

Technical Evaluation Report

SAS-141 Research Symposium on “Deterrence And Assurance Within An Alliance Framework”

Matthew Tattar, PhD
Technical Evaluator
Naval War College
UNITED STATES

matthew.tattar@usnwc.edu

David Rudd
Programme Committee Chair
National Defence Headquarters
CANADA

David.Rudd@forces.gc.ca

ABSTRACT

This technical evaluation report summarizes the main contributions of the presentations given during the NATO symposium, Deterrence and Assurance Within an Alliance Framework, in January 2019. It augments the papers collected in the proceedings, addresses the main points of keynote speakers, and presents a summary of discussion and identifies key insights of these deterrence experts working in support of the Alliance. It recommends future research based on the papers, presentations, and discussions summarized here. These observations represent the view of the technical evaluator and are in no way meant to portray a comprehensive account of the entirety of the symposium. They also do not represent the views of the United States Government, Department of Defense, the United States Navy, or the US Naval War College.

1.0 INTRODUCTION

NATO has been able to achieve its mission objectives in large part by staying at the forefront of technology and concept development, and maintaining its technological and conceptual advantages over potential adversaries. The NATO Science and Technology Organization (STO) contributes to this by helping position the Nations’ and NATO’s science and technology investments as a strategic enabler. It conducts and promotes activities that augment Alliance capabilities in support of NATO’s objectives. It contributes to NATO’s ability to enable and influence security and defence related capabilities in accordance with NATO policies. It also supports decision-making in the NATO Nations and NATO. Within STO, the System Analysis and Studies (SAS) Panel provides expert analytical advice. It conducts studies, analysis, and information exchange activities that explore how operational capability can best be provided and enhanced through exploitation of new technologies, new forms of organization, or new concepts of operation. [1] The focus of the 2019 symposium was deterrence and assurance theories, activities, evolving issues affecting and affected by Alliance dynamics.

The NATO Science and Technology Organization (STO) sponsored the “Deterrence and Assurance Within an Alliance Framework” Symposium at King’s College London. It brought together scholars and policy

*Technical Evaluation of the proceedings of the NATO STO SAS Symposium on
“Deterrence and Assurance Within an Alliance Framework,”
held in London, United Kingdom, 17-18 January 2019, and published in STO-MP-xxx-xxx*

makers from NATO member and partner nations in order to explore deterrence concepts with respect to NATO. STO also aims to set a research agenda to better inform NATO's strategic and operational planners. Papers with significant potential impact on NATO deterrence planning included those discussing application of operations research in comparing deterrence and malign activities over time, improving societal resilience (both physically and in the cyber/social media area), and ways to enhance NATO's deterrence posture, both nuclear and conventional. Despite many public assertions that today's world is more complex and dangerous than ever before, both keynote speakers and many presenters noted that the NATO deterrence problem is not novel, overly complex, or unprecedented when viewed in historical context. Russia is widely recognized as a dangerous adversary that is "playing a weak hand extraordinarily well," similar to (but diminished from) the role played by the USSR during the Cold War.

The subject of war-gaming arose numerous times and therefore deserves a special mention. The symposium highlighted areas that would benefit from exploration through war-gaming. Especially useful were the papers and discussion of deterrence in the space, cyber, and maritime domains. Presenters discussed the state of these domains in both the "real world" and how they are portrayed in war gaming. Of special concern to war gaming is overcoming the notion held by players (and decision-makers) that once deterrence has failed in the space domain (i.e., conflict has started), then the deterrence task is over. Players need to realize that the need for deterrent signals between adversaries do not stop, even after the most intense violent conflict has commenced. In the cyber domain, the papers and associated discussions indicated that when facing a peer competitor's malign activities, alliances such as NATO that have difficulty forming a consensus for action may find it easier to pursue defensive, "resilience" strategies, rather than launching counter-attacks. Salient deterrence issues that exploration through war gaming can address include: what balance of restraint and aggression is necessary for assurance of allies while avoiding undue provocation of adversaries; how can a game represent a defensive strategy of resilience during play and assess the "results" of player decisions, and; how might maritime forces enhance deterrence.

2.0 KEYNOTE SPEAKERS

STO SAS augmented the symposium with two keynote speakers - one at the beginning of each day. The first speaker provided a historical perspective of deterrence from both the academic and practitioner's viewpoints. Given the topics of the first day's presentations, this arrangement added theoretical depth to the totality of the presentations. The second day's keynote represented the current practitioner's viewpoint, and also issued a call to action for researchers supporting the Alliance.

2.1 "Success of Deterrence," Dr. Kori Schake

The first keynote address was delivered by Dr Kori Schake, Deputy Director-General, International Institute for Strategic Studies. Dr Schake oversees the Institute's world-class research programme and acts as a driving force behind initiatives to enhance the Institute's work and profile. She has worked with both the military and civilian staffs of the Pentagon, in the White House at the National Security Council, and at the US State Department as Deputy Head of Policy Planning.[2]

Dr. Schake opened the symposium by highlighting past challenges and successes of NATO deterrence and assurance. The current challenge is to apply deterrent thinking when we cannot persuade our own citizens of the threat, or definitively pin responsibility for malign acts on any particular aggressor. However, she charged participants to remember that the current international environment is not the most challenging faced by NATO. Accomplishing the tasks of deterrence and assurance simultaneously is hard, and the task was much harder during the height of the Cold War.

To illustrate her point, Dr. Schake discussed three cases of deterrence and assurance within the Alliance. The United States pushed for German rearmament in 1954 because of the looming Soviet conventional threat.

However, given Germany's history as an aggressor less than a decade previous, the US also needed to provide a heavy dose of assurance to the rest of the Alliance, especially France. In the end, the US could not provide enough assurance to France, but went ahead with German rearmament so that it could maintain its deterrent by strengthening the military capability of NATO. The second example of deterrence and assurance that is illustrative of the challenge was the Berlin Crisis of 1958. In response to a Soviet demarche threatening to cut off land access to the city, President Eisenhower strongly signalled to the Soviets the US willingness to fight a war for Berlin, while sending Secretary of State Foster Dulles to assure the German Chancellor of the same willingness. Eisenhower's reputation as the general who liberated Europe from Nazi Germany meant his threat was particularly credible. Even though the promise of fighting a war over Berlin scared more than assured the Germans, the balance between deterrence and assurance was enough to preserve the status quo between east and west. Dr. Schake's final example was the 1962 Berlin Crisis. Faced with the same Soviet threat to isolate Berlin, President Kennedy drastically overreacted. Not only did he pledge to defend Berlin, but also made policy decisions that increase American defence capabilities and proved threatening to the Soviets. This extra step of increasing US capabilities was needed because he did not have the same formidable reputation as Eisenhower. However, the overreaction intensified the Cold War - an unintended reaction.

In comparing the present era to that of the Cold War, Dr. Schake emphasized that deterring hybrid and cyber warfare is easier than nuclear deterrence while simultaneously managing a potential conventional and nuclear escalation ladder was. The balancing act was to deter the adversary, but not in a way that was too "scary" to assure allies.

History teaches us three lessons about deterrence and assurance. First, who makes the deterrent threat matters; credibility matters. Eisenhower could make a stark military threat as a former commanding general that Kennedy could not. Second, in an alliance context one has to work both sides of the deterrence and assurance equation at the same time. Deterrence signals are linked to those of assurance. Third, if you do not have a theory about what an adversary is doing, you will waste a lot of time and effort as well as sending the wrong deterrent message to the adversary.

In the estimation of the technical evaluator, Dr. Schake's address provided an important "sanity check" ("Math class is not newly hard; math has always been hard" is her apt metaphor) on the current deterrence and assurance discourse. By providing historical context to the current debate, she reinforced the notion that the task for NATO is not impossible. The good news, she asserted, is that NATO is well equipped to accomplish this and has proven adept at it. The Alliance has been able to "speak out of both sides of its mouth" about nuclear weapons, simultaneously asserting that it is a nuclear alliance and committed in the long term to disarmament. It can continue to do the same for the lesser challenge it faces today. Yet a word of caution is still necessary, in this author's view. While NATO members have always had varied interests and perspectives, the gulf between those who feel the Russian threat most acutely and those that do not has arguably never been wider. A key difference from the Cold War period is that NATO's most powerful continental member, Germany, also is one of the least concerned about the current threat. This is in stark contrast to the time prior to its unification, and could have profound effects when coherent Alliance actions may be needed in the future.

2.2 Brigadier J.J. de Quincy Adams, OBE

On Day 2 the keynote address of the symposium was given by Brigadier General Jasper John De Quincy Adams, Director of Comprehensive Crisis and Operations Management Centre, Supreme Headquarters Allied Powers Europe NATO (SACEUR). He completed three tours in Iraq (Op TELICs 5, 8 and 11). Subsequently, he was posted to the UK's Permanent Joint Force Headquarters (PJHQ) before deploying to Afghanistan (Op HERRICK 10 and 11) as the mentor to the Helmand Provincial Chief of Police, establishing the Police Mentoring Advisory Group. His recent work included time at the UK Ministry of Defence in Army Resources and Plans, SHAPE Team Leader of Task Force Ukraine Team leader, and two years as a Special Advisor to the Chairman of the NATO Military Committee.[3]

Brigadier Adams spoke about NATO's deterrence challenge from a practitioner's point of view. He outlined the evolution of NATO, the current state of relations between members, and highlighted challenges that need urgent attention. He noted that NATO has adapted to the threat since its inception, and has done so quite successfully. He counted four times that NATO has "reinvented" itself. During the Cold War, it was a threat-based Alliance, unified in the face of the Soviet menace. At the end of the Cold War, it reoriented towards enlargement, expanding its membership eastward. With the September 11th attacks, the Alliance shifted again, this time towards out of area campaigns in Afghanistan, Iraq, and Libya. The current reinvention is to the era of "Strategic Challenge Management," in which the Alliance faces a resurgent and opportunist Russia. However, one of the key challenges for NATO is that international terrorist groups are still the primary threat in the eyes of many members. "There are 29 different interpretations of the threat... Fourteen care more about international terrorist groups than a resurgent Russia." NATO must consider both threats in order to maintain cohesion. It cannot afford to ignore transnational threats like terrorism in its focus on strategic competition.

While Alliance members have found US political statements with respect to NATO hard to understand, Brigadier Adams highlighted that US military leadership has always been well-disposed towards NATO. Actions matter more than words, and US investment in logistical infrastructure and troop rotation from the continental US have reinforced deterrence in a very significant way. Demonstrating the ability to move large combat formations from the US to Europe every six months, he asserted, has a much greater deterrent effect than British Army maneuvers on Salisbury Plain. Also important to remember is that in the "conventional space, there is no competition – we will beat them." NATO can call upon conventional forces that over time will outmatch anything the Russian Federation can bring to bear. However, the Alliance faces a strategic competitor that uses tools that "put us on the back foot." Despite NATO's military superiority, "all military officers need to be clear that their part is tiny – the military is only a single instrument of power." Currently, NATO is delivering its deterrent effect through the US Treasury, in the form of economic sanctions.

Brigadier Adams outlined seven challenges that NATO, and specifically his organization within NATO, is facing. Research into these areas will assist NATO planners in addressing the deterrent challenge posed by Russia and transnational threats.

1. Political Challenge: political leadership needs to articulate in a sophisticated way the deterrent requirement for the military;
2. Horizon Scanning: improve the ability to identify hybrid activity so that it can be countered;
3. Deterring Non-State Actors: how can international terrorist groups be deterred;
4. Russian Intent: we understand Russian capabilities, but not intent. NATO needs a greater appreciation of what the Russian threat is;
5. Understand the Risk of Miscalculation and Potential Mitigations: how to develop common NATO databases, allow members to enter and view data, and facilitate better information-sharing. Better and common understanding of NATO's own activities would allow for better planning assumptions, knowledge of what signals the Alliance as a whole is sending, and therefore avoid sending the wrong messages to the adversary;
6. Identify the Value of Deterrence: individual components of a deterrent are not equal. What part does a military operation play in comparison to a political or economic action and how can this be measured;
7. What Comes Next? NATO's indication and warning system is good; Russia cannot mass force to conduct conventional operations without the Alliance knowing it. However, this capability is not as good with respect to "hybrid activity." NATO needs to develop a "deterrence response options menu"

for the range of potential adversary behavior, and then run those response options through war games and simulations so that plausible outcomes can be explored.

In the view of this technical evaluator, the Brigadier's comments were especially helpful in framing the policy research problem facing NATO. What is needed most of all is a hard connection between academic research, political decision-making, and military action (within the context of the diplomatic, informational, and economic domains). The remarks also put recent political upheaval into perspective. While allies may find US political rhetoric disturbing and indicative of some future abandonment, it helps to recognize that significant outlay of resources (both human and financial) send more meaningful signals. NATO has also dealt with this phenomenon throughout its past. US abandonment was a pervasive fear for the European members throughout the Cold War, but never actually manifested itself. US investments in infrastructure, and its robust program of military exercises and rotations should serve as strong examples of assurance. However, US policy makers should be cognisant of how European allies receive messages that seem to undermine cohesion. It can be argued that in the heavily psychological realm of assurance, "seeming" to undermine alliance cohesion actually *does* undermine it.

3.0 SESSION 1 – DETERRENCE AND ASSURANCE: NEW THEORIES

The first session comprised three presentations that looked at deterrence through a theoretical lens in order to help further the knowledge of deterrence and assurance dynamics.

3.1 Leveraging Behavioural Game Theory for the Study of International Relations

Captain William Caballero, US Air Force, presented a paper that he co-authored with Brian J. Lunday. Schelling noted in 1980 that game theorists of the era tended to focus on the mathematical frontier of conflict. Game theorists have increasingly focused on mathematical models, and devoted less attention to applications. Caballero and Lunday seek to bridge this divide by illustrating the utility of selected behavioural game theoretic techniques in international relations scenarios, and to revitalize the study of what Schelling called the theory of conflict. By re-examining classic Cold War deterrence models and other international relations games, they aim to illustrate how modern game theoretic techniques that are based upon agent psychology, and their ability to think strategically or learn from past experience, can provide additional insights beyond what can be derived via perfect rationality analysis. These demonstrations emphasize the complementary nature of research between international relations and behavioural game theory, and how developments in both fields further the advancement of the other.

The international system has changed in since the maturation of Game Theory, so it is entirely appropriate to re-examine its application and attempt to refine it. In making the theory more "realistic" and hence more informative, Caballero is making an important contribution to the literature. Significant questions remain to be addressed, however. Given the need for improved NATO planning and decision making, further work should demonstrate how this game-theoretic approach is better than both "common sense" and an examination of historical case studies in deterrence. In other words, the process of how deterrence works may be just as informative as models. The actual number of deterrence and assurance "objects" (leaders, countries) are not likely to produce statistically-significant findings. For example, NATO has not had to deter hundreds of different Soviet/Russian leaders; it has had to deter eight: Stalin, Khrushchev, Brezhnev, Andropov, Chernenko, Gorbechev, Yeltsin, and Putin. How would the formal modelling of behavioural game theory perform better than taking a close analytical look at the behaviour of those eight leaders? Finally, mathematical models can be opaque to broader audiences. How might the authors "translate" the theory for use by other academics and, more importantly, practitioners?

3.2 Applying Soft OR to Assessing Conduct

Stuart Smith of Joint Forces Command, Brunssum presented his work on applying operational research techniques to assessing hybrid warfare.

To date the approaches taken to assess deterrence have applied hard Operations Research (OR). Hard OR is appropriate for problems that are well-defined; it is possible to define a model of the problem which, ideally, can be verified and validated and the desired outcome is to identify an optimum or range of acceptable solutions. Soft OR is appropriate for problems that are not well-defined; it is not possible to define a model that can be verified and validated, and the desired outcome is to improve our understanding of the problem. Soft OR can be a precursor to hard OR. The author applied soft OR to a range of hybrid tactics in mid-2017. This paper reports on the results and analysis of a pairwise comparison of observed hybrid tactics and sets the stage for future research.

This type of research shows great promise for deeper understanding of the deterrence problem facing NATO. This is a potential first step at getting at elusive measures of effectiveness. Researchers need to do significant work for this project to bear fruit, but the effort would be worth it, since a better definition of “hybrid activity” is needed. In a broad sense, “hybrid” implies a combination of many activities, but the paper uses activities that are homogenous: “media ops”, “distributing Russian passports”, and “cyber attacks on NATO and neutral CIS”, are not hybrid by themselves, for example. Arguably, it is the combination of these activities that would make them “hybrid.” As noted in the presentation, researchers need to focus on gathering data on NATO and Russian activity over time, defining “hybrid” and “unacceptable” behaviours, and start to uncover what NATO activities (if any) have had a deterrent effect. Additionally, detailed case studies of deterrence may supplement the soft OR approach in establishing causality between NATO activity and deterrence of Russia (if such cases exist). [4]

3.3 A “New Look” at First Strike Stability

Harrison Schramm provided a refinement of the Cold War era concept of strategic stability, updated for the current international environment. During the Cold War analysts studied the strategic stability of their nuclear weapons postures, where preventing war was a coequal objective to winning. The First Strike Stability Index was developed to analytically compare the utility of different forces. Since the end of the Cold War, thinking about nuclear conflict in this particular construct has fallen out of favour. This paper provides a modern-day update to the First Strike Indices.

This paper poses an interesting follow-on question: is NATO a victim of its own success? In the eyes of Russia, NATO has built a “war winning” arsenal while attempting to build a “war preventing” one. Coupled with NATO’s eastward expansion, this has encouraged more aggressive Russian actions. The result has been that many NATO members are feeling less secure than previously. It would seem to be a textbook example of the “security dilemma” in action: measures to improve one’s own defence are perceived as offensive, provoking a response that makes one less secure. Assurance as a concept is traditionally applied to allies. However, this phenomenon leads one to ask how much (if any) assurance does NATO owe the Russians? Are assurance messages enough to mitigate the effects of a security dilemma? [5] Is there is typological issue that requires attention – one that distinguishes between assurance (for allies) and *re*-assurance (for adversaries)?

4.0 SESSION 2 – DETERRENCE AND ASSURANCE IN PRACTICE

Session 2 looked at deterrence and assurance in the practical application context. All three papers presented some aspect of practicing deterrence within the Alliance, be it from the perspective of member nations, domain-specific applications, or deterring new kinds of threats.

4.1 National Perspectives of European Countries in Deterring Russia

Dr. Nora Vanaga of the National Defense Academy of Latvia argued that for the more vulnerable members of the Alliance, “defensive” signalling is not enough for assurance. The approach chosen by Russia in Ukraine, has rendered lessons learned from the Cold War deterrence only partially applicable to the present security situation in Europe. The emergence of the cyber realm, less emphasis on nuclear deterrence, and the increasing importance of non-military threats are among the key differences from the Cold War period. Her presentation focused on the defence and military responses of northern and eastern European countries. It identified particular challenges these countries are facing to balance between NATO deterrence posture and national deterrence efforts, and proposed ideas for aligning them. It would also help to formulate national expectations when it comes to the existing NATO deterrence posture.

Dr. Vanaga’s research poses an interesting conundrum for NATO policy-makers. NATO’s current deterrence policy does not do enough to assure its more vulnerable members – i.e., those closer to Russian borders. How should the Alliance address this assurance deficit, while not provoking the adversary? Further, other members may fear more aggressive deterrent signals precisely because of their potential for provocation. Research may need to explore the balancing point between deterrence, assurance, and alliance cohesion.

4.2 Deterrence and Assurance as a Daily Activity: NATO’s Maritime Operations

Mr. Andrew Bell of Allied Maritime Command describes and compares NATO’s and its adversary’s maritime capabilities and operations. Mr. Bell’s paper provides a review and comparison of both NATO and potential adversary maritime capabilities and activities, reviews the plans and aspirations for the near future, and attempts to identify gaps and challenges that will impact upon the balance required for NATO to achieve a sustainable level of deterrence and assurance. Recently, the Russian Federation Navy has been pursuing an ambitious fleet modernisation and renewal programme. In response, the need for NATO to react to developments in the maritime domain has been recognised for some time now.

Mr. Bell provided a good description and comparison of NATO (as well as Russian and Chinese) maritime activity. Yet this paper could have gone further in specifying the deterrence role that maritime forces can and do play. Do maritime forces represent the capability to deter via denial and/or punishment? The latter is obviously the case with the current submarine-based nuclear deterrent, but could expand to cover other maritime assets with long-range strike capabilities. Additionally, NATO faces a time, space, and force disadvantage when compared to Russia at the outset of a terrestrial conflict along shared borders. Therefore, there is a real risk of *fait accompli*-type operations proving successful before NATO can bring its full conventional capabilities to bear. Can maritime capabilities aid in deterring such operations while assuring allies? (Examples of modern-day “gunboat diplomacy” include periodic deployments and exercises by NATO navies in the Baltic and Black Seas. Yet their value would obviously go beyond mere diplomatic signalling if a crisis escalates.)

4.3 Assuring Allies by Effectively Deterring Hybrid Actors: Challenges and Opportunities

Dr. Vlasta Zekulic of NATO Headquarters Operations Division articulated an effects-based approach to countering hybrid threats. Like the keynote speaker, she notes that hybrid threats are not new. NATO has been monitoring and responding to this concept of warfare since 2009. At the same time, the rapid enhancement of information technologies, alongside our increased dependency on them, creates a vulnerability that hybrid actors can exploit. Hybrid activities are typically applied across all physical, social and psychological domains, blurring lines between war and peace and challenging traditional definitions of the “battlefield.” This makes countering hybrid strategies a challenging and long-term endeavour. Dr. Zekulic sets out to assess NATO’s efforts in countering hybrid threats by highlighting challenges faced in recognition, attribution, and response

to hybrid acts. Additionally, she proposes an application of effects-based approach in developing response options at the strategic level of the Alliance.

Dr. Zekulic is correct in her assessment that hybrid threats are not new. In fact, their use in the European context goes back at least as far as the Cold War. Similarly, the use of ambiguity is nothing new, but highly effective. People will believe what they want to believe in order to avoid uncomfortable action that may lead to violent conflict. Therefore, as the Crimea crisis demonstrated, even ambiguity that strains credulity can have a chilling effect on taking actions to address hybrid threats. Also compelling is her argument for an “effects based” approach to deterrence. However, there is some danger in applying nuance in deterrent signals. Since signals are difficult to accurately send and receive, nuance may be lost. The Alliance must take care in sending signals, lest it be perceived as weak on one hand, or overly aggressive on the other.

5.0 SESSION 3 – DETERRENCE AND ASSURANCE: LESSONS LEARNED?

This panel examined lessons learned from recent applications of deterrence concepts. A particularly novel concept presented was that NATO may serve as a vehicle (in some form) for the implementation of sanctions. What deterrent effect might this new role have? [Two presentations were unaccompanied by papers.]

5.1 Deterrence and the Use of Sanctions

Mr. Ian Bolton presented his work on use of sanctions in a deterrence context. Sanctions have seen increased use as a response to international challenges such as humanitarian abuses and proliferation of weapons of mass destruction. Nation-states have used them both multi- and unilaterally, and many of the sanction regimes in place have been driven by NATO members. Sanctions are most commonly used as a diplomatic option before potential armed intervention: to coerce, constrain, and signal the target state. While many question the decisiveness of sanctions, they undeniably have effects. Mr. Bolton explores the use of sanctions as a method of deterring armed conflict and examine the relevance of this to NATO. Specifically, he considers whether sanctions represent a tool that the NATO alliance could use, and whether there is more NATO could be doing to support the enforcement of sanctions.

The idea of sanctions within the context of NATO is a novel idea and one that merits further exploration. However, the mission and structure of NATO mean that it would be, at most, a forum for coordination. Deterrence requires capability and credibility. Individual member states of NATO have used sanctions repeatedly to various levels of success. But none have used NATO as a conduit to coordinate and impose sanctions on an outside entity. Using sanctions as a deterrent, therefore, implies that NATO would have to use coercion on some third party so that sanctions could serve as a credible deterrent to Russian aggression. Also, sanctions are applied after the target entity has committed some action to warrant it. As a deterrent, therefore, sanctions are problematic because they are (initially) applied *post facto*, whereas threats of denial or punishment are usually applied beforehand to prevent unwanted behaviour in the first place. Yet additional sanctions can potentially be brandished as part of a multi-stage, non-kinetic response to tensions.

It is important also to not overstate the effect of sanctions. Mr. Bolton notes that sanctions helped prevent further aggression by Iraq in 1990. However, it is more likely that the massive force build-up during Operation Desert Shield was more instrumental to that end than any sanctions regime.

6.0 SESSION 4 – NEW TRENDS AND METHODS I

This panel explored new trends in deterrence, specifically the concepts of societal resilience and instilling a common understanding of deterrence lexicon. Improving societal resilience may make deterrence by denial of the aggressor’s intended effects possible. Common and harmonized deterrence lexicon will enable more effective deterrence in action in the long run.

6.1 Modern Resilience as a Deterrent

Elisabeth Braw of the Royal United Services Institute pointed to resilience of modern society as a potential deterrent. The primary concern of every government is the safety and security of its population and territory. However, to a large extent, hybrid-style aggression is not impeded by geography; cyber attacks and malign influence campaigns know no geographical impediments, and can still cause harm to a homeland like overt military aggression. Also, many of the targets of hybrid aggression are in the private, not government, sector. They are critical for smooth operation of society but not classified as critical national infrastructure that qualifies for additional protective measures. This means that governments need to work with business to create a model of comprehensive resilience and thus deterrence. No country, however, has comprehensive societal resilience plans. Since NATO and partner countries face similar hybrid threats there is a need to build such plans. This is a challenging move for governments since it shifts to a deterrence mind-set that reaches across society, where everyone plays a part.

Ms Braw's paper raises some very important points and even more questions. Some groundwork needs to be done on societal resilience. What makes societies resilient? Are NATO members less resilient today, or do they lack resilience? By what definition? Further, are member-state societies gaining resiliency naturally? By any measure, they have been the subject of numerous malign influence campaigns from abroad. But are there also internal socio-political pressures against which societies must inoculate themselves, without NATO's help? Do societies develop mental "callouses", or do they stay vulnerable despite (or because of) their experience? Again, an expansive understanding of resilience may be of help here, if only to distinguish between what the Alliance can deliver for its members and what it cannot. Many scoffed at civil defence measures during the Cold War; it may return in different forms in the age of hybrid warfare, where entire societies are on the front lines.

6.2 Acculturation of the Core Concepts of European Security

Dr. Andrew Corbett and Dr. Annamarie Sehovic argue that policy ambiguity that is designed to accommodate national preferences hinders effective deterrence. Deterrence is a psychological process designed to influence the decision making of a potential adversary; it works best prior to the decision being made. Current NATO definitions of deterrence and other key terms such as resilience are very carefully constructed but deliberately ambiguous in order to accommodate differing national interpretations of how deterrence works. Functionally, these policy ambiguities hurt the Alliance's ability to conduct a coherent deterrence strategy, while creating serious tensions in the development and implementation of strategies for deterrence and resilience. NATO members would benefit greatly from an acknowledged understanding of the use of key terms in their own security lexicon.

Drs. Corbett and Sehovic raise an important point about language and the ability to execute a coherent deterrence policy. Unity of language and common understandings of key terms are undoubtedly instrumental. One only has to look to the importance of a well-articulated commander's intent during the operational planning process in order to illustrate this. In many cases conscious and coherent language-policy linkages should produce better policy outcomes. However, as Dr. Schake noted in her keynote address (discussed above), part of NATO's effectiveness in balancing deterrence and assurance lies in its ability to send conflicting messages. Ambiguity has proven to be a useful tool for Alliance cohesion. There is a danger that "settling disagreements" in terms may cause some members to become less supportive in the overall NATO mission because their particular national interest would conflict with unified NATO language. Similar to other issues, harmonizing NATO's deterrence rhetoric requires a balanced approach.

7.0 SESSION 5 – NEW TRENDS AND METHODS II

The fifth session further explored new methods and trends in deterrence research, delving into the areas of artificial intelligence (AI) and grey-zone threats. AI promises great upheavals in the commercial and military

worlds, and the realm of deterrence is no different. Studies of grey zone conflict have focused on tactical-level actions, but potential grey zone activities are not limited to that level of war. [One presentation was unaccompanied by a paper.]

7.1 Artificial Intelligence and Deterrence: Science, Theory and Practice

Dr. Alexander Wilner presented his paper on Artificial Intelligence and deterrence. While a consensus is forming among military experts, policymakers, and academics that Artificial Intelligence (AI) will prove useful for national security, defence, and intelligence purposes, no academic study has explored how AI will influence the logic, conceptualization, and practice of deterrence. Debates on AI in warfare are largely centered on the tactical use and misuse of the technology within autonomous weapons systems, and the associated risks AI may pose to the ethical use of force. No concomitant debate exists, however, as to the strategic and deterrent utility of AI in times of crisis, conflict, and war or in matters of cybersecurity. Nor has any country openly published a strategic document on the nexus between AI and deterrence. The dearth of knowledge is surprising given the expectation that the future of warfare will be autonomous. Dr. Wilner's research is intended to provide a comprehensive conceptual map of how AI influences both deterrence in theory and in practice. It does so by exploring the science of AI and by providing a synthesis of how states are approaching AI in warfare and deterrence.

Dr. Wilner's discussion of AI and deterrence speculated on a number of important implications of AI adoption. Namely, AI will enable better offense and defense by improving methods of denial and punishment, respectively. Coercion may also improve because AI-augmented planning and logistics will make coercive actions more efficient. Other notable effects may be that AI could enable deterrence through "delegitimization": manipulation of data could undermine a threatening regime and therefore prevent it from action. Since "first mover" advantages are fleeting (e.g., innovation leads rapidly evaporate as other actors catch up), many of these AI-driven effects may end up being a "wash." AI could help both aggressor and defender, weak and strong, deterring and deterred. One worrisome potential effect does not fall into this category, however. If AI enables or conducts decisions at "machine speed", Wilner notes, the imperative to strike first may increase over time. AI would have the potential to heighten instability by creating the incentive to act so as not to have the adversary get inside (and stay inside) one's decision-making loop.

7.2 Re-Orienting Deterrence: The Reality of Grey Zone Strategic Threats

Major David Stuckenberg, USAF, attempted to articulate the nature of strategic-level grey zone threats and suggested two approaches for their mitigation including, (1) better cognitive understanding of where deterrence can and cannot work in modern warfare and; (2) dissuasion as an international strategy. NATO finds itself increasingly confronted with new types of warfare. These types may lie outside of NATO's cognitive understanding. As a result, the utility of NATO's long-standing deterrence methods have been extended into the grey zone, beyond their "theoretical limits." There is strong evidence that a strategic gap has opened that is not addressed by contemporary NATO strategies. Threats that may manifest within this gap range from un-attributable intercontinental ballistic missiles and space-based weaponry to the manipulation of natural disasters and social media to achieve strategic ends.

Major Stuckenberg points to a "strategic gap" in the spectrum of conflict. Most inquiry into "grey zone" threats focuses on lower-level, "tactical" actions that pose tricky attribution problems and therefore are difficult to counter. There is less understanding and study of "strategic level" grey zone threats. In his presentation, Major Stuckenberg raises the spectre of an electromagnetic pulse (EMP) attack with no attribution, which would pose a significant deterrent challenge. If an adversary could be confident of its ability to inflict damage on a NATO member without being blamed, how can that adversary be truly deterred? This is an especially vexing problem, but one that is very unlikely to manifest itself in this author's opinion. A large-scale EMP attack or other acts of similar scale are 1) not really "grey zone" at all since they pose a threat to national survival, and 2) unlikely to be completely un-attributable. Even if the perpetrator nation successfully hid its involvement, one must ask

who would benefit at that particular time from inflicting such grievous harm? With such drastic strategic actions and damage in play, is concrete discrimination necessary? Arguably, it is not.

8.0 SESSION 6 – DETERRENCE IN AND FROM SPACE

The final session explored deterrence concepts and dynamics in the space domain. Policy makers and planners have struggled with the implications of the space domain for deterrence. It has been an enabler and force multiplier for Alliance militaries for an extended period. However, it also represents a vulnerable point for those same militaries. How to deter action in space when it is both a source of great strength and a potential Achilles heel? The two papers set the stage for deterrence in the space domain and describe its unique characteristics.

8.1 21st Century Deterrence in the Space Warfighting Domain: Not Your Father's Century, Deterrence, or Domain

Mr. Bryan Boyce (Major, USAF – retired) outlined the implications of the space domain for deterrence. Effective twenty-first-century deterrence that includes the space domain needs to be national and multinational, multi-disciplinary, and multi-domain. Further, actions must be applied through diplomatic, informational, military, and economic (DIME) means to prevent terrestrial conflicts from extending into space.

Mr. Boyce raises important points about the relative novelty of the space domain. While perceived as relatively benign in the years following the end of the Cold War, space has become both an enabler for important NATO capabilities and technological advantages, as well as a new source of conflict as it becomes more congested and contested. Implications of his work warrant further investigation, including how to use war-gaming in assisting decision-makers. “Conditioning” leaders in the types of decisions they may have to make has long been a fundamental task of war-gaming in all domains. The Alliance may find it particularly useful to run multilateral space war games in order to investigate the effects of alliance dynamics on the space domain. Member states have their own perceptions about how they would employ space in a deterrent or conflict situation, but few have ideas about how their allies would behave.

8.2 The Increasing Importance of the Space Domain in Strengthening NATO's Deterrence

Dr. Donald Lewis presented his work on deterrence in the space domain. NATO has depended upon the space domain to support its deterrence objective for decades. NATO's asymmetric military advantages enhanced by space have contributed a major element to the Alliance's overall deterrence posture. As space becomes a domain of operations in its own right (like cyber), it will become important to both leverage perceptions of its strengths for deterrence, and manage its vulnerabilities. Space provides force enhancement and enables command and control, while enabling information superiority in the battlespace. However, the Alliance's space capabilities must be protected against environmental and adversarial action to ensure their continued deterrence value. Managing deterrence messaging in the space domain must take into account advantages for the Alliance as well as those for potential adversaries. Failure to consider the implications of adversary perceptions may precipitate escalation in space, including the possible use of advanced counter-space capabilities by the adversary.

Dr. Lewis presents a thorough description of the space domain situation facing NATO. Where his work is most useful to the analyst is where it compares the space contributions to NATO strength with factors that weaken those contributions, not all of which come from an adversary. Besides adversarial space and counter-space capabilities, the environment is hostile to all kinds of equipment, and the equipment is both expensive and hard to produce. While strengthening the deterrence value of space assets is an important goal, he notes that adversaries may consider holding Alliance space assets (given their high value) at risk a viable means of

detering NATO. This line of argument sets up some important follow-on questions for NATO. Namely, how does NATO achieve a balance between deterrence and provocation? In other words, how does the Alliance increase its space capabilities for deterrence purposes while also preventing space assets from becoming a source of deterrent leverage for the adversary?

9.0 SUMMARY AND RECOMMENDATIONS

The objective of this symposium was to gather information on NATO's concepts of Deterrence and Assurance (D&A) so as to underpin new approaches to planning, education, and training. This will enable comprehensive planning, execution and assessment of D&A activities, ensuring that the Alliance remains effective in the face of evolving threats.

A number of themes arose repeatedly from the panel presentations and discussions, signifying their relative importance:

- The deterrence task facing NATO is not necessarily more complex than in the past, but its new aspects require a fresh look at deterrence in theory and in practice;
- Resilience is a key concept, especially in a relationship between an alliance with varied interests and a dangerous adversary;
- Grey zone and hybrid warfare are of particular concern;
- The meanings of deterrence and assurance vary among NATO's members.

The proceedings highlighted many potential research opportunities, as noted in the above discussion of the panels. Some hold particular promise. Fittingly, these manifest themselves in the form of questions raised, which are discussed below. Some are primarily theoretical in nature, but most point towards ways to take the next step and practically apply new knowledge in NATO decision making.

- Once we have developed an improved Game Theory that more accurately reflects human behaviour, how might we apply it to improve NATO deterrence decision making? Perhaps the most salient comment during discussion of Behavioural Game Theory was "We don't know who is right because we don't know what game we are playing." Researchers should not only work on refining their models, but find out, as definitively as possible, which "game" NATO is playing. While social science does not lend itself to certainty, being able to characterize with confidence the game-theoretic situation between NATO and Russia would positively inform decision-making.
- What are the appropriate Measures of Effectiveness (MOE) for deterrence operations? NATO should lead a concerted, unified effort to develop reliable MOE that will inform staffs across NATO's members. MOE, unlike Measures of Performance (MOP), are challenging to identify and (especially in the realm of deterrence) quantify. The "soft operations research" approach outlined in this symposium can potentially show the way. What is needed is a systematic comparison of Russian and NATO activities over time. The success or failure of past deterrence efforts is one potential way to identify MOE for future operations.
- How can NATO improve its assurance of the more vulnerable member-nations while not provoking its adversary? The nature of deterrent signals towards adversaries affects how assurance signals are received by allies. Because NATO members vary widely in capability and vulnerability (among other factors), one message is unlikely to be capable of satisfying all. It is evident from the proceedings that "defensive" signals (i.e., of the capability to deny an aggressor's attempt to gain) can be insufficient to assure more vulnerable member states. "Offensive" signals (i.e., those that signal punishment for aggression) may be required. This poses a problem for NATO, however. How can the Alliance make its signals sufficiently "offensive" without being overly aggressive in the eyes of the adversary –

particularly when an adversary may be inclined to treat almost any move as escalatory? Erring too far on the side of aggressiveness may provoke a reaction that hurts NATO's interests in the long run.

- Can NATO provide a venue for the implementation of economic sanctions? While this would be outside the realm of traditional NATO activities, providing the forum for coordinated and synchronized sanctions against a malign actor may be appropriate when responding to grey zone or hybrid activities. However, sanctions are fundamentally a coercive activity, rather than a deterrent. This raises the subsequent question of whether or not NATO needs to economically coerce another actor in order to effectively deter Russia. In order for NATO to develop sanctions as an instrument of deterrence, it would arguably need to demonstrate the capability and willingness to impose sanctions on a third party – most likely an out-of-area threat. The prospects for this seem remote given that the Alliance is re-focussing its attention on the Euro-Atlantic area. Yet this approach does have the advantage of side-stepping the UN Security Council, where Russia would certainly veto any sanctions regime of which it was the target.

The next set of questions revolve around the concept of resilience. This was a recurring theme throughout the symposium, and pointed towards a number of research opportunities and challenges.

- What is resilience, and what kinds or types of resilience are of particular interest to the Alliance? The symposium produced discussion about “societal resilience” in particular, but arguably there are issues of resilient nation-state structures and militaries as well. Where increasing “resilience” falls clearly within the nation-state’s area of responsibility, what role or roles can NATO play in a resilience effort?
- Another basic question requires answering: how resilient are NATO’s members? The current social media environment seems to indicate that malign activities can have an outsized effect on societies. However, systematic analyses are needed to determine how well malign activities actually attain material results (e.g., influence members’ internal policies or political power dynamics) vice merely creating “Twitter-storms” or other less meaningful social media phenomena. Against what “results” of malign activity should members guard?
- Discussions about resilience point toward both a typology and spectrum of resilience. Types of resilience could include military, political, infrastructure, as well as societal. Which types are most important? As a defensive military alliance, NATO has always had to be militarily resilient. Its primary challenge historically has been to maintain a capability to absorb the first blow from an adversary and continue to function. This could be termed “high-intensity resilience.” At the other end of the spectrum might be the societal and political forms of “low-intensity resilience” focussing on the ability of liberal-democratic societies to withstand subversive pressures from without and within. In between the two lies the ability to effectively resist grey zone or hybrid threats.
- Once NATO “solves” the resilience problem, might it be able to simply ignore threats below the threshold of armed conflict? If hybrid or grey zone threats can be simply ignored because their intended effects are denied, resilience will eventually have a deterrent effect.
- In a period during which gaining consensus for action is increasingly difficult, improving Alliance members’ resilience at all levels may be the most effective deterrent. Would sufficient resilience obviate the need to actively respond (and thus preserve alliance cohesion) to threats below the level of armed conflict?

The seven questions/challenges outlined by the Day 2 keynote speaker cover these and other issues, and represent a clear call to action for scholars looking to bring value to the work of those dealing with deterrence and assurance at the operational level.

As possible themes for future Deterrence and Assurance symposia, the following topics emerged.

- Resilience: Concepts, Theories, and Practical Applications

- Deterrence Theory to Practice: Putting Social Science to Work for NATO
- Deterrence in Strategic and Operational Planning: Measures of Effectiveness

The symposium demonstrated that there are many potential avenues of future research. Of particular usefulness to NATO would be for it to focus on supporting the decision-maker in improving deterrence in action. The short list above reflects that philosophy in that the proposed titles aim to steer toward connecting academic rigor to application.

REFERENCES

- [1] NATO Collaboration Support Office information pamphlet: “System Analysis and Studies (SAS) Panel”
- [2] <https://player.fm/series/war-studies/event-assurance-and-deterrence-within-an-alliance-framework-kori-schake-keynote>
- [3] <https://player.fm/series/war-studies/event-assurance-and-deterrence-within-an-alliance-framework-brig-jj-quincy-adams-keynote>
- [4] For a debate about the use of rational choice and formal modelling methodology in security studies, see *Rational Choice and Security Studies: Stephen Walt and His Critics*. Michael Brown, Owen Cote Jr., Sean Lynn-Jones, and Steven Miller, eds. (Cambridge: MIT Press 2000). For qualitative methods of theory development, see for example: Alexander George and Andrew Bennett. *Case Studies and Theory Development in the Social Sciences*. Cambridge, Massachusetts: MIT Press, 2005.
- [5] Further reading on strategic (crisis) stability is available in: Elbridge A. Colby and Michael S. Gerson, eds., *Strategic Stability: Contending Interpretations*, forward by Thomas C. Schelling (Carlisle, PA: US Army War College Press, 2013)