Hybrid threats and the Asia – Pacific region: Hybrid warfare and cyber-attacks within the Australian – Pacific context

Global peace and security has seen the arrival of new security threats in the form of hybrid threats and cyber-attacks.

Throughout history, conflict has been an ever-present aspect of human activity, but war has of course evolved over the centuries as technology and military strategies changed. The concept of hybrid war has emerged since the end of the Cold War and describes new forms of conflicts and war which are multi-faceted, combining strategies that blend conventional and asymmetric warfare, and utilise a blend of conventional and unconventional means of warfare. Hybrid war has seen the utilisation of additional capabilities such as cyber-warfare, the use mass communication and social media to distribute propaganda and strategic communication, law-fare, the use of criminal and illicit activities to achieve strategic goals and objectives. Hybrid war often involves a fluid, non-state adversary on its own or as proxy of a state actor.

This conference brings together academics and military professionals from the region and beyond to discuss new security challenges from a Asia-Pacific and especially an Australian perspective.

The symposium

This symposium provides a platform for the discussion of a new form of warfare, namely 'hybrid warfare'. Hybrid war is the use of a range of non-conventional methods (e.g. cyber warfare and lawfare) in order to disrupt, discourage and disable an adversary's capabilities without engaging in open hostilities and may use the full range of military and non-military options for achieving its strategic objectives. Such hybrid warfare might include aspects of 'cyber terrorism', 'cyber war' and cyber-based 'information operations', a topic of particular interest given Russia's 'Ukrainian Spring', the continuing threat posed by radical Islamist groups in Africa, the Middle East and the Asia-Pacific region as well geopolitical shifts.

The interdisciplinary symposium will discuss military doctrines, new and traditional approaches to war and peace and its perceptions, the use of cyber warfare, the use of mass media communication to meddle in internal state affairs, including impact on state elections and public sentiment, as well as the use of lawfare (the strategy of using – or misusing – law as a substitute for traditional military means to achieve a war-fighting objective) to achieve military goals in a non-kinetic way and the use of various means to disrupt a nation's economy, public services and national interests.

At the heart of the symposium stand the questions of how to increase resilience and whether responses to such hybrid threats need to change in the future.

We invite papers on the following topics:

I. The role of the military

Examples of topics: Hybrid threats/warfare in a regional context: today and in the future; The European/NATO experiences; Ukraine/Iraq/Syria: lessons learned; the role of intelligence; and civil-military cooperation.

II. Cyber in a hybrid context

Examples of topics: cyber-attacks on the armed forces; the role of cyber within influence operations; cyber and mass media

communications; the role of information operations in current security scenarios; the use of cyber within the context of election meddling and influencing public opinions; the use of cyber to impact upon critical infrastructure.

III. Emerging security threats and responses

Examples of topics: Use of social media to influence opinion; Countering online hate and extremism; Corruption and political influence; Increasing integration of IOT and critical infrastructure; The frailty of financial systems; Digital financing of terrorists; Digital identity: Threats and opportunities. Mass surveillance in the digital era.

IV. Hybrid warfare and hybrid threats: The legal grey area and the role of lawfare

Examples of topics: The legal implications of hybrid war; Lawfare; Information operations and hybrid warfare within its legal context; Legal mandate for countering hybrid threats in Australia; Mandate abroad; Lawfare as hybrid warfare; Lawfare in Info Ops; Lawfare in the Arctic and South China Sea; Legal considerations in election interference.

V. The Asia – Pacific region: Perspectives on threats and opportunities

Example of topics: Lessons learnt from Russia; States and cyber-warfare; Cyber intelligence threats in the region; Political control and cyber infrastructure; Regional collaboration to increase cyber resilience; Foreign direct investment strategies and their implications; Potential for influence in regional politics; Hybrid warfare and territorial disputes in the region (South China Sea; Kashmir, North Korea etc); Rising extremism and cyberspace.

Deadline for submissions: 1 October 2018

Symposium Date: 25 - 26 March 2019

Place: La Trobe University,
Melbourne, Australia

General inquiries and submission of proposals:

Proposals must contain the suggested title, the author's name, affiliation and contact details, an abstract not exceeding 500 words and the symposium topic with which it is linked.

Proposals must be sent by email to the Lead Convenor: Professor Sascha Dov Bachmann (email: sbachmann@bournemouth.ac.uk).

Symposium proceedings:

It is planned to have some of the presentations/papers published after the conference in a peer reviewed journal or as an edited book. We would appreciate if you could indicate in your email re attendance if you were planning to produce a full paper (of around 6000 words) within 3 months after the conference.

Convenors:

- Professor Sascha Dov Bachmann (email: sbachmann@bournemouth.ac.uk (Lead Convenor)
- Professor Pompeu Casanovas (P.CasanovasRomeu@latrobe.edu.au) and Professor Louis de Koker (L.deKoker@latrobe.edu.au).