Christian Kaunert

Kris Stoddart

Hybrid Warfare Security Conference

5th & 6th June 2023

Room 221 Digital Technium, Singleton Campus, Swansea University & Online

Prof Dr Christian Kaunert is Professor of International Security at Dublin City University, Ireland. He is also Professor of Policing and Security, as well as Director of the International Centre for Policing and Security at the University of South Wales. In addition, he is Jean Monnet Chair, Director of the Jean Monnet Centre of Excellence and Director of the Jean Monnet Network on EU Counter-Terrorism (www.eucter.net). Previously, he served as an Academic Director and Professor at the Institute for European Studies, Vrije Universiteit Brussel, a Professor of International Politics, Head of Discipline in Politics, and the Director of the European Institute for Security and Justice, a Jean Monnet Centre for Excellence, at the University of Dundee. Prof Kaunert has researched and taught in many international universities, such as University of Shandong, Jinan, China, IBEI Barcelona, Spain, Diplomatic Academy Yerevan, Armenia – United Nations Development Mission, University of Cairo, Egypt, Collegio Carlo Alberto, Turin, Italy, Ecole nationale d'administration Paris, European Institute of Public Administration Maastricht, Netherlands, European Studies Institute (ESI) at Moscow, University of Porto, Portugal, etc. He was previously Senior Lecturer at the University of Dundee, Marie Curie Senior Research Fellow at the European University Institute Florence, and Senior Lecturer in EU Politics & International Relations, University of Salford.	**Dr Kris Stoddart** is an Associate Professor for Cyber Threats in the School of Social Sciences as well as working with the Hillary Rodham Clinton School of Law. At Swansea he is a member of the Cyber Threats Research Centre (CYTREC). Previously he was a Reader in the Department of International Politics at Aberystwyth University where he was also the Deputy Director of the Centre for Intelligence and International Security Studies. From 2014 to 2017 he was a PI on a £1.2 million project examining Cyber Security Lifecycles funded by Airbus Group and the Welsh Government and was a member of the UK's Independent Digital Ethics in Policing Panel for around four years through to 2018. He is a member of the Project on Nuclear Issues at the Center for Strategic and International Studies in Washington DC, a Fellow of the Higher Education Academy, and a Fellow of the Royal Historical Society. In 2022 he was also made a Fellow of the Royal Society of Arts (FRSA). He has spoken at a wide number of conferences, nationally and internationally, including NATO, GCHQ, and US Strategic Command, and for various forms of media, including the BBC. He is the author or co-author of five books and over 25 articles and book chapters. He has recently completed three further books: Cyberwar: Threats to Critical Infrastructure (Palgrave/Springer, 2022). Two others are in the publication pipeline: Russia's cyber offensive against the West, and China and its embrace of offensive cyber espionage.

Hybrid Warfare/Security Conference Programme Final

Swansea University, Singleton Campus,

Room 221, Digital Technium.

All timings are British Summer Time (BST)

Zoom Link Day 1:
https://swanseauniversity.zoom.us/j/95236484381?pwd=aU56NENrcGpBRkJORGU0TEFoQzdPQT09

Meeting ID: 952 3648 4381
Passcode: 510863

Zoom Link Day 2:
https://swanseauniversity.zoom.us/j/95119920542?pwd=UndYMTlpN05La1dyTDNzTEdBdjUxUT09

Meeting ID: 951 1992 0542
Passcode: 337734

Day 1: Monday 5 June 2023 9am-9:15pm

Conference opening and welcome: Dr Kristan Stoddart

9:15am-10:30am: Panel 1: What is hybrid Warfare?

The Evolution of the Cyber Threat: The Juxtaposition of Cyber Operations and Cyber Warfare

Presenter: John Davies

Abstract

Cyber is not a word in its own right. It is a bound morpheme that has been hijacked and turned into an all-encompassing noun and it's the word it is bound to, which gives it true meaning. Just like the personal computer, the Internet and millennials, the ‘cyber' prefix also emerged in the 1980’s. This paper makes use of a panoply of cyber morphemes to explore the evolution of activity in cyberspace, from the first documented cyber-operation in 1986 to the most recent culmination of cyber-warfare in the Ukraine. Using a timeline analysis, a technique more usually associated with complex life-history research, to visualise data on disparate activities that, at first glance, do not appear to have any discernible pattern, a new perspective on the emergence, evolution and extent of cyberattacks becomes evident. The paper expands on a few of the ideas and hypotheses that have emerged from this research, however, the aim is not to present new findings but to offer insights into some of the possible new lines

of inquiry which, if embraced, may expand current understanding of the single threat which, thanks to the bastardisation of a prefix, so often looks like multiple unconnected threats.

Keywords:

Author: John Davies, Founder Cyber Wales.

In-person or Zoom: In-person

Hybrid War, What Hybrid War?

Presenter: Rizwan Zeb

Hybrid warfare, apparently a new type of warfare or is it? Hybrid warfare is increasingly becoming the part of the military vocabulary the world over. However, unlike the generally held view, military history is rich with examples where a state used multiple means to hurt its enemy: Iberian leader Virathus expedition against Sertorius in 2nd century BC is among the earliest examples of what is today defined as Hybrid Warfare. The proposed paper aims to trace the origin of and critically examine the concept of hybrid war by analyzing different definitions of hybrid warfare and by looking at the Russian offensive into Ukraine and Crimea, Hizbullah's successful campaign against Israeli Defence Force and the rise of ISIS. What is common in all these cases? and what combines them that can be used in favor of their argument by the proponents of hybrid warfare? The paper would argue that the concept has its limitations such as an absence of a universally accepted definition and lack of clarity on how it is different from other similar or identical concepts such as Mary Kaldor's 'new wars,' 4th generation warfare and the Chinese's concept of 'unrestricted warfare'?

Keywords:

Author: Rizwan Zeb, PhD, Professor of International relations & Strategic Studies, PAF Air war College Institute, Karachi, Pakistan.

In-person or Zoom: Zoom

Cultural intelligence in hybrid warfare

Presenter: Professor Kobi Michael

Abstract

This article deals with the increasing importance of human terrain and cultural intelligence in the contemporary urban warfare and elaborates on the interfaces between human terrain and cultural

intelligence. After defining the concepts and explaining their rationales and necessity we describe the modern historical development of both, emphasizing the American experience in Afghanistan, Iraq and Syria, and briefly mentioning on the Israeli experience in Lebanon and the Palestinian territories. Using the theoretical foundations of both concepts enables us to add another analytical and theoretical layer to the existing literature. https://www.inss.org.il/publication/role-human-terrain-cultural-intelligence-contemporary-hybrid-urban-warfare/

Keywords:

Author: Professor Kobi Michael. Institute for National Security Studies (INSS). 40 Haim Levanon St. Tel Aviv, Israel.

In-person or Zoom: Zoom

Coffee break 15 minutes

Panel 2: Hybrid warfare and regionality 10:45am-12midday

Hybrid warfare in Mali

Presenter: Sophie Sikorska-Mazur

Abstract

Contemporary hybrid warfare has become synonymous with the conflict in Ukraine, where *hybrid* is generally understood to mean a mixture of conventional and irregular methods to conduct warfare. Most recently, and in the case of Ukraine, additional element are also included in the mixture, that of cyber, fake news, electoral intervention.

However, neither conventional warfare, irregular warfare or the "modern" concepts of cyber, fake news and intervening in elections are not new. Each of these forms of warfare can be seen as a tool which can be applied to a specific environment to achieve a specific goal, adapted, adjusted and evolved to maintain the upper-hand over an adversary.

Due to its rapidly evolving nature, hybrid warfare presents a fascinating and ever changing threat which presents a wide range of security challenges. This research study will examine the roots of *hybrid warfare* and the threat it presents in Mali which stands out as being at significant risk of the threats which *hybrid warfare* presents, due to a combination of factors: an ongoing problem with non-state armed groups, terrorism, and organised crime; a transitional government; the withdrawal of French troops; and allegations of China and Russia aiming to fill the security vacuum left behind following the French military departure.

Keywords: Russia, state-sponsored assassination, post-Soviet, ACH, process tracing, vengeance logic

Author: Sophie Sikorska-Mazur, University of South Wales.

In-person or Zoom: Zoom

The Role of Lawfare in the Ukraine Conflict: A Legal Analysis of Russia's 'Special Military Operation'

Presenter: Arpan A Chakravarty

In this paper, the author will examine Russia's use of lawfare in conflicts, specifically focusing on the Crimean takeover in 2014 and the ongoing Ukrainian crisis. While Moscow has refused to classify its actions as "*war*" and instead suggests using the term "*Special Military Operation*," this terminology has been used to justify its actions as conforming to *jus ad bellum* norms and invoking Article 51 of the UN Charter on the '*inherent right of individual and collective defence*'.

Nowadays, it is consistently seen that countries are increasingly using legal systems to manipulate means and using law to achieve political goals. This paper aims to discuss the role of lawfare in shaping the narrative of the conflict and influencing public opinion, as well as its impact on the use of force, territorial integrity, and respect for sovereignty.

Therefore, this paper will examine the ways in which Russia and Ukraine, both have used lawfare in the conflict, including its attempts to justify and counter its actions under international law. Finally, this paper will focus on the importance of upholding the rule of law and international law principles to prevent, counter, and possibly resolve conflicts, both in Ukraine and around the world.

Keywords: Lawfare, Russia, Ukraine, International law, rule of law.

Author: Arpan A Chakravarty, BA LLB (Hons.), LLM. (India)

In-person or Zoom: Zoom

Cyber Warfare Amenability and the Pursuit of India's Cyber Offensive Strategy: Tracing the Contours of Sino-Indian Cyber Conundrum

Presenter: Abhigyan Guha

Abstract:

Exemplifying an operational space between the normative binarisation of war and peace, China's amalgamation of myriad instruments of state power while blurring the distinction between military and non-military actions translated into the augmentation of hybrid warfare tactics ranging from Informationisation, 'salami slicing', cognitive warfare to cyber warfare, thereby debilitating India's geo-strategic environment. As cyber technologies buttress military communication, data storage,

surveillance, and weapon systems, an incursion into military cyberspace culminates in the misfiring of military systems, which has been reflected in Chinese cyber espionage campaigns orchestrated by the state-sponsored threat activity group, RedFoxtrot, followed by the 2020 and 2021 Chinese cyber-attacks on Maharashtra's electricity grid and the information technology systems of India's leading vaccine manufacturers while targetting Ladakh's power grid in 2022, endangering India's national security. China's pervasive monitoring, the amassment of intelligence on military technology and defence, systematic weaponising of information while holding the Critical Information Infrastructure hostage, have exposed the power differentials in the skewed trajectory of India-China relations post-Galwan Valley skirmish. The paper highlights the limitations of India's National Cybersecurity Policy while tracing the immediate obstacles vis-à-vis China's cyber hegemony, establishing the efficacy of increasing deterrence to the hybrid realm while advancing a robust cyber offensive capability.

Keywords: Cyber Warfare; Cybersecurity; Hybrid Warfare; India-China Relations; Informationisation.

Author: Abhigyan Guha, Independent Researcher, Working Member of Geopolitics Research Committee at the International Political Science Association (IPSA).

In-person or Zoom: Zoom

Lunch 1-1:45pm

Panel 3: The EU and Europe: Monday afternoon 2pm

The European Union's Response to the Instrumentalisation of Migration Flows as a Hybrid Threat

Presenters: Professor Sarah Léonard (University of South Wales/Dublin City University) and Professor Christian Kaunert (University of South Wales/ Dublin City University)

In 2021, the Belarusian authorities began attracting migrants from various countries including Yemen, Iraq, Syria and Afghanistan, before encouraging them – or even in some cases forcing them – to cross the borders into the European Union (EU). Thus, they attempted to use migration flows for political purposes. There have been other instances of such instrumentalisation of migration flows in relation to the EU, notably by the Turkish and Moroccan authorities. This paper analyses the EU's responses to these attempts in the broader context of the development of its framework on countering hybrid threats. This notably includes a legislative proposal for a 'Regulation addressing situations of instrumentalisation in the field of migration and asylum'. The paper compares the EU's response to the

Belarusian, Turkish and Moroccan cases of instrumentalisation of migration flows and seeks to explain their differences by considering the diplomatic relations between each of these three countries and (a) the EU neighbours concerned by the migration flows, (b) the EU as a whole and (c) the West, more broadly.

Keywords:

Authors: Professor Sarah Léonard (University of South Wales/Dublin City University) and Professor Christian Kaunert (University of South Wales/ Dublin City University).

In-person or Zoom: In-person

EU Hybrid Toolbox

Presenter: Dr Kenneth Lasoen

Abstract

The EU Strategic Compass has emphasized the need to counter hybrid threats and deal with them comprehensively. The EU Hybrid Toolbox (EUHT) gathers all civilian and military instruments that can be employed to counter hybrid campaigns, put at the disposal of member states, should they choose to invoke the assistance of the EU. Intended to be operational at the end of 2022, the implementation of the Toolbox has encountered some bureaucratic difficulties but is mainly impeded by differences in vision between member states. One of the issues is whether the EU's counter hybrid capability should only be reactive or if it can also have proactive, offence-as-defence features. This contribution will outline the current status of the EU Hybrid Toolbox and discuss possible avenues to add proactive possibilities, from the contention that countering hybrid warfare is essentially a counterintelligence/counterdeception issue. So far most research on hybrid warfare describes the problem while lamenting vulnerability, but when it comes to countering it there is very little because this is seen as too complex and difficult to achieve. However, counterintelligence and counterdeception practices could help better understand how hybrid operations are set up, while reversing that planning process might come up with means to detect, counter, and even penetrate hybrid operations to turn them against the aggressor. This paper looks at what CI practices can be applied to understand hybrid operations planning and subsequently counter those operations with age-old counterdeception tradecraft.

Keywords:

Author: Dr Kenneth Lasoen, Assistant Professor Conflict & Security, University of Utrecht.

In-person or Zoom: Zoom

Small Nations Getting Ready for the Future: Adapting Special Operations Forces for the Age of Global Subversive Warfare

Presenters: Dr Cyprian Aleksander Kozera and Branimir Bekavac

The aim of the following paper is to define needs, challenges and prospects that Central European (CE) nations' Special Operations Forces (SOF) face when adapting to the new era of global competition among the great powers. The predominant hypothesis of our reasoning is that the overall environment in which SOF may be used in the future will plausibly significantly differ from that previously experienced by the majority of NATO SOF in the last two decades. Thus, the context will no longer be that of counterinsurgency

(COIN) but rather evolves swiftly towards the one of global competition between near peer adversaries. In such an environment the preciously gained expertise of the last twenty years in the global COIN/CT missions may suddenly lose relevance as primary SOF tasks and necessities significantly change. In a conflict of a great power such as the US with a near-peer adversary (e.g. Russia, China) other NATO member states may get involved and their SOF may be among the first tools used. The SOF missions may no longer be Direct Action (DA) heavy but rather focus more on Special Reconnaissance (SR) and various subversive operations, also with close relation to the cyber domain – presently an inseparable element of the operational environment. The CE SOF capacity for a swift adaptation to new types of missions is, however, far lower than their better funded and more flexible allies. This article aims to define these needs and challenges, as well as describe prospects and provide recommendations for smaller nations' SOF in their quest for relevance and efficiency in the era of great power competition.

Authors: Branimir Bekavac and Dr Cyprian Aleksander Kozera

Key words: Special Operations Forces, Global Competition, Great Powers, Hybrid Warfare, Subversion, Small Nations

Preferred mode of presentation: Hybrid (1 author on-site + 1 author on-line).

The Northern Epirus Struggle 1912-1914: A hybrid warfare study that shaped contemporary Greco-Albanian Relations

Presenter: Manolis Peponas

Abstract

Epirus is a geographical entity beginning from the Amvrakikos Gulf and ending in the Skoubi River. There, Albanian-speaking and Greek-speaking populations lived together for centuries under Ottoman

rule. This area contained Albanian and Greek nationals, causing several problems for the Great Powers that tried in 1912 to determine the borders of newborn Albania. As a consequence, the Florence Protocol (17 December 1913) de facto divided Epirus into two parts; the Albanian North and Greek South.

However, that decision caused frustration in Athens. In February 1914, the "Northern Epirus Struggle" began as hybrid warfare organized secretly by the Greek government, where Cretan guerillas and spies from Athens aimed to provoke greater Greek autonomy in the region. That conflict concluded in October 1914 with the recognition of the Greek national minority in Albania by the Great Powers and the grant of several privileges to Albania nationals.

This presentation aims to illuminate the circumstances under which the Northern Epirus Struggle took place and illuminate the involvement of the Greek government and Prime Minister Eleftherios Venizelos. Also, it will analyze how this case of hybrid warfare has shaped contemporary Greco-Albanian relations.

Keywords:

Author: Manolis Peponas, PhD candidate, National and Kapodistrian University of Athens.

In-person or Zoom: Zoom

Panel 4: From Artificial Intelligence to proxy forces and false flag operations 3:30pm-4:45pm

The AI Arms Race: Using AI to Conduct IO and Wage Hybrid Warfare

Presenter: Yuval Sinay

Influence operations and hybrid warfare are no longer the stuff of spy novels and action movies. With the rise of digital communication and social media, these tactics have become increasingly prevalent and effective. And with the advent of Artificial Intelligence (AI), attackers now have a whole new set of tools at their disposal. One of the most alarming developments in the use of AI for influence operations is the emergence of deepfake and deep news technology. These techniques allow attackers to create highly realistic videos and articles that are designed to deceive individuals and spread false information. By using AI to generate these materials at scale and target them to specific audiences, attackers can manipulate public opinion on a massive scale.

AI is also being used to develop avatars and chatbots that can simulate human interactions and engage with individuals on social media and other online platforms. By analyzing vast amounts of data and identifying patterns and trends, these systems can be used to develop targeted messaging and propaganda that is designed to manipulate perceptions and sow division. Social network algorithms

manipulation is another way in which attackers can use AI to spread their message. By analyzing social media data and identifying vulnerable individuals and groups, attackers can create targeted campaigns that are designed to manipulate these algorithms and spread their message to a wider audience.

Overall, the use of AI in influence operations and hybrid warfare represents a major threat to global stability and security. It is critical that policymakers, researchers, and civil society work together to develop effective strategies for detecting and countering the use of AI in these operations. By doing so, we can help ensure that these technologies are used in ways that promote transparency, accountability, and respect for human rights.

Keywords- Influence Operations, Cyber Influence Operations (CIO), Hybrid Warfare, Whole-of-society Approach (WoSA), False Flag Operations, AI Resilience, Cyber Operations, Cyber Espionage

Author: Yuval Sinay

In-person or Zoom: Zoom

Proxy forces and Israeli security

Presenter: Dr Ori Wertman

Abstract:

Using Hezbollah, Hamas and Palestinian Islamic Jihad (PIJ) as its proxies, Iran has been waging a hybrid war against Israel since the Islamic revolution of 1979. Consequently, Hezbollah, Hamas and PIJ are integral to the Iranian strategy of indirect war through its proxies against Israel, the West, and other regimes in the Middle East. In an era when conventional wars have given way to a different method, hybrid warfare, the main challenge facing states is how to deal with this new type of security threat. Thus, while states have previously faced security threats from regular enemy states' armies, nowadays hybrid warfare in which non-state actors play a key role has become a widespread security threat that requires democratic states to use very different strategies and tactics to overcome it. Using securitisation theory, which explores how normal issues transform into security threats, this article analyses how the State of Israel has securitised Iranian hybrid warfare. It does so by applying a revised version of the Copenhagen School's securitisation framework, which focuses on security practices and is underpinned by an understanding of security as belonging to a continuum. The proxy terror organisations have moved towards the end point of the continuum, which is characterised by survival, existential threats, and militarisation, albeit without completely reaching the end point.

Keywords:

Author: Dr Ori Wertman, Research Fellow, University of South Wales.

In-person or Zoom: Zoom

Unleashing the Power of Generative Artificial Intelligence in Cyberterrorism: Reducing Transaction Costs for Critical Infrastructure Attacks

Presenter: Dr Ethem Ilbiz

Abstract:

This article explores the potential transformative impact of generative artificial intelligence (AI) in the field of cyberterrorism. It specifically focusses on its ability to reduce the transaction costs associated with targeting critical infrastructure in target countries. This conceptual analysis challenges the prevailing assumption that terrorist organizations, acting as proxies, lack the necessary human and technical capabilities for large-scale cyberterrorism attacks. Contrary to these assumptions, the article argues that the low barrier accessibility of generative AI, enabled by prompt engineering techniques and the ability to impersonate critical personnel, may potentially equip terrorist groups with new strategies and tools for writing malicious code and gaining unauthorized access to crucial data. By examining existing literature, this paper sheds light on the underlying theories, risks, and implications of generative AI in the context of cyberterrorism. Additionally, it discusses the broader implications for national security and underscores the importance of proactive measures to mitigate potential threats. Through this analysis, the article aims to inspire further research and provide policymakers with valuable insights into the evolving landscape of cyberterrorism, ultimately facilitating the development of effective countermeasures to safeguard critical infrastructure.

Keywords:

Author: Dr Ethem Ilbiz, Senior Research Fellow, University of South Wales.

In-person or Zoom: In-person

False Flag Operations in the Middle East After the Arab Spring

Presenter: Arushi Singh

Early in 2023, Major General Oleg Yegorov, deputy chief of the Russian Center for Reconciliation of the Opposing Parties in Syria stated that Syrian militants were planning a false-flag operation in the Idlib de-escalation zone. The militants belonged to the terrorist group Hay'at Tahrir al-Sham, which is banned in Russia. The plan was to provoke Syrian government forces by opening fire near Al-Atarib

and Kafr-Jum, to provoke retaliation on the Kafr-Dian refugee camp. The militants aimed to create videos showing civilian casualties and blame the Russian and Syrian armed forces for the alleged use of excessive force.

In a similar vein, the instability in Libya has attracted the attention of several regional powers, including Turkey, which have reportedly engaged in clandestine activities in the country. Regional powers along with covert operatives in Libya, may have been involved in a false flag coup attempt in July 2016 as illustrated by recent reports. This research will endeavour to explore the historical and geopolitical context of the contemporary dimensions of false flag operations in conflicts in the region; to analyse the current nuances of false flag operations in the Middle East after the Arab Spring; and to examine the future implications of false flag operations in the Middle East after the Arab Spring including the emergence of "digital false flag" attacks.

Keywords- False Flag Operations, Middle East, Arab Spring, Syria, Civil War

Author: Arushi Singh, Geopolitics Risk Analyst (MENA).

In-person or Zoom: Zoom

Conference dinner for in-person attendees – details to follow

Day 2: Tuesday 6 June 2023

9:30am-10:45am Panel 5: Global to regional power competition

Surrogate Warfare in Great Power Competition

Presenter: Leontine von Felbert

In today's multipolar and interconnected world, where the US is no longer the undisputed hegemon and Russia has returned to the world stage, conventional state-on-state war has become increasingly rare and conflicts are often fought through other means. In an effort to stay underneath the threshold of direct conventional war with a great power competitor, while still being engaged in conflicts abroad, states often use surrogates in order to pursue their interests and expand their influence. This paper proposes a conceptualization of surrogates that includes all human actors that patrons, who can be both state or non-state actors, delegate some or all of the burden of warfare to. Surrogates could thus be other states, non-state actors, or private military companies.

The paper will then explore how surrogates can be used for strategic advantage in a military intervention in the context of great power competition. The idea of victory in great power competition, and what strategies may lead to success will be analysed, as well as different strategies and approaches great powers use to compete with one another, such as gray zone warfare or hybrid warfare. The concept will be applied to the case of the great power competition between the US and Russia.

Author: Leontine von Felbert, PhD candidate, Kings College London.

Keywords:

In-person or Zoom: In-person

Hybrid Warfare and Influence Operations: Exploring Manipulation of Perceived Reality and the Potential for Radicalisation

Presenter: Mike Edwards

Abstract:

Hybrid warfare, a combination of conventional and unconventional tactics, has become a significant challenge in the global security landscape. This presentation aims to explore the relationship between hybrid warfare, influence operations, and the potential for strategic radicalisation. By examining several case studies, this research seeks to understand the complexities of this evolving phenomenon.

The presentation uses reflexive control theory and social constructivism as theoretical frameworks to analyse how hybrid warfare strategies exploit the manipulation of perceived reality to achieve set objectives. Reflexive control theory explores how adversaries shape decision-making processes by subtly influencing the information environment, while social constructivism examines how shared meanings and beliefs can be weaponised to sway public opinion and fuel radicalisation.

The research highlights the tactics employed in hybrid warfare, such as information manipulation, psychological operations, and targeted disinformation campaigns. It delves into the impact of these strategies on social, political, and economic systems, exploring their potential to undermine democratic processes, disrupt societal cohesion, and fuel radicalisation.

The presentation also emphasizes the role of technology in hybrid warfare, particularly cyber espionage and cyber warfare using social media. It elucidates the interconnectedness between the digital realm and influence operations, exploring the potential for cyber capabilities to amplify the effects of social polarisation and contribute to wider hybrid warfare strategies.

Overall, this research seeks to contribute to the body of knowledge on this complex and rapidly evolving field, offering insights into the nature of contemporary security challenges while informing UK national security policy for countering hybrid threats in the future.

Keywords:

Author: Mike Edwards, Senior Lecturer, University of South Wales.

In-person or Zoom: Zoom

China's Belt and Road Initiative (BRI): Debt-entrapment and development as a form of hybrid warfare

Presenter: Lewis Jones

Abstract:

My thesis investigates the relationship between the Belt and Road Initiative (BRI) and Hybrid Warfare through the act of debt-entrapment. Debt-entrapment refers to a strategy that extends loans to weaker and developing countries for projects involving infrastructure. The long-term goal of this is to gain strategic advantages, economic influence and resource access, all at the expense of the debtor country. There are indications that China uses debt-trapping while conducting BRI business with other countries as Chellaney, B (2017) reveals China saddles poorer countries with vast amounts of debt which in turn leads them to being under Chinese influence, geo-politically speaking. The concept was recently covered by MI6 Chief Richard Moore, as Bowden, G (2021) tells us debt-trapping is China's way of getting people on a financial hook in order to exert leverage. Regardless, there is no clear-cut evidence that China is guilty of. Herein lies the purpose of this research, to investigate the relationship between Hybrid Warfare and the BRI using debt-trapping and to benefit the Chinese military and to ascertain why some countries resist while others succumb to this Chinese influence. To answer this question, I will conduct case studies on countries that have both fallen to and resisted Chinese influence. With supporting frameworks, indicators, and variables specific to each country will be shown that gives insight as to why this is.

Presenter: Lewis Jones (USW PhD candidate)

Keywords:

Author: Lewis Jones, PhD candidate, University of South Wales.

In-person or Zoom: In-person

Coffee break 11am-11:15am

Panel 6: Plausible deniability and hard power contestation 11:15am-12:45pm

Giving up on Plausible Deniability -- the case of Israeli Assassinations

Presenter: Or Arthur Honig

Abstract:

This article seeks to explain the process whereby since the mid to late 1990s the Israeli government has de-facto been slowly giving up on its policy of maintaining plausible deniability with regards to its assassinations of its enemies. This de-facto reduction of ambiguity is manifested in: a growing willingness of former officials to brag about taking part in these assassinations or of politicians about ordering them, a greater willingness to employ military units in an overt way, a growing willingness to undertake operations abroad that risk exposing the identity of the Mossad operatives. This is a problematic phenomenon since it provides ammunition to attack Israel demanding that it be treated as a pariah in the international arena given its willingness to ignore the international law. I argue that there are five major causes for this growing trend. Some reasons have to do with factors or processes which are unique to Israel, like for instance the entry into politics of multiple former intelligence top officials, the desire of top officials to tell their stories before they die, or the desire of Israeli policymakers to deter or provoke their enemies by making assassinations more public. Other factors have to do with processes which are less unique to Israel and which make governments and agencies around the world forgo secrecy. These include: the growing difficulty to keep operations entirely secret with all the CCTV cameras recording everything, the importance of publicizing some things in order to recruit the best minds to intelligence agencies (especially given the growing competition from the hi-tech industry).

Keywords:

Author: Or Arthur Honig, Associate Professor, TIU

In-person or Zoom: Zoom

Why the proliferation of Short Range Air Defence (SHORAD) and Counter Unmanned Aerial Systems (C-UAS) systems could help normalise and spread Unmanned Combat Aerial Vehicles (UCAVs): An isomorphic analysis

Presenter: Dr Scott N. Romaniuk others TBC

Abstract:

The prevailing body of scholarship on the proliferation of armed drones has primarily centred on the role of states in their production and dissemination as the principal driver of the norm proscribing their use. However, little consideration has been paid to the significance of counter-drone systems in the mutual relationship promoting the spread of these systems. This research analyses the rapid development of SHORADs—anti-drone weapon systems—and the apparent shifts in state attitudes and behaviours towards them. Our study is embedded in the wider body of work on international norms and research on the spread of armed drones. Our theoretical framework for explaining how the proliferation of SHORADs, including C-UAS systems, may contribute to the normalisation and proliferation of UCAVs is anchored in the literature on isomorphism in the evolution of militaries. Our case studies are based on the SHORAD military systems developed and produced in the People's Republic of China (PRC), Russia, and the United States (US). We examine three different counter-drone weaponry systems in these nations and how they influence states' acceptance of armed drones through their counter-drone adversaries. We assess their contribution to the spread of weapons in general and the continued acceptance of the practise of using armed drones. Our research adds to the body of knowledge on norms and the deployment of armed drones while also outlining potential future research directions.

Keywords: armed drones, China, military modernisation, norms, Russo-Ukraine war, SHORAD systems

Authors: Dr. Scott N. Romaniuk, University of South Wales, United Kingdom; Dr. Péter Marton, Corvinus University of Budapest, Hungary; and Dr. Tobias Burgers, Fulbright University Vietnam, Vietnam.

In-person or Zoom: TBC

Transnational criminality after cessation of hostilities in Ukraine – challenges and opportunities for tackling new kevels of criminality

Presenter: Euan Grant

Abstract:

The purpose of this briefing would be to inform a current or future roundtable discussion on the strengths and weaknesses of international governmental and law enforcement efforts to prevent, prosecute or disrupt strategic criminality from ex Soviet States. Particular emphasis is on Russia and Ukraine, because of impacts from the current war, and on plausible developments following cessation of hostilities.

Strategic criminality means state protected or facilitated criminality and is intended to have implications for future studies of the Chinese equivalents, where information is rapidly emerging, from a low base. Such criminality requires different approaches, given the operations of current or future criminal organisations are typically in hostile or non- cooperative strategic jurisdictions such as Dubai, Latin America and Sub Saharan Africa, where the foundations of what became the components of the Wagner Group were laid decades ago, in plain sight of international organisation such as the UN.

A basic thesis is that cessation of hostilities would release significant numbers of well organised young and middle-aged men, with access to sophisticated logistics capabilities, and connections with existing supply chains for cocaine, synthetic drugs, and to illegal forestry and mining products, particularly diamonds, gold and strategic minerals. Ukrainian state agencies, especially the armed forces and the State Security Service, can provide invaluable information on both Russian and Ukrainian intercontinental criminality. Such data would assist in enhancing Western public support for Ukraine. This material would be likely to generate a Russian response, including disinformation, cyber-attacks and the taking of hostages.

Keywords:

Author: Euan Grant, Contributing Writer, United Kingdom Defence Forum

In-person or Zoom: In-person

Lunch break 1pm-1:45pm

Panel 7: Contemporary hybrid warfare 1:45pm-3pm

Cyber Rollback: Popular Resistance in the Cyber Age

Presenter: Professor Matthew J. Flynn

Abstract:

In the Red Zone of conflict and war, and when assessing hybrid warfare/security, the edge more open societies once enjoyed in this arena is still vibrant, as my submission makes clear: “Cyber Rollback: Popular Resistance in the Cyber Age.” Striving for an asymmetrical advantage remains a crucial option for states opposed to draconian oversight of cyberspace. A lead article in the *Washington Post* just a few days ago (May 7, 2023) points to the inclination of democracies to greet online realities with a

pronounced fear and trepidation: "How the Democratic Hopes of the Sudan Spring Went so Horribly Wrong." Concerns abound in cyberspace, as does the opportunity to continue to extol the virtues of an open society. That norm of empowering people to set their own standards of governance remains intact and as always, a threat to authoritarian regimes, and as always, roils a state and threatens violence—even states valuing political plurality. In the continued civilian push-back in the face of state oppression, setting cyber events alongside the Cold War parallel of rollback tests the permanence of war as a measure of violence and the ability of cyberspace to create a new space subsuming the Red Zone.

Keywords:

Author: Matthew J. Flynn, Ph.D., Professor of War Studies, Marine Corps University, Quantico, VA

In-person or Zoom: Zoom

On their effects should they be judged': A new framework for understanding attacks in contemporary hybrid war

Presenter: Dr Christopher Ankersen, NYU Center for Global Affairs

Abstract:

Up until now, the body of international law that concerns itself with armed conflict has tended to focus on matters related to the journey to war (jus ad bellum) and the conduct of warfare (jus in bello). Both of these approaches tend to follow a material train of thought: what harm was done? Was a threshold crossed? Was some particular conduct unbecoming? This material bias, though, may blind us to the fact that much of what is now considered 'hybrid war' or 'grey zone war' actually operates below the threshold of armed conflict or outside the regular military domain. If these 'irregular' aspects, such as propaganda or offensive cyber activities, are integral to a 'new way of war' being fought, then can we afford to dismiss them as something 'other than war' (e.g. crime, espionage, disinformation)? Just because an attack does not fit into an existing material understanding of harm, is it justifiable to discount it as relating to war? What this paper proposes is a framework that treats a variety of different attacks on the basis of their effect (rather than any pre-existing category of the nature of the activity itself). This framework can then allow for some form of 'valuation' to be carried out that could lead to the application or development of legal measures to manage these effects. In short, this paper suggests an expansion of our understanding of the 'the law of armed conflict' and provides a framework for appreciating the elements of contemporary war so that this might be carried out.

Keywords:

Author: Dr. Christopher Ankersen, NYU Center for Global Affairs.

In-person or Zoom: Zoom

Catastrophic Cyber Risks: Insights and Challenges from a Multi-Disciplinary Expert Panel Study

Presenter: Elisabeth Dubois and/or Omer Keskin

Abstract:

This presentation delves into the topic of catastrophic cyber risk and its implications for insurance companies, reinsurers, regulators, and society. By conducting a multi-disciplinary expert panel study using the red teaming methodology, valuable insights were elicited and synthesized regarding the framing of catastrophic cyber risks, available tools and methods for addressing these risks, and the associated challenges. The panel discussions covered diverse aspects, including the definition of catastrophic cyber risk, response strategies, and scenario analysis. The findings contribute to a comprehensive understanding of this critical subject, facilitating the development of effective strategies and policies to address the growing threat and enhance cyber resilience.

Keywords:

Author: Dr Unal Tatar, Assistant Professor, Dr Omer Keskin, Assistant Professor, Elisabeth Dubois, PhD candidate. All Albany University, New York.

In-person or Zoom: Zoom

Coffee break 3pm-3:15pm

Panel 8: Disruption and decoding 3:15pm-4:30pm

Decoding Disinformation

Presenter: Javier Luque Martinez (IPI)

Abstract: https://ipi.media/harassed-threatened-and-sued-the-state-of-fact-checking-in-europe/

In-person or Zoom: Zoom

Hybrid Warfare, Iranian Regime Proxies, the PLO and Israel:

Presenter: Dan Diker

Hybrid warfare as a term of art has played a key role in Israel's ongoing wars with a wide variety of adversaries across the Middle East. First, Hizbullah' s use of Hybrid warfare must be considered in its classic Western military context of regular and irregular warfare within the traditional battlefield space, as Frank Hoffman has explained. Second, Hybrid Warfare in the Palestinian case must be considered in its Soviet-Russian context as rooted in active measures that evolved in the post-2014 notion of "unrestricted" and "omni-directional" warfare as military scholar Offer Fridman has outlined.

I suggest here that the Israeli case constitutes a unique paradigm within war studies as the only democracy in the UN system that continues to face both forms of hybrid warfare; Hezbollah as a hybrid warrior has operated as both a regular and irregular force, with operational integration, advanced weaponry and sophisticated information warfare. Simultaneously, the PLO and its PA subsidiary have pursued the Soviet and Russian hybrid warfare concept that is rooted in Soviet Cold War active measures- - and modern-day Russian *gibridnaya voyna*. This is where the weaponization of politics, diplomacy, international law, human rights, media and social networks can match the power, influence, and damage of a massive conventional land, sea, and air assault. How can scholars assess the success of these forms of Hybrid Warfare and how effectively has Israel confronted these discrete hybrid warfare challenges?

Keywords:

Author: Dan Diker, PhD candidate at the University of South Wales. Dan is President and a Senior Fellow of the Jerusalem Center for Public Affairs.

In-person or Zoom: Zoom

Misinformation as a Disruptive Force in Alliances

Presenter: Dr. Saltuk Karahan, Old Dominion University

Abstract:

This paper will explore the effects of misinformation campaigns in U.S. allies and analyze the reflection of such campaigns in social media. The paper will first provide a general overview of anti-Americanism in Europe and look into factors exacerbating the sentiments against transatlantic alliances. The paper will analyze anti-American sentiment in Turkey as a case study and look deeper into this case to understand sources of anti-Americanism. While the research will initially be based on Machine Learning supported sentiment and emotion analyses, manual investigation of the activities of users in social media and the timeline of events will also be taken into consideration. Finally, the paper will

assess the broader, long-term ramifications of such campaigns from an international studies perspective and suggest policy recommendations.

Keywords:

Author: Dr. Saltuk Karahan, Old Dominion University.

In-person or Zoom: Zoom

Cyber activism from the front line

Presenter: A former network and server security professional with 24 years experience at a high level

Abstract:

Working to counter Russian disinformation related to the Russo-Ukraine war, as well as crowdfund Ukrainian units. A member of the North Atlantic Fellas Organization (NAFO).

Panel 9: 4:45pm-6pm The Russo-Ukraine War, Presentations followed by a Round Table with the presenters joined by Kristan Stoddart and Euan Grant

Reinventing the Mercenary: Russian Hybrid Warfare

Presenter: Dr Emmet Foley

Abstract:

Russian private military companies (PMCs), such as RUSCORP, Slavonic Corps, Moran Group and the Wagner group, have signaled a resurgence of Russian machinations on the world stage. Aside from supporting large scale military operations in Ukraine they have also been involved in activities in Africa and Latin America involving the exploitation of extractive industries as well as Outside of that so called Russian Private military companies have become an integral part of Russian Foreign policy and signal not just a resurgence of mercenary activity but significantly a reinterpretation in the Russian image. Russian soldiers for hire differ from the traditional mercenary and if examined closely they can be viewed as a military microcosm of the Russian State. The first section of this paper will highlight how the Russian state has allowed the development of mercenary companies over the last 20 years. Secondly how the Russian Mercenary fits in the broader picture of Russian Foreign Policy and how the Russian state has utilized mercenaries to further its agenda. Lastly what this utilization of military companies means in terms of international security and terrorism.

Keywords:

Author: Dr Emmet Foley, Dublin City University

In-person or Zoom: Zoom

The Logic of Vengeance: Patterns of Escalation of the Post-Soviet Targeted Killings

Presenters: Kiril Avramov; Adam Hanzel; Mykhaylo Simanovskyy, Department of Slavic and Eurasian Studies (DSES). All LBJ School of Public Affairs, Global (Dis)Information Lab. The University of Texas at Austin.

Abstract:

The Russian government's post-Soviet program of targeted assassinations has gained increased attention from scholars and policymakers due to recent cases of state-affiliated killings used as retaliation, especially the ones that include the deployment of CBWs as a method of elimination. Our findings indicate that Russian state-sponsored assassinations are primarily retaliatory and aim at the targets' terminal elimination. Our analysis of over 100 post-Soviet assassinations shows that these attacks have unique characteristics attributed to the operational practices of intelligence services and their proxies. The typologies and distinctions of these killings are determined by the attacker's approach, influenced by the target's affiliations and location. We support our argument with our database, codebook, and analysis of competing hypotheses (ACH). Through process tracing methodology, we have analyzed prominent illustrative cases of the Russian government's targeting of groups. Our findings demonstrate a distinctive "vengeance logic" pattern at play. We have examined these illustrative cases to identify unique characteristics and practices specific to each target's affiliations, public and organizational prominence, and location. As a result, our research provides further evidence of the retaliatory nature of the assassinations carried out by the Kremlin.

Keywords: Russia, state-sponsored assassination, post-Soviet, ACH, process tracing, vengeance logic

Author: Dr Kiril Avramov, Assistant Professor and Co-Director of the Global (Dis)Information Lab, Adam Hanzel; Mykhaylo Simanovskyy.

In-person or Zoom: Zoom

Conference close 6pm