Think
new things
Make
new connections

MODERN DETERRENCE: WHAT DOES THE COMBINATOIN OF NUCLEAR, BCW, CYBER AND AI MEAN FOR THE EVOLUTION OF WESTERN DETERRENCE AGAINST STATE AND NON-STATE ACTORS?

8-10 November, 2018

Concern is growing among NATO members that the nuclear postures of the alliance and its three nuclear-armed members may not fit newly emerging threats, both technological and political. This Ditchley conference will bring together an innovative and cross cutting group of high level decision makers, defence leaders, strategy experts and technology leaders to probe the assumptions underlying these concerns; to identify deterrence challenges and opportunities that have not received adequate attention; and to build towards a consensus on strategy on how best to combine a decades old approach to nuclear and other WMD deterrence, with both the new technological possibilities of cyber and AI, and a newly fractured world order.

The United States and its allies arguably face an "unprecedented range and mix of threats, including major conventional, chemical, biological, nuclear, space, and cyber threats, and violent non-state actors." [1] This mix is said to result from proliferation and technological developments, as well as a return to great power competition and aggressive regional competitors. We will ask:

- Is this picture accurate? If not, why not?
- What non-nuclear threats are sufficiently serious that nuclear use could be a credible, effective, and proportionate response?
- How does the effectiveness of nuclear deterrence depend on the size of a state's nuclear force and the diversity of its weapon types?
- For which threats and to what extent can non-nuclear options reduce reliance on nuclear weapons?
- Which threats actually require intervention —rather than deterrence—to address? (For example coercing an adversary to give up capabilities or to change existing behaviour, rather than deterring it from acquiring new capabilities or using them.)
- Are there plausible cooperative approaches to reducing the risk from any of these threats, for example by finding common ground with China and/or Russia?

State threats

China and Russia are modernising their nuclear forces, including by developing new capabilities. Many Western analysts believe that Russia's nuclear doctrine now envisions the use of low-yield nuclear weapons very early in a conflict. There are also concerns about the credibility of China's no-first-use pledge and the possibility of its adopting a launch-under-attack posture. North Korea is determined to use its nuclear power status to negotiate the survival of the regime, or to develop a capability to hit mainland US cities as a powerful deterrent.

[1] 2018 US Nuclear Posture Review

DITCHLEY

- To what extent are Russia's and China's nuclear doctrine really well understood? How do they exacerbate escalation risks?
- Should the United States, France and the United Kingdom respond to changes in Russian and Chinese nuclear capabilities and doctrine, and if so, how (whether in terms of nuclear capabilities, non-nuclear capabilities or doctrine)?
- Are there plausible cooperative approaches to managing potential strategic competition?
- What are the implications for deterrence and proliferation of any deals struck with North Korea?
- What are the implications for deterrence if Iran resumes its weapons programme?

Non-state threats

The current terrorist threat is characterised by a just do it pragmatism that has brought car and knife attacks to the fore. But equally ISIS would certainly seize on any opportunities to deploy weapons of mass destruction of any form if they came their way. Is deterrence relevant at all in this context or is it simply a matter of prevention by intelligence and police action?

New technologies

An array of new non-nuclear technologies might have implications for nuclear deterrence: sophisticated information-gathering technologies; non-nuclear strike systems (including anti-satellite and cyber weapons); strategic defences; drones; autonomy and artificial intelligence; and the increasingly widespread adoption of dual-use weapons and dual-use command-and-control assets. A feature of many of these new technologies is that the bulk of the innovation will take place in the commercial world and is therefore much harder to bring under control by agreements through states.

- Could these technologies make nuclear deterrence more effective and, if so, how could they be incorporated into nuclear forces and command-and-control systems? Could artificial intelligence, for instance, be usefully integrated into nuclear operations? What would be the risks of doing so?
- To what extent might these technologies undermine deterrence or exacerbate escalation risks? Could improved information-gathering make mobile missile hunting more feasible? Might non-nuclear attacks on dual-use command-and-control assets catalyse escalation?
- Are there plausible cooperative approaches to managing the escalation risks of new technologies?

New political and economic challenges

Nuclear deterrence is facing new political challenges in the form of the humanitarian impact movement, and more recently, the UN Treaty on the Prohibition of Nuclear Weapons. The long-term goal is to encourage opposition to nuclear deterrence within civil society in the nuclear-weapon states and their allies. To what extent is this strategy working already? What are the long-term prospects for its success? What is the best strategy for promoting unity within NATO? Is there a constructive way for the United States, France, the United Kingdom, and their allies to engage with the ban movement? Will the UK and France continue to be able to afford viable nuclear deterrents at a spending level of 2 percent of GDP on defence? Are they ready to make the hard choices necessary on defence and what will be the implications?