Regional Workshop and Dialogue on International Law in Cyberspace: *Asian Perspectives and Current Trends*

18 and 19 April 2023

Centre for International Law, National University of Singapore (NUS)

Hybrid (In Person & Zoom)

In Person Venue: NUS Bukit Timah Campus Block B Seminar Room 4-3

Address: 469 Bukit Timah Rd, Singapore 259756

Background

This regional workshop and dialogue is a collaborative effort between Chatham House and the Centre for International Law at the National University of Singapore (NUS). It will be carried out as part of Chatham House's 'Cyberspace4All Project', which is supported by the Dutch Ministry of Foreign Affairs and co-led by Chatham House's International Security Programme (ISP) and International Law Programme (ILP). The project's main goal is to promote a more inclusive approach to cyber governance through a series of activities. The planned outputs include regional briefings, workshops, roundtables, research reports, and multimedia outputs. In particular, the project seeks to convene regional international law capacity building workshops to foster understanding and networks around the application of international law in cyberspace among diplomats, government legal advisers, the private sector and civil society in non-European states. This Regional Workshop and Dialogue on International Law in Cyberspace (in hybrid format), is held in hybrid format in partnership with the NUS and with the support from the Shaw Foundation and Jesus College, University of Oxford.

The sessions will provide a broad overview of how various rules of international law apply to cyberspace, focussing on the most pressing issues of the moment, and with input from experts working on related fields, such as cybersecurity and cyber policy. They will be tailored to participants' interests and level of knowledge, and follow a practical, operational approach to international law, drawing on case studies. This event will be targeted at representatives of governments, international organisations, industry, and civil society based in ASEAN member states and other Asian countries, such as Japan, South Korea and China.

Programme (as of 10 April 2023)

Day 1

International law in cyberspace: Overarching issues

8.30 – 9.00 **Registration**

9.00 – 9.15 **Welcome (15 min)**

Welcome address by **Dr Nilufer Oral**, Director, Centre for International Law
Welcome address by **Rashmin Sagoo**, Director, International Law Programme, Chatham House (online/pre-recorded)
Welcome address by **Stephanie De Ridder**, Counselor, Cyber, Embassy of the Kingdom of the Netherlands in Singapore

9.15 – 10.30 **Session 1: International law and the contemporary cyber threat landscape (1 hr 15 min)**

Chair:
Dr Talita Dias, Senior Research Fellow, International Law Programme, Chatham House

Speakers:
Daphne Hong, Solicitor-General, Attorney General's Office, Singapore
Willis Lim, Director for the National Threat Analysis Centre, Cybersecurity Agency of Singapore
Jacqueline de Lange, Head Africa Joint Operations Against Cybercrime (AFJOC) Desk, INTERPOL

The world continues to face unprecedented challenges in cyberspace. Examples include ransomware attacks that have destabilised key service providers in different states, such as Costa Rica's Social Security Fund and the UK's Royal Mail, highly unpredictable Chat GPT-generated polymorphic malware, cyberattacks against critical infrastructure in the context of the hybrid war in Ukraine, and Twitter's debacle under Elon Musk. In this light, the time could not be riper to discuss the various issues surrounding the application of international law in cyberspace. At both the United Nations (UN) Group of Governmental Experts and the Open-Ended Working Group (OEWG) on cyber, states have agreed that "existing international obligations under international law are applicable to State use of [information and communications technologies (ICTs)]". But this general, simple statement hides beneath the surface a number of complex and contested legal and practical issues, particularly on which exact rules of international law apply in cyberspace. This session will do two things. First it will map out existing cyber threats, including cyber operations that have already led to actual harm and those whose risk remains latent. Second, it will unpack the reasons for disagreement among states and academics on the extent to which international law applies to those malicious cyber operations.

10.30-10.45 **Coffee break (15 min)**

10.45–12.00 **Session 2: Current OEWG dynamics and prospects on the application of international law in cyberspace (1 hr 15 min)**

Chair:
Danielle Yeow, Adjunct Senior Research Fellow, Centre for International Law

Speakers:
James Shires , Senior Research Fellow, International Security Programme, Chatham House (pre-recorded)
Dr Jovan Kurbalija, Executive Director, DiploFoundation (pre-recorded)
Mary-Elisabeth Chong, Deputy Senior State Counsel, Attorney-General's Chambers, Singapore

Discussants:
Farlina Said, Institute of Strategic and International Studies, Malaysia (online)
Eugene Tan, Associate Research Fellow. S Rajaratnam School of International Studies
Isaac Morales, Senior Director for Cybersecurity and Data Privacy Communications, FTI Consulting (online)
Anna Iwanicka-Quinn, First Counsellor, Deputy Head of Mission, Embassy of the Republic of Poland in Singapore

In its latest Progress Report issued in August 2022, the UN OEWG reaffirmed the cumulative and evolving framework for responsible state behaviour in the use of ICTs and made concrete, action-oriented and non-exhaustive proposals on international law. It also acknowledged that it could convene discussions on specific topics related to international law, focussing on identifying areas of convergence and consensus and encouraging continued sharing of national views, on a voluntary basis, on how international law applies in the use of ICTs. However, legal and political divisions between member states of the OEWG remain stark, especially between the Global North and South, and following the war in Ukraine. States that have expressed their views on the application of international law in cyberspace – within and outside the OEWG – including traditional allies, diverge on key topics. And several states have either strategically chosen not to disclose their views on the topic or simply lack the capacity to do so. This is the case of several states in the Asian region. Text negotiations at the OEWG are difficult, and the inclusion of every single word in each report or outcome document is hard-fought. This raises the question of whether the next sessions of the OEWG sessions can realistically go beyond what they have achieved so far, i.e., simply reaffirming the basic international legal rules and principles applicable to ICTs as well as the non-binding norms of responsible state behaviour articulated by the GGE in 2015. This session will try to better understand the current geopolitical dynamics underlying the OEWG's discussions of international law in cyberspace and consider what may come next as the Group transitions into a permanent forum – the 'Programme of Action'.

12.00 – 13.45 **Informal Working Lunch (1 hr 45 min)**

Emerging Technologies and International Law (in person only)

Artificial intelligence (AI) and other emerging technologies now pervade almost every single aspect of human life. From navigating on the World Wide Web to the provision of private and public services, these technologies have made our lives so much easier. However, their use by

states and non-state actors is not always rainbows and butterflies: emerging technologies have raised unprecedented challenges in all walks of life and corners of the world. Examples range from AI's bias and discriminatory uses in different fields, the lack of human oversight and the power of this and other technologies to generate new content and material, including influence operations and malware, as well as to behave in ways that can lead to real-world harms.

This session will try to better understand the challenges and opportunities of emerging technologies from an international law perspective. It will discuss the latest developments in the emerging technology landscape, including by introducing and demonstrating some of those technologies to participants (such as OpenAI's ChatGPT and DALL.E). It will also critically evaluate current debates on their impact on states and non-state actors, including by debunking misconceptions. Finally, the session will try to better understand the extent to which existing international legal rules and regimes, such as general principles, international huma rights law and international humanitarian law (IHL), apply and limit the use of these technologies.

Keynote:
Simon Chesterman, Vice Provost (Educational Innovation), David Marshall Professor, NUS; Senior Director of AI Governance, AI Singapore

Discussants:
Marcus Bartley Johns, Asia Regional Director for Government Affairs and Public Policy, Microsoft.

13.45–15.45 **Session 3: Applying the principles sovereignty, non-intervention and the prohibition on the use of force in cyberspace (2 hr)**

Chair:
Dr Talita Dias, Senior Research Fellow, International Law Programme, Chatham House

Speakers:
Dr Priya Urs, Junior Research Fellow, St John's College, Oxford (online)
Seung-hyun Nam, Associate Professor, Korean National Diplomatic Academy
Harriet Moynihan, Associate Fellow, International Law Programme, Chatham House (online)
Zhixiong Huang, Changjiang Outstanding Young Scholar Professor, Wuhan University Institute of International Law/Institute for Cyber Governance

Among the specific rules and principles of international law that states have agreed are applicable to ICTs are sovereign equality, the prohibition on "the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations" – including the right to self-defence as recognised in the UN Charter, and "non-intervention in the internal affairs of other States." But both the GGE have recognised the need for continued discussion, including through capacity-building courses, and exchanges of views by states on how these rules and principles apply to ICTs. Despite being a cornerstone of the international legal system, sovereignty remains one of the most contested issues of international law in cyberspace. When it comes to non-intervention, there seems to significant disagreement both in principle and practice on its core elements of "coercion" and "internal or external affairs". Likewise, even if the test for assessing when the prohibition on the use of force has been breached in cyberspace has received significant support among states and academics – comparing the scale and effects of cyber operations to kinetic ones – much uncertainty surrounds the application of this test to

real scenarios. The same goes for the 'armed attack' threshold, which triggers the application of the right to self-defence in cyberspace. This session seeks to identify areas of uncertainty and disagreement when it comes to the application of the principles of sovereignty, non-intervention, the prohibition on use of force, and the right to self-defence in cyberspace. The ultimate aim is to foster better understanding and hopefully agreement among states on those core issues.

15.45-16.00 **Coffee break (15 min)**

16.00 – 17.45 **Session 4: Cyber due diligence in theory and practice (1 hr 45 min)**

Chair:
Danielle Yeow, Adjunct Senior Research Fellow, Centre for International Law

Speakers:
Dr Talita Dias, Senior Research Fellow, International Law Programme, Chatham House
Tomohiro Mikanagi, Legal Advisor, Ministry of Foreign Affairs, Japan (online)
Dr Tara Maria Davenport , Assistant Professor, Faculty of Law, National University of Singapore
Janine Ensing, Legal Officer, international Law Division, Legal Affairs department, Ministry of Foreign Affairs (The Netherlands) (online)

Due diligence is a fundamental concept in the ICT environment. It encapsulates the idea that prevention is better than cure, and that states must behave with due care with a view to preventing, stopping or redressing certain types of harm to other states or even within their own territories. States and scholars have differing views as to whether due diligence in cyberspace is required as a matter of law or is simply expected of states as a voluntary norm of responsible state behaviour. This session will look at the nature of due diligence generally in international law, whether or not it applies to cyberspace, and, if so, to what extent it does apply, i.e., what is its scope and content. This session will also look at the importance of the voluntary norms of responsible state behaviour to the concept of cyber due diligence and what they require in practice, as well as reviewing the positions of governments that have commented publicly on the subject so far.

17.45 – 18.00 **Daily wrap-up (15 min)**

Dr Talita Dias and **Danielle Yeow**

Day 2

International law in cyberspace: Discrete issues

9.00–10.30 **Session 5: Countermeasures in cyberspace (1 hr 30 min)**

Chair:
Danielle Yeow, Adjunct Senior Research Fellow, Centre for International Law

Speakers:
Dr Przemysław Roguski, Associate Professor of International Law, Jagiellonian University, Krakow

Dr Talita Dias, Senior Research Fellow, Chatham House
Dr Yang Fan, School of Law, Xiamen University, China (online)
Phu Nguyen, Deputy Director General, Ministry of Foreign Affairs, Vietnam (online)

This session will examine the contentious issue of countermeasures in cyberspace, i.e., whether and to what extent states can respond to internationally wrongful acts committed in cyberspace/through ICTs by adopting countermeasures (i.e., measures that would otherwise be contrary to the international obligations of an injured state vis-à-vis the responsible state in order to procure cessation and reparation). According to the International Law Commission (ILC)'s 2001 Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA), a state may resort to countermeasures when it is directly injured as a result of the breach by another state of obligations owed by the latter state to the former. The ARSIWA also list a number of substantive and procedural requirements for a state to be able to engage in countermeasures, including proportionality and notification. However, several states have questioned the customary nature of countermeasures, their conditions and/or the ILC's interpretation thereof. There is also little clarity as to whether or not non-injured states may resort to 'collective' countermeasure at the request of the injured state or in response to a breach of an *erga omnes* rule of international law. Resort to countermeasures, whether individually or collectively, raises additional legal and policy questions in the cyber context. The aim of this session is to unpack those key legal and policy controversies surrounding countermeasures in cyberspace. In particular, it will discuss how the substantive and procedural conditions apply in this context as well as the policy implications of watering down those conditions and allowing collective cyber countermeasures to be taken by states.

10.30 – 10.45 **Coffee break (15 min)**

10.45 – 12.15 **Session 6: The role of non-state actors in cyberspace (1 hr 30 min)**

Chair:
Dr Przemysław Roguski, Associate Professor of International Law, Jagiellonian University, Krakow

Speakers:
Michael Karimian, Director, Digital Diplomacy, Asia and the Pacific, Microsoft
Benjamin Ang, Deputy Head, Centre of Excellence for National Security, S Rajaratnam School of international Studies
Sahar Haroon, ICRC Legal Advisor, Kuala Lumpur (online)

The Internet and other ICTs have been in large part designed, deployed, and owned by private entities. These range from the Internet Corporation for Assigned Names and Numbers (which is responsible for the World Wide Web's Domain Name System), to companies that operate servers and cables, provide key cybersecurity tools to protect against malicious cyber activity, and run online platforms. The role of Starlink and Microsoft in the defence of Ukraine against Russian cyber operations illustrates the key role that private actors play in maintaining international peace and security in cyberspace. Likewise, the vast majority of those technologies, including online services, are used by private individuals and groups. In recognition of the role of multiple stakeholders in cyberspace, the OEWG has been gradually seeking their views in different formats and fora alongside its main substantive sessions. Several non-state stakeholders such as Chatham House, the Oxford Process on International Law Protections in Cyberspace, and the Tallinn Process have been instrumental in the clarification of the extent to which international law applies in cyberspace. However, the involvement of non-state stakeholders, such as the private sector and civil society, at the

OWEG, remains low despite their continuous efforts to be formally included in the process. This lack of access to participation was especially the case with non-governmental stakeholders from the Global South. More generally, international law remains state-centred. This is particularly concerning in the cyber context, given that the vast majority of cyber operations are carried out by non-state actors and cannot be attributed to any particular state. This session will look at the role of non-state actors in the application of international law in cyberspace, including their rights, obligations and their contribution to the clarification and development of the discipline.

12.15 – 13.45 **Lunch (1 hr 30 min)**

13.45 – 15.15 **Session 7: Bridging the Global North-South and other legal divides (1 hour 30 min)**

Chair:
Danielle Yeow, Adjunct Senior Research Fellow, Centre for International Law

Speakers:
Judge Kriangsak Kittichaisaree, Judge of the International Tribunal for the Law of the Sea; former member of the UN International Law Commission (2012-2016) (online)
Dr Shashi Jayakumar, Senior Fellow, Head of Centre of Excellence for National Security; Executive Coordinator of Future Issues and Technology, S Rajaratnam School of International Studies (online)
Farlina Said, Institute of Strategic and International Studies, Malaysia (online)
Zhixiong Huang, Changjiang Outstanding Young Scholar Professor, Wuhan University Institute of International Law/Institute for Cyber Governance

It is no surprise that economic and political divisions between states reflect themselves in how international law is interpreted, applied, and implemented. This discrepancy is most striking between Global North and Global South countries, as well as between those that follow Western, liberal traditions and those adopting alternative approaches to national and international policy, such as Non-Aligned and communist states. Yet international law cannot be truly international if there is no common language, method or basic understanding between those nations. One of the key drivers of such discrepancy is an unequal distribution of legal capacity, i.e., financial, human, educational and time resources that would enable particularly less developed states to develop their understanding of international law. The same is true of issues surrounding the application of international law in cyberspace, including its clarification and development. A lack of understanding of the application of international law to cyberspace is prevalent among many states, particularly developing countries. Yet this is a significant hurdle to reaching agreement on how the rules apply to ICTs. The number of developing countries that have issued a statement or formally expressed their views on the application of international law in cyberspace is meagre. And even those that have done so lack the resources to put together an elaborate position paper. Overall, current avenues for the clarification and development of international law in cyberspace are not sufficiently diverse or inclusive. The aim of this session is to try to fill this gap in Asia, with an emphasis on low-and middle-income countries that were not active in the first OEWG but are most likely to benefit from capacity-building. It will also try to bring together countries from the US/EU-like-minded group and the Russia/China-like-minded group, which currently have little or no substantive dialogue on the application of international law in cyberspace.

15.15 – 15.30 **Coffee break (15 min)**

15.30– 17.15 **Session 8: The international regulation of online content (1 hr 45 min)**

Chair:
Harpreet Dhillon Kaur, Senior Legal Counsel, Dispute Resolution (APAC) Paypal *(formerly Senior Legal Counsel and Lead Counsel APAC, Content and Regulatory Enforcement, Twitter)*

Speakers:
Marzuki Darusman, Founder, Foundation for International Human Rights Reporting Standards (FIHRRST); Former Attorney General of Indonesia, Former Special Rapporteur on the situation of human rights in the DPRK, and Former Member of the Independent International Fact-Finding Mission on Myanmar (IIFFMM) (online)
Munira Mustaffa, Founder and Executive Director, Chasseur Group
Ou Meimin, Senior Policy Specialist and Regional Lead, Trust and Safety, Google
Frederick Rawski, Head of Human Rights Policy, APAC, Meta
Lee Huan Ting, 2nd Director (designate), Information Policy Division, Ministry of Communications and Information, Singapore

Unlike traditional means of communication such as the press, radio and TV, online content can be disseminated at an unprecedented speed and scale. Its effects can also be easily amplified, thanks to ranking and recommendation algorithms deployed by various online platforms. Notably, widespread information or influence operations have played an increasingly significant role in a number of offline harms – from health mis- and disinformation hampering the fight against COVID-19 to online hate paving the way for acts of violence in the developed and developing world.

The effects of information operations deployed by both states and non-state actors – including propaganda, dis- and misinformation, malinformation, and online hate speech – have shaken up traditional views about how international law regulates or limits the dissemination of content. There is growing agreement that international law does place limits on information operations, either under general rules and principles such as sovereignty and non-intervention or under specific regimes such as international human rights law and humanitarian law. This session will explore key issues surrounding the international regulation of online content, particularly how different international legal rules or regimes apply concurrently (such as freedom of expression and the prohibition of subversive propaganda and incitement to violence or discrimination).

17.15 – 17.35 Daily wrap up and next steps (20 min)

Led by **Dr Talita Dias** and **Danielle Yeow**

Networking Dinner (by invitation)