The thirteenth iteration of the Kingston Conference on International Security (KCIS), which took place 11–13 June, continued the proud tradition of the event, bringing together practitioners and academics from around the world to discuss theory, explore practical issues, and to share ideas. This year’s theme, *The Return of Deterrence: Testing Credibility and Capabilities in a New Era*, re-introduced and re-booted concepts and understanding of deterrence, and outlined the challenges that face NATO in particular in attempting to practise deterrence in a threat environment that is very different to that of the Cold War.

Co-hosted by the Centre for International and Defence Policy (CIDP) at Queen’s University in Kingston, Ontario, the Canadian Army Doctrine and Training Centre, the US Army War College, and the NATO Defense College in Rome, KCIS is widely acknowledged as a forum for informed debate on defence and security; the discussion and debate that occurred during KCIS 2018 promise to be of significant value to policymakers, academics, and military personnel alike.
Conference Design
The conference was designed to progress from the traditional to the current concepts of deterrence, and from general to context-specific deterrence challenges. It commenced with a review of traditional deterrence theory fundamentals and then proceeded to examine current defense and deterrence debates in NATO. The second day’s focus was new-era deterrence challenges. First, presenters explored the mix of nuclear and conventional force deterrence in Europe, ‘narrative warfare’ driven by social media, and ongoing cyber competition. Following this, two panels offered context-specific deterrence considerations associated with China, North Korea, and Pakistan, and challenges on NATO’s Southern Flank respectively. The final conference panel drew together key insights that were brought up throughout the conference, and highlighted their relevance to future national security deterrence policy and military strategy development.

Interspersed among the panels, four distinguished keynotes provided unique perspectives on the core conference theme:

- LGen Bowes (Canada) provided insights into the relevance and challenges of new era deterrence to the Canadian Joint Force and NATO.
- M. Elaine Bunn (US) addressed deterrence from a civilian policy development perspective.
- MGen Dorman (US) offered a practitioner's perspective on the importance of logistics in presenting a credible and general-purpose force deterrent.
- Gordon Venner, associate deputy minister of National Defence, presented a perspective on Canada’s deterrence policy and some of the key challenges of its implementation.

In bringing KCIS to an even wider audience, the War on the Rocks Bombshell podcast, hosted by Loren DeJonge Schulman and featuring Stéfanie von Hlatky, Stephanie Carvin, and Elaine Bunn, was recorded at the event. The podcast can be downloaded and listened to at http://bombshell.libsyn.com/mutually-assured-dysfunction. KCIS was delighted to welcome the Bombshell podcast, and we look forward to continuing the relationship at future conferences.

Report
Deterrence as a strategic imperative is as significant as it has ever been. However, our understanding of the foundations of the concept, what it can be used for, and where its shortfalls may be, have to be re-booted. The Cold War lessons about deterrence remain valuable, and the foundations of deterrence are applicable today. However, as understanding of deterrence diminished in the years following the fall of the Berlin Wall, these lessons need to be re-learned, but they also need to be adapted to today’s security environment. Unless we understand the dynamics of twenty-first century international security, deterrence will be improperly applied. Unlike the Cold War, deterrence today is not going to rest primarily on nuclear capability, and understanding of deterrence must be dynamic and flexible enough to enable it to be used to counteract the activities that have already commenced in the ‘Grey Zone’ short of ‘war.’

Twenty-first Century Deterrence and the ‘Grey Zone’
The array of actors able and willing to engage in aggressive and destabilising activity against NATO and the West has grown, as has the spectrum of threat vectors. In particular, imposing costs through the use of cyberspace and manipulation of information flows has become a viable threat. These forms of actions challenge our binary understanding of ‘war’ and ‘peace’ and require us to engage all components of national power in order to develop effective deterrence that is tailored to distinct new environments. Logistics at the national level, industry engagement, and academic input are crucial. The process of
developing deterrent strategies must, however, have its foundation on a clear understanding of ‘deterrence’ as a concept, as well as an appreciation that deterrence is simply a means to an end, not the end in itself. For NATO in particular, deterrence in the twenty-first century requires a re-assertion of common values and objectives in order to communicate commitment to the risk of escalation that is necessary for an effective deterrent strategy.

The emergence of Grey Zone competition and new approaches to imposing costs on an adversary does not mean that the foundations and core tasks of deterrence are fundamentally altered. At its core, deterrence remains premised on credibly communicating to an adversary that they will be unable to achieve their objectives through aggressive means, and convincing them that, if they attempt to do so, the costs would outweigh the perceived benefits. Signalling and perception are therefore critical to influencing leader decision-making, and thus to effective deterrence. There is an absolute need to ensure that the actions that the deterring party find unacceptable are clearly communicated, and that the threatened response will be realized. This communication is at least as important as the capabilities that back up any deterrent posture. Western policymakers in particular have not always followed through on suggested threats, and it is difficult for Western governments to delineate interests and clear responses to threats that their societies universally deem to be acceptable. The first stage of developing this process is, therefore, for the deterring party to understand their own identity and interests, as well as what others believe their intentions to be. In all contexts, maintaining a consistent posture is key in both reassuring allies and persuading adversaries that threats are credible.

Communication and Perception
Psychology is thus central to deterrence, and it is imperative to signal clearly to adversaries the actions that will trigger a response, and those that will not. In both cases, the credibility of the deterring party is crucial: if a threat is not carried through then future threats may not be believed, and inaction on the part of the deterring party may be interpreted as weakness or lack of resolve. At present, there is a great deal of ambiguity about actions and reactions in the Grey Zone, and a demonstrated will to act in the face of this ambiguity is required if deterrence in that arena is to be effective. Notably, collective deterrence through co-operative strategies are crucial in preventing a further rise in coercive activities within the Grey Zone.

Even if full information of an adversary’s interests, motives, capabilities, and decision-making process cannot be attained, deterrent actions should be based on informed judgement founded on deep and extensive study. Deterrence theory emerged on the premise of ‘rational actions’, but humans are not always ‘rational’ in the *homo economicus* sense of the term, and an awareness of an adversary’s priorities are crucial in engaging in effective deterrence. There is thus no single foundational deterrence doctrine that is universally applicable and successful, despite there being a broad continuity of the principles of capability, resolve, and communication that underlie it. Tailoring deterrence to specific contexts, regions, and capabilities is therefore critical, and the deterring party must understand not only what an adversary values, but also their decision-making processes. The importance of this has been highlighted by the US and NATO emphasis on deterring large-scale traditional conflict, while adversaries have increasingly operated in the Grey Zone, leveraging cyber capability and information to cause effects that may be sufficient to achieve the outcomes that they intend.

Particularly for NATO, alliances are crucial in generating effective deterrence. Fostering steadfast alliances can create a force multiplier effect on capability and communicated resolve. Consequently, ‘sunk costs’ and ‘tying hands’ through activities such as public statements, military deployments, and joint exercises may be immensely valuable in producing successful deterrent effects. The Enhanced
Forward Presence, despite protestations to the contrary from many of those involved in the force, is a ‘tripwire’ or the ‘point of the spear’: in itself, it is unlikely to defeat a concerted Russian advance. However, it is the existence of the force that is most significant, signalling that an attack will bring together the weight of the Alliance’s power. Assuring allies of support is, however, difficult, and there is always likely to be doubt that a state will risk its own personnel, or its security more broadly, for another. Differences between allies can also make operations and clear signalling challenging, especially in the context of ‘caveats’. Thus, for example, it is not entirely clear how stakeholders involved in Enhanced Forward Presence would respond to the local chain of command in the event of a Russian invasion. Furthermore, self-interested state behaviour puts pressure on alliances and can heighten the fears that one or both parties will renege on their agreements to combine power.

*Nuclear Weapons and Cyberspace: Not Just ‘the Old and the New’*

Although deterrence now stretches far beyond the deployment and threat of nuclear weapons, this capability remains a facet of many deterrence strategies, particularly if there is concern about regional crisis escalation. The most recent US Nuclear Posture Review indicates that the US is maintaining its ‘first-use’ policy prerogative, thereby retaining the ability to escalate to a nuclear level without the adversary using similar weapons. There is, however, some ambiguity about what actions would constitute sufficient threat or provocation for nuclear escalation to occur, and this is not unique to the US. While conventional force deployment has replaced the overt threat of nuclear escalation in many contexts, where maintaining this presence is too costly, nuclear weapons have provided a stop-gap solution. Russia, for example, has attempted to bridge the conventional military capability gap with the US by maintaining a quantitative advantage in tactical nuclear weapons. The danger, however, is that if this deterrent fails, the risk of escalation to a broader nuclear conflict is significant. Nuclear weapons may also be of limited value in the context of deterrent strategies that are required to take into account a broad array of threats and threat vectors, including those presented by non-state actors.

The emergence of cyberspace as an adversarial arena and the manipulation of narratives have been the most notable threat vectors that have emerged in the Grey Zone that impose costs but do not fit traditional linear concepts of ‘war.’ Indeed, the existence of such actions indicates that, in this environment, deterrence has failed. These forms of actions can be immensely difficult to deter, not least because of the challenges of attribution, and highlight significant vulnerabilities in the West. Deterring these forms of aggression requires the creation of clear ‘red lines’ to indicate what constitutes unacceptable behaviour and risks escalation to kinetic conflict – it is currently difficult to predict the shape of a response, or if a response will occur at all. A response to these forms of attacks must also be creative – it is not necessary for it to be symmetrical, and other forms of national power can be brought to bear. Additionally, the concept of a linear and clear ‘escalation ladder,’ the existence of which may have always been exaggerated, has now become even more complex, making controlling such escalation hugely challenging.

Deterrence is unlikely to be effective if it is approached with the perception that one strategy is universally applicable, or that deterrence is a singular concept. Developing defence and resilience while providing assurance to allies may ultimately be the most appropriate pathway to deterrence in the Grey Zone. Conducting effective deterrence therefore requires a whole-of-government approach which leverages all components of national power in a manner that is particular to a given context and situation. One’s own capability and vulnerabilities — and that of one’s adversaries — must be understood across the complete spectrum of military, government, and society. Deterrence should therefore involve a variety of actors, approaches, and capabilities, and incorporate the introspection required to appreciate the instances when we ourselves have been deterred. Engaging a deterrent
strategy is also only one option available to policymakers, and it is thus imperative that deterrence, and its distinction from other options, is fully understood. As a means to an end, deterrence can undoubtedly lay the platform for the further action and dialogue that is required to improve security relationships, and the holistic insight provided by KCIS into the meaning of deterrence in the context of twenty-first century security provides an exceptional platform for its further study and use.

Authored by:
A. Thomas Hughes
Centre for International and Defence Policy
Queen’s University

William G. Braun, Ill
Strategic Studies Institute,
U.S. Army War College

October 2018

KCIS is a partnership between the Centre for International and Defence Policy at Queen’s University; the Canadian Army Doctrine and Training Centre; the Strategic Studies Institute at the US Army War College; and the NATO Defense College, Rome.