Conference Report

Modern Deterrence Autumn Conference

Oliver Major
188 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world’s oldest and the UK’s leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today’s complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 188 years.

The views expressed in this publication are those of the authors, and do not reflect the views of RUSI or any other institution.

Published in 2019 by the Royal United Services Institute for Defence and Security Studies.

This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.


Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)
Acknowledgements

The conference was organised by RUSI’s Modern Deterrence project in cooperation with the Konrad Adenauer Foundation.
Modern Deterrence Autumn Conference

Summary

THE CONFERENCE, THE third organised by RUSI’s Modern Deterrence project, took place on 13 November 2019 at RUSI in London in cooperation with the Konrad Adenauer Foundation. As a result of late withdrawals by UK members of parliament Jeremy Hunt, Madeleine Moon and Damian Collins – necessitated by the just-called 12 December general election – the speaker lineup had quickly been reconstituted. The conference featured a strong list of European and American speakers covering a wide range of issues.

Beginning with a keynote by Dan Eliasson, Director-General of the Swedish Civil Contingencies Agency (MSB), the panels looked at the role of defence and offence in:

- The deterrence of greyzone aggression, recognising that today’s aggression is often of a non-kinetic nature and directed against civil society.
- Communicating such greyzone deterrence capabilities.
- Climate change as a national security threat, and how to deter aggression that exploits climate change.

A full list of speakers is available here: <https://rusi.org/conference/modern-deterrence-conference-autumn-2019>. The event was conducted under the RUSI rule; issues discussed off the record during the Q&A sessions are therefore included but not attributed.

Key issues and themes

Despite the apparent divergence of the issues being addressed, several themes were interwoven throughout the conference:

- The continuing need to develop resilience in societies echoed through all the panels. The importance of the link between resilient civilian structures and the ability of the armed forces in conjunction with civil society to deter external actors was repeatedly stressed. So was the need for citizens to understand the threats and risks posed to them and to be clear on what they need to do for themselves, their communities and wider society. Responses are most likely to be effective when prepared and delivered across government, industry, the third sector and the wider population.
- The need for more robust rules and codified behaviour in emerging areas of international and national affairs was the second constant theme. This is based on the fragility of existing international frameworks to govern behaviour in the information domain and
cyberspace. Several speakers highlighted the need for revitalisation of reliable media sources, while others suggested that those sources that do not provide balanced and honest reporting and coverage should be subjected to more robust challenge. Speakers were not unified on whether multinational or national solutions are optimal but several observed that behaviours are not currently supporting the emergence of norms.

- Panels saw a high appetite for increased public attribution of cyber attacks, and several speakers advocated publicly challenging malign and disguised state actors and their proxies. Some of the speakers felt that the current tendency was to act too apologetically when attributing a cyber attack and that an aversion to risk was causing states to inadvertently misrepresent the threat picture to their citizens. A trend for Western news organisations and online media outlets to be increasingly judgemental about their own governments’ motives is also contributing to a reduction in governments’ ability to regulate new means of communication and to deliver fully trusted information when needed as it may lack vehicles to do so.

- The emerging security and quasi-security challenges resulting from climate change caused significant discussion and some uncomfortable thoughts. This is an area which will require further study and development, but the extent of the turmoil climate change will cause, and the opportunities it affords practitioners of blended (hybrid) aggression left participants with a sense of significant unease.

**Keynote: Dan Eliasson**

Dan Eliasson (Director-General, Swedish Civil Contingencies Agency, MSB) began by noting that the West is more prosperous but more vulnerable than ever before. He identified several key trends that affect deterrence, notably:

- The just-in-time model for commodities including food.
- The growing trust gap between citizens and governments.
- The impact of climate change.
- The pressure of modern, increasingly urban lifestyles.

Based on the Swedish experience, he advocated deterrence based on resilience. That, Eliasson stated, includes total defence planning, which he sees as reducing the risk of unwanted escalation, although he also noted that risks to Western societies are exacerbated by offensive behaviours that are not controlled by an agreed set of norms. Furthermore, he emphasised the need for common systems and modus operandi for all types of crises between peace and war. Eliasson further noted that resilience and deterrence are increasingly multilateral concerns that cannot be addressed through unilateral solutions alone. He further stressed that resilience works best when delivered through consensus rather than through top-down approaches.

---

1. Off the record questions to the keynote speaker are not included.
Panel 1: The Role of Defence and Offence in Deterring Greyzone Threats

- **Vice Admiral Keith Blount** (Commander, NATO Maritime Command) emphasised the importance of understanding the nature of the threat and focusing on deterring the right people, a theme developed by Liis Mure (Director-General, Estonian Ministry of Defence, Department of NATO and the European Union), who strongly argued the need for focus of resources. Vice Admiral Blount also praised the NATO military strategy as a key step forward, which must now be given form through adaptation of training and exercises. These in turn must produce a posture that can challenge the very aggressive behaviour shown by Russia.

- **Liis Mure** was clear that the idea of a peace/war divide is no longer relevant and noted that it does not reflect the way the West sees current tensions. She strongly advocated a more robust approach in communicating concrete threats and acts of aggression, both in order to deter and to increase public awareness. At the same time, she stressed that deterrence must remain a nationally focused activity and that hard military power remains highly valuable, especially in removing the temptation for actors to seek short conflicts.

- **Joachim Finkielman** (Deputy Director-General, Danish Emergency Management Agency, DEMA) emphasised the value of civilian leadership in further developing conventional geopolitical thinking, arguing that the resulting changes in the logic of deterrence mean that deterrence by denial may no longer be feasible. He emphasised the increasing challenge in defining normal security situations based on which abnormal security situations can be identified. Finkielman further stressed the need to engage citizens in the planning and execution of deterrence options.

- **Lieutenant Colonel Matt Cavanaugh** (NORAD/USNORTHCOM, but not speaking on behalf of the US Army or any part of the US Government) promoted the idea of fast and slow deterrence as an alternative to offensive and defensive options. Slow deterrence is based on the likelihood of protracted pain for any actor who seeks to dominate another state. Cavanaugh sees this as a step beyond resilience, rather creating a situation where long-term costs outweigh benefits, even if initial gains can be achieved with relatively little early outlay. He linked this to the total defence concept in Norway, as a layered approach which removes adversary options.

A wide range of issues were raised during the Q&A.

- The threat from China is seen as more opaque than the Russian threat and as a step beyond NATO’s current ability and authority. It was remarked that the EU is probably a better forum for addressing China at this stage.

- On recent events in the Persian Gulf, such as the Iranian seizure of the Stena Impero oil tanker and the drone attack on a Saudi Aramco oil refinery, it was felt that it demonstrated the challenge of achieving cross-state consensus. It was also remarked that one potential policy response is increasing national resources to deny the effect of actions such as
attacks on Saudi installations. Such a response could be to stockpile oil to limit the effects of attacks (including drone and cyber attacks) on oil refineries.

- There was recognition that diplomatic measures are the key driver for deterrence but also that other means, especially military ones, must be available. Further discussion included rehabilitating escalation and covert action as means of deterrence and response, with escalation seen as valuable where the consequences can be well understood, and where it is balanced and appropriate tools are available. Covert action, however, was seen as unhelpful because it was ineffective in sending deterrent messages, given that with covert action the sender does not identify themself. Similarly, the challenges of focusing cyber responses were seen as a significant block to their use. The importance of deterrence options being bespoke was stated and restated several times.

Panel 2: Communicating Deterrence Capabilities

- **Per Brekke** (Deputy Director-General, Norwegian Directorate for Civil Protection, DSB) commented on the need for smaller countries to ensure that they can focus resources in support of the armed forces during crises. He emphasised that cognitive resilience within the population is as important as physical and institutional resilience. Brekke also called for increased levels of attribution, stating that silence or non-attribution creates an incentive for malign behaviours.

- **Åsa Sundberg** (CEO, Teracom) described the resilience architecture for assured public communications in Sweden and Denmark and the considerable efforts required to maintain it and address acts of sabotage. Teracom, which owns such infrastructure, is by definition at the forefront of responding to such acts of aggression. Sundberg pointed out that the level of investment required was significantly in excess of that which could be borne by private industry but emphasised the essential nature of such a system for crisis situations and highlighted the mutual benefits which could be achieved by continuing to cooperate across sectors.

- **Mogens Christoffersen** (Deputy Head of Cyber and Security Department, Danish Ministry of Defence) stressed the extent to which states like Denmark are reliant on information systems and cyberspace. He explained the extent to which Denmark was feeling the effects of malign cyber activity which was not directly aimed at it but significantly affected the country, citing the 2017 NotPetya attack on Ukrainian institutions and business, which was subsequently attributed to the Russian government. After having hit Ukraine, NotPetya travelled on, severely harming several multinationals including Maersk, Denmark’s largest company. Christoffersen highlighted the importance of attribution in such cases. He noted that all cases of attribution have a political focus, and that before publicly attributing attacks governments must therefore be clear on the specifics of the public attribution as well as its purpose. In addition, Christoffersen stressed the value of governments of countries targeted by cyber attacks naming and shaming the perpetrators of such activity which sets a baseline for acceptable behaviour and an emergent set of norms.

- **Richard Caseby** (former managing editor, Sunday Times and The Sun; former director of communications for governments including the UK) discussed the decline of traditional
media, and the extent to which journalists’ and the public’s tendency to unfairly judge government action in the intelligence sphere might weaken governments’ capacity to protect the nation from state actors and other aggressors in the information space. This mistrust contributes to an unintended increase in insecurity regarding the validity of information. He argued that there is significant potential for better partnerships between media and technology companies, and that there is considerable potential for the development of better evidence standards using AI. On the latter matter, Caseby pointed to the need for better cooperation in fact-checking and examination of dubious news material between governments, traditional print, radio and television journalists, web-based news outlets, and AI technology platforms though he emphasised that journalists must always operate independently from government when investigating and reporting stories.

Issues in the Q&A centred on attribution and fact-checking.

- The issue of attribution was discussed at length. Speakers felt that responses had to remain linked to a formal attribution process, mostly because of policy concerns about responding without evidence. The media has significantly more freedom in this space than governments. The actual impact of attribution in changing behaviours cannot be demonstrated but is an important element in establishing norms.
- Further discussion suggested that the mainstream media was not living up to some of its responsibilities in establishing facts. However, it was suggested that investigative web-based media outlets such as Bellingcat may have a better impact with citizens, especially younger ones. There is an ongoing challenge in reconciling journalistic freedom and support to state principles and freedoms.

Panel 3: Climate Change as a National Security Threat

- Hélène Galy (Director, Willis Research Network) gave a detailed and compelling review of the breadth and nature of climate impacts based on current trends. She emphasised several geographical regions currently considered stable which are highly unlikely to remain so. The challenges which they are likely to have to address range from the viability of current physical structures to drastically reduced fish stocks. Building on this introduction, Galy outlined a series of potential impacts such as water stress, increased death from heat stress and issues linked to land and food security. Galy suggested that the current depictions of securitisation and sustainability are unlikely to be valid in the medium term and identified emerging issues such as the lack of protection for climate refugees under current UN laws as matters that must be addressed. Finally, she noted the increasing global interest in the Sustainable Development Goals, which present a marked increase on the Millennium Development Goals.
- Howard Jones (CEO, Born Free Foundation) then gave a case study presentation on the effects of climate change on Ethiopia, demonstrating how climate change effects are exacerbating local issues around habitation. He also demonstrated the adverse effects of Chinese construction projects in Ethiopia, which in combination with climate change
severely limit the number and size of inhabitable areas available to Ethiopians. Jones also demonstrated the already high number of internally displaced persons in the country, and then showed the potential for mass refugee migration as habitation areas become non-viable. This has considerable national security implications for Western countries, primarily countries in Europe, as Europe is the likely destination for climate change-linked migration from countries such as Ethiopia.

- **Peter Roberts** (Director, Military Sciences, RUSI) then drew together the issues presented and led a conversation on their impact and whether, and how, these issues should be brought into the deterrence area. It is clear that there are significant consequences for both the security sector and for the way we approach security challenges in the future.

### Closing remarks

Felix Dane (Director UK and Ireland, Konrad Adenauer Foundation) delivered the conference’s closing remarks, thanking the speakers and noting the importance of German–UK collaboration regardless of the eventual outcome of the Brexit negotiations. He went on to highlight the importance of focusing on emerging areas of national security, especially threats and forms of aggression targeting civil society. Dane identified political education as one of the instruments that holds particular potential when it comes to countering threats. This, Dane noted, is precisely the reason that the Konrad Adenauer Foundation and RUSI are ideally suited to cooperate and complement each other on matters of modern deterrence.

*Oliver Major is the Chief of the General Staff’s Visiting Fellow at RUSI.*