Executive Cybersecurity Workshop (Virtual)

"Cybersecurity Interconnectivity and Interdependencies"
19-23 April 2021 (in-region)
Honolulu, Hawaii

Execution times:

Date	Time	Country	GMT
16 &18-22 April 2021	19:00-22:00	Honolulu	GMT-10
16 & 19-23 April 2021	07:00-10:00	Germany	GMT+2
16 & 19-23 April 2021	10:00-13:00	Maldives	GMT+5
16 & 19-23 April 2021	10:00-13:00	Pakistan	GMT+5
16 & 19-23 April 2021	10:30-13:30	Sri Lanka	GMT+5:30
16 & 19-23 April 2021	10:30-13:30	India	GMT+5:30
16 & 19-23 April 2021	10:45-13:45	Nepal	GMT+5:45
16 & 19-23 April 2021	11:00-1400	Bangladesh	GMT+6
16 & 19-23 April 2021	11:00-1400	Bhutan	GMT+6
16 & 19-23 April 2021	12:00-15:00	Cambodia	GMT+7
16 & 19-23 April 2021	12:00-15:00	Indonesia	GMT+7
16 & 19-23 April 2021	12:00-15:00	Laos	GMT+7
16 & 19-23 April 2021	12:00-15:00	Thailand	GMT+7
16 & 19-23 April 2021	12:00-15:00	Vietnam	GMT+7
16 & 19-23 April 2021	13:00-16:00	Malaysia	GMT+8
16 & 19-23 April 2021	13:00-16:00	Mongolia	GMT+8
16 & 19-23 April 2021	13:00-16:00	Philippines	GMT+8
16 & 19-23 April 2021	14:00-17:00	Palau	GMT+9
16 & 19-23 April 2021	14:00-17:00	Timor-Leste	GMT+9
16 & 19-23 April 2021	15:00-18:00	Papua New Guinea	GMT+10
16 & 19-23 April 2021	16:00-19:00	FSM	GMT+11
16 & 19-23 April 2021	16:00-19:00	Solomon Islands	GMT+11
16 & 19-23 April 2021	16:00-19:00	Vanuatu	GMT+11
16 & 19-23 April 2021	17:00-20:00	Marshall Islands	GMT+12

Workshop Expectations:

The five-day workshop will be hosted for three hours each day. Each day attendees will be required to:

- Attend daily plenary sessions;
- Actively participate in breakout discussions by providing their insights from the assignments;
- Review self-study materials (readings and videos); and
- Complete three (3) writing assignments (answer questions on daily presentation slides).

At the completion of the workshop, the attendees will be awarded with a certificate of completion.

Agenda:

Day 0: Friday, 16 April 2021	
Time: GMT+2	**Session:**
0700-0800	Workshop login, overview and connectivity test
	Self-Study: Preparation for Day #1 1. **Reading**: New Zealand Ministry of Foreign Affairs and Trade, "Christchurch Call: To Eliminate Terrorist & Violent Extremist Content Online," accessed March 30, 2021, https://www.christchurchcall.com/call.html 2. **Reading**: David Koh, "The Geopolitics of Cybersecurity," *The Diplomat*, December 9, 2020, https://thediplomat.com/2020/12/the-geopolitics-of-cybersecurity/ 3. **Reading**: Jacinda Ardern, "Significant Progress Made on Eliminating Terrorist Content Online," September 24, 2019, https://www.beehive.govt.nz/release/significant-progress-made-eliminating-terrorist-content-online
Day 1: Monday, 19 April 2021	
Time: GMT+2	**Session:**
0630-0700	**Login / Setup / Connectivity Test**
0700-0705	**Workshop Opening** (Introduction and welcome) **Speakers**: Dr. Inez MIYAMOTO (DKI APCSS) & Professor Philip LARK (GCMC)
0705-0735	**Keynote Speaker:** Mr. Paul ASH. Director of National Security Policy Directorate. (NZ). - Christchurch Call, responsible state behavior, and cybersecurity trends in the Indo-Pacific region
0735-0755	**Q&A Session**: Professor Philip LARK (GCMC)
0755-0815	**Regional Cybersecurity Challenges and Trends:** CDR Richard FRODERMAN. Planning Branch Chief. U.S. Fleet Cyber Command. (USA)
0815-0820	**Transition to Small Group Breakouts**
0820-0930	**Small Group Breakouts: Icebreaker, Discussion & Assignment #1** Breakout Group #1: Professor Philip LARK (GCMC) & CAPT Kim MCCANN (USN) Breakout Group #2: Dr. Bill WIENINGER (DKI APCSS) & CDR Jonathan ODOM (USN) Breakout Group #3: Professor Sean COSTIGAN (GCMC) & Dr. Beth KUNCE (DKI APCSS) Breakout Group #4: Dr. Ethan ALLEN (DKI APCSS) & MAJ Mike LAKATOS (CAN Army) Breakout Group #5: Dr. Inez MIYAMOTO (DKI APCSS) & LTC Arne LOSSMANN (DEU Army)
	Self-Study: Assignment #1 (See "Cybersecurity Workshop Participant Assignments.ppt") and Readings 1. **Video**: ASPI, Responsible State Behavior in Cyberspace, 9 Dec 2019, https://youtu.be/Ua8Ca0z2Uk4 2. **Reading:** United Nations, Office for Disarmament Affairs, "Open-ended Working Group," accessed March 1, 2021, https://www.un.org/disarmament/open-ended-working-group.

	3. **Reading:** United States Mission to the United Nations, "Explanation of Position at the Conclusion of the UN Open-Ended Working Group," March 12, 2021, https://usun.usmission.gov/explanation-of-position-at-the-conclusion-of-the-un-open-ended-working-group/. 4. **Reading:** Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 30 July 2010 A/65/201 Report (https://undocs.org/A/65/201); 24 June 2013 A/68/98 Report (https://undocs.org/A/68/98); and 22 July 2015 A/70/174 Report (https://undocs.org/A/70/174). 5. ***Optional Video:*** The Hague Program for Cyber Norms, "Panel: 'How it Applies': International Law and Responsible State Behaviour in Cyberspace," Nov 30, 2020, https://www.youtube.com/watch?v=cSR2awCLKX0 6. **Interactive Online Course**: OSCE Learning, "OSCE Cyber/ICT Security Confidence-Building Measures," accessed March 30, 2021, https://elearning.osce.org/courses/course-v1:OSCE+TNTD-CYBERCBM_v1+2020_11/about [*To access the course, register using the "Register Now" button.]*
Day 2: Tuesday, 20 April 2021	
0645-0700	**Login**
0700-0740 (20 minutes) (20 minutes) 0740-0800	**Topic 1: Responsible State Behavior** This module covers the evolving framework of responsible state behavior in cyberspace. It includes a discussion of how the framework supports the international rules-based order and affirms the applicability of international law to state-on-state behavior, the adherence to voluntary norms of responsible state behavior in peacetime, and the development and implementation of cyber confidence building measures to help reduce the risk of conflict stemming from cyber incidents. **Speakers:** **1.** Dr. Benjamin ANG. Deputy Head of Centre of Excellence for National Security. S. Rajaratnam School of International Studies (RSIS). (SGP). • Summarize the Framework for Responsible State Behavior in Cyberspace. **2.** Ms. Szilvia TOTH. Cyber Security Officer. Organization for Security and Co-operation in Europe (OSCE) Secretariat. Transnational Threats Department. (HUN). • Discuss Cyber Confidence Building Measures (CCBMs). **Q&A Session:** Dr. Inez MIYAMOTO (DKI APCSS)
0800-0805	**Break**
0805-0900	**Breakout Discussion**
0900-0910	**Break & Transition to Elective**
0910-1000	**Optional Elective**: ***Elective #1:*** **Cyber Mission Assurance & Resilience**, Major Michael Lakatos, Canadian Armed Forces, Canada, and Dr. Inez Miyamoto, DKI-APCSS. • Cyber mission assurance is the security posture to enable the operational authority to conduct all missions in a cyber-contested

	environment. This elective discusses how to build cyber resilience in the military and government. ***Elective #2:*** **A “Rules-Based” Approach to Cyber Security**, Commander Jonathan G. Odom, GCMC. • This elective session highlights the rules of international law applicable to cyberspace, analyzes the legality of cyber activities, and examines lawful ways in which states may counter cyber threats. The international community, including nation-states individually and groups of U.N. member-states collectively, have declared that international law is applicable to cyberspace. To date, however, there is not an international consensus about exactly how the particular rules of this body of law apply. This elective session provides participants with an overview of the applicable sources of international law. The session then examines and analyzes a range of legal cyber activities, as well as ways in which a target states may respond lawfully. ***Elective #3:*** **5G and National Security**, Dr. John Hemmings, DKI-APCSS • The development of 5G technology is not merely like the shift from 3G to 4G, but a whole revolution in information communications technology. This is because the high levels of reliable data-usage will open up to new downstream technological applications, such as the 4th Industrial Revolution, smart cities, tele-medicine, and drone-logistics. States are deeply aware that these applications will impact first-mover economic growth as well as defense capabilities of system leaders.
	Self-Study: Assignment #2 (See “Cybersecurity Workshop Participant Assignments.ppt”) and Readings 1. **Reading**: European Union Agency for Cybersecurity (ENISA), “National Security Strategies,” accessed February 11, 2021, https://www.enisa.europa.eu/topics/national-cyber-security-strategies 2. **Reading**: Internet Governance Project, “What is Internet Governance?,” Georgia Tech School of Public Policy, accessed February 11, 2021, https://www.internetgovernance.org/what-is-internet-governance/ 3. **Reading:** Global Cyber Security Capacity Centre, **“**Cybersecurity Capacity Maturity Model for Nations (CMM),” accessed March 1, 2021, https://gcscc.ox.ac.uk/the-cmm#/ 4. **Reading*:*** The Mitre Corporation, "Notional Cyber Security Governance Framework," Mitre Corporation, 2019, https://drive.google.com/file/d/1OvdlTcTSixOP-7u8f2uMnvOIO6kLx4Zm/view?usp=sharing 5. **Reading:** The Mitre Corporation, "Considerations and Notional Models for Establishing a National Cyber Coordinator," 2019, https://drive.google.com/file/d/1H1Mskv8EpK7svtP0wJqnOqMbyxkCUfCo/view?usp=sharing 6. **Video**: “What is Internet Governance?,” MAPPING Awareness Campaign, 25 Jan 2018, https://www.youtube.com/watch?v=oaeyu2ipyTQ **7.** **Optional Reading**: European Union Cyber Direct, Ecole nationale de cybersécurité & National Cyber Security Index, 19 Nov 2019, https://eucyberdirect.eu/good_cyber_story/national-cyber-security-index/
Day 3: Wednesday, 21 April 2021	
0645-0700	**Login**
0700-0740	**Topic 2: Assessment, Strategy & Policy** A national cybersecurity strategy is a plan of actions designed to improve the security and resilience of national infrastructures and services. The strategy helps a nation to address

	cybersecurity risks and establish national objectives and priorities. In order to know where to start, an assessment tool can be used to evaluate a nation's cybersecurity maturity. This module provides examples of how countries have used assessment, strategy, and policy to build their cybersecurity.
(20 minutes)	**Speakers:** 1. Dr. James BOORMAN. Head of Research and Capacity Building. Oceania Cyber Security Centre. (AUS). • Discuss cybersecurity maturity model • Provide examples from the Indo-Pacific region
(20 minutes)	2. Professor Philip LARK. GCMC. • Summarize how strategy and policy are utilized to strengthen cybersecurity, focusing on best practices and the need for whole-of-society engagement
0740-0800	**Q&A Session:** Dr. Inez MIYAMOTO (DKI APCSS)
0800-0805	**Break**
0805-0835	**Topic 3: Internet Governance** In this module, internet governance (i.e., the development and application of shared principles, norms, rules, decision-making procedures, and programs shaping the evolution and use of the internet) and internet freedom will be discussed.
(30 minutes)	**Speaker**: 1. Mr. Pablo HINOJOSA, Strategic Engagement Director. Asia Pacific Network Information Centre (APNIC). (MEX). • Explain how internet governance is a decentralized, bottom-up coordination of mostly private-sector entities across the globe • Discuss internet freedom
0835-0850	**Q&A Session:** Professor Phil LARK (GCMC)
0850-0900	**Break & Transition to Breakout Discussion Groups**
0900-1000	**Breakout Discussion**
	Self-Study: Assignment #3 (See "Cybersecurity Workshop Participant Assignments.ppt") and Readings 1. **Reading**: World Economic Forum, Cyber Information Sharing: Building Collective Security, October 2020, http://www3.weforum.org/docs/WEF_Cyber_Information_Sharing_2020.pdf 2. **Reading:** Carnegie Mellon University, "NatCSIRT Resources," *Software Engineering Institute*, 2021, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=505132 3. **Reading:** European Union Agency for Cybersecurity, *NatCSIRT Resources*, accessed April 4, 2021, https://www.enisa.europa.eu/topics/csirt-cert-services?tab=publications 4. ***Optional Reading*:** European Union Agency for Cybersecurity, *Publications*, accessed April 4, 2021, https://www.enisa.europa.eu/topics/csirt-cert-services?tab=publications 5. ***Optional Video*:** BBC News, "How worried should we be about deadly cyber-attacks?" 26 Sep 2020, https://www.youtube.com/watch?v=zSLDT7st7DI

	6. ***Optional Video*:** CNA Insider, "The Digital Threat To Nations | Secret Wars, Episode 1/2" 6 April 2020, https://www.youtube.com/watch?v=1oj91oe3API
Day 4: Thursday, 22 April 2021	
0645-0700	**Login**
0700-0740	**Topic 4: Incident Response** Incident response is a systematic approach to managing a security incident or breach. In this module, incident response processes, procedures, best practices, and information sharing will discussed. **Speakers**:
(20 minutes)	1. Mr. Tomoo YAMAUCHI. Deputy Director-General, National Center of Incident Readiness and Strategy for Cybersecurity (NISC). (JPN). • Discuss national-level incident response • Discuss the value of information sharing and preparation in cybersecurity
(20 minutes)	2. Mr. Rob Hubertse. Head, Security Operations Center, Defense Cyber Security Center. (NLD). • Discuss the Dutch Defense approach to cybersecurity. • Discuss incident response, continuity and information sharing
0740-0800	**Q&A Session:** Dr. Inez MIYAMOTO (DKI APCSS)
0800-0805	**Break**
0805-0900	**Breakout Discussion**
0900-0910	**Break & Transition to Elective**
0910-1000	**Optional Elective**: ***Elective #4:*** ***<u>Information Resilience in an Age of Disinformation & Misinformation</u>*****,** Dr. Beth Kunce (DKI APCSS) • This elective provides an overview of the information ecosystem as part of the operational environment. It focuses on how the information ecosystem and flow of information can support or harm community stability. ***Elective #5:*** **<u>Cryptocurrencies and Economic Disruption: A Discussion</u>,** Dr. Bill WIENINGER • The first cryptocurrency, Bitcoin, was created in 2008 and since then there has been an explosion in both its value as measured in US dollars and in the number of other cryptocurrency platforms. While these two facts are not in dispute, there is considerable disagreement on what cryptocurrency means for our economies and our security. Trumpeted by advocates as a replacement for fiat currency and decried by opponents as a tool for illicit trade, this elective examines the nature of the technology itself and what it likely means for the future impact of cryptocurrency ***Elective #6***: ***<u>Internet of Things: Security and Privacy</u>***, MAJ Nathan HOFFERMAN (DKI APCSS) • The world we live in today is a digital ecosystem comprised of billions of interconnected devices that all serve a purpose in our everyday lives. This elective provides an overview of 'Internet of Things' along with the security vulnerabilities and privacy implications we face co-existing with these devices.

	Self-Study: Presentation Preparation and Readings 1. **Reading:** European Union Agency for Cybersecurity, Public Private Partnerships PPPs, accessed 7 March 2021, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps 2. **Video**: Benjamin Eng, "Cyber Threat Information Sharing for Better Cybersecurity," 5 November 2020, https://www.youtube.com/watch?v=YXvGiRcw70A 3. **Video**: Cyber Future Foundation, "CFD2019 Davos Cyber Adversaries and Public-Private Partnership," 17 Feb 2019, https://www.youtube.com/watch?v=HCyNQEAsGxk 4. **Optional Reading**: Henry Harrison, "How to Build a Public-Private Cybersecurity Partnership for the Modern Era," World Economic Forum, July 15 2020, https://www.weforum.org/agenda/2020/07/why-its-time-for-a-new-era-of-public-private-cybersecurity-partnerships/ 5. ***Optional Video***: World Economic Forum, A New Architecture for Cyber-Cooperation, 9 Feb 2019, https://www.youtube.com/watch?v=VdaBDAbB__E
Day 5: Friday, 23 April 2021	
0645-0700	Login
0700-0740 (20 minutes) (20 minutes) 0840-0800	**Topic 5: Public Private Partnership & Cooperation** **Speakers**: 1. Ms. Mihoko MATSUBARA. Chief Cybersecurity Strategist. NTT Corporation. (JPN). • Discuss public-private cooperation for information sharing and responding to cyberattacks • Discuss how government can better work with the private sector on incidents. 2. Ms. Gaukhar ZHAKHMETOVA. Security Operations Center Analyst. Tengri Labs. (KAZ). • Discuss how government built trust and cooperation to secure critical infrastructures • Discuss whole-of-society approaches to respond to cyber incidents **Q&A Session:** Professor Phil LARK (GCMC)
0800-0840 0840-0850	**Breakout Back-Briefs:** *1. Breakout Group #1 (8 minutes)* *2. Breakout Group #2 (8 minutes)* *3. Breakout Group #3 (8 minutes)* *4. Breakout Group #4 (8 minutes)* *5. Breakout Group #5 (8 minutes)* **Wrap-up, Comments, & Survey:** Dr. Inez MIYAMOTO & Professor Phil LARK
0850-0900	**Closing:** Dr. Inez MIYAMOTO (DKI APCSS) and Professor Phil LARK (GCMC)