ZHSS 8456: AUSTRALIA AND CYBER WAR: TEN QUESTIONS

For three years, UNSW Canberra has been running its unique Master's degree in cyber war and peace (formally known as Master of Cyber Security, Strategy and Diplomacy). Over 100 students have enrolled in the degree or related courses. "Australia and Cyber War" is the name of one of the courses. It was renamed for 2019 from "Australia's Cyber Forces". Here are ten questions the students had to address s part of their assessment for the course. We would welcome you feedback: G.Austin@unsw.edu.au. We have a Research Group on Cyber War and Peace that includes university staff and a very small number of serving members of the ADF. We would like to expand its membership. In the meantime, feel free to look over the questions, and reflect on them. If you want to send in substantive comments, we will consider them for posting to our website.

Greg Austin
Professor of Cyber Security, Strategy and Diplomacy
UNSW Canberra

Week1: The Cyberspace Revolution in Military Affairs

Most world leaders accept that in social and economic affairs the information age represents a political revolution every bit as transformational as the industrial revolution centuries ago. In around 400 words, please describe your view of whether the advent of cyber-enabled warfare constitutes a revolution in military affairs that demands radical changes in war-fighting and force structure. This is not about Australia. This week we need look only at the question in a global sense. You could ask whether Chinese and American leaders believe there has been a revolution in military affairs because of the advent of cyber weapons and cyber military vulnerabilities.

Week 2: Middle Powers and Cyber Military Strategy

Pick a middle power not including Australia which has a global reputation for rapid development of cyber military forces. Explain the main influences (military environment, political, economic) on that country on how it has shaped its cyber forces (400 words).

Week 3: Australia's Strategic Environment in Cyberspace Evaluate the following statement and say why you agree or disagree with it. In the 2030s, as far as we can judge today, cyber-enabled warfare capabilities and information dominance concepts will be seen by China, Indonesia and terrorist groups alike as the primary determinants of political success in combat. This will mean that these actors, if engaged in a war with Australia, or preparing for an imminent war, would want to be able to undertake as many wide-ranging cyber attacks against its critical infrastructure, its population and its military forces as they could with a view to crippling the country's forward deployment of forces or its successful use in combat of key weapons systems.

Week 4: Australia's Military Cyberspace Ambitions

Australia has decided what type and how many submarines it needs and can afford to build for the 2030s. How should it decide what type and how many cyber forces it needs for the 2030s? What are the considerations shaping the politically acceptable and economically viable force structure for Australian cyber forces in the 2030?

Week 5: Politics of Transformational Change in the ADF Does the ADF need cyber champions at the Chief of Service level to make a breakthrough in commitment to building cyber war capability or is it sufficient that government has flagged the need for some sort of transition, fairly vaguely, in the 2016 Defence White Paper? How important will a new operational concept paper for cyber warfare doctrine be in building constituencies in the ADF for a more rapid transition to cyber warfare capabilities?

Week 6: Australia's Force Structure Choices for Cyber Warfighting

Australia has several strategic choices to make about force structure for cyber-enabled warfighting. They all involve dilemmas and trade-offs: how much to centralise in the Joint Cyber Unit or ASD; or how much cyber capability to put in the Navy versus the RAAF. Less obvious choices include whether to assign a key role to the Australian Secret Intelligence Service, the government's primary vehicle for covert sabotage operations. Choices need to be made about the balance between offensive cyber capabilities and defensive ones. Doctrinal and policy choices also need to be made about the primacy to be given cyber-enabled capabilities over more classic kinetic forms: e.g. cyber fires versus artillery fires.

Your task this week: in 400 words, make a case for up to three features of a design for a standing, forward-deployed joint cyber unit that the ADF would need to create on short notice for the following scenario.

Australia agrees on one day's notice in September 2018 to send a joint task force of naval, air and ground forces to the Middle East in response to imminent combat hostilities between the United States and an enemy alliance with advanced cyber offensive capabilities. The Australian task force will represent 25 per cent of the available operational combat capability of the Australian Defence Force, with a heavy preponderance of navy and air assets.

The Australian Task Force, at the invitation of the host government, will need to take primary responsibility for an area of operations (AO) on the coast of the Arabian Peninsula, including the physical security of a small harbour and its port operations against possible attack by sea, from the air, or on land. The port city is home to a major civil airport normally servicing international routes to all Middle Eastern countries. There is a major road and rail link heading north along the coast from the port beyond the AO. There is no other inter-city or regional road or rail infrastructure from the city. The port city is surrounded by desert for at least 300 km in all landward directions.

Within minutes of the Australian commitment to send its task force to imminent war, you have been tasked as part of a team of ten military and civilian officers to provide important design principles to assist VCDF and the Commander Joint Capabilities Group to shape the ad hoc joint cyber unit that will be deployed. Your team has two hours to compile a list from its members. VCDF has asked for force design principles 3 only, not detailed unit composition. He has stipulated that cost should not be a constraint. What would you put on the list and why?

Week 7: Information Operations Doctrine

Identify a coherent set of 4-5 force structure changes that one of Australia's singe services (Army, Navy or Air Force) should have made by 2020 if we are to maintain appropriate readiness in the cyber domain for combat operations involving a major power adversary with

high capability to degrade, through opportunistic cyber attacks, almost any of Australia's combat systems, its ISR or C2 capabilities? Your proposed force structure changes must relate to specific combat missions for Australian forces (such as "defeat small scale enemy ground force emplacements on the territory of a friendly Southeast Asian state" OR "interdict or disrupt an adversary's naval task force intent on exercising sea denial or sea control in the strategic straits of the Indonesian and/or Philippines archipelagos".

Week 8: National Security Innovation Priorities

In 2016, the Australian government set up a Cyber Security Growth Network, now called Austcyber, to promote development of the industry. Please offer your view of how effective this policy measure has been and what its potential might be with reference to Austcyber's 2017 publication, Cyber Security Sector Competitiveness Plan. What does your assessment mean for Australian military planning for cyber space operations?

Week 9: ADF Training and Education for Cyber-Enabled Warfare

In 2010, an officer of the United States Marine Corps made the following assessment: " The Department of Defense will need change how the military services organize, train and equip to support a theater campaign by providing a Joint Task Force Commander the tools he needs to prevent the cyber domain from becoming a critical vulnerability." In 2015, a U.S. Army officer recommended wide-ranging innovations in the same vein: "1) to empower the Geographic Combatant Commands with control authorities over cyberspace capabilities; 2) to communicate to national policy makers the strategic utility of future military cyberspace requirements; 3) to develop technical cyberspace situational awareness capabilities at all echelons; and 4) to task organize, versus assign, cyber forces to the tactical level units." For this Forum, please discuss the implications of these recommendations for Australian cyber force structure, planning and training.

Week 10: An Australian Cyber Militia?

Please provide your critique, for and against, of the ideas in the short paper proposing the establishment of an Australian Cyber Civil Corps.