation depends heavily on an astute understanding of how the adversary will perceive and interpret events that have not yet occurred—not only in a general sense, but also under the specific and often difficult-to-predict conditions that will shape the opponent’s perceptions and responses when a particular event occurs.”240 The United States can both mitigate escalation and contribute to deterrence by adding an element of ambiguity to its deterrence threats that leave something to chance but also allow a response that limits or controls the escalatory response of the adversary.

When the United States responds with an instrument of state power in any DIME category, such as the expulsion of 60 Russian diplomats in response to the Russian nerve agent attack on a British citizen in 2018, it can strengthen cumulative deterrence credibility. Some of the literature on cumulative deterrence suggests that deterrence works by banking “wins” by responding to events with military power. However, when adapted to the gray zone, it seems critical that all elements of state power must be utilized, not just the military. The military is sometimes—not always—an appropriate response to an action in the gray zone, so threatening military retaliation for every tactic in the gray zone is not credible; however, a state must still have the ability to impose costs on an adversary for an action to make cumulative deterrence successful.

#### Strategic ambiguity spurs escalation in cyberspace specifically because it’s an offense-dominant domain---norms solve

Mariarosaria Taddeo 19, Fellow in Cyber Security and Ethics in the Department of Politics and International Studies at the University of Warwick and Research Associate at the Uehiro Centre for Practical Ethics, University of Oxford, UK, “Norms and Strategies for Stability in Cyberspace,” Chapter 3 in “The 2019 Yearbook of the Digital Ethics Lab,” edited by Christopher Burr and Silvia Milano, https://link.springer.com/chapter/10.1007/978-3-030-29145-7\_3

Escalation follows from the nature of cyber attacks and the dynamics of cyberspace (Floridi and Taddeo 2014a, b; Taddeo 2014a, 2016, 2017). Non-kinetic cyber attacks—aggressive uses of information and communications technologies that do not cause destruction or casualties, e.g. Distributed Denial of Service (DDoS) attacks—cost little in terms of resources and risks to the attackers, while having high chances to be successful, e.g. impairing the services of targeted server or website. At the same time, cyber defence is porous by its own nature (Morgan 2012): every system has bugs in the program (vulnerabilities), identifying and exploiting them is just a matter of time, means, and determination. This makes even the most sophisticated cyber defence mechanisms ephemeral and, thus, limits their potential to deter new attacks.

Even when successful, cyber defence does not lead to strategic advantages, insofar as dismounting a cyber attack, may bring tactical success, but very rarely leads to the ultimate defeating of an adversary (Taddeo 2017). This creates an environment of persistent offence (Harknett and Goldman 2016), where attacking is tactically and strategically more advantageous than defending.

As Haknett and Goldman argue, in an offence-persistent environment, defence can achieve tactical and operational success in the short term if it can adjust constantly to the means of attack, but it cannot win strategically. Offence will persist and the interactions with the enemy will remain constant. This is why inter-state cyber defence have shifted from reactive (defending) towards an active (countering) defence strategies.

In this scenario, state actors make policy decisions to protect their abilities to launch cyber attacks. Strategic ambiguity is one of these decisions. According to this policy, states decide neither to define nor to inform the international community about their red lines—thresholds that once crossed would trigger state response— for non-kinetic cyber attacks (Mariarosaria Taddeo 2011). This approach leaves de facto unregulated cyber attacks that remain below the threshold of an armed attack. Strategic ambiguity has often been presented as a way to confuse the opponents about the consequences of their cyber attacks. As the US National Intelligence Officer for Cyber Issues officer put it:

Currently most countries, including ours, don’t want to be incredibly specific about the red lines for two reasons: You don’t want to invite people to do anything they want below that red line thinking they’ll be able to do it with impunity, and secondly, you don’t want to back yourself into a strategic corner where you have to respond if they do something above that red line or else lose credibility in a geopolitical sense.6

By fostering ambiguity, state actors also leave open for themselves a wider room for manoeuvring. Strategic ambiguity allows state actors to deploy cyber attacks for military, espionage, sabotage, and surveillance purposes without being constrained by their own policies or international red lines. This makes ambiguity a dangerous choice, one that is strategically risky and politically misleading.

The risks come with the cascade effect following the absence of clear thresholds for cyber attacks. The lack of thresholds facilitates a proliferation of offensive strategies. This, in turn, favours an international cyber arms race and the weaponization of cyberspace, which ultimately spurs the escalation of cyber attacks. This is why strategic ambiguity is a policy hazard that fuels, rather than arrests, escalation of interstate cyber attacks. Cyber attacks would be deterred more effectively by a regime of international norms (defining proportionality criteria for responses, setting red lines, and procedure for accountability, and for capability building) that makes attacks politically costly to the point of being disadvantageous for the state actors who launch them.

As I mention in Sect. 3.1, stability of cyberspace hinges on both regulations and strategies. Having considered the limits of the existing approaches to the regulation of state behaviour in cyberspace, I shall now focus on existing view for the designing deterrence strategies for cyber attacks.

#### Strategic ambiguity fails – triggers fights that slow responses, crack cohesion, and undermines Article 5 writ large

Lonergan and Moller 22 - Erica D. Lonergan is an assistant professor in the Army Cyber Institute and a research scholar at the Saltzman Institute of War and Peace Studies at Columbia University. Sara B. Moller is a former Eisenhower Fellow at the NATO Defense College and will be joining the Center for Security Studies at Georgetown University later this year (Erica and Sarah, “Opinion | NATO’s Credibility Is on the Line with its Cyber Defense Pledge. That’s a Bad Idea,” Politico, 4-27-22, <https://www.politico.com/news/magazine/2022/04/27/nato-credibility-cyber-defense-pledge-russia-ukraine-00027829>) //nt-sg

But despite this rhetoric, exactly how and when Article 5 applies to cyberspace remains unclear. This ambiguity is a problem — with potentially **disastrous consequences**. Staking the credibility of Article 5 to what are often murky activities in cyberspace threatens to **undermine** the broader principle of **collective defense.** We can’t risk fracturing the transatlantic alliance at a critical juncture in its history over a debate on what constitutes a major or minor cyberattack. For that reason, NATO should move quickly to clarify its policy on cyberattacks and **explicitly state** the threshold for what would trigger an Article 5 response. Furthermore, NATO members should commit to treating cyberattacks that do not rise to the level of a major attack as a national matter — not one for the alliance.

Such a shift might face some initial resistance, particularly in light of the Kremlin’s history of malicious cyber activities. One of the first state-initiated cyberattacks was perpetrated by Russia against Estonia, a NATO member, in 2007. In the intervening years, Moscow has increased its malicious cyber activities, such as the SolarWinds breach uncovered in December 2020 in which Russia gained access to a treasure trove of U.S. data. Russian President Vladimir Putin’s maneuvers against NATO members, along with the annexation of Crimea in 2014, spurred the alliance to adopt a Cyber Defense Pledge in 2016 that recognized cyberspace as a military domain. Two years later, NATO created a Cyberspace Operations Center in Mons, Belgium to improve situational awareness and coordinate cyber operations. Since then, the alliance has consistently reaffirmed the application of Article 5 to cyberspace. At the 2021 summit in Brussels, NATO committed to a new Comprehensive Cyber Defense Policy, with allies agreeing to employ the “full range of capabilities” at all times to “deter, defend against, and counter the full spectrum of cyber threats.”

Notably, NATO refined its language with last summer’s summit communique to account for the fact that some cyber incidents may not be individually decisive, but nevertheless significant when viewed in the aggregate. Specifically, the allies recognized “the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack.” In practice, however, NATO leaders have **avoided clarifying** the conditions under which a cyberattack would trigger Article 5 and how NATO would respond. When pressed about Russian cyberattacks in the Ukraine context, Stoltenberg cautioned that, “we have never gone into the position where we give a potential adversary the privilege of defining exactly when we trigger Article 5.”

This equivocation is not surprising, for several reasons. The nature of cyberspace often **confounds** unequivocal deterrence declarations. States tend to operate in cyberspace with **plausible deniability**, which can make it difficult to rapidly ascertain responsibility for cyber incidents. Also, it can be challenging to understand the **intent** behind observed cyber behavior, and there is often a **substantial time lag** between when an initial penetration of a network occurs and when the target even realizes the breach. And the vast majority of cyber operations cause **virtual, not physical, damage**, complicating efforts to assess and evaluate the implications of the costs inflicted. Moreover, it can take time to develop and identify a way to infiltrate a network as well as the computer code that takes advantage of a vulnerability for malicious ends. This means states may **lack a palatable cyber response** option for retaliatory purposes at the desired time.

This creates a **slew of** practical **problems** if Article 5 were to be invoked for a cyberattack. From an implementation perspective, it would trigger deliberations within the North Atlantic Council, NATO’s primary decision-making body. Decisions made within the NAC require **unanimity**, which can be difficult to achieve for many issues but is especially **burdensome** for cyber ones, given all of the ambiguities outlined above. The most likely outcome of this process would be a long, drawn-out deliberation resulting in a **divided alliance** unable to agree on how or whether to respond. Quite simply, some allies are unlikely to want to risk World War III for a cyberattack that disrupts the financial infrastructure, for instance, of another country but doesn’t lead to loss of life or sustained damage.

These challenges have major **strategic implications** for NATO. After years of publicly and repeatedly linking Article 5 to cyberspace and reinforcing that policy in response to the Ukraine conflict, a failure to achieve consensus and respond to a Russian cyberattack against a NATO member could **imperil Article 5** in other areas. The disunity that is likely to be revealed during NAC deliberations would then undermine the broader political cohesion that has, for the most part, been remarkably strong throughout the war in Ukraine. This would make it more **difficult for the alliance to respond** to other forms of Russian behavior. As Biden emphasized at a press conference last month, “the single-most important thing is for us to stay unified … We have to stay fully, totally, thoroughly unified.”

### A5 Key---2AC

#### Need to determine thresholds for ‘armed attack’---the CP results in both over-escalation AND incoherent response

de Boer ’14 [Florentine; December; Legal Fellow at NATO SCHOOL Oberammergau; NATO Legal Gazette, “Examining the Threshold of “Armed Attack” in light of Collective Self-Defence against Cyber Attacks: NATO’s Enhanced Cyber Defence Policy,” Issue 35, https://www.act.nato.int/images/stories/media/doclibrary/legal\_gazette\_35.pdf]

While it is exciting that, according to the Wales Summit Declaration, NATO’s Enhanced Cyber Defence Policy for the first time explicitly mentions that Article 5 can be invoked in case of cyber attacks, it is unfortunate that there is no more guidance on criteria for cyber attacks to reach the required threshold. Indeed, there is no definite procedure available with regard to Article 5. The decision to invoke Article 5 is a political decision as it is taken by the member countries through the NAC, NATO’s principal political decisionmaking body.38 A general challenge for the NAC is to take decisions by consensus as views will differ among 28 sovereign States. Similarly, States have different views on the threshold of “armed attack” in the context of cyber attacks.

The threshold of “armed attack” is generally understood to entail physical damage, destruction, injury or death. However, some States already, or will, support a lower threshold to include highly disruptive cyber attacks without physical consequences.39 It may require a long debate to reach agreement on whether such cyber attacks constitute an “armed attack” and trigger the application of Article 5. The controversy surrounding the threshold is also demonstrated by the fact that the International Group of Experts, consisting of legal practitioners, academics, and technical experts, could not agree on whether cyber attacks without physical consequences qualify as armed attacks.40 Likewise, it will be a significant challenge for the NAC to reach agreement on whether the threshold has been reached.

NATO not only faces general challenges as described above in the case of cyber attacks, but cyber attacks also pose a particular challenge to NATO. National policies on cyber defence will differ even more due to rapid technological developments and growing technological capabilities. States are having a hard time keeping up with all the developments. Some States have more progressive cyber defence policies, whereas other States opt for a conservative policy. Additionally, no cyber attack has thus far been publicly declared as an “armed attack” by a State.41 A particular issue of the disruptive cyber attacks is that their effects are so remote from the effects of traditional attacks that reach the threshold of “armed attack.” Cyber attacks are capable of doing so much more without actually causing physical damage, destruction, injury or death. The effects of disruptive cyber attacks do not correspond with the described effects and examples given by the ICJ. Consequently, States could be or are more reluctant to recognise certain disruptive cyber attacks without physical consequences as “armed attacks.”

By invoking Article 5 in response to the terrorist attacks of 9/11, NATO member countries demonstrated that they could quickly reach an agreement and take a step forward.42 Nevertheless, taking a step forward with regard to the threshold of “armed attack” may encounter more resistance from individual member countries. It could be “dangerous” to set a precedent with regard to the criteria for highly disruptive cyber attacks to constitute an “armed attack.” Both thresholds of “the use of force” and “armed attack” must be preserved and the latter must remain higher. If the threshold is lowered too much, more cyber attacks would reach the threshold and it would become easier for States to use force in self-defence.43 The standard must remain sufficiently high to ensure that only the gravest forms of cyber attacks can trigger the application of Article 5.

A long debate will be required to determine whether Article 5 can be invoked in the case of a highly disruptive cyber attack without effects equivalent to traditional armed attacks. The envisaged disagreement on the threshold of “armed attack” in cases of cyber attacks could have an adverse effect on NATO’s ability to swiftly respond to a cyber attack. There is a significant risk in waiting until such a cyber attack occurs to decide whether the criteria are met to trigger the application of Article 5. NATO’s ability to swiftly respond will not only be severely hampered, but it may also entirely prevent NATO to respond collectively with force. When the NAC is unable to reach consensus, the NATO ally that is the object of a serious cyber attack without physical consequences, is left without one of the crucial benefits of being a member of NATO. The member country would be unable to rely on collective self-defence under Article 5.

#### Fixing Article V pre-req to other NATO cyber policies---prevents allied cohesion breakdown

Pernik ’14 [Piret Pernik, Research Fellow at ICDS; “Improving Cyber Security: NATO and the EU;” RKK ICDS, September 2014, https://icds.ee/wp-content/uploads/2010/02/Piret\_Pernik\_-\_Improving\_Cyber\_Security.pdf]

Given the existing capability, policy and doctrinal divide between the Allies and the absence of criteria what constitutes an armed attack, deliberations would be thorny. NATO’s decision-making process might be delayed also by the scarce understanding of operational and technical aspects of cyber defence, as well as the lack of general consensus on key cyber security terms at the strategic level. to speed up the decision-making process and craft effective responses, the preexisting consensus including a set of possible response options for strategic level decision-makers to choose from, as well as a list of Allies’ operational cyber capabilities must be made available. 53 Pre-existing consensus should include criteria of a cyber attack as an armed attack, if and when pre-emptive cyber strike or kinetic response would be allowed (the response might be limited to entirely non-kinetic measures) 54, which kind of response would be proportional, etc.55 It has been suggested to institute a high level advisory body, a Senior Cyber Committee (similar to a NATO’s nuclear planning group) consisting of technical experts, policy personnel, and military representatives to discuss regularly cyber security in the Allied context. 56 This would help to reduce the lack of understanding between technical and strategic levels, keep senior decisionmakers attention on cyber security and facilitate timely decision maki

#### NATO discussion on Article 5 key

Jarno Limnéll 16, Professor of Cybersecurity, Aalto University, Finland, Charly Salonius-Pasternak, Senior Research Fellow, The Finnish Institute of International Affairs, Challenge for NATO – Cyber Article 5, Briefing Paper, Published by the Center for Asymmetric Threat Studies, June 2016, Swedish Defence University, https://www.diva-portal.org/smash/get/diva2:1119569/FULLTEXT01.pdf

Another solution that might be less effective than the development of a new international regime is to continue the work that has already started within NATO related to finding solutions for cyber defense that are binding for NATO member and partner states. In this regard, political consensus has to be achieved between 28 member states, especially considering those situations when cyber threats have given reason for the activation of Article 4 or Article 5 of the North Atlantic Treaty. This task is because here allies must agree upon kinetic actions that might be taken against state and non-state actors out of NATO if necessary in specific situation.

This consensus process would also be a significant step forward in finding solutions for countering hybrid threats considering the strong connection between hybrid and cyber threats. A positive aspect is that after the 2007 cyber-attacks against Estonia the NATO Cooperative Cyber Defense Centre of Excellence was created and one of its tasks is to analyze and seek legal solutions related to NATO cyber defense.235 The products made by NATO of course will be subject to criticism and interpretation or the open ignorance of non-NATO countries, especially those that consider the Alliance as threat to their security. Yet participation in norm creation that might be binding for the entire international society will give NATO significant political credit when dealing with the cyber threat issue on a strategic level both internally within the Alliance and externally with other international actors.

Finally, there is a solution based on the worst-case scenario or casus that is the creation of a normative regime as an outcome of a real life situation, usually of catastrophic consequences. Despite the fact that terrorism as a mode of irregular warfare has existed for long time, the attacks on United States’ soil on 11 September 2001 created a new and much more effective international legal regime in dealing with the fight against terrorist organizations in spheres that included the control of money laundering and other financial activities aimed to support terrorism, arms smuggling and illegal routes of arms export, the proliferation of weapons of mass destruction, and finally, the cooperation to trace and put on trial separate individuals and terrorist organizations.236 Although effective in creating new norms that are helping the international society in fighting against terrorism, it would still be the worst solution for NATO to evolve a form of a legitimate regime against cyber threats based on the catastrophic consequences and sufferings of allied members’ populations and the destruction of critical infrastructure objects under cyber-attacks.

C. CONCLUSIONS

The North Atlantic Treaty is a universal legal document that may serve as an appropriate instrument in the case that NATO faces an imminent cyber threat and subsequent cyber-attack that may cause a catastrophic chain of reactions in combination with other types of threats, united in a hybrid threat constellation or separately used to decapitate technologies or influence information space. For this reason, however, the Alliance must show itself as a robust organization that is able to provide political consensus when cyber threats are projected against one or more NATO members. One does not need to doubt the outcomes when cyber threats emerge again with similar situations when compared to Estonia in 2007 or in NATO’s partner state Georgia in 2008.

Nevertheless, the Alliance would feel much more comfortable if cyber threats are regulated under a collective security shield and an established international regime that is founded upon the basis of a treaty ratified by the majority. The current international norms that regulate questions about collective security, rights for self-defense, jus ad bellum and jus in bello are obsolete because they have been created in order to regulate kinetic conflicts not cyber space, which was just science fiction at the time when documents such as the Geneva Conventions or the UN Charter were created. Therefore, there is space to maneuver for those state and non-state actors that are developing cyber warfare capabilities—not only for defense purpose but also for offensive objectives— because existing international law allows a wide interpretation regarding what might be considered a cyber-attack and what kind of defense states are authorized to realize. This leaves NATO, as an organization created on the basis of international law, with challenging conditions in which it has to seek its own solutions and legitimation for taking a justified response against those that project cyber threats against the Alliance.

In this regard, NATO is forced to take action and create a cyber-defense doctrine that includes all possible kinds of responses. The New Strategic Concept gave political authorization for allied cooperation, strategic commands together with member nations are institutions that provide control and resources, and the center of excellence is a think tank that is seeking applicable solutions for both the Alliance’s needs and those of NATO’s partners. This combination makes NATO a crucial actor, not only at national and regional levels but also at an international level when dealing with the cyber threats issue. NATO’s interest in finding solutions for cooperative cyber defense gives added value to the whole international system and does not exclude the possibility that NATO will be the founding organization to create new norms acceptable to everyone.

It is still hard to predict exactly what kind of cyber threats might be considered as NATO’s jus ad bellum because each case is unique and scenarios in which cyber threats might emerge are complicated, not only from a legal aspect but also from political, diplomatic, and technological aspects as well. Nevertheless, NATO must continue its work in seeking the best methods to defend against cyber threats. Otherwise the Alliance might experience a repetition of a cyber 9/11 and subsequent improvements in cyber threats at all levels, which will undermine the spirit and letter of the North Atlantic Treaty as well as question the legitimacy of the Alliance itself.

#### Application of article V to any cyber threat unravels the international legal order

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

The legal challenges that hybrid threats present for collective security guarantees have been recognized at the highest political level. At their Warsaw summit held in July 2016, NATO’s member states confirmed their readiness to assist each other at any stage of a hybrid campaign and to counter hybrid warfare as part of collective defense.294 They also underscored that the North Atlantic Council “could decide to invoke Article 5 of the Washington Treaty.”295 They repeated these points at their Brussels summit in July 2018.296 By drawing an express link between hybrid warfare and collective defense, NATO leaders signaled their resolve not to allow Article 5 to be hollowed out.297 Still, their declarations of intent strike a rather conservative note. Whilst they accept that NATO may assist an Ally at any stage of a “hybrid campaign,” it is only in cases of “hybrid warfare” that they foresee a potential role for Article 5. This is not an unreasonable position to take. As we saw earlier, recourse to the use of force to counter hybrid threats falling below the threshold of an armed attack is neither permissible nor necessarily appropriate. A pledge to invoke the mutual defense commitment in response to every type of hybrid threat would be a promise to use the proverbial sledgehammer to crack a nut. It would be unrealistic and therefore lack credibility in the eyes of hybrid adversaries.298 By accepting that the role of Article 5 is confined to situations of hybrid warfare, the Warsaw and Brussels Summit Declarations avoid such empty gestures. However, in the same breath they also concede that the application of Article 5 is contingent on the legal threshold between warfare and peace, and thus vulnerable to subversion along the lines discussed in the preceding sections.

It may be tempting to deal with the problem of legal thresholds by attempting to escape them altogether, but this is not a feasible strategy. Even if the contracting parties were to revise Article 5 NAT and Article 42(7) TEU to avoid references to “armed attack” and “armed aggression,”299 they would remain bound by the rules governing the use of force under the UN Charter and customary international law. Although the member states of NATO and the EU make up an influential part of the international community, it is not within their ability to adjust these general rules of international law unilaterally. In any event, lowering the threshold for the use of force in order to facilitate the application of Article 5 and Article 42(7) would come with significant costs, since it would loosen the legal restrictions for all states, including hostile powers. The applicable thresholds therefore cannot be unilaterally modified at will and without the risk of unraveling key elements of the international legal order as it currently stands.

A more promising approach is to strengthen legal interoperability among NATO and EU nations. One line of effort is to reduce legal gray zones,300 for example by narrowing disagreements over the gap that lies between the definition of force and armed attack. This could prepare the ground for developing a shared understanding of what kind of hybrid threats may trigger the applicability of Article 5 NAT and Article 42(7) TEU. Given that the assessment of any security threat depends heavily on its context, it may prove somewhat sterile to build such a consensus in the abstract. Drawing on war-gaming and exercises may offer a more fruitful way forward. Bearing in mind how attractive the use of proxies is to a hybrid state adversary,301 developing a common approach to attribute their activities to the sponsoring state also merits attention. Although many aspects of the rules governing the attribution of wrongful acts are settled, certain questions could benefit from a joint posture.302 NATO and EU nations should also strengthen their collective mechanisms for unmasking attempts at plausible deniability in order to deny its use as a hybrid instrument,303 as illustrated by their united response to the Skripal incident and to Russian cyber operations.304

### Secrecy Solves---2AC

#### Doesn’t assume secrecy – strategic ambiguity’s deterrence is toothless without assurance of quick retal

James **Prideaux 20** – MA in Applied Security Strategy and BA in History and International Relations from the University of Exeter. (“Should NATO Adopt a Joint Offensive Cyber Capability?” University of Exeter, September 2020, <http://www.exeter.ac.uk/media/universityofexeter/strategyandsecurityinstitute/pdfs/mstrat/James_Prideaux.pdf> ) PJW

Additionally, a unified offensive cyber C2 structure would aid scenario planning and speed up decision-making. This is important, because NATO needs to streamline its current decision-making process in the cyber domain.115 A single command would help members agree on appropriate forms of retaliation in cyberspace in different scenarios, bolstering the credibility of deterrence-bypunishment even further. Without a clear command structure, it is very difficult for the 30 NATO allies – who have different threat perceptions and suffer from a lack of cohesion – to agree on effective response scenarios in contingency planning.116 As a case in point, Estonia is willing to strike back when attacked online, given its memory of the 2007 attack and its proximity to Russia.117 However, Estonian officials do not know whether other allies will support them, validating some scholars’ arguments that NATO needs to find common ground in cyber contingency planning.118 The secrecy that shrouds allies’ capabilities and the uncertainty surrounding cyber scenario planning might explain why offensive cyber effects do not feature in NATO’s mission planning process.119 **This is not to say that NATO needs to publicly agree on a ‘red line’ in cyberspace that could trigger an Article 5 response.** If anything, NATO’s current **strategic ambiguity is key for deterring attacks that fall just below a defined threshold**.120 However, unifying cyber C2 would help them carry out scenario planning **behind closed doors**, improving the Alliance’s readiness. Speeding up the decision-making process is crucial given how long it can take to attribute and then launch a retaliatory attack.121 Overall, streamlined scenario planning and decisionmaking, augmented by improved coordination of cyberattacks, would **strengthen the credibility of deterrence**-by-punishment. Although aggressors like Fancy Bear would not know when a certain threshold has been crossed, it would tilt their risk-benefit calculus knowing an attack could trigger a faster, well-coordinated retaliatory attack.