Cambodia's Emergent Cyberdiplomacy

Chhem Siriwat, Tean Samnang, Bong Chansambath

Chhem, Siriwat, Samnang Tean, and Chansambath Bong
Cambodia's Emergent Cyberdiplomacy

ISBN-13: 978-9924-9704-2-2

Published by Asian Vision Institute, 2nd Floor, Jaya Smart Building, Street 566, Boeung Kak 2, Toul Kok, Phnom Penh, Cambodia: Postal Code: 120408

For information on all Asian Vision Institute publications
Visit our website: https://www.asianvision.org/publication-1

Printing graciously sponsored by:

“Nothing exists except atoms and empty space:

Everything else is opinion.”

- Democritus (ca. 460-370 BC)

Acknowledgements

This book project was led by the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI). Firstly, I would like to start by thanking our first co-editor H.E. Tean Samnang, previously President of the National Institute of Diplomacy and International Relations (NIDIR) and now Director General of the Information, Research, and Analysis Group at the Ministry of Foreign Affairs and International Cooperation (MFA-IC), for contributing his insightful research findings and project work to the book. Secondly, I would like to thank Mr Bong Chansambath, Deputy Director of CIDE at AVI, for contributing his valuable time and expertise in bringing the book together.

Furthermore, I would like to thank H.E. Dr Sok Siphana, H.E. Dr Chhem Kieth Rethy, and Dr Chheang Vannarith, Chairman, Vice-Chairman, and President of AVI, respectively, for their invaluable guidance. In addition, I would like to thank H.E. Sous Yara, Director General of the Asian Cultural Council (ACC), for his unwavering support.

I would also like to thank the supporting team members of CIDE for their commitment and dedication. A special thanks to Ms Costa Monica for designing the book cover once again.

Finally, I would like to thank the KMH Foundation and ISI Group for sponsoring the publication of our books and supporting other policy research and capacity-building initiatives of CIDE over the past few years. Their support has exhibited the valuable contribution and impact of the private sector on think tanks for the socioeconomic development of Cambodia.

Chhem Siriwat, MDTM, MA
Centre for Inclusive Digital Economy
Asian Vision Institute

Kingdom of Cambodia
Ministry of Foreign Affairs
& International Cooperation

Foreword

The use of digital technology in daily diplomatic practices has become ubiquitous given the advances in telecommunications. Digital diplomacy was accelerated during the COVID-19 global pandemic, as face-to-face interactions were restricted to minimise the risk of spreading the virus. While digital technology has been a great enabler for effective workflow at ministries of foreign affairs, embassies and international organisations, it also carries significant privacy risks making cybersecurity a paramount concern. Digital technology applications must be managed through proper regulations to protect against cyberattacks and espionage. New technological challenges occur in parallel with the unstoppable rise of cyber activities that permeates all human actions. In this context, cyberdiplomacy defines new norms for international governance in this changing era. Contrary to global nuclear security that can be, to a certain degree, be negotiated and mitigated at multilateral organisations like the International Atomic Energy Agency, cybersecurity is even more challenging as its governance intersects across domains, including non-state actors. The publication of this book is therefore timely and needed.

The co-editors should be praised for their initiative to bring such new knowledge to diplomats. Chhem Siriwat is Director of the Centre for Inclusive Digital Economy of the Asian Vision Institute. He is a digital expert with combined qualifications in Digital Technology Management, Artificial Intelligence and cyberdiplomacy. This book is an extension of his Master thesis on Diplomacy. In order to enhance the perspective of his book, he invited two contributors with

different, yet complimentary expertise and academic qualifications. This collaboration enriched the book with valuable inputs from Tean Samnang's work on cyberdiplomacy taken from the context of his PhD research on cyberspace governance at the Southwest University of Political Science and Law (Chongqing). Bong Chansambath who holds a Master degree in Security Studies from Kansas State University, brought a global security perspective and provided further inputs on cyberdiplomacy. Together, these three cast a broad perspective stemming from their exposure to American, European and Chinese academic traditions. For several years, they collaborated through research and participation in national, regional and international debates on this emerging field. This book adds to the anthology on "Cambodia in Cyberspace" edited by Chhem Siriwat, Ou Phannarith and Chea Vatana.

I heartily congratulate these brilliant scholars of diplomacy for their remarkable pioneering work in addressing this emerging field, dedicated to meeting the new challenges of cyberdiplomacy. I would strongly recommend this book to those who wish to learn more about the global debates and narratives of cyberdiplomacy, whether they are practicing diplomats or scholars of international relations in the era of cyberspace.

Phnom Penh, 07 March 2023

H.E. Prak Sokhonn
Deputy Prime Minister
Minister of Foreign Affairs and International Cooperation
Royal Government of Cambodia

Preface

“Cambodia’s Emergent Cyberdiplomacy” is the second publication of the Centre for Inclusive Digital Economy (CIDE) at the Asian Vision Institute (AVI), as an extension of its first book - “Cambodia in Cyberspace”. Although the previous book was more of an overview of the digital economy in Cambodia and related issues of cyberspace, this new book dives deeper into the development of digital diplomacy and cyberdiplomacy in Cambodia.

The inspiration for this book was based on my Master's Thesis entitled “Sovereignty and Diplomacy in Cyberspace: A Philosophical Inquiry” at the Pannasastra University of Cambodia (PUC). In addition, H.E. Tean Samnang added his insightful PhD research on cyberdiplomacy and cyber governance.

This book was categorised into the following themes: 1) Philosophy of Cyberspace; 2) Cyber Sovereignty; 3) Cyberdiplomacy; 4) US-China Rivalry in Cyberspace; 5) Geopolitics of Cyber Governance in the World, ASEAN, and Cambodia; 6) Cambodia and Cyberspace Issues; and 7) Regional Capacity Building in Cyberdiplomacy.

With the monumental increase in interconnectivity around the world, diplomats will have to prepare for the new age of diplomacy in the digital era, where communication and interaction via cyberspace are inevitable. Traditional international relations theories will have to be revisited in order to address the emerging challenges of cyberdiplomacy.

Chhem Siriwat, MDTM, MA
Centre for Inclusive Digital Economy
Asian Vision Institute

Meet the Co-Editors

Chhem Siriwat is Director of the Centre for Inclusive Digital Economy at the Asian Vision Institute (AVI), Advisor to the Council for the Development of Cambodia (CDC), with the rank of Director General, and Advisor to the Cambodia University of Technology and Science (CamTech). He focuses on digital and cyberspace issues from policy, academics, and business perspectives. His professional experiences include leadership and advisory roles at think tanks, government agencies, science and technology universities, commercial banks, and tech start-ups. He has a combined academic background in science, arts, and business, specialising in Digital Technology Management, Artificial Intelligence, Diplomacy, Chemistry, Physics, and Environmental Science. He has published numerous papers and is regularly invited as a guest speaker at international conferences on digital economy and Cyberdiplomacy.

Tean Samnang is Director General of the Information, Research and Analysis Group at the Ministry of Foreign Affairs and International Cooperation (MFA-IC) of Cambodia. Before this position, he recently served as President of the National Institute for Diplomacy and International Relations at MFA-IC.

Bong Chansambath is Deputy Director of the Centre for Inclusive Digital Economy at the Asian Vision Institute and a lecturer at the Institute of International Studies and Public Policy, Royal University of Phnom Penh. He holds an MA in Security Studies from Kansas State University, where he was a Fulbright scholar from 2018 to 2020. His research focuses on Cambodia's foreign and defence policy, Southeast Asian security and the geopolitics of cyberspace and technology. Most recently, Sambath has been selected as an inaugural fellow of the EU Cyber Diplomacy Fellowship, a capacity-building program supported by the European Union.

Dedication

This book is dedicated in memory of H.E. Dr Trond Gilberg (1940-2022), previously Dean of the Faculty of Social Sciences and International Relations and Director of the Peace Conflict Studies Institute at Pannasastra University of Cambodia (PUC), Advisor to the Centre for Inclusive Digital Economy at the Asian Vision Institute, and Advisor to the Ministry of Foreign Affairs and International Cooperation (MFA-IC), with the rank of Secretary of State. Dr Trond was my supervisor at PUC for my thesis entitled "Sovereignty and Diplomacy in Cyberspace: A Philosophical Inquiry", and he always pushed me to strive for academic excellence and integrity. Dr Trond was a respected scholar, teacher, and mentor in Cambodia, who dedicated his time and shared his wisdom in training the next generation of Cambodian diplomats. He will be dearly missed and forever remembered by his family, friends, colleagues, and students.

Chhem Siriwat, MDTM, MA
Centre for Inclusive Digital Economy
Asian Vision Institute

Table of Contents

Chapter 1: Introduction

Digital technology is evolving at an exponential rate, heavily relied upon across all sectors. Applications of digital technology such as 5th Generation Telecommunications Technology (5G) and Artificial Intelligence (AI) bring about the great potential for national economic productivity but also create significant security issues in unfamiliar territory – Cyberspace. Traditionally, nations conform to the concept of "Westphalian Sovereignty". With the increased shift into cyberspace, global connectivity is at an all-time high. Individuals, organisations, and nations are heavily interconnected in cyberspace through their phones, laptops, and endless mobile devices. Cybersecurity is now a top priority of national security in protecting Critical Information Infrastructure (CII), just as Digital Diplomacy has evolved due to the increased use of highly influential social media platforms. Traditional international relations theories are now being challenged like never before, as observed by the heated China-US rivalry. In an interconnected world, whoever controls the data, controls the power. Outdated international relations theories no longer hold their validity, and there is a dire need to revisit them to modify those theories in the context of rapidly evolving digital technology applications and platforms.

In the fundamental image of realism, states are the dominant unitary actors acting rationally to protect their top national security priority. More emphasis is placed on state actors than non-state actors, such as international and transnational organisations, multinational corporations, and terrorist groups. The aforementioned non-state actors try to act independently but are either not significant or of lesser importance. As a result, states, as unitary actors, are integrated entities represented by their governments in the international arena. Most importantly, national security is the top priority of international affairs. Military security and strategy are prioritised over economic and social aspects.

States mainly use force to solve conflicts with other states, protect their territorial integrity, and maintain international stability.[1]

In contrast to realism, two other existing international relations theories are pluralism and globalism. The aforementioned theories suggest that states are not the only actors and that non-state actors, such as private enterprises and non-government organisations, play crucial roles in the dynamics of international relations. Pluralism highlights that international organisations operate independently while still influencing national agendas and political priorities. Multinational corporations also play key roles in the world economy, which contributes to their weight in impacting international relations, even surpassing state authority in some cases. Furthermore, military and security issues are not the only national priorities but economic, social, and welfare issues. However, the latter issues are only focused on when tension on the international scale decreases. From this perspective, pluralism is analysed in terms of the internal forces of a nation rather than the interaction between states. On the other hand, globalism emphasises that states and non-state actors are not only equal players but all act within a global system. In other words, each nation plays a different role in the international arena, which determines its strategies with respect to other nations and non-state actors. This complex network of interconnections considers historical, cultural, and especially economic factors.[2]

However, now that the world is progressing into the digital era, where we are becoming exponentially more connected, how will this affect the fundamental theories of international relations? One could argue that these traditional images are no longer adequate frameworks to explain contemporary international relations. For example, in realism, where military and security issues are the top priorities of a nation's agenda, the landscape is rapidly changing with the

emerging of digital technologies. Considering the immense potential of 5G and AI across all sectors, they epitomise a double-edged sword. Although 5G is a cellular network technology, its smarter and more efficient communication of data could be seen as a threat if utilised in the context of weaponisation.

On the other hand, AI optimises large amounts of data in order to make decisions based on pre-determined algorithms. In other words, whichever nation stores the most data and either creates or understands appropriate algorithms to implement will have the competitive edge. Similar to 5G and any other digital technology, AI could potentially be weaponised. Therefore, in today's global context, although a nation might be progressing in terms of science and technology innovation, this advancement might not just be seen as an economic driver but as a threatening shift in the military and security arena.

Geopolitics, in its purest form, refers to politics and international relations influenced by geographical factors. However, cyberspace has no true geographical dimensions, only dimensions within cyberspace that represent the physical world. This dilemma naturally creates philosophical challenges in linking the physical world and cyberspace in terms of space, time, objects, and interactions. Nonetheless, emerging technologies play a significant role in contemporary geopolitics. Not only referring to sophisticated technologies such as AI and 5G but even social media platforms and messenger applications can be weaponised or utilised for malicious intent in the geopolitical arena. Politicians, diplomats, and government officials are all connected to the Internet through mobile devices.

Advancements in telecommunication technologies allow for exponentially faster distribution of information across the globe. On the one hand, the enhancement of work infrastructure and methods continues to push the boundaries of productivity and efficiency, particularly in the unique case of remote work during

the COVID-19 era. On the other hand, the more interconnected we are, the more vulnerable we are to cyber threats and attacks. AI and 5G allow individuals, organisations, and states to process vast amounts of data in shorter periods of time than ever before. Social media platforms and messenger applications allow information to be distributed and shared instantly, without boundaries. Reflecting on the aforementioned examples, these forms of emerging technologies are all double-edged swords – unlimited potential for positive impact in the right hands but equally devastating in the wrong hands. States actually intend to use these technologies for good or bad, and opposing states will likely experience a security dilemma whereby they fear the potential weaponisation of technology by the other states. For example, AI algorithms and social media platforms both play a role in global politics through Facebook, Twitter, and more. However, the dark side of this reality could lead to political polarisation, both intentionally due to data manipulation behind the scenes or even unintentionally due to algorithm bias. Taking into consideration both sides of the coin, the world of geopolitics has indeed benefitted from more efficient communication around the world. However, it has also become increasingly more complex – as physical reality seems to be evermore immersed and overlapping with cyberspace.

The increased interconnectivity of the world has resulted in higher economic potential for respective states. However, this transformative shift has also led to increased risks of cyber threats and attacks. The more interconnected we are, the more potential sites for attacks there are, and the more vulnerable we are overall. Having the technical potential to connect with other individuals and their devices around the world at any moment was once a dream. Now that this dream has become a reality, users have to face the potential risks associated with emerging technology. Cybersecurity has become a top priority for all nations in protecting their citizens, organisations, and CIIs linked to essential industries and services.

From a fundamental perspective, the technological rivalry between China and the US represents a clash between a rising and declining global power. Strategic moves carried out in the trade war are all acts of balancing technological supremacy. Both sides protect the free flow of ideas and individuals from each other. The trade war has significantly damaged business relations between the US and Chinese companies such as Huawei, limiting the inflow of American software and hardware. In response, China needs to continue developing its own industry for chips and operating systems. Government strategies must push for the large-scale production of domestic semiconductors, in order to contribute towards technological independence. On the other hand, China holds a monopoly in the global market for Rare Earth Elements (REE), which are essential in modern electronic devices. The US and China have leverage over each other in this technological rivalry, as seen from their dynamic interactions in the context of the trade war.

Furthermore, the US is attempting to suppress China's push for 5G, which would be a catalyst for all of its technological advancements. This shift of power in their technological rivalry will impact global trade and security. What will happen when China no longer relies on the US for technological support? Will the trade war become obsolete? With all nations interconnected within this rivalry, surpassing technological supremacy could likely cause a clear divide. Aside from the effects on global trade, security on an international level is at risk due to the potential weaponisation of 5G and AI. Just as with any new form of technology, there are both beneficial and malicious ways to utilise them. In order to govern the use of these technologies, all nations should prepare teams of experts to deal with both technical and ethical aspects. A small state like Cambodia cannot escape the consequences of this technological shift. How can Cambodia be prepared to survive the future cyber conflict?

Cambodia is a rapidly developing country with more than 7% annual GDP growth over the last 20 years and a young population where more than 65% are under 30, and the median age is 25.6 years old.[3,4] Being a young country in the digital age, the Cambodian youth are naturally tech-savvy, which consequently drives the high national digital adoption rate. Any major technological trends, including digital payment, transportation, and delivery applications, catch on quickly across the nation. Furthermore, social media and messenger platforms are uniquely integrated into countless aspects of work and life in Cambodia. Facebook and Instagram are widely used as e-commerce platforms, conveniently using various methods of digital peer-to-peer transfers between individual buyers and sellers to carry out financial transactions. Telegram and WhatsApp are often used as primary channels of work communication for organisations to transfer official or confidential files conveniently and instantly. Transportation or ride-hailing applications such as Grab and PassApp can get taxis to a customer's physical location in less than a minute, while food delivery services such as NHAM24 and Foodpanda deliver endless options of food and drinks, within 30 minutes to an hour. These applications and platforms all include integrated digital payment methods that are linked to the bank account or credit card of the customer.

From the previous examples, it is clear that Cambodian citizens enjoy the benefits of digital technology applications, as they bring about much convenience in everyday work and life. However, as with all advancements and innovations in technology throughout history, they give rise to as many consequences as they do benefits. For example, when humanity shifted from horses to cars, it was evident that cars would be more convenient and efficient in getting from point A to point B. Nonetheless, whether it was foreseen or not, the corresponding increase in car-related accidents and deaths was inevitable. The industry continued to evolve by

improving car performance and safety from the manufacturing sector, as well as reinforcing car manufacturing requirements and traffic rules from the regulatory side. Around the world, the risks related to driving are well- understood, but we still choose to drive – knowing what we know. This analogy highlights the conventional timeline relevant to technological advancements; new inventions must first be used and tested – policies, regulations, and laws follow after.

In the case of Cambodia, in the last 20 years, the national economic boom resulted in mass construction across the country. Both local and international construction companies were, and still are, developing projects at an exponential rate. However, the official law on construction was only legislated in recent years. Policy implementation in terms of national law formulation is a long and rigorous process, with a high risk of these laws being outdated or insufficient by the time they are officially released. Furthermore, technology evolves at an incomparably higher rate than policies are being written, even more so in this rapidly transforming digital era. Despite Cambodia's relatively young market and a late start in terms of adopting digital technology applications and platforms, the nation has pushed the limits of convenience and efficiency, particularly when it comes to e-commerce. There is a wide range of e-commerce platforms in the local market, joined by countless e-commerce entrepreneurs from the comfort of their homes. Selling products via Facebook, Instagram, Telegram, and other platforms has become a national trend. With the law on e-commerce only recently coming into play in Cambodia, there is still much room for flexibility due to the lack of regulations. On the one hand, this emergence of the e-commerce market in Cambodia, accelerated by the COVID-19 pandemic, is a golden opportunity for young Cambodian entrepreneurs to build their businesses without many limitations and restrictions. On the other hand, laws are indeed meant to protect citizens, and a lack thereof puts these vulnerable entrepreneurs at risk.

Fast forward to Cambodia today, the national law on cybersecurity is currently being drafted by a diverse local team of technical and legal experts under the Ministry of Post and Telecommunications (MPTC). Although the law on cybercrime is being simultaneously drafted under the Ministry of Interior (MOI), cybercrime and cybersecurity cover different aspects of the regulation of cyberspace in Cambodia. Around the world, some nations combine cybersecurity and cybercrime under one law, while others decide to keep them separate – as in Cambodia's case. Despite the national cybersecurity law not yet being promulgated, individuals and organisations across all sectors continue to fully integrate digital applications and platforms into their businesses and everyday life, whether or not they are aware of the potential risks. Without a robust national legal framework in place to protect consumers and producers in cyberspace, in addition to a lack of basic cybersecurity literacy and education, navigators of cyberspace are treading insecure and unsafe. What might appear as ordinary or innocent as clicking on a link sent via email, or opening a document from a seemingly trusted source, might actually turn out to be an attempted cyberattack.

To answer the million-dollar question: Who is at risk of a cyberattack? Or, in less technical terms: Who is at risk of getting hacked? Anyone who is connected to an internet-connected device such as a phone, computer, and other mobile devices – almost everyone. The Internet is a double-edged sword. From one perspective, the Internet is an almighty global network and an infinite source of instantaneous information. From a different perspective, it is also the root of hacks and cyberattacks. John Chambers, CEO of Cisco, famously stated that "There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked." The unfortunate truth and reality of cyberspace are that everyone is at risk and vulnerable to cyberattacks. Many experts in the field of cybersecurity refer to the term "cyber-insecurity", implying that the more one knows about cybersecurity and its associated consequences, the more insecure

they become when interacting with cyberspace. With that being said, raising public awareness and providing basic education on cybersecurity literacy and practices greatly impact today's undeniably interconnected society and world.

However, as much as diplomats are always updated, new challenges arise in terms of cybersecurity. Diplomats have privileged access to confidential information of national significance in terms of trade, security, and the list goes on. In turn, diplomats can be easily targeted as victims of cyberattacks, especially through basic methods of social engineering. For example, hackers can send diplomats seemingly-innocent website links or documents, which are in reality – malicious viruses. Taking it one step further, hackers can even pose as colleagues, friends, or family members, with the aim of extracting usernames, passwords, or other details of access to private accounts. Therefore, basic cybersecurity education and training are crucial for diplomats as they act as communication channels for top-secret and confidential information, both domestically and internationally, for high-level government officials and nation leaders.

This book aims to address the following research questions from a philosophical point of view in the context of contemporary international relations:

1) How do we define sovereignty in cyberspace or "Cyber Sovereignty"?
2) How can we use diplomacy in cyberspace or "Cyberdiplomacy" to reconcile two opposing views (US – Internet Freedom, China – Internet Sovereignty) on international cyberspace governance?

As such, the first step of this approach will be to explore the philosophy of cyberspace, in terms of ontology, epistemology, and ethics, as a foundation for this research endeavour. In other words, diving deep into the fundamental questions that surround cyberspace: who, what, where, when, why, and how.

Chapter 2: Philosophy of Cyberspace

"Space and time are the framework
within which the mind is constrained
to construct its experience of reality."
- Immanuel Kant (1724-1804)

Before diving into sovereignty and diplomacy in cyberspace, we will first explore the underlying philosophy of cyberspace. We understand that the world and reality we live in is a physical space. However, we also live in co-existing cyberspace through our mobile devices connected to the Internet. How do we draw the lines between our lives in the physical space of the real world and cyberspace? Furthermore, do the same ways of thinking and behaving apply in both worlds equally? These considerations must be addressed at the individual, organisational, and national levels. Behind the screen of a computer, an individual can target any other individual, organisation, or even an entire state. The interactions in cyberspace are not limited to the conventional structure of the physical world. Although the processes and infrastructure of cyberspace are indeed technically complex, its concept is highly philosophical and must be evaluated and regulated accordingly. The following section will focus on the philosophy of cyberspace, digging deeply into the ontology, epistemology, and ethics of cyberspace.

Moor and Bynum (2002) refer to "cyberphilosophy" as the intersection of philosophy and computing, including all interactions between both disciplines. Thomas Hobbes, a renowned Empiricist philosopher of the 17th century, proposed that human reasoning was based on the manipulation of signs. Much like today's

advancements in Artificial Intelligence (AI) that are based on the manipulation of signs, Hobbes had unknowingly drawn the connection between humans and computers hundreds of years ago. Furthermore, French philosopher Rene Descartes established a method to differentiate man and machine back in the 16th century, which then developed into the Turing Test of the 20th century by Alan Turing. In the 20th century, the heated debate about the co-existence of man and machine intensified. Men were making computers more intelligent, with the ultimate goal of using machine intelligence to replace human intelligence in carrying out specific tasks. Although these technological advancements were increasing productivity and efficiency across all sectors, "The deployment of computing technology in the twentieth century raised conceptual and ethical questions about privacy, property, and power."[5]

Computing has had a profound impact on philosophy in terms of research, teaching, and other forms of interaction. "The Digital Phoenix" (Moor and Bynum 2002) emphasised that computing created new subject matter, models, and methods within the field of philosophy. With regard to the new subject matter, the components of computing in terms of information, algorithms, programs, and intelligence all came into question. Furthermore, computer models are a foundation for philosophical inquiry, as they reflect the way that computers think, process, and behave in contrast to humans. Finally, computers have also provided philosophers with new methods of research and communication, such as search engines, distance learning, and other computer applications and platforms. This evolution of methods challenges whether new philosophical findings are indeed the result of organic human conceptualisation or, rather, the empirical construction of knowledge heavily influenced by computer intelligence. The influence of pre-determined algorithms on our behaviour and everyday lives as humans are inevitable. Notifications, advertisements, and other

forms of instantaneous accessibility to the Internet, create seemingly trivial psychological ripples that, in turn, play major roles in our decision making.

Moreover, "The Digital Phoenix" narrows the link between computers and minds, agency, reality, and communication. Comparing computers to minds, both take in symbols, manipulate them, and then finally output representations of external occurrences. The role of programmers is to manipulate symbols in a way that will most accurately represent corresponding situations in reality.[6] However, the main distinction and most challenging question are: Who is manipulating the symbols that enter our minds as humans? The human mind is extremely complex both mentally and cognitively, further affected by our physical, emotional, social, and spiritual well-being as individuals. Moreover, our past experiences provide us with an intuition that moulds our way of thinking without knowing why or how.

Today's AI researchers are advancing Deep Learning (DL), which is based on Deep Neural Networks (DNN) – bioinspired by the human brain. In a nutshell, DL is a branch of AI, which integrates multiple layers of computation. One step below this level of technical sophistication, Machine Learning (ML) is a common AI application which utilises past data to learn and improve through algorithms. The main difference between DL and ML is that DL is a subset of ML.[7] Deep learning is indeed more advanced, often referred to as "general AI", with the purpose of creating AI that can carry out different types of tasks.

On the other hand, ML or "narrow AI" focuses on carrying out one specific task. For example, many search engines and recommendation algorithms through Google, YouTube, Facebook, and Instagram are powered by ML and DL.[8] As convenient and useful as this may be for consumers and customers connected to the Internet, this also creates a form of streamlined bias. Not only one single

application but multiple different platforms that are interoperable can collect an individual's data simultaneously to predict the closest matching search results or suggestions. This phenomenon describes what producers or suppliers aim to provide, as personalisation and customisation in customer experience – using customer data and consumer patterns across various platforms to predetermine what customers want.

ML-powered search engines and recommendation algorithms not only play a role in the commercial sector but also in the field of academia. Based on an individual's personal data, their online search results and suggestions for literature or sources will vary. This consequently results in a skewed representation of available sources by narrowing down to sources that are filtered through ML. One common and relatable example is that when we search on Google, the results produced depend on where we live. The country, city, or even area that we live in can affect the results that we retrieve from the very same search engine using the same search keyword. Taking a step back, this case of ML algorithms in search engines is a double-edged sword. While they allow us to find information online instantaneously, they also contribute to a significant but intangible influence on the search results provided to us. In the field of academia and, more particularly, in philosophy, this dynamic could potentially create extreme polarisation between opposing schools of thought. Increased polarisation can already be observed in the field of politics. The general public is easily swayed by what they see on social media, with ML algorithms further perpetuating what they want to see and hear. This vicious cycle of one-sided information delivered through text, audio, video, and more intensifies their political views and in turn – could result in radical behaviour. Regular citizens and scholars are exposed to the risk of bias creation through their interactions with cyberspace. If philosophy is the study of the nature of knowledge, reality, and existence, how will the field progress differently, moving forward into the

age of cyberspace, where those aforementioned pillars are all distorted by algorithmic filters and manipulators. However, Google AI recognises this dilemma in which they play such an influential global role: “We will assess AI applications in view of the following objectives. We believe that AI should: (1) Be socially beneficial; (2) Avoid creating or reinforcing unfair bias; (3) Be built and tested for safety; (4) Be accountable to people; (5) Incorporate privacy design principles; (6) Uphold high standards of scientific excellence; and (7) Be made available for uses that accord with these principles: primary purpose and use, nature and uniqueness, scale, and nature of Google’s involvement.” Focusing on “(2) Avoid creating or reinforcing unfair bias”, Google understands the potential bias resulting from the AI algorithms and datasets that are utilised, where different cultures and societies around the world will live by different norms and conventions. With that being said, as AI algorithms become more sophisticated and datasets continue to grow in size, controlling and regulating them will be correspondingly more challenging.

Going one step further, Google AI (n.d.) adds that they will not intentionally develop or implement AI applications in the following areas: “(1) Technologies that cause or are likely to cause overall harm; (2) Weapons or other technologies whose principal purpose or implementation is to cause or directly facilitate injury to people; (3) Technologies that gather or use information for surveillance violating internationally accepted norms; and (4) Technologies whose purpose contravenes widely accepted principles of international law and human rights.”[9] Reflecting on the aforementioned points, Google emphasises protecting their users from harm while not infringing international law and human rights in reality and cyberspace. This particular case highlights that even though Google is undoubtedly one of the global powerhouses in the hi-tech arena, they still have

an immense responsibility of ethical practice in the utilisation of technology – if not, one of the greatest responsibilities.

Furthermore, Marvin Croy (2003), Professor of Philosophy from the University of North Carolina in Charlotte, argues that philosophy is developing into an interdisciplinary field more than ever. Particularly with the inevitable widespread use of computers worldwide, Croy suggests that the methodology used in philosophy is becoming more empirical – based on experience and observation rather than logic and conceptual theories. As a result, the coming generations of philosophers will transform how philosophy is taught and learned. Detailed simulations will allow philosophers to test their theories and make more sophisticated predictions based on large amounts of data contextualised in an interdisciplinary approach.[10] Regarding the future of cyberphilosophy, Moor and Bynum (2002) believe that computing technology will continue to catalyse philosophical activity in the future more than any other discipline of science and technology. The main reason behind this bold prediction is the high rate at which computing technology is advancing, in addition to the exponentially increasing interconnectivity between humans and computers. A philosophical framework is needed now more than ever for individuals, enterprises, and states to refer to and reflect upon in tackling social and ethical issues related to technology. There exists a common misconception that cyber-related issues are the sole responsibility of technical IT experts. However, non-IT experts play an equally important role in providing expertise to contextualise the issue with specific domain knowledge. In addressing the key research questions of this book, experts in philosophy, sovereignty, and diplomacy are also needed to develop a more complete understanding of the context of philosophy and international relations.

The first level of philosophical inquiry in this book will explore the ontology of cyberspace. Ontology is a branch of metaphysics concerned with the nature and relations of being, dealing with abstract entities or things that have existence.[11] Therefore, the following section will assess the nature of cyberspace in terms of existence and being. Rebecca Bryant (2001), in "What Kind of Space is Cyberspace?", starts with the definition of the keyword: "Space is the three-dimensional medium in which all physical things exist."[12] Bryant compares physical space and cyberspace, linking their similarities in terms of place, distance, size, and route. However, although these former characteristics are indeed an extension of physical reality, they are still considered arbitrary in cyberspace. "Cyberspace represents the new medium of communication, electronic communication, which is fast outmoding, or even replacing, more traditional methods of communication."[13] Despite this journal article being published 20 years ago, back in 2001, McLuhan (1964) and Bryant (2001) already reflected that electronic communication was inevitably replacing traditional communication. Letters were being replaced by emails, physical journal articles were being replaced by online texts, and basically, everything paper was being gradually replaced by electronic means. McLuhan (1964) further emphasised that "the medium is the message", implying that the medium (print, visual, musical, etc.) determines how a message will be perceived.[14] Moreover, McLuhan and Powers (1992) also coined 'The Global Village', whereby the world was seemingly evolving into a small world of itself through the utilisation and ecosystem created by technology.[15] In the last 20 years, methods of electronic communication have come a long way. Instant messaging and social media platforms allow us to stay globally connected with one another at any time of the

day – cyberspace never sleeps. The speed at which information is distributed across the world is essentially instantaneous. Moreover, the electronic content being shared and distributed has evolved significantly. Expanding from mere texts, now audio, video, and endless other forms of media content are able to travel through cyberspace. Both the size of these electronic objects and the speed of their delivery are increasing exponentially.

By questioning the nature of the existence and being of cyberspace, a comparison is drawn where physical objects exist in physical space, while cyber objects exist in cyberspace. Bryant (2001) then "explores aspects of the new spatial relationship between cyber objects and cyberspace. Are physical space and cyberspace roughly equivalent concepts? Can we relate traditional philosophical arguments about physical space to cyberspace? And do these arguments tell us anything about the nature of cyberspace?"[16] These ontological inquiries are fundamental in developing a true understanding of cyberspace, as well as the objects that exist within it. When considering sovereignty and diplomacy in cyberspace, the domain of definition for the latter must first be clearly established. Sovereignty and diplomacy in the physical space of reality concern the state as a physical object and the dynamics of international relations. However, when specifically looking at these interactions within cyberspace with their equivalents as cyber objects, how do we translate their corresponding relations in terms of space and time? Bryant (2001) explores several theories that apply in physical space (substantival, relational, Einsteinian, and Kantian) to characterise cyberspace, to some extent, with those same concepts.[17] From a philosophical standpoint, the nature of space can be discussed from two schools of thought: Netwon's substantivalism and Leibniz's relationalism.

Based on these philosophical pillars of substantivalism and relationalism, where exactly does cyberspace lie? Moreover, how can we extend these principles into the international governance and regulation of cyberspace? Moreover, Bryant also refers to Einstein's Special Theory of Relativity, "Einstein's work shows us not only that space and time are, in a fundamental sense, observer-dependent, but also that space and time must be treated together, rather than as two separate mediums."[18] Bryant (2001) concludes that "Despite the differences, cyberspace is, in one way, intimately connected with the physical world. Cyberspace depends, for its very existence, on hardware and software, cables and routers—it depends on physical objects existing in physical space. Moreover, of course, this intimate connection between the two also represents a fundamental difference – physical space, if it exists, depends on nothing at all."[19]

Transitioning from the ontology of cyberspace, where we questioned, "What is cyberspace?", we now move to the epistemology of cyberspace, which focuses on "Why?", "How do we know what we know?" and "What are the implications of what we believe?" Schaefer (2009) begins by quoting the second law of blissful ignorance: "Inside every small problem is a large problem struggling to get out."[20] In the context of computer security, non-IT experts, for the most part, have little understanding of how deeply interconnected individuals, organisations, and states truly are. From the perspective of mere consumers of technological products and devices, we only see what is on the user-end and believe in what we think is apparent. Unfortunately, most of this sentiment lacks validity, for the very fact that cyberspace and the concept of cybersecurity or computer security, is seemingly intangible. Indeed – mobile devices, computers, and other technological infrastructures are tangible hardware. However, what consumers

do not see are the infinite volumes of data and information being transmitted around the world via an “invisible” global network.

Furthermore, with the emergence of cloud technology, Virtual Private Networks (VPNs), and automated bots, deciphering where and whom these digital bits are being sent from becomes exponentially more complex. Ironically, as the current generation further undergoes a digital transformation from all aspects – the human dimension is lifted to a level of paramount importance in ensuring the safe, secure, and ethical practice of interacting in cyberspace. Human core values and morals of trust and integrity are the only pillars that can truly protect us from cyber threats and attacks, just as they do in reality. The only changed variable at play is the medium of interaction – cyberspace.

States must realise that collectively developing an all-encompassing global governance framework that would address all challenges of cyberspace while simultaneously catering to their respective contrasting needs and expectations is close to impossible. International organisations such as the United Nations (UN) contribute significantly to issues of global importance by bringing together states for the peaceful resolution of controversial international matters. However, no matter how sound or ideal these mediations and regulations might be on paper, implementation and enforcement are the largest obstructions to reaching the ultimate goal of conflict prevention and resolution. As such, it must be reiterated that states, as a representation of the core values, morals, and ethics of their governing bodies, must be relied upon to act harmoniously with other states. Cultural and ideological differences are inevitable, but focusing on the moral conditions of states in cyberspace could go a long way in preventing and alleviating international conflict. Michelfelder (2000) argues that just like the weaponisation of modern technology in World War II, cyberspace technology: “dramatically divorces our moral condition from the assumptions under which

standard ethical theories were first conceived."[21] This claim is based on German Philosopher Hans Jonas' "ethics of responsibility". Throughout his paper, Michelfelder (2000) explores the impact of cyberspace technologies on our power of causal efficacy, as well as on self-identity. Consequently, a new paradigm of global cyberspace ethics must be developed collaboratively, if states wish to reach a mutual understanding of what exactly is right or wrong in cyberspace. Ethics and morals allow states and global governance entities to step away from this complex technical debate and rely more on a framework of trust and mutual understanding based on recognising each other's foundational differences.

Now that we have discussed the philosophy of cyberspace, we will transition into how the traditional concepts of sovereignty have evolved due to increasing integration into cyberspace. Sovereignty in cyberspace goes beyond our understanding of borders and jurisdictions in the traditional mediums of land, sea, air, and space, where physical and digital layers now overlap in complex and abstract dimensions.

Chapter 3: Cyber Sovereignty

Traditional Sovereignty

Sovereignty can be viewed from several perspectives. Sociologists explain sovereignty as "a shared cognitive map that facilitates but does not determine outcomes."[22] International lawyers stem the definition of sovereignty back to the fundamentals of realism, where states are the foundational components in international relations. "These states are sovereign in the sense that they are judicially independent and can enter into treaties that will promote their interests as they themselves define them."[23] Political scientists consider sovereignty to be merely an assumption in the analysis of international relations, further supporting the image of realism, "where states are assumed to be rational, unitary, independent actors."[24] Although too many external factors are involved in assuming so, this conceptual framework aids states in decision-making at the international level.

Sovereignty can be categorised into four different pillars: interdependence sovereignty, domestic sovereignty, international legal sovereignty, and Westphalian sovereignty. Interdependence sovereignty focuses on the government of an individual state, having control over the mobilisation of goods, capital, people, and ideas in and out of its national borders. Domestic sovereignty describes a state's national framework of authority and its corresponding efficacy in control over domestic affairs, whereas international legal sovereignty concerns independent territorial entities being juridically recognised states. Meanwhile, Westphalian sovereignty describes the autonomy and independence of domestic authority structures without intervention from authoritative external forces. The

dilemma arises when political entities are independent in practice, but the very rules that are being enforced might have been established by an external entity. With the four aforementioned pillars of sovereignty being mentioned, it becomes apparent why absolute sovereignty or an agreement between states on the recognition of each other's sovereignty is a tricky issue in the global context.

Krasner (2001a, 2001b) provides numerous cases of problematic sovereignty around the world. The aforementioned examples highlight the challenges of a state's territorial sovereignty by various ambiguous definitions, which has been going on for decades, and even centuries in the cases of others. In the extension of this complex debate regarding territorial sovereignty, the issue pertaining to cyberspace sovereignty is rapidly emerging and exponentially more complicated. However, the root cause remains the same – individuals, states, and international organisations will always face disagreements regarding global governance due to clashing ideologies. These ideologies, in some cases, stem from a state's culture and history, which is deeply ingrained into the mindset and behaviour of respective states.

On the other hand, narratives of global governance are often manipulated and strategically framed to meet the national agenda of states during a specific time. Krasner suggests that "Conventional rules of sovereignty are the default when actors are unwilling to use force or cannot make unilateral or multilateral commitments to different institutional arrangements, and these alternatives are more likely to be durable if they are the result of voluntary initiatives rather than coercion."[25] To contextualise, even if rules were to be established concerning cyberspace sovereignty, they would only be effective if states agreed to conform voluntarily, not by coercion. Given the unfamiliar nature of cyberspace, states

have even more reasons to claim that the grounds for conforming to these rules are uncertain and insufficient.

Regarding the conceptualisation of sovereignty, Heller and Sofaer (2001) mentioned that: “The concept of sovereignty is not a set of established rules, to which states must bend their conduct in order to preserve their capacities. It is instead an ever-changing description of the essential authorities of states, intended to serve rather than control them in a world that states dominate.”[26] This perspective is a reminder that the concept of sovereignty, no matter by which definition, is more of a guideline than an absolute determination. Furthermore, the nature of state authorities is dynamic, evolving over time and dependent on varying contexts between nations.

Furthermore, there are multiple variable constraints at play. Given the numerous universal definitions of sovereignty, time plays a significant role in the relevance of the former. These aforementioned concepts of sovereignty in themselves are not majorly constraining; however, they indeed give rise to behavioural patterns that lean towards certain concepts more than others. These tendencies can stem from a nation’s culture and ideology or even the vision and mission of a particular individual or organisation. These underlying factors highlight the difference between sovereignty as a concept, in contrast to domestic and international law as a practice. “In sum, absent voluntary initiatives or coercion, the conventional bundle of sovereignty rules is the default. These rules constrain options in situations in which neither coercion nor cooperation is viable. Nevertheless, rulers can devise innovative solutions, and these solutions can work, especially if they are the results of voluntary agreements that establish equilibrium outcomes.”[27] Upon exploring the various perspectives, definitions, conceptualisation, and variable constraints of sovereignty, one can understand the

problematic nature of sovereignty around the world. The complexity of sovereignty creates ideological and legal disagreements within and between states when it comes to national authority and control. Sovereignty in cyberspace reflects the same problematic challenges as in the traditional territorial sense. In today's digital world, states and international organisations need not only legal, political, and academic experts in sovereignty and international relations but Information Technology (IT) experts who understand cyberspace at the technical level to contextualise sovereignty in cyberspace. The conventional frameworks of territorial sovereignty cannot be fully applied in this case without a true understanding of the interactions and environment of cyberspace. Lawyers, politicians, and academics without technical expertise in IT might lack crucial knowledge about cyberspace, which could have major impacts on their decision-making regarding sovereignty and international relations.

Sovereignty in Cyberspace

Ayers (2016) breaks down her discussion of "Rethinking Sovereignty in the Context of Cyberspace" into three parts: (1) Policy, (2) Strategy, and (3) Theory and Operations. Based on a series of workshops run by the Mission Command and Cyber Division, Center for Strategic Leadership, United States Army War College, in collaboration with the United States Cyber Command and United States Army Cyber Command, some of the key findings and recommendations are as follows: enforcing cyber sovereignty, protecting Critical Infrastructure, identifying security standards, developing cyber international law and norms, and emphasising cyber education. In line with the aforementioned findings and recommendations, themes for future follow-up workshops were also suggested: "critical infrastructure", "international law and norms", "public/private sector – risk analysis and prioritisation", "cyber theory", "diplomatic statement and communication strategy to publicise US position on cybersecurity and incidents",

"cyber education and workforce recruitment and retention", and "cyber maneuver warfare".[28]

Schia and Gjesvik (2017) highlight that cybersecurity refers to the actual protection of infrastructure and processes related to the Internet, while cyber sovereignty entails more of the information and content that flows through the Internet.[29] The Chinese Cyber Sovereignty Concept is based on the unwanted influence of a state's "information space" and the transition of internet governance from academics and companies to international entities (Lindsay 2015).[30] China's perspective regarding cyber sovereignty aims at protecting its citizens from ideas and opinions that would be considered detrimental to their society. Furthermore, China's standpoint on global internet governance would shift power to states rather than individuals or companies.

On the other hand, Segal (2020) also framed "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace", evaluating the effectiveness of Chinese domestic policy and diplomacy on the Internet. China's initiative in the cyber sovereignty arena is argued to ultimately result in a less open and free internet. The concept of cyber sovereignty aims to address the associated challenges of an unregulated or underregulated internet. Therefore, the reason for the ideological debate is evident – fighting for a free and open internet, but at the potential expense of "the spread of disinformation, threats to privacy, and concentration of economic and political power by technology firms."[31]

Freedom House created an infographic, "Rising Cyber Sovereignty Threatens to Further Splinter the Internet", by depicting the movement by governments on restricting the flow of information across national borders, scaled from "more

open internet" to "more closed internet" (Repucci 2020). The European Union (EU), India, and the US fall under the category of "more open internet". Hong Kong, Russia, Turkey, and Vietnam are categorised in the mid-range, between "more open internet" and "more closed internet". Finally, China and Iran are categorised as having "more closed internet".[32] Although these evaluation criteria might be arbitrary and argued against, they still provide a useful visual and conceptual representation nonetheless.

The divergence between opposing national views on cyber sovereignty is clear: an open or closed internet. However, global consensus on any form of sovereignty will always give rise to contrasting and conflicting perspectives, which are sometimes irreconcilable. As with all other forms of sovereignty, diplomacy will be key to mediating mutual understanding between nations concerning cyberspace.

Chapter 4: Cyberdiplomacy

Modern Diplomacy

In the context of international relations, diplomacy refers to political interactions between a diverse range of actors and representatives of different nations. “Track 1” diplomacy involves professional diplomats such as government officials, whereas “Track 2” diplomacy involves non-governmental actors such as scholars, athletes, or even regular citizens. Traditional forms would include economic diplomacy or cultural diplomacy. Many factors influence the behaviour and actions of a nation when it comes to dealing with bilateral or multilateral relations. Localisation, regionalisation, and globalisation contribute towards the evolution and transformation of diplomacy.[33] However, at the end of the day, diplomacy comes down to easing tensions and strengthening relations between nations, considering all push and pull factors at the local, regional, and global levels.

Representation and communication are the two main processes involved in diplomacy. International actors interact and behave differently towards each other, depending on their political agendas and own interests. Therefore, it is of great importance for these actors to establish political ties around the world, to represent and communicate their national interests with others. Furthermore, change and continuity are both key influencers of diplomatic activities. Governance becomes more complex due to the increased interconnectivity and interdependence across different levels. International structures such as diplomatic services and networks allow representation and communication through the aforementioned political channels.[34] However, increased globalisation over the years has challenged the existing framework for traditional

diplomacy. From traditional state-to-state interactions, modern diplomacy now takes place on different platforms and through different channels.

Diplomacy is rapidly evolving with the advancement of digital technologies. Just as new technology is disrupting all sectors, from the way we distribute information, the way we receive information, and the way we interact with each other. In the big picture of international relations, these fundamental processes and interactions completely transform the landscape in which diplomats and world leaders communicate and interact. For example, social media platforms act as channels for communications and vast sources of both relevant and fake news in real-time. The field of modern diplomacy and international cooperation has been completely shaken by the use of social media platforms and is continuing to change significantly as diplomats become more comfortable and accustomed to utilising them in diplomacy. This new form of interaction in diplomacy will result in both positive and negative impacts in dealing with international relations.

International Relations in Cyberspace

Choucri and Clark (2019), in "International Relations in the Cyber Age", discuss the "layer model" as a framework of layers and actors to analyse international relations in today's context of cyberspace. The layers include people, information, application, servicers, internet, and physical. On the other axis, the actors include the net, businesses, citizens, NGOs, illegitimates, providers, suppliers, standards, international policy, and governments.[35]

This matrix of classes allows for the analysis of specific layer-actor combinations. Regarding analysing international relations in cyberspace, this layer model is beneficial for pinpointing actors and activities in the different layers of interaction. Furthermore, patterns can be observed about which layers are more

concentrated with the activities of a certain actor. These activities could even span several layers, showing more of how cyberspace is structured. From a big-picture perspective, rather than just focusing on one interaction, the model emphasises the interconnection of layers and interactions. Therefore, the transformations of a system can be easily tracked and traced back to its causal variables. In such a complex crossover between the physical and digital world, actors, platforms, activities, and interactions within cyberspace must be structured clearly. As it is already challenging to compare tangible and intangible factors, establishing a clear flow of interactions will result in more effective conclusive linkages.

So how does this integrated system affect the analysis of traditional international relations? The different horizontal layers and vertical levels of the constructed matrix create a structure format, to begin with. Levels, in this case, include individual, state, international, global, non-profit, and profit-seeking.[36] The integrated system is as follows:

However, changes in cyberspace over time will question users of the matrix and whether certain activities are appropriately positioned in their cells. These new and different scenarios concerning international relations and cyberspace will make the model more robust based on the construction of our evolving knowledge. Although this model represents a specific point in time, it considers all key factors and is flexible and open to change over time. This phenomenon is coined by Choucri and Clark (2019) as “The Co-Evolution Dilemma”. As the Internet is evolving at an exponential speed, rules, regulations, and policies are not able to catch up. This dilemma significantly impacts the concept of power and politics in cyberspace. Due to the possibility of digital interactions, the balance of power between traditionally weak and strong actors has been completely transformed. Individual hackers can threaten entire states, private companies like

.

Facebook and Google have more power than governments, and cyberspace blurs international boundaries – this new reality is disturbing.

In conclusion, although the traditional concepts and philosophies that underlie international relations still apply, the types of interactions have changed drastically in the cyber age. Cyberspace is a complex structure, interconnecting and overlapping the physical and digital world. Simply fitting today's cyber interactions into outdated models or theories of international relations analysis will not suffice. In order to effectively analyse contemporary issues of international relations, new models must be used that consider the different layers and levels of cyberspace.

Based on the infographic created by EU Cyber Direct (2018), cyberdiplomacy aims at "preserving a free, open and secure cyberspace as the backbone for modern societies". The concept of "free" refers to "the promotion and protection of human rights and fundamental freedoms in cyberspace", while "open" refers to "the promotion of universal, affordable and equal access to the internet", and finally, "secure" refers to "the strengthening of cybersecurity and improving cooperation in fighting cybercrime". In recent years, states have increased their censorship of the internet (23% of states in 1993, compared to 37% in 2017), with 3.9 billion people having used the Internet by 2018 – this number continues to grow significantly, as a result of inevitable digital transformation around the world. However, the frequency of cyber threats and attacks has increased correspondingly. In 2017, the NotPetya and WannaCry attacks alone infected over 300,000 computers in over 150 countries, resulting in $4 billion in economic damages.[37] Risks, threats, and attacks related to cyberspace will continue to rise unless states recognise the severe consequences of such a deeply interconnected global network. As such, initiatives such as EU Cyber Direct (n.d.) have been

established to conduct policy research and capacity building in cyberdiplomacy related to international cyberspace law and governance, cyber norms, and confidence-building measures.[38] Cyberdiplomacy will play an increasingly important role in preventing, deterring, and managing cyber threats and attacks, both domestically and internationally.

Deterrence is a key policy component in managing attacks in cyberspace in the context of cybersecurity. The main challenge stems from the lack of consensus by nations to agree on behavioural norms and protocols, further amplified by the increasing amount of cyber-criminal entities. As such, deterrence policies require a rule-based system to assess behaviour, detect infringements, and respond accordingly to deviances. “Generally, cyberspace deterrence strategies seek to influence an adversary’s behaviour, discouraging them from engaging in unwanted activities. In contrast, denial strategies endeavour to improve technology, process, or practice so that despite adversarial ventures, a cyberattack might have a low rate of success” (Jaikaran 2022). Denial strategies seem to have had a significant impact in lowering the success rate of cyberattacks, as the defence mechanism is self-dependent. However, attempts at deterrence have not been as successful, as they depend on influencing the behaviour of malicious actors instead – which are abundant in the limitless cyberspace. As such, a balanced approach of deterrence policies and denial strategies should be implemented to strengthen cyberdiplomacy efforts from both sides. Theoretically, concepts of cyberdiplomacy may be suggested as a tool to relieve geopolitical tension underlying cyberspace. However, real-world phenomena often stray far from theory. Therefore, theory must be met with reality, with the US-China rivalry in cyberspace as the prime example of cyberdiplomacy.

Chapter 5: US-China Rivalry in Cyberspace

The growth of interconnected global cyberspace and the rise of cyberespionage have intensified geopolitical relations between China and the US. In such an unfamiliar and rapidly evolving arena for international relations, how do states and international governing entities draw the intangible boundaries of global cyberspace? The fierce geopolitical rivalry between China and the US is based on trade and security, with military, political, and economic pillars as the foundation of this superpower competition. Advancements in digital technologies and the exponential increase in their adoption further drive this ideological clash of sovereignty, heavily influenced by the China-US technological rivalry.

In the context of traditional territorial sovereignty, not only territories in terms of land but also in terms of the seas bring about challenges to sovereignty. Linking back to the China-US rivalry, the South China Sea (SCS) dispute has been a contentious topic of geopolitical debate for many years. The main dilemma arises from the attempt to translate international land boundaries into international sea boundaries. The "territorial sea" describes a nation's sovereignty at sea as an extension of its sovereign land. Although the concept of Mare Clausum and Mare Liberum has been around for hundreds of years, nations are still disputing their claims of the sea. This age-old debate reflects the disparity of clashing ideologies between different states, whether the territories should be "free" or "closed", "sovereign" or not.[39] Fast-forward to the digital era of today's generation, an all-too-familiar dilemma arises from the inevitable adoption of digital platforms and applications, not only as a normalised form of interaction but as a way of life. Mobile devices have transformed into extensions of the human body and mind, converting almost everything we own physically into digital information, deeply rooting us into cyberspace, both in terms of space and time. The more

interconnected the physical world becomes with the digital world, the more pressing the issue becomes of establishing boundaries and reinventing the concept of sovereignty in the context of cyberspace.

Over the recent years, incidents of cyber espionage have significantly increased between China and the US. China's anti-access/area denial zones and its disagreement with the US model of internet governance are attributed to China's rapidly advancing military and technological power. Although research and development in the technology sector often stem from economic objectives, these developed findings create an equally significant impact on national security, creating fear from the misuse of powerful emerging technologies in the form of cyber espionage and attacks on Critical Information Infrastructure (CII). Moreover, mutual allegations of cyber espionage can lead to mistrust. In a nutshell, the fear of being spied on through cyberspace triggers the insecurity to spy on the other party. In addressing this problem, China-US vested interest should lead to cyberspace collaboration.

In 2015, China and the US attempted to ease tensions by coming to an agreement on cybersecurity and interactions within cyberspace. The 2015 Agreement between China and the US had the following objectives: "(1) Respond to requests for information and assistance for malicious cyber activities. (2) Investigate cybercrime emanating from the signatories' respective territories. (3) Exchange information on the status of the aforementioned investigations. (4) Refrain from conducting or supporting cyber espionage for economic purposes and theft of intellectual property. (5) Make efforts to identify and promote international norms of state behaviour in cyberspace. (6) Create a high-level joint dialogue

mechanism for fighting cybercrime and related issues. (7) Create a hotline to discuss issues related to cyber activities."[40]

The aforementioned objectives were mainly established to prevent acts of economic cyber espionage through cyberdiplomacy initiatives between China and the US. The reason is that cyber espionage can be carried out for national security or economic purposes. In other words, both states recognised their ongoing tension related to cybersecurity and interactions within cyberspace. As a result, China and the US conducted cyberdiplomacy activities to reach a bilateral agreement to reconcile their opposing views on international cyberspace governance. In the geopolitical context, national security will always be a top priority with high sensitivity. Therefore, China and the US came to an agreement on at least deterring economic cyber espionage from the two types. However, nations could justify that their cyber espionage campaigns targeted at businesses or companies are for national security reasons. The main fear was misinterpretations of cyberattacks as acts of hostility or confrontation from one nation to another. Furthermore, conflict in cyberspace could eventually escalate into potential warfare, in reality, if not appropriately monitored and carefully mediated. Surely enough, acts of economic cyber espionage decreased between China and the US after the 2015 bilateral agreement. However, alleged national security cyber espionage still occurred and resurfaced during the South China Sea dispute, where involved US technology firms were targeted. This cyber espionage campaign highlights the inevitable link between geopolitical tensions and interactions within cyberspace.

Due to rising tensions between China and the US, a narrative arose that Chinese hackers associated with the Chinese government allegedly aimed at US technology firms contracted under the US government or maritime agencies

related to the South China Sea dispute. Furthermore, bilateral relations between China and the US have recently worsened, in both the physical world and cyberspace, simultaneously. The China-US trade war exposed the feeling of mutual insecurity from each nation, portrayed by the back-and-forth trade sanctions.[41]

When discussing the geopolitics of emerging technology, it would be unusual not to mention the ongoing US-China technological rivalry. The US and China exemplify the highest level of international tension between the two states as a result of their technological advancements and innovations. Although the ultimate purpose of these technologies might be for economic development and social impact, one cannot ignore the possible weaponisation and misuse of powerful and misunderstood tools. Furthermore, the US and China are also amid "Chip Wars", battling for semiconductor supremacy, while Taiwan Semiconductor Manufacturing Company (TSMC) offers the most advanced technology that can produce a chip of 2 nanometers by the end of 2021. It is worth noting that Rare Earth Elements (REEs), as both crucial components for a majority of technological hardware and infrastructure, further fuel international tensions and impact global commerce. Therefore, as the US and China continue to develop AI, 5G, and other forms of emerging technology for seemingly peaceful and beneficial purposes, they will continue to create fear and uncertainty amongst states in the geopolitical arena. At the end of the day, no matter how advanced and automated these technologies might be, there will always be a "human in the loop" or an invisible hand controlling them behind the scenes.

Another pressing technological conflict in the geopolitical arena is the rise in demand for semiconductors. Semiconductors found in computers, phones, cars and more are an integral underlying technology for computing in today's world.

China has spent hundreds of billions of dollars to catch up with the US in recent years, surpassing the US in terms of share of global semiconductor manufacturing capacity before 2020. China takes a "whole of society" approach with their national chip industry: subsidies and zero-interest loans to disseminate Chinese technology internationally, promoting education such as Artificial Intelligence programs, and "civ-mil" fusion (civil and military interaction in the form of public-private partnership to develop and promote technology). Most advanced chips are designed in the US and the machines that produce those chips. The biggest customer of US-designed chips and chip machines is China. These chips are first designed in the US, then manufactured in Taiwan, Japan, and South Korea, shipped to China, assembled into endless products, and finally shipped worldwide (Foxconn, Apple, etc.) as part of an international ecosystem.

The global chip shortage has now lasted more than two years since the start of the pandemic. On 9 August 2022, the CHIPS and Science Act was signed into law by US President Joe Biden, providing $280 billion to domestic chip research and development, including $52.7 billion to processor manufacturers over five years. The CHIPS Act aims to boost US semiconductor productivity and dominance, shaken by Chinese, Taiwanese, and South Korean firms in recent years. However, results will not be immediate as these chip factories take years to build, and chip makers are more interested in investing in the most advanced manufacturing methods to remain competitive. As such, the effects of the CHIPS Act will inevitably be delayed. Furthermore, even with the CHIPS Act in place, it would not be feasible to move the whole electronics industry to the US – there are various other aspects of the supply chain to be considered. The Boston Consulting Group estimates $1 trillion to create self-sufficient semiconductor supply chains worldwide, with around $400 billion just for the US. All in all, splitting the electronics supply chain will not do the relevant nations any good. Trade barriers, such as those implemented during the Trump administration on Huawei, will hurt

the US in the long term by pushing Huawei away from US-made chips. Furthermore, US chip manufacturing factories in Taiwan and Korea remain in close geographical proximity to China, which will always create sentiments of insecurity for the US. The CHIPS Act, which started with provisions from the House Committee on Science, Space, and Technology, will play a pivotal role in reinforcing US economic and national security and ensuring that the US is equipped to lead in science and innovation.

The global chip supply chain is heavily intertwined between the US, China, Taiwan, South Korea, and Japan, and breaking it into smaller parts does not make sense. The nations involved must strike a sensitive balance between their respective geopolitical and economic interests. The global chip market has economic potential for all, and complete decoupling should be avoided at all costs. To address security concerns related to the militarisation of advanced chips, specifically tailored export controls could be placed only on the equipment that warrants these risks. Aside from that, the remaining segments of the global chip supply chain should be nurtured in a conducive environment for international trade and economic prosperity.

Furthermore, Kastner (2021) emphasises that "The value of frontier technologies is high. 5G alone is projected to generate $13 trillion in global economic value and 22 million jobs by 2035. And artificial intelligence is projected to add over $15 trillion to the global economy by 2030. That China and the United States have announced or are considering large investments in these fields sends a clear signal of the significant geostrategic role these technologies will play in the near future."[42] Although the potential for economic development and job creation is high, large state investments by China and the US create uncertainty related to

associated security implications. AI as an enabling technology is often compared to nuclear technology, as the weaponisation or militarisation of AI will drastically challenge national defence measures and international strategies of all states. Consequently, ethical practices and regulations are absolutely critical for the utilisation, distribution, and management of AI applications at the national level. The race to achieve global technological superiority plays an ever more significant role in the "tragedy of great power politics". Mearsheimer (2000) emphasises that states will continue to act according to "offensive realism" in the context of international relations and security, whereby conflict and competition between great powers for global hegemony will never stop.[43] Moreover, this ongoing technological war has continuously contributed towards US-China decoupling - whereby trade, investment, and the global supply chain has been severely impacted by deliberate measures from both sides.

The five most frequently used words were "sovereignty", "cyberspace", "state", cyber", and "internet". These statistics imply that the reoccurrence of key terminology shows their importance and relevance linked to the two fundamental research questions of this book:

1) How do we define sovereignty in cyberspace or "Cyber Sovereignty"?
2) How can we use diplomacy in cyberspace or "Cyberdiplomacy" to reconcile two opposing views (US – Internet Freedom, China – Internet Sovereignty) on international cyberspace governance?

Since the focus of this book is to offer a philosophical inquiry into sovereignty and diplomacy in cyberspace and the research questions above and examine Cambodia's emergent cyberdiplomacy, some of the most frequently used words were naturally: "sovereignty", "cyberspace", "state", "cyber", "internet", "diplomacy", and "nation". However, if we dive deeper into this textual analysis,

some other interesting key terms mentioned were: “internal”, “govern”, “territory”, “right”, “power”, and “control”. These terminologies emphasise the importance of an individual state’s right, power, and control of cyberspace in the local context, as well as its internal governance. Furthermore, territorial sovereignty as a fundamental international relations theory is considered a foundation for evaluating sovereignty in cyberspace – contrasting physical space with cyberspace.

From a philosophical standpoint, conventional international relations theories will always rely on the same principles of states interacting with each other based on their national interests and agenda for global trade and security. Realism, pluralism, and globalism are still very much alive, but the methods of interaction between states have evolved significantly. The ongoing transition from physical to cyber dimensions contributes to their increased overlap. As a result, these traditional concepts must be revisited and re-evaluated from a different perspective. States, diplomats, and international organisations must come to terms with this inevitable digital transformation, whereby all actors will continue to become more immersed in cyberspace in the future. A strong focus must be placed on the changing nature and environment of the geopolitical arena due to the explosive growth and adaption of emerging and disruptive technologies.

The US-China rivalry sheds light on the various geopolitical complications deriving from cyberspace related to sovereignty and diplomacy – with cyber governance at the epicentre of it all.

Chapter 6:
Geopolitics of Cyber Governance in the World, ASEAN, and Cambodia

Introduction

Cyberspace is considered the fifth battlefield in global affairs after land, sea, air, and space domains that can be deployed to destabilise rivals' politics, economy and security (Kolton 2017). The technological revolution has played a vital role in influencing almost every medium, including diplomacy and bilateral relations among states (Stanley and Olumoye 2013; Westcott 2008). During the Internet Governance Forum in 2019, United Nations Secretary-General Antonio Guterres stated that:

> 'Technological developments are unfolding at a speed with no parallel in human history……. Digital technology is shaping history (United Nations 2019).'

To date, there is no uniform definition of cyberspace around the world (Mbanaso and Dandaura 2015). Although it serves a large global community, the issue of sovereign demarcation or territorial boundaries for cyberspace remains debatable (Chang and Grabosky 2017; Deibert and Crete-Nishihata 2012). With the relatively new emergence of this realm, the chapter sets out to examine potential clashing areas among great powers surrounding political, economic and military rivalry. This chapter argues that political, economic, and military are the key areas that perpetuate global and regional division, specifically ASEAN context, while it also triggers state's responses individually due to the disparity among developed and developing states focusing on Cambodia.

Cyberspace

The emergence of the technology era and cyberspace took off mainly due to the proliferation of the Internet. Along with other technological advancements, the Internet originated in the US and Europe (Major 2000; Skoudis 2011). To be clear, the Internet here does not solely refer to cyberspace, but it plays a part in this domain. The ARPAnet, the first Internet network system, was introduced in the 1960s for military purposes and later altered for commercial usage. There is no doubt that this development has attracted many users and has transformed into a social norm (Major 2000). As mentioned, the Internet is only one element of cyberspace; however, it also encompasses computer networks, broadband, wireless, and sophisticated software. These create a merged environment for the computerised system, network, and communication (Skoudis 2011).

The International Organization for Standardization (ISO) defines the term 'cyberspace' as a "complex environment resulting from the interaction of people, software and services on the Internet using technology devices and networks connected to it, which does not exist in any physical form" (ISO 2014). The expansion of cyberspace also brings about consequences for cybersecurity when ill-intended individuals or entities conduct cyberattacks and other criminal activities (Willard 2015).

Split in Cyber Governance

At the international level, it is necessary to illustrate the United Nations' role in maintaining world peace and security. The same is right in the field of information and communication technology. During the 53rd session of the UN General Assembly in 1998, the UN began discussing cyberspace security, and, as a result, the United Nations Group of Governmental Experts (UNGGE) was formed without a permanent mandate to deal with such matters. In 2015, the UNGGE

report titled “Developments in the Field of Information and Telecommunications in the Context of International Security” was adopted and incorporated into the principle of sovereignty and the UN charter. Nevertheless, states can be perpetrators of cybercrimes committed against their adversaries, as seen from the accusation between the United States and China (Eichensehr 2014).

The uncertainty, scepticism and animosity between countries may have led to the lack of uniform action for global cyber governance. The current governance of this sphere has separated into two camps: state-led initiative backed by China and Russia, on the one hand, and multi-actors-led initiative backed by Western powers, namely the United States, on the other hand (Liaropoulos 2013, 2017). The state-led initiative aims to govern cyberspace through state power and emphasises less on Internet corporations such as Facebook, Google, non-state actors, and civil society groups because the responsibility to protect and maintain national security and sovereignty belongs to the central government (Barrinha and Renard 2020; Budnitsky and Jia 2018; Liaropoulos 2017).

On the contrary, the multi-actors-led initiative advocates that states alone cannot effectively control Internet usage. Therefore, cyberspace governance must be regulated collectively with non-state actors (Budnitsky and Jia 2018; Liaropoulos 2017). Furthermore, this model argues that the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit entity created by the United States to command the internet domain system, and the NETmundial Initiative (NMI), a multi-actors-led discussion forum for cyber governance, should help manage cyberspace (Carr 2015). Unfortunately, the rivalry between these two initiatives has fueled competition to the point that some have claimed it resembles the Cold War between the US and the former Soviet Union (Richards 2014).

Political and Legal Factors

Powerful states can use international law as a tool to pressure others to support their rules, regulations and practices (Zidar 2019). The aim is to continue their strategic predominance or maintain legalised hegemony (Simpson 2009). That is a reason why historical international laws and norms, such as the International Bills of Human Rights (UDHR, ICCPR and ICESCR), the International Investment Law, and the Responsibility to Protect (R2P), have been pioneered by Western countries potentially to protect their interest through shaping a global narrative, especially through the use of international law (Anghie 2005).

China and Russia, on the one hand, and the West, on the other, are highly vigilant about each other's foreign policy and activities. For China, Internet freedom is a Western hegemonic intent that interferes with its internal affairs (Shen 2016). In a speech at the opening ceremony of the Second World Internet Conference in 2015, Chinese President Xi Jinping highlighted the inequities and imbalances in cyberspace management, emphasising the principle of non-interference in internal sovereignty, which began with the hegemony of cyberspace. Historical controversies such as the Treaty of Nanking, which forced China to submit to the West, still linger in the minds of many Chinese leaders today (Cai 2019). The unequal treatment from the powerful states under the pretext of complying with international law serves their political benefits.

Military Factors

Cyberspace can pose a security threat, especially in the military field (Scullen 2019). The "security dilemma" and the arms race could be the basis for the two poles to disagree (Mbanaso and Dandaura 2015). The United States has developed and possessed offensive cyber capabilities. According to a 2018 report by the US Cyber Command, the US government intends to "achieve cyberspace

superiority by seizing and maintaining the tactical and operational initiative in cyberspace, culminating in strategic advantage over adversaries" (United States Cyber Command 2018). On the other hand, the National Cyber Strategy declares, "The United States will maintain an active international leadership posture to advance American influence and to address an expanding array of threats and challenges to its interests in Cyberspace. To maintain this leadership position, the United States has a policy of promoting openness to the Internet and against non-open states" (The White House 2018).

The United States' firm commitment to achieving superiority in cyberspace may have been linked to China's ability to conduct cyberattacks, especially for political and military advantage. Numerous reports indicated China's cyber capabilities. For instance, the attack on the US Chamber of Commerce, US Internet companies, and American Intellectual Property (IP) and supply chain information online are examples (Lai 2012). On the other hand, the US has also accused China of stealing classified military and technological secrets from major companies, such as Google and Amazon, infiltrating its electrical grid system in 2009, infecting computers and airport systems, and disrupting flight schedules (Hjortdal 2011). If these accusations are true, Chinese actions could significantly affect US national security through the cyber domain.

The United States' freedom of cyberspace principles is inextricably linked to its national security strategy and serves as a guiding principle for other foreign policy issues, such as cybercrime and counterterrorism efforts. All of this underscores Washington's intention to preserve its dominance and superiority in cyberspace. In 2013, Edward Snowden publicly leaked highly classified secrets that the US National Security Agency (NSA) had been monitoring and stealing information from the American public and citizens of other countries globally, including China (Shen 2016). China has claimed that the United States has engaged in cyber economic espionage against its domestic firms and leaders

(Baezner 2018). China claims that, in addition to having the world's most powerful military, the US has also developed the first offensive capabilities in cyberspace (Segal 2013).

Another view is that cyber espionage can be used to covertly steal military knowledge, which will increase one side's advantage over the other (Hjortdal 2011). Therefore, the protection of technological infrastructure, especially those used for the military realm, is crucial. Moreover, the crisis spurred by cyber espionage could lead to a military concern since the state spied on may view it as a provocative action, an aggressive behaviour, while the spying country may justify it as an action to deter or compel its adversaries (Kolton 2017). Therefore, it may cause misunderstanding and may escalate existing tension.

Economic Factors

The United States has acknowledged that China's offensive cyber capabilities are as capable as theirs (Mbanaso and Dandaura 2015). It also claims to have lost billions of dollars each year due to intellectual property theft and stealing of financial information by China (Baezner 2018; Ravich and Fixler 2020). US politicians have reacted by saying that cyber espionage for national security is still acceptable, but cyber espionage should not be done for economic purposes (Baezner 2018). Cyber surveillance for economic purposes also facilitates and accelerates economic modernisation. The United States, for example, has accused Huawei, one of the world's largest technology companies, of stealing trade secrets from its big tech companies (Ball 2011; Ravich and Fixler 2020).

If the allegations are true, cyber-surveillance spying for economic purposes could disrupt one group's business operations and increase the other group's rapid development. Besides, the competition for Huawei to control part of the submarine cables, which are a backbone for communication technology and

previously entirely under Western dominance, is also now under threat (Chhem et al. 2020). That is an issue that cannot be overlooked. Nevertheless, in the United States, spying on Chinese companies under the pretext of state subsidiaries is justified as cyber espionage for national security. Hence, what is the division between cyber surveillance and spying? For national security or for economic goals, where is it, and who determines it? This place seems ambiguous for US action (Baezner 2018).

Cyber Governance in ASEAN

Regarding the governance of cyberspace in Asia, particularly ASEAN, the region tends to uphold sovereignty in cyberspace management due to two factors. First, the Shanghai Cooperation Organization (SCO), which consists of China, Russia, India, Pakistan, and several other states, supports sovereignty in cyberspace management (Alcântara 2019). Second, the 3rd ASEAN Ministerial Conference on Cyber Security (AMCC) in 2018 reaffirmed the consensus in principle on the 11 voluntary norms or norms proposed in the 2015 UNGGE Report, highlighting the UN Charter and national sovereignty. On the contrary, the Asia-Pacific Economic Cooperation (APEC) also discussed strengthening cyberspace but proposed a solution in line with the Budapest Convention (Thomas 2009). At a glance, there seems to be no uniform approach to cyber governance in Asia with different groupings and interests.

There is a technological disparity among Asian nations, especially among the ASEAN states. It should be noted that technological infrastructure and Internet penetration into individual societies in Asia are not equal, and differences in political, economic, and market management systems may cause states in the region to adopt different approaches to cyberspace. For example, Japan and South Korea allow Internet freedom, whereas countries in ASEAN, such as Vietnam, Laos, Thailand, and Singapore, have adopted a strict approach to restricting and

controlling cyberspace (Thomas 2009). The gap and unreadiness among ASEAN members relating to cyberspace potentially limit the group's chance of having a regional guiding law or principles (Krisman 2013). With this, the uncoordinated response from this organisation had left them prone to open attacks that had happened before, such as operation shady RAT, which attacked the ASEAN secretariat, and various attacks on political figures and institutions (Heinl 2014). The lack of regional law for cyberspace may be linked with the reasons above relating to the unreadiness of member states and the concern about its use as a tool to achieve political, economic, and military goals (Chang 2017). Therefore, in the ASEAN context, precautions must be taken, mainly at the domestic level, to ensure that the organisation would not be caught in the middle of superpower rivalry and that it can leverage the interests of its respective members (Heinl 2014; Krisman 2013).

Some actions have been taken in the ASEAN frameworks. However, they mostly deal with member states' integration, tackling cybercrime, and terrorism, promoting cooperation, information exchange and promoting e-commerce, rather than in-depth discussions on cyberspace management (Noor 2015). In recent years, cyberspace issues have been mostly limited to cybercrime and terrorism in this region (Heinl 2014). Other initiatives, such as the ASEAN ICT Master Plan 2015, the ASEAN Digital Master Plan 2025, and the Master Plan on ASEAN connectivity 2025, however, have set out to exploit cyberspace mainly for its potential benefit, more or less focusing on commercial benefits and linkages (Chang 2017). Thus, by looking at the international and regional levels, technical factors, and concepts of practical governance, differences between the great power states may result in competition for global hegemony due to political, legal, military, and economic reasons. The competition has fueled non-traditional issues such as cybercrimes and attacks affecting ASEAN. Nevertheless, the sphere also brings about economic benefits for the organisation.

Cyber Governance for Cambodia

In Cambodia, the Internet user has increased significantly from about zero users in early 2000 to about 14 million users in 2019 (Willem te Velde et al. 2020). However, the development has brought about consequences not far from ASEAN counterparts, especially regarding politically motivated cyberattacks on key or political figures (CDRI 2020). On the one hand, this shows that Cambodia's cyber advancement and capabilities are limited despite its recent progress. To be precise, there are four main underlying problems for Cambodia's cyber development, including limited human resources, lack of awareness, underdeveloped critical cyber infrastructure, and insufficient capacity for this relatively new field (CDRI 2020; KOICA 2014). In response, the Cambodian government has been aware of the concerns and the importance of cyber technology and, therefore, proceeded to adopt various approaches as a countermeasure. First, the importance of cyberspace has been incorporated into the government's rectangular strategies phase four, emphasising the digital economy and a shift toward a technology-driven era (Willem te Velde et al. 2020). Second, Cambodia has put forward the Cambodian ICT Masterplan 2020 to tackle the mentioned problems (KOICA 2014). Third, it has recently issued a sub-decree on establishing the National Internet Gateway (NIG) to ensure national security and order in cyberspace, as stated in article 1 (Sub-Decree on Establishment of National Internet Gateway 2021).

Nevertheless, with the three key regulations in place, there is still scepticism about Cambodia's effectiveness and readiness. However, it should be noted that relevant ministries have taken part and are committed to developing cyber awareness and capability (Beschorner et al. 2018). To put it into perspective, the Internet only became available in Cambodia in 1997 (Minges et al. 2002). Therefore, it may not be appropriate to expect effectiveness overnight as progress requires resources and preparation that should be treated as a marathon, not a

sprint and not to mention the capacity differences between the developed and the developing nations (Muller 2015). Hence, although Cambodia's cyber capability is currently limited and prone to cyber-attacks, in the long run, with peace and stability, there will be an opportunity for the nation to create a conducive environment and an effective platform to develop skills, infrastructure and capability for the cyberspace as mentioned out in the rectangular strategies and the Cambodian ICT Masterplan 2020.

Conclusion

In conclusion, whether state- or multi-actors-led, cyberspace governance is driven by national interest, as reciprocal criticisms and complaints between the two competing models are potentially caused by the conflict of interests and hegemonic competition. Cyberspace is a new frontline where states compete for political, economic, and military gain. Given the lack of a unified legal framework to govern cyberspace at the international level, regional organisations and individual states are responsible for making this realm less anarchic.

Due to the fragmentation mentioned above, the following policy suggestions should be considered for possible convergence between the two blocks. First, in the global context, a possible breakthrough would be to support international organisations, particularly the UN and its specialised agencies like the International Telecommunication Union (ITU), to lead cyber governance simply because they are mandated to maintain global peace and security. International organisations may foster confidence and trust among states, especially in preserving sovereign equality and equal participation from all states following the UN Charter. This would also help limit the unequal projection of power by the big states, namely in creating legal norms.

Second, cyberdiplomacy should not be underrated. Aside from bringing cooperation and reducing tension, diplomacy can offer win-win solutions and benefits for all parties. Moreover, the transboundary character of cyberspace means that working together to some extent, if not all, is inevitable. Therefore, all relevant actors should turn this crisis into an opportunity.

Third, even with international organisations' supervision, parties involved should practice and strengthen global multilateralism to reduce scepticism caused by political, military, and economic factors. With asymmetrical power resulting from unilateralism, global solidarity will be further hindered, and the solution to the deadlock will still be far-reaching.

Fourth, at the regional level, there has yet to be a uniform legal framework for cyberspace governance. In a sense, the great power competition may affect ASEAN members' unity, and the organisation may be caught in a crossfire between the Internet freedom model and the cyber sovereignty model. Therefore, it is optimal for ASEAN to remain flexible and uphold its respect for international laws and principles. Hence, ASEAN members should uphold their consensus principles and adhere to the 11 voluntary norms for responsible state behaviours in cyberspace (proposed in the 2015 UNGGE Report) as agreed during the 3rd ASEAN Ministerial Conference on Cyber Security (AMCC) in 2018.

Fifth, with international uncertainty and regional governance of cyberspace yet to be agreed upon, Cambodia's establishment of the National Internet Gateway (NIG) may serve the purpose of protecting national security, especially from terrorism and cyberattacks. Nonetheless, the NIG merits a holistic and strategic assessment so that Cambodia can safeguard civil liberties and excise its due diligence and responsibilities stipulated under the 11 UN norms of responsible state behaviours in cyberspace put forward in the UNGGE's 2015 report.

Finally, as a dialogue partner of the Shanghai Cooperation Organization (SCO) and an ASEAN member, Cambodia has played an active role as a channel between the two regional organisations, which tend to strongly favour state sovereignty on the Internet. Hence, Cambodia should consider maintaining its stance that aligns with regional and international groupings to limit potential political friction with the groups and create a conducive opportunity for its cyber capacity building and technological development.

Chapter 7: Cambodia and Cyberspace Issues

Cybercrime-related issues are challenging for Cambodia to coordinate and respond (Beschorner et al. 2018). A study by CDRI (2020) on cyber governance suggests a large gap between the rapid adoption of new technologies and the capacity to take measures against consequent cyber threats. Clearly, there is a shortage of cybersecurity professionals in Cambodia, and even Prime Minister Hun Sen's Facebook account was hacked in February 2019, although he got it back a few days later with help from Facebook (Chheng 2019). During the COVID-19 pandemic, preventing fake news and misinformation from circulating throughout social media is another challenge the Cambodian government has addressed. Cybercrimes can happen anywhere, as perpetrators or so-called hackers, malicious insiders, cybercriminals, hacktivists, cyberterrorists, or industrial spies, have used varieties of hacking techniques tools via Phishing, Worms, Trojan Horse, Rootkits, Ransomware, DDoS, Spam, and Blackmail to commit cyber-enabled crimes and advanced cybercrimes. Amid the growing 80% of cybercrime incidents in Cambodia, the Ministry of Post and Telecommunication, in close collaboration with the Ministry of Interior, are strengthening existing laws related to cybersecurity in order to tackle cybercrimes in Cambodia, which are mostly result from Facebook, online money transaction, fraud, scam, and cyber extortion.

Inadequate Governance and Diplomatic Engagements

The cybercrime-related issues above are generally related to poor protection management systems, lack of adequate legal and regulatory frameworks, and limited human and financial resources. To tackle the growing threats of cyberattacks, Cambodia has established the Anti-Cybercrime Department, a specialised unit under the National Police of Cambodia, and Cambodia's National

Computer Emergency Response Team (CamCERT). Nevertheless, there is no law to regulate cyberspace in Cambodia, although the Ministry of Interior (MoI) is now reviewing the draft of a cybercrime law. However, this law mainly focuses on user protection from cybercrimes rather than national security (Nguon and Srun 2020). There is a law on telecommunications promulgated in 2015, but again it is to regulate the telecom sector rather than to protect users and the country from cyberattacks.

Furthermore, due to the nascent policy framework, there are a few joint efforts between private organisations and government ministries in Cambodia in managing and responding to cyber risks (CDRI 2020). Despite ASEAN's declaration to prevent and combat cybercrime in 2017, Cambodia has no clear cybersecurity strategies and no commonly shared legal framework in the region it can adopt to combat cybercrimes and strengthen cybersecurity (ASEAN 2017). That said, there are ways Cambodia can mitigate cyber risks, such as cyber hygiene, licensed software, physical security and Internet of Things infrastructure, highly trained digital talents, backup of data using physical hard drives, two-factor authentication, termination of unknown devices from active app sessions, and extra precaution towards suspicious digital correspondences.

Infrastructure Problems

With a high proportion of its young population, Cambodia is one of the most competitive mobile markets in the region, with 116 mobile-cellular subscriptions per 100 people, and almost half of its population has access to the Internet, mainly through mobile phones (ITU 2009). According to the United Nations' E-Government survey in 2020, Cambodia's E-Government Development Index (EGDI) has markedly improved in recent years, thanks to improved telecommunication infrastructures and engagement of citizens in decision-making through social media platforms (United Nations 2020). Being cognizant

of the importance of this digital technology, Cambodia fully supports the development of digital connectivity and a digital-led society and economy to achieve resilient and sustainable development. With the proliferation of Information and Communication Technologies (ICTs) and the advent of the "Internet of Things" projected to attract an exponential number of devices connected to the network, cyberspace and ICTs carry enormous potential for economic and social development across societies. However, their all-encompassing, ubiquitous nature and their growing political application pose increasingly significant risks to global economic value and international peace, stability, and security. As a result, cybersecurity has reached head-of-state-level attention and has become a major source of concern for policymakers, as it has been considered the fifth domain of warfare after land, sea, air and space.

Although ICTs provide opportunities for the country to accelerate social and economic growth, they come at a price. Considered one of the fastest-growing economies with annual GDP growth of about 7% for several consecutive years, Cambodia has rapidly expanded its use of ICTs. The number of connected users and devices in the country doubled from 4.9 million in 2017 to 8.4 million in 2019, which was half of Cambodia's current population. While these promising circumstances augur well for Cambodia, the rapid technological advancement could put the country at a higher risk of cyberattacks. For instance, a survey conducted in 2014 and 2017 by the Australian Strategic Policy Institute's International Cyber Policy Centre reveals that Cambodia is still facing problems with cyber awareness, infrastructure, cybersecurity expertise and international cooperation.

Way Forwards

1. Development of a Robust National Legal Framework

Currently, the main laws regulating cybercrime in Cambodia include the 2009 Criminal Code, the Press Law, the 2015 Telecommunications Law, and the new draft law on cybercrime. The 2009 Criminal Code deals with crimes such as infringement on the secrecy of correspondence and telecommunication, offences in the information technology sector, defamation and insult and lese-majeste violation against the monarchy. Meanwhile, the Press Law discourages journalists from spreading false information that affects the honours and dignity of others, as the 2015 Law on Telecommunications authorises the Ministry of Post and Telecommunications (MPTC) to manage telecommunication and ICT service data, clarify the roles and responsibilities of the Telecommunication Regulator of Cambodia (TRC), and specifies authorisation, licenses, fees, consumer protection. The law also prohibits actions affecting the general public and national security. The draft law on cybercrime is currently under inter-ministerial discussion and is led by the Ministry of Interior (Nguon and Srun 2020; Starkey and Y 2020). Likewise, the draft law on cybersecurity is being developed in accordance with the Cambodian government's Rectangular Strategy Phase 4, indicating that information security is a priority that supports the country's mitigation of digital risks.

According to the Cambodian Minister of Post and Telecommunications, the draft cybersecurity law is being discussed to ensure the sustainability of Cambodia's essential national services, national security, international relations, economy, public health, public safety and public order through the establishment of principles, rules, and mechanisms to prevent, manage and respond to cybersecurity threats and cyber incidents and the effective and timely protection of CIIs.

2. Engagement in Cyberdiplomacy

For geopolitical and economic reasons, Cambodia needs to balance the global and regional powers by strengthening its diplomatic relations with various actors. In cyberdiplomacy, it has indicated its support towards China by seeking a dialogue partner status of the Shanghai Cooperation Organisation (SCO) since 2015 and endorsing the Global Initiative on Data Security soon after China launched it in 2020 (Ministry of Foreign Affairs of the People's Republic of China 2020). Although Cambodia's foreign policy, which prioritises national sovereignty and non-interference in others' internal affairs, seems to align with China's state sovereignty model, cooperation and dialogues with other key players, such as Australia, the US, Japan, India, the EU, and fellow ASEAN members, would enable the country to foster its cybersecurity, engage proactively in international cyberdiplomacy, maintain its strategic autonomy, and opt for an optimal path towards global cyber governance that truly serves its national interest. In addition, Cambodia needs to adapt to the rapidly evolving nature of cyberspace, and national leaders need to pay more attention to cyberdiplomacy as it contributes to internal peace, stability, and credible projection of Cambodia's foreign policy credibility to domestic and foreign audiences.

Likewise, in response to the COVID-19 pandemic and the global rise in e-commerce, Cambodia has been fostering its cyberdiplomacy through the use of digital technologies and the Internet to engage in diplomatic dialogues and conferences organised overseas. However, the country needs to develop its ICT infrastructure further, both hardware and software. At the same time, a clear vision and a strong political will are required to develop a robust cyberdiplomacy, address its chronic low level of digital talent, and strengthen infrastructure to promote self-reliance and self-development in this critical sector. Moreover, since cybercrimes have become a prevalent national concern, Cambodia needs to strengthen its cybersecurity by raising public awareness, promoting cybersecurity

capacity building, investing more in cybersecurity, and developing a whole-of-government national cybersecurity strategy to secure its digital economy and bring more resilient and inclusive growth for all its citizens.

Chapter 8: Regional Capacity Building in Cyberdiplomacy

Introduction

For decades, sovereign states have operated and interacted with one another through air, sea, land, and outer space domains. In each of these domains, states have worked together through bilateral and multilateral fora to set international norms regulating their interactions in a legal, peaceful, open, and transparent manner to avoid armed conflicts and instability. However, the emergence of the Internet and the increasing prominence of cyberspace has forced states to respond to non-traditional types of threats and security risks posed by digital technologies and online activities, be they military, political, strategic, or commercial in nature. Meanwhile, the rapid development of the digital economy, ICTs, and IoTs have made lives more convenient and forged closer connectivity between states, peoples, communities, and individuals globally. Nonetheless, these new technologies present new challenges and risks to policymakers and diplomats whose primary responsibilities, among others, are to mitigate international security threats and promote harmonious relationships across nations.

As a developing country, Cambodia has rapidly embraced cyberspace and digital transformation in order to foster inclusive, sustainable, and resilient economic growth that benefits its citizens. The COVID-19 pandemic has accelerated Cambodia's adaptation and reliance on the digital economy and cyberspace-enabled activities, including government communications, electronic commerce, and financial transactions. According to one report, as of January 2022, Cambodia has 13.44 million Internet users, and its Internet penetration rate stood at 78.8% (Kemp 2022). Between 2021 and 2022 alone, the number of Internet users in Cambodia rose by approximately 177,000, indicating a steep and continuous increase for a small country of 17 million people (Kemp 2022). While these favourable circumstances enable Cambodia to accelerate social and

economic growth, technological advancement comes with a price, potentially putting the country at a high risk of cyber-related threats and issues. Studies reveal that Cambodia is still facing cyber awareness and infrastructure problems, which have become even more urgent given the ongoing strategic competition and competing political narratives between major powers over how cyberspace should be governed now and into the future (Chhem 2019; Corrado and Morokot 2021; Sang et al. 2022).

Due to the circumstances described above, countries in the region must equip their diplomats and foreign service officials with the knowledge and skills they need to operate effectively and protect their national interests in cyberspace. As a result, with support from China's Lancang-Mekong Cooperation Special Fund, the National Institute for Diplomacy and International Relations (NIDIR), acting as the project implementer under the Ministry of Foreign Affairs and International Cooperation (MFA-IC), has implemented a ground-breaking project titled "Regional Capacity Building in Cyber Diplomacy", which was approved in 2020 and ran between January 2021 to December 2022. The scope of this project covers three mainland ASEAN members: Cambodia, Laos, and Myanmar.

To address emerging security and non-security challenges posed by cyberspace, upon the recommendations and support of Dr Chhem Kieth Rethy (then Executive Director of Cambodia Development Resource Institute), NIDIR has put together this project to bolster awareness and skills among diplomats of Cambodia, Laos, and Myanmar in cyberdiplomacy, which refers to the use of diplomatic means to achieve states' interests in cyberspace. This project aims to build qualified diplomats for regional peacebuilding and economic development from the Mekong-Lancang countries in cyberdiplomacy.

Phase I: Research and Training Need Assessment

To achieve its goals, NIDIR implements the project in two phases and works closely with expert consultants from the Centre for Inclusive Digital Economy (CIDE) of the Asian Vision Institute (AVI), a policy think-tank based in Phnom Penh, Cambodia. First, NIDIR conducted an in-depth literature review on cyberspace and cyberdiplomacy to form an in-depth understanding of the existing cyber landscape, challenges, opportunities, and applications to contemporary international relations from theoretical and practical standpoints for the three Mekong countries. The literature review was completed in December 2021.

Then, NIDIR, in tandem with AVI experts, conducted a comprehensive internal training needs assessment (TNA) of approximately 70 mid-ranking and senior MFA-IC officials from across all general departments to gain a holistic understanding of the level of skills and knowledge currently possessed by Cambodian foreign service officials and their training needs. Key questions during the TNA process included (1) How crucial do you think cyberdiplomacy is in Cambodia's foreign policy and (2) What specific skills and subjects do you want NIDIR to provide?

Phase II: Training Design and Dissemination Workshops

Once the literature view and TNA processes were finished, NIDIR then proceeded to the second phase of the project on capacity building activities, which consisted of two elements: (1) training curriculum design and (2) a series of dissemination workshops. Concerning training curriculum design, NIDIR has been working closely with AVI to put together a comprehensive and holistic training programme based on the specific needs of MFA-IC officials highlighted in the outcomes of the TNA conducted in Phase I. The curriculum aims to incorporate in-depth presentations and lectures by cyberdiplomacy and

cybersecurity experts from in and out of Cambodia but peer-to-peer exercises, and various educational activities for trainees. The whole training programme will consist of five modules: 1) introduction to cyberspace and cyberdiplomacy, 2) cybersecurity and handling of diplomatic documents in the digital era, 3) global governance of cyberspace, 4) cyberdiplomacy, and 5) digital diplomacy. Each module will last five hours and be conducted by a different expert in a physical setting in Phnom Penh. As of this writing, NIDIR and AVI have finalised the curriculum and plan for the training, which will commence in the coming months.

In addition to training curriculum design for MFA-IC officials, NIDIR has hosted several major dissemination workshops with MFA-IC officials, policymakers, scholars, and relevant stakeholders across the Cambodian government to foster greater awareness about cyberdiplomacy, cyberspace, and cybersecurity. Each workshop galvanised significant turnouts with participants from various governmental ministries, academic institutions, think tanks, the press, and private companies. For instance, the first workshop was held on 12 August 2020 under the theme "Cybersecurity and Cybercrimes: Challenges and Solutions". The workshop intended 1) to raise awareness and meaningful discourses about cybersecurity strategy and cybercrimes and 2) to identify key challenges and opportunities. It targeted mainly MFA-IC officials with the rank of Director and above and consisted of two panels with distinguished guest speakers as follows:

- H.E. Dr Chhem Kieth Rethy, Minister Attached to the Prime Minister, Council of Ministers, Cambodia
- Mr Ou Phannarith, Director of ICT Security, Ministry of Post and Telecommunications, Cambodia
- H.E. Mr Prak Phalla, Advisor to Samdech Prime Minister Hun Sen, and Head of Data Digitization Program and ICT Management, MFA-IC, Cambodia
- H.E. Mr Chea Peou, Director of Anti-Cybercrime Department, General Commissariat of National Police, Cambodia

- Mr Sorn Chanrithy, Focal Point for Cybersecurity, MFA-IC, Cambodia
- Mr Chhem Siriwat, Director of CIDE, AVI

The second workshop took place on 23 March 2022 under the theme "Cyber Diplomacy: Enhancing Cybersecurity and Tackling Cybercrimes". Unlike the first workshop, this seminar galvanised around 149 participants from MFA-IC and the public, namely members of Cambodia's largest youth organisation, the Union Youth Federation of Cambodia (UYFC). Its purposes were to iterate the importance of global norm-setting mechanisms at the UN level and raise public awareness about cyber-related issues. The workshop invited a group of speakers from both the public and private sectors:

- Dr Alamgir Hossain, Professor of Artificial Intelligence and Vice President of Cambodia University of Technology and Science
- Mr Touch Ra, Cybersecurity Trainer at Proseth Solutions Co., Ltd
- H.E. Mr Chea Peou, Director of Anti-Cybercrime Department, General Commissariat of National Police, Cambodia
- Mr Sorn Chanrithy, Focal Point for Cybersecurity, MFA-IC, Cambodia
- Mr Ou Phannarith, Director of ICT Security, Ministry of Posts and Telecommunications, Cambodia
- Mr Bong Chansambath, Deputy Director of CIDE, AVI

Most recently, NIDIR hosted its third dissemination workshop on 24 August 2022 under the theme "Diplomacy in Cyberspace: Thriving through geopolitical storms". Given that major states are competing at the global level to try to advance their respective initiative to shape the governance of the Internet, this third workshop aimed to achieve two main goals: 1) To address the challenges of digital diplomacy and identify ways to optimise ICTs in diplomacy, and 2) to understand the challenges of global governance of the Internet. Unlike the previous two seminars, this third workshop targeted officials from various

ministries and executive agencies of the Cambodian government and key partners in the research and academic communities. With two panels on digital diplomacy and cyberdiplomacy, this third workshop hosted the following guest speakers:

- H.E. Dr Hing Vutha, Advisor to National Council of Industry, Science, Technology and Innovation, Cambodia
- H.E. Dr Tat Puthsodary, Advisor to Ministry of Commerce, Cambodia
- H.E. Mr Tean Samnang, President of NIDIR, MFA-IC, Cambodia
- H.E. Mr Chhem Siriwat, Director of CIDE, AVI
- Mr Bong Chansambath, Deputy Director of CIDE, AVI
- Mr Ou Phannarith, Director of ICT Security, Ministry of Post and Telecommunications, Cambodia

Together, the three dissemination workshops NIDIR has hosted since August 2020 have shed light on the importance of public awareness about cyberspace and cybersecurity challenges, how small states should navigate the contesting narratives about the global governance of cyberspace, what skills and knowledge diplomats in small countries need to have to operate effectively and securely at the national, regional, and international levels. Detailed concept notes and agendas of the three workshops can be found in Annex 3.

It is worth noticing that although NIDIR has initially planned to host physical dissemination workshops in partner Mekong countries, Myanmar and Laos, due to the outbreak of the COVID-19 pandemic and the unfortunate political circumstances in Myanmar over the past two years, it has been able to host workshops only in Cambodia for the time being.

In addition to the workshops mentioned above, NIDIR and AVI have worked closely together to promote public awareness about cyberdiplomacy and cybersecurity-related issues in Cambodia through several research papers. For instance, before the current project was approved, in December 2019, Chhem

Siriwat (2019), Director of AVI's Centre for Inclusive Digital Economy, published a paper on how Cambodia should prepare for cyberconflicts in the future, proposing that the Kingdom needs to raise awareness among policymakers and partake in regional policy discourses. Soon after the project was approved for implementation, the second paper was co-authored in February 2021 by Tean Samnang, then-President of NIDIR, and Phon Sokpanya, Advisor to NIDIR, under the title "Cyber Diplomacy: An International Cooperation Instrument for Cambodia in the Digital Age." This paper recognises that Cambodia needs to have a clear vision and political will to develop its cyberdiplomacy (Tean and Phon 2021). A few months later, Tean Samnang penned another paper to examine the geopolitics of the governance of cyberspace, which is partially incorporated as chapter 6 of this book (Tean and Ros 2021). These publications contribute to academic and policy discourses in Cambodia by identifying existing challenges, opportunities presented to Cambodia in cyberspace, and ways forwards.

Since cyberdiplomacy requires a whole-of-nation effort and approach, NIDIR has thrived to galvanise together experts from different disciplines and educational backgrounds and provide them with a national platform to engage in policy discourse and examine ways forward in the development of cyber diplomats in Cambodia and the Mekong region. Moreover, it is worth noticing that, to maximise the diversity and efficiency of its workshops, NIDIR has invited speakers educated in various countries, such as the United States, Australia, Italy, Cambodia, and Canada. This indicates that although China's LMC Special Fund funds this project, NIDIR has not been obligated by the donor in both substantive and logistical matters to involve speakers with an educational background in China. In fact, none of the invited speakers in all three seminars was educated in China. Because NIDIR has enjoyed complete autonomy in its decision and implementation of this project, it has made commendable progress towards fostering capable and qualified cyber diplomats in the Mekong region.

Conclusion

The emergence of cyberspace and digital technologies has posed serious security and non-security risks to small countries of the Mekong region. With support from China's LMC Special Fund, NIDIR has implemented the "Regional Building Capacity in Cyber Diplomacy" project since January 2021. As of today, the project has completed its first phase of research and continues to push towards the end of the second phase focusing on training curriculum design and dissemination workshops. With this ground-breaking project, it is hoped that diplomats from Cambodia, Laos, and Myanmar will be better equipped with the skills and knowledge they need to operate effectively in cyberspace and cyberdiplomacy negotiation at the regional and international levels. With this achievement, the Mekong region is poised to harness the full potential of the digital economy, foster greater dialogues and cooperation with regional countries and partners such as China in combatting cybercrimes, and, more importantly, promote inclusive, stable and safe cyberspace for all.

Chapter 9: Conclusion

In conclusion, based on the literature review, interview findings and discussion throughout this book, “Cyber Sovereignty” remains challenging to define, just as with traditional sovereignty. The concept of sovereignty entails a state’s jurisdiction or authority as a geographical territory in physical space. As an extension of the former, “Cyber Sovereignty” concerns a state’s jurisdiction or authority as an intangible territory in cyberspace but can also represent a state’s stand on international cyberspace governance. Moreover, “Cyber Diplomacy” can be used to reconcile two opposing views (US – Internet Freedom, China – Internet Sovereignty) on international cyberspace governance by supporting the co-existence of inevitably contrasting views due to differing histories, cultures, and philosophies in a harmonious global context.

Upon reflection, aside from semiconductors as crucial components for modern electronic hardware, submarine communications cables and satellites also play a significant role in the geopolitics of technology. This is because these key physical infrastructures are the backbone of cyberspace, allowing for the transmission of data between the physical and digital world through the Internet. However, regardless of how free or sovereign the Internet and cyberspace might be of respective states, they are still controlled by government entities or private companies. As a result, whoever controls these submarine cables and satellites has an inevitable influence on the data travelling through them, regardless of the state of domestic internet or cyberspace governance.[44] Therefore, national policies on internet gateway and data privacy play a significant role in providing a legal framework to support the regulation of the Internet and cyberspace within and between states.

From a security perspective, emerging technologies bring about new and different challenges to the realm of geopolitics. Kastner, in the World Economic Forum article "7 views on how technology will shape geopolitics", mentions the following views: "(1) We need to agree on norms and rules, (2) We may see a further erosion of interconnection, (3) Tech companies are becoming a battleground for geopolitical influence, (4) Democracies need data sharing, common standards, technological infrastructure, (5) We must address challenges jointly across borders, (6) We must work together to address both the vast benefits and the enormous risks of data, and (7) We must understand the basis of unnecessary and dangerous geostrategic conflict."[45] These views are relevant to Cambodia in the context of technology geopolitics, centred around mutual understanding and agreement on utilising emerging technologies.

One could argue that the US-China technological rivalry is a matter of protecting national security. According to realism, military security is prioritised over all other national issues. Advanced technologies enhance the various capabilities of a nation's military force. These advancements create a security dilemma, where China and the US are in perpetual competition to stay ahead of each other regarding technological innovation. Thus, closely monitoring and counter-balancing each other's technological progression are strategies for China and the US. Furthermore, once non-state actors, such as private enterprises or academic institutions, contribute to significant technological advancements, states are not the only players in international relations. Non-state actors show their prevalence in the global context, highlighting the relevance of globalism compared to realism. At the end of the day, the underlying philosophies of the fundamental theories of international relations remain. However, the tools and space for interaction between states have transformed into digital components. As a small

state with both US and Chinese economic and political influence, Cambodia must consider the positive impact of emerging technologies while still keeping a close eye on the heated technological rivalry between the two superpowers and its consequent security implications. In the meantime, Cambodia should prepare for cyberconflicts that will arise due to global digitalisation and increased interconnectivity. Policy research, capacity building, and international dialogue relevant to Cambodia's interaction within cyberspace will all play a significant role in strengthening national security, as well as Cambodia's emergent cyberdiplomacy.

Just as with all past technological advancements in history, cyberspace has brought about the unimaginable positive impact both economically and socially. However, the potential risks, threats, and consequences associated with cyberspace are of equal magnitude. In conclusion, we would like to quote former US President Barack Obama (2011): "By itself, the internet will not usher in a new era of international cooperation. That work is up to us."[46] The issues of sovereignty and diplomacy in cyberspace are extremely complex and cannot be neglected just because non-IT experts do not understand them. The majority of the world is now connected to the Internet, and these connections will only grow deeper. We all have a role to play, regardless of our technical knowledge and understanding of cyberspace.

Moving onto recommendations based on philosophical inquiry and an examination of Cambodia's emergent cyberdiplomacy, we realise that cyberspace – much like physical space, is still based on the concept of space. However, cyberspace is undoubtedly more of a human construct under our direct control, as compared to physical space – which has been around long before human existence. Moving forward, we must take action to fill in these gaps of

understanding through multistakeholder engagement and raising public awareness of the nature of cyberspace, as well as the associated advantages and disadvantages of its utilisation. Furthermore, academics, diplomats, lawyers, and cybersecurity experts must convene under the framework of global cyber governance to address matters of sovereignty and diplomacy in cyberspace.

Moreover, the purpose of this book is to dive deeper into the evolving field of international relations, concerning the nature of cyberspace, under the framework of philosophical inquiry. Technological advancement and the adoption of cyberspace have created a paradigm shift in international relations. Traditional and conventional IR theories are inadequate and will no longer hold due to the overlapping international boundaries of the physical world with cyberspace. The integration of evolving human-to-human interaction via machines interconnected in cyberspace must be prioritised when considering cyber-related issues in the arena of contemporary international relations. At the end of the day, there is always a "human in the loop" behind any technology. Therefore, using a philosophical approach to understand the nature of cyberspace, as well as how humans interact in cyberspace, will be absolutely crucial in the extrapolating decision-making process by states in the context of sovereignty and diplomacy. As the human race increasingly relies on machines, we must focus less on the complexity of machines and more on the human dimension.

As a small state sitting in a strategically contested Indo-Pacific, Cambodia's ability to adopt new technologies, mitigate cyber risks posed by internal and external actors, and engage proactively in regional and global cyberdiplomacy is crucial in safeguarding its national security, digital economy, and international stability. Despite its nascent state, Cambodia's emergent cyberdiplomacy holds a promising future, which, with a long-term vision and whole-of-government effort, would prepare the country for future uncertainties, risks and threats posed in cyberspace. Nonetheless, the road ahead is certainly going to be challenging.

Endnotes

[1] Paul R. Viotti. and Kauppi, Mark V. (1999). "International Relations Theory: Third Edition".

[2] Paul R. Viotti. and Kauppi, Mark V. (1999). "International Relations Theory: Third Edition".

[3] "GDP growth (annual %) Data". *Worldbank*. Retrieved October 1, 2022, from https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?locations=KH+

[4] "Cambodia Population (Live)," Worldometer, Retrieved June 1, 2021, from https://www.worldometers.info/worldpopulation/cambodiapopulation/#:~:text=Cambodia%202020%20population%20is%20estimated,year%20according%20to%20UN%20data

[5] James H. Moor and Terrel W. Bynum. no. 1-2 (January 2002): 4 "Introduction to Cyberphilosophy*," Metaphilosophy* 33.

[6] Moor and Bynum, "*Introduction to Cyberphilosophy*," 5-6.

[7] "AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the Difference?" (2022, January 19). *IBM*. Retrieved October 1, 2022, from https://www.ibm.com/cloud/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks

[8] Covington, P., Adams, J., & Sargin, E. (2016, September 7). "Deep Neural Networks for YouTube Recommendations". *Proceedings of the 10th ACM Conference on Recommender Systems*. https://doi.org/10.1145/2959100.2959190

[9] Google AI. (n.d.). "Our Principles" –. Retrieved October 1, 2022, fromhttps://ai.google/principles/

[10] Croy, Marvin. no. 1-2 (January 2003): 49-69 "Philosophy of Mind, Cognitive Science, And Pedagogical Technique." *Metaphilosophy* 33. https://doi.org/10.1111/1467-9973.00216

[11] Merriam-Webster Dictionary. "Ontology." Retrieved June 1, 2021, from https://www.merriam-webster.com/dictionary/ontology

[12] Chambers Pocket Dictionary 1992 in Rebecca Bryant. "What Kind of Space Is Cyberspace?" *Minerva – An Internet Journal of Philosophy* 5 (2001): 138. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.125.5433&rep=rep1&type=pdf

[13] Bryant. "What Kind of Space Is Cyberspace?" 138.

[14] Marshall McLuhan and Lewis H. Lapham, (1964). "Understanding Media: The Extensions of Man*"*. *MIT Press.*

[15] Marshall McLuhan and Bruce R. Powers, (1992). "The Global Village: Transformations in World Life and Media in the 21st Century". *Oxford University Press.*

[16] Bryant. "What Kind of Space Is Cyberspace?" 139.

[17] Bryant, "What Kind of Space Is Cyberspace?" 143-153.

[18] Bryant. "What Kind of Space Is Cyberspace?" 148.

[19] "What Kind of Space Is Cyberspace?", 154.

[20] Schaefer, R. (2009, December 3). "The epistemology of computer security". *ACM SIGSOFT Software Engineering Notes*, *34*(6), 8–10. https://doi.org/10.1145/1640162.1655274

[21] Michelfelder, D. P. (2000, September 1). "Our moral condition in cyberspace". *SpringerLink.* Retrieved October 1, 2022, from https://link.springer.com/article/10.1023/A:1010049320893?error=cookies_not_supported&code=2c3a569b-7e04-42cc-8ba6-4f8b42e5507a

[22] Stephen D. Krasner, (2001). "Problematic Sovereignty". *New York Chichester: Columbia University Press*, 1.

[23] Stephen D. Krasner, (2001) "Problematic Sovereignty".

[24] Stephen D. Krasner, (2001) "Problematic Sovereignty".

[25] Krasner, "Problematic Sovereignty", 5.

[26] Krasner, "Problematic Sovereignty".

[27] Krasner, "Problematic Sovereignty*"*, 21.

[28] Cynthia E. Ayers, (December 2016). "Rethinking Sovereignty in the Context of Cyberspace: The Cyber Sovereignty Workshop Series". *Center for Strategic Leadership – US Army War College*. Retrieved from https://www.hsdl.org/?view&did=802916

[29] Niels N. Schia and Lars Gjesvik, (February 2017). "China's Cyber Sovereignty." *Norwegian Institute of International Affairs.* Retrieved from https://www.jstor.org/stable/resrep07952?seq=1#metadata_info_tab_contents

[30] Lindsay (2015) in Schia and Gjesvik, "China's Cyber Sovereignty," 1.

[31] The National Bureau of Asian Research. (2020, August 25). "China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace". *The National Bureau of Asian Research (NBR).* Retrieved October 1, 2022,

from https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/

[32] Adrian Shahbaz and Allie Funk, (2020). "The Pandemic's Digital Shadow." *Freedom House:*
Freedom on the Net 2020. Retrieved from https://freedomhouse.org/sites/default/files/202010/10122020_FOT2020_Complete Report_FINAL.pdf

[33] Juliane Schmidt, (August 2014) "Between Irrelevance and Integration? New Challenges to Diplomacy in the 21st Century and the Role of the EEAS." *Department of EU International Relations and Diplomacy Studies* – College of Europe. Retrieved from https://core.ac.uk/download/pdf/76799351.pdf

[34] Schmidt. "Between Irrelevance and Integration? New Challenges to Diplomacy in the 21st Century and the Role of the EEAS."

[35] Nazli Choucri and David D. Clark, (2019). "International Relations in the Cyber Age: The Co-Evolution Dilemma". *MIT Press.*

[36] Choucri and Clark, "International Relations in the Cyber Age".

[37] Choucri and Clark, "International Relations in the Cyber Age".

[38] "Cyber Diplomacy Infographic,". *EU Cyber Direct*, Retrieved June 1, 2021, from https://eucyberdirect.eu/wp-content/uploads/2019/11/factsheet_cyber-diplomacy_print.pdf

[39] "About: Supporting the EU's Cyber Diplomacy," *EU Cyber Direct*, Retrieved September 10, 2021, from https://eucyberdirect.eu/about

[40] Vieira, M. B. (2003, July). "Mare Liberum vs. Mare Clausum: Grotius, Freitas, and Selden's Debate on Dominion over the Seas". *Journal of the History of Ideas*, 64(3), 361. Retrieved from https://doi.org/10.2307/3654231

[41] Marie Baezner, (April 2018) "Cybersecurity in Sino-American Relations." *Center for Security Studies, ETH Zurich: CSS Analyses in Security Policy*, no. 224: 2. Retrieved from https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse224-EN.pdf

[42] Jinghua, L. A. L. (2019, March 15). "Is There Common Ground in U.S.-China Cyber Rivalry?". *Carnegie Endowment for International Peace*. Retrieved October 1, 2022, from https://carnegieendowment.org/2019/03/15/is-there-common-ground-in-u.s.-china-cyber-rivalry-pub-78725

[43] Kastner, “7 Views.”

[44] John J. Mearsheimer, (2014). “The Tragedy of Great Power Politics”. *New York: WW Norton.*

[45] Rethy Chhem, Geeta Tripathi, and Trond Gilberg, (August 2020). “Submarine Cable Geopolitics.” *Asian Vision Institute*, no. 10. Retrieved Oct 1, 2022, from https://drive.google.com/file/d/1oMmOdMsc2kAvCVTmsOhXqyad0g-5dXB0/view

[46] Ariel Kastner, (April 7, 2021). “7 Views on How Technology Will Shape Geopolitics.” *World Economic Forum*. Retrieved from https://www.weforum.org/agenda/2021/04/seven-business-leaders-on-how-technology-will-shape-geopolitics/

[47] Obama in Barrinha and Renard, “Cyber-Diplomacy”, 1.

References

Alcântara, Bruna Toso de. 2018. “SCO and Cybersecurity: Eastern Security Vision for Cyberspace”. *International Relations and Diplomacy* 6:549–555. doi:10.17265/2328-2134/2018.10.003.

Anghie, Antony. 2005. *Imperialism, Sovereignty and the Making of International Law*. Cambridge University Press: New York.

Association of Southeast Asian Nations (ASEAN). 2017. “ASEAN Declaration to Prevent and Combat Cybercrime.” *ASEAN*. Accessed 25 February 2023. https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf.

Ayers, Cynthia E. 2016. “Rethinking Sovereignty in the Context of Cyberspace: The Cyber Sovereignty Workshop Series”. *US Army War College*. https://csl.armywarcollege.edu/usacsl/Publications/Rethinking%20sovereignty.pdf.

Baezner, Marie. 2018. “CSS Analyses in Security Policy No. 224: Cybersecurity in Sino-American Relations.” *Center for Security Studies*. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse224-EN.pdf.

Ball, Desmond. 2011. “China’s Cyber Warfare Capabilities.” *Security Challenge* 7: 81–103.

Barrinha, Andre, and Thomas Renard. 2017. “Cyber-Diplomacy: The Making of an International Society in the Digital Age.” *Global Affairs* 3:353-64. doi: 10.1080/23340460.2017.1414924.

Barrinha, André, and Thomas Renard. 2020. “Power and Diplomacy in the Post-Liberal Cyberspace.” *International Affairs* 96: 749–766. doi:10.1093/ia/iiz274.

Beschorner, Natasha, James Neumann, Miguel Eduardo Sanchez Martin, and Bradley Larson. 2018. “Benefiting from the Digital Economy: Cambodia Policy Note.” *The World Bank*. https://openknowledge.worldbank.org/handle/10986/30926.

Bryant, Rebecca. 2001. “What Kind of Space Is Cyberspace?” *Minerva - An Internet Journal of Philosophy* 5:138–155.

Budnitsky, Stanislav, and Lianrui Jia. 2018. “Branding Internet Sovereignty: Digital Media and the Chinese–Russian Cyberalliance.” *European Journal of Cultural Studies* 21:594–613. doi:10.1177/1367549417751151.

Cai, Congyan. 2019. *The Rise of China and International Law: Taking Chinese Exceptionalism Seriously*. Oxford University Press, New York.

Cambodia Development Resource Institute (CDRI). 2020. “Cybergovernance in Cambodia: A Risk-Based Approach to Cybersecurity.” *CDRI*. https://cdri.org.kh/publication/cybergovernance-in-cambodia-a-risk-based-approach-to-cybersecurity.

Carr, Madeline. 2015. “Power Plays in Global Internet Governance.” *Millennium: Journal of International Studies* 43:640–659. doi:10.1177/0305829814562655.

Chang, Lennon YC, and Peter Grabosky. 2017. “The Governance of Cyberspace.” In *Regulatory Theory: Foundations and Applications*, edited by Peter Drahos, 533–552. ANU Press: Canberra.

Chang, Lennon YC. 2017. “Cybercrime and Cyber Security in ASEAN.” In *Comparative Criminology in Asia*, edited by Jianhong Liu, Max Travers, and Lennon Chan, 135–148. Springer.

Chhem, Rethy, Tripathi Geeta, and Trond Gilberg. 2020. “AVI Perspective: Submarine Cable Geopolitics.” *Asian Vision Institute*. https://asianvision.org/archives/publications/avi-perspective-issue-2020-no-10-submarine-cable-geopolitics.

Chhem, Siriwat. 2019. “AVI Perspective: Cyberconflict: How Should Cambodia Prepare?” *Asian Vision Institute*. https://www.asianvision.org/archives/publications/avi-perspective-issue-2019-no-12.

Chheng, Niem. 2019. “Prime Minister Hun Sen Thanks Facebook for Restoring Account after being Hacked.” *The Phnom Penh Post*. https://www.phnompenhpost.com/national/prime-minister-hun-sen-thanks-facebook-restoring-account-after-being-hacked.

Choucri, Nazli, and David D. Clark. 2019. *International Relations in the Cyber Age: The Co-Evolution Dilemma*. MIT Press

Corrado, Riccardo, and Sakal Morokot. 2021. “Commentary: Cybersecurity in Cambodia: Awareness as a First Step.” *Cambodia Development Center*. https://cd-center.org/wp-content/uploads/2021/08/P124_20210805_V3IS11_EN.pdf.

Covington, Paul, Jay Adams, and Emre Sargin. 2016. “Deep Neural Networks for YouTube Recommendations.” in *Proceedings of the 10th ACM Conference on Recommender Systems:* 191–198. https://doi.org/10.1145/2959100.2959190.

Croy, Marvin. 2003. “Philosophy of Mind, Cognitive Science, and Pedagogical Technique.” *Metaphilosophy* 33:49–69. doi:10.1111/1467-9973.00216.

Deibert, Ronald J., and Masashi Crete-Nishihata. 2012. “Global Governance and the Spread of Cyberspace Controls.” *Global Governance* 18: 339–361. doi:10.1163/19426720-01803006.

Eichensehr, Kristen E. 2014. “The Cyber-Law of Nations.” *Geo.* LJ 103: 317–380.

EU Cyber Direct. 2018. “Cyber Diplomacy Infographic.” *EU Cyber Direct*. Accessed 1 June 2021. https://eucyberdirect.eu/wp-content/uploads/2019/11/factsheet_cyber-diplomacy_print.pdf.

EU Cyber Direct. n.d. “About: Supporting the EU’s Cyber Diplomacy.” *EU Cyber Direct. https*://eucyberdirect.eu/about.

Google AI. n.d. “Artificial Intelligence at Google: Our Principles” *Google AI*. Accessed 1 June 2021. https://ai.google/principles/.

Heinl, Caitríona H. 2014. “Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime.” *Asia Policy* 18: 131–159.

Heller, Thomas, and Abraham D. Sofaer. 2001. “Sovereignty: The Practioners’ Perspective.” In *Problematic Sovereignty*, edited by Stephen Krasner, 24–52. Columbia University Press: New York.

Hjortdal, Magnus. 2011. “China’s Use of Cyber Warfare: Espionage Meets Strategic Deterrence.” *Journal of Strategic Security* 4:1–24.

International Organization for Standardization and The International Electrotechnical Commission (ISO). 2014. “Glossary of IT Security Terminology.” Int*ernational Organization for Standardization and The International Electrotechnical Commission*.. https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.

International Telecommunication Union (ITU). 2009. “Information Society Statistical Profiles 2009: Asia and the Pacific.” *ITU*. Accessed 25 February 2023. https://www.itu.int/ITU-D/ict/material/ISSP09-AP_final.pdf.

Jaikaran, Chris. 2022. “Cybersecurity: Deterrence Policy.” *Congression Research Service*. Accessed 25 February 2023. https://crsreports.congress.gov/product/pdf/R/R47011.

Kastner, Ariel. 2021. “7 Views on How Technology Will Shape Geopolitics.” *World Economic Forum*. https://www.weforum.org/agenda/2021/04/seven-business-leaders-on-how-technology-will-shape-geopolitics/.

Kemp, Simon. 2022. “Digital 2022: Cambodia.” *Data Reportal*. https://datareportal.com/reports/digital-2022-cambodia.

KOICA. 2014. “Summary on Cambodian Masterplan 2020.”*Open Development Cambodia*. Accessed 23 February 2023. https://data.opendevelopmentcambodia.net/en/library_record/summary-on-cambodian-ict-masterplan-2020.

Kolton, Michael. 2017. “Interpreting China’s Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence.” *The Cyber Defense Review* 2:119–154.

Krasner, Stephen D. 2001a. “Sovereignty.” *Foreign Policy* 122: 20–22+24+26+28-29 (7 pages). https://doi.org/10.2307/3183223.

Krasner, Stephen D. 2001b. *Problematic Sovereignty*. Columbia University Press.

Krisman, Khanisa. 2013. “A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation.” *JAS (Journal of ASEAN Studies)* 1: 41–53. doi:10.21512/jas.v1i1.60.

Lai, Robert. 2012. “Analytic of China Cyberattack.” *The International Journal of Multimedia & Its Applications* 4: 37–56. doi: 10.5121/ijma.2012.4304.

Liaropoulos, Andrew N. 2013. “Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multistakeholderism, and Power Politics.” *Information Warfare* 4: 14–26. doi: 10.1002/9781118381533.

Liaropoulos, Andrew N. 2017. “Cyberspace Governance and State Sovereignty.” In *Democracy and an Open-Economy World Order*, edited by George C. Bitros and Nicholas C. Kyriazis, 25–35. Springer: New York.

Lindsay, Jon R. 2015. “The Impact of China on Cybersecurity: Fiction and Friction.” *International Security* 39:7–47.

Lyu, Jinghua and Ariel Levite. 2019. “Is There Common Ground in U.S.-China Cyber Rivalry?” *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2019/03/15/is-there-common-ground-in-u.s.-china-cyber-rivalry-pub-78725.

Major, April Mara. 2000. "Norm Origin and Development in Cyberspace: Models of Cybernorm Evolution." *Washington University Law Quarterly* 78:59.

Mbanaso, U M, and E S Dandaura. 2015. "The Cyberspace: Redefining A New World." *IOSR Journal of Computer Engineering* 17: 17–24.

McLuhan, Marshall, and Bruce R. Powers. 1992. *The Global Village: Transformations in World Life and Media in the 21st Century.* Oxford University Press.

McLuhan, Marshall. 1964. *Understanding Media: The Extensions of Man.* MIT Press.

Mearsheimer, John J. September 2000. *The Tragedy of Great Power Politics*. WW Norton: New York.

Merriam-Webster Dictionary. "Ontology." *Merriam-Webster Dictionary* Accessed 1 June 2021. https://www.merriam-webster.com/dictionary/ontology.

Michelfelder, Diane P. 2000. "Our Moral Condition in Cyberspace." *Ethics and Information Technology* 2: 147–152.

Minges, Michael, Vanessa Gray, and Lucy Firth. 2002. "Khmer Internet: Cambodia Case Study." *International Telecommunication Union*. https://www.itu.int/ITU-D/ict/cs/cambodia/material/KHM%20CS.pdf.

Ministry of Foreign Affairs of the People's Republic of China. 2021. "Wang Yi Holds Talks with Cambodian Deputy Prime Minister and Foreign Minister Prak Sokhonn." *Ministry of Foreign Affairs of the People's Republic of China.* https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1823796.shtml.

Moor, James H. and Terrel W. Bynum. January 2002. "Introduction to Cyberphilosophy." *Metaphilosophy* 33: 4–10.

Muller, Lilly Pijnenburg. 2015. “Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities.” *Norwegian Institute of International Affairs*. https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/284124/NUPI%2bReport%2b03-15-Muller.pdf?sequence=3&isAllowed=y.

Ngoun, Somaly, and Sopheak Srun. 2020. “Cambodia vs Hackers: Balancing Security and Liberty in Cybercrime Law.” Konrad-Adenauer-Stiftung Cambodia. https://www.kas.de/en/web/kambodscha/single-title/-/content/cambodia-v-hackers-balancing-security-and-liberty-in-cybercrime-law.

Noor, Elina. 2015. “Strategic Governance of Cyber Security : Implications for East Asia.” In *Navigating Change: ASEAN-Japan Strategic Partnership in East Asia and in Global Governance*, edited by Rizal Sukma and Yoshihide Soeya, 150–163. Japan Center for International Exchange: Tokyo.

Ravich, Samantha F, and Annie Fixler. 2020. “The Economic Dimension of Great- Power Competition and the Role of Cyber as a Key Strategic Weapon.” *The Heritage Foundation*. https://www.heritage.org/military-strength-essays/2020-essays/the-economic-dimension-great-power-competition-and-the-role.

Repucci, Sarah. 2020. “Freedom in the World 2020: A Leaderless Struggle for Democracy.” *Freedom House* https://freedomhouse.org/sites/default/files/202002/FIW_2020_REPORT_BOOKLET_Final.pdf.

Richards, Julian. 2014. “A New Cold War? Russia, China, the US and Cyber War.” In *Cyber-War The Anatomy of the Global Security Threat*, 43–56. Palgrave Pivot: London.

Sang, Sinawong, Phallack Kong, Phannarith Ou, and Siriwat Chhem. 2022. “AVI Perspective: Cybersecurity Legislation in Cambodia: Policy to Improve Cyber Readiness and Resilience” In *Cambodia in Cyberspace*, edited by Siriwat Chhem, Phannarith Ou, and Vatana Chea, 95–108. Asian Vision Institute: Phnom Penh.

Schaefer, Robert. 2009. “The Epistemology of Computer Security.” *ACM SIGSOFT Software Engineering Notes* 34: 1–20. doi: 10.1145/1640162.1655274.

Schia, Niels N. and Lars Gjesvik. 2017. “China’s Cyber Sovereignty.” *Norwegian Institute of International Affairs Policy Brief 2.* https://www.jstor.org/stable/resrep07952?seq=1#metadata_info_tab_contents.

Schmidt, Juliane. 2014. “Between Irrelevance and Integration? New Challenges to Diplomacy in the 21st Century and the Role of the EEAS.” *College of Europe: Department of EU International Relations and Diplomacy Studies.*
https://core.ac.uk/download/pdf/76799351.pdf.

Scullen, Cameron Ryan. 2019. “Cyberspace : The 21st Century Battlefield Cyberspace : The 21 St Century Battlefield.” *U. Miami Nat’l Security & Armed Conflict L. Rev* 6 .

Segal, Adam. 2013. “The Code Not Taken: China, the United States, and the Future of Cyber Espionage.” *Bulletin of the Atomic Scientists* 69: 38–45. https://doi.org/10.1177/0096340213501344.

Segal, Adam. 2020. “China’s Vision for Cyber Sovereignty and the Global Governance of Cyberspace.” *The National Bureau of Asian Research Special Report No. 87*. https://www.nbr.org/publication/chinas-vision-for-cyber-sovereignty-and-the-global-governance-of-cyberspace/.

Shahbaz, Adrian, and Allie Funk. 2020. “Freedom on the Net 2020: The Pandemic’s Digital Shadow.” *Freedom House*. https://freedomhouse.org/sites/default/files/202010/10122020_FOTN2020_Complete_Report_FINAL.pdf.

Shen, Yi. 2016. “Cyber Sovereignty and the Governance of Global Cyberspace.” *Chinese Political Science Review* 1: 81–93. doi: 10.1007/s41111-016-0002-6.

Simpson, Gerry. 2009. *Great Powers and Outlaw States: Unequal Sovereigns in the International Legal Order*. Cambridge University Press.

Skoudis, Edward. 2011. “Evolutionary Trends in Cyberspace.” In *Cyberpower and National Security*, edited by Kramer, Franklin, Stuart H, Starr, and Larry K. Wentz, 147–170. University of Nebraska Press.

Stanley, Osezua, and Yinusa Olumoye. 2013. “Information and Communication Technology (Ict) and Diplomacy: A Conceptual Overview.” *International Affairs and Global Strategy* 17:38–44.

Starkey, Tom, and Seav Kouy Y. 2020. “Ministry Holds Consultation on Draft Tech Crimes with US Expert.” *Khmer Times*. https://www.khmertimeskh.com/50734633/ministry-holds-consultations-on-draft-tech-crime-law-with-us-experts.

Sub-Decree on “Establishment of National Internet Gateway”. 2021.

Tean, Samnang, and Sayumphu Ros. 2021. “AVI Policy Brief "Geopolitics of Cyber Governance in the World, ASEAN, and Cambodia.” *Asian Vision Institute*. https://www.asianvision.org/archives/publications/avi-policy-brief-issue-2021-no-07-geopolitics-of-cyber-governance-in-the-world-asean-and-cambodia.

Tean, Samnang, and Sokpanya Phon. 2021. “AVI Policy Brief: Cyber Diplomacy: An International Cooperation Instrument for Cambodia in the Digital Age.” *Asian Vision Institute.* https://www.asianvision.org/archives/publications/avi-policy-brief-issue-2021-no-04-cyber-diplomacy-an-international-cooperation-instrument-for-cambodia-in-the-digital-age.

The White House. 2018. “National Cyber Strategy of the United States of America.” *The White House*. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf%0Ahttps://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/.

The World Bank Data. n.d. “GDP Growth (Annual %) – Cambodia.” *The World Bank*. Accessed 1 June 2021. https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?locations=KH.

Thomas, Nicholas. 2009. “Cyber Security in East Asia : Governing Anarchy Cyber Security in East Asia : Governing Anarchy.” *Asian Security* 5: 3–23. https://doi.org/10.1080/14799850802611446.

United Nations. 2015. “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.” *United Nations*.

United Nations. 2019. “Internet Governance Forum: We Must Act Now to Tackle the Threats of Cyberspace.” *United Nations*. https://www.un.org/tr/desa/internet-governance-forum-we-must-act-now-tackle-threats-cyberspace.

United Nations. 2020. “E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development.” *United Nations*. https://digitallibrary.un.org/record/3884686?ln=en.

United States Cyber Command. (2018). “Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command.” *United States Cyber Command*. Accessed 23 February 2023. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

Westcott, Nicholas. 2008. “The Impact of the Internet on International Relations.” *Oxford Internet Institute Working Paper No. 16*. http://do.rulitru.ru/docs/22/21978/conv_1/file1.pdf.

Willard, G.N. 2015. “Understanding the Co-Evolution of Cyber Defenses and Attacks to Achieve Enhanced Cybersecurity.” *Journal of Information Warfare* 14: 17–31.

Willem te Velde, Dirk, Chandarany Ouch, Hokkheang Hiev, Monyoudom Yang, Tim Kelsall, Alberto Lemma, Aarti Krishnan, Karishma Banga, Astrid Broden, Michelle Nourrice, and Jessica Evans. 2020. “Fostering an Inclusive Digital Transformation in Cambodia.” *Supporting Economic Transformation*.

Worldometer. n.d. “Cambodia Population (Live).” *Worldometer*. Accessed 1 June 2021. https://www.worldometers.info/world-population/cambodia-population/#:~:text=Cambodia%202020%20population%20is%20estimated,year%20according%20to%20UN%20data.

Zidar, Andraz. 2019. *The World Community between Hegemony and Constitutionalism.* Eleven International Publishing.

Annexes

- **Annexe 1: Cyber Diplomacy Short Stories by Cambodians**

Informant **#1**	
Question 1	How do we define sovereignty in cyberspace or "Cyber Sovereignty"?
Response	From the Policy point of views: Refers to the national **governance of the internet** aiming at managing and controlling to protect its national security and the sovereignty of its **national policy** or **interest** in terms of **politics**, **economics**, and **technology** for the shake of their cyberspace. From the technical point of views: Refers to **technological infrastructure** and **tools** to control or set the boundary of its sovereignty in the cyberspace, including the **flow and the exchange** of **data** and **information** over the cyberspace. This may consider the ethical issues of data privacy, sovereign independence, the power of data etc.
Question 2	How can we use diplomacy in cyberspace or "Cyber Diplomacy" to reconcile two opposing views (US-Internet Freedom, China- Internet Sovereignty) on international cyberspace governance?
Response	To use **cyber diplomacy** as a **mechanism**: ▪ To deal with the issues of **geopolitics** and **politics** as the application of diplomacy to **cyberspace** ▪ To respond to the **international law** in term of **cyberattacks** or cyber risks that may occur. ▪ To consider it as a **norm** in **cyberspace** for **collaborative partner** countries

	▪ To consider it as the **heart** of **foreign policy** and **soft power strategy** to whom diplomats engage with the geopolitics of cyberspace ▪ To respond to **challenges** in the cyberspace

	Informant **#2**
Question 1	How do we define sovereignty in cyberspace or "Cyber Sovereignty"?
Response	To define sovereignty in cyberspace or "Cyber Sovereignty", it is important to first establish an understanding of the international legal framework on the principle of state sovereignty as well as definition of cyber/internet governance. As stipulated within Article 2, paragraphs 1 and 7 of the UN Charter, the rules-based multilateral system under the UN is based on, "the principle of **sovereign equality** of all its members", and "nothing contained in the present Charter shall authorize the UN to intervene in matters which are essentially within the domestic jurisdiction of any state". Furthermore, paragraph 5 of the General Assembly Resolution 2131 (XX) on the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty elaborates that, "every State has an **inalienable right to choose its political, economic, social and cultural systems**, without interference in any form by another State". Cyberspace on the other hand is anarchic in nature and is supported, controlled, and developed through cooperation and collaboration between countries and organisations across the globe. In fact, the World Summit on the Information Society (WSIS) defined internet governance as, "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet".[47]

[47] Tunis Agenda for the Information Society-World Summit on the Information Society-WISI II

	Thus, Cyber Sovereignty balances the sovereign rights of countries to define their own cyber developmental path with the necessity of a multi-stakeholder international regime that governs the World Wide Web. Sovereignty in cyberspace must consider that there is no single solution for cyber governance as it must be adapted according to each country's capacity, institutional and regulatory context in conjunction with the fact that these structures are not constant and are in flux[48] States must exercise their right and jurisdiction to determine their own path of cyber development concerning policy, regulation, infrastructure within their national borders in a manner that best synergises with the multilateral regime governing cyberspace to further the best interest of their respective peoples and national context.
Question2	How can we use "Cyber Diplomacy" to reconcile two opposing views (Internet Freedom v. Internet Sovereignty) on international cyberspace governance?
Response	**Cyber Diplomacy (CD)** is perceived to originate in the wake of 2007, when Estonia was attacked. In this sense, CD is a diplomatic tool to prevent and counter threats – cybersecurity. Overtime, CD has become increasingly complex, **demanding a more holistic approach**, which must consider security, economic, social and, most importantly, political aspects as they are all interdependent. **Internet Freedom**: Internet being a single and uniform experience across the world. A liberal and global view of the internet, expected by the American at time of inception. **Internet Sovereignty**: The division or breaking up of the internet into each system that is tailored to and governed by individual state. It may include censorship, limit of access, strict laws and regulations, data localisation and storage, etc.

[48] OECD. 2019. Going Digital: Shaping Policies, Improving Lives.

	For CD to be effective, it must aim to **strike a balance**, or reach a compromise, between the two. This can also be between liberty and security, and transparency and confidentiality. The balance is also necessary given the **nature of global governance** – **an anarchy** where all states are sovereign – and the fact that the two ideologies are backed by superpowers (the U.S. and China). **Internet is neither entirely open nor entirely free.** Almost all man-made creations bear goals and visions. For instance, our way of using the internet is technically compromised by our location, language, control over data, etc. **Internet sovereignty is not inherently negative**. Some believe that overly restrictive internet would shift humans away from 'universal freedom'. Though an internationally accepted notion, it can be problematic in practice. Who shapes it? Let alone judging it. This is where states choose to resort to sovereignty; nevertheless, they shall do so in the best interest of their people. **It is a matter of national interests when states aim to preserve control over internet use** within their territory or jurisdiction. Online national interest promotion should also be encouraged through the spirit of multilateralism and respect for sovereignty. Sole reliance on global governance remains a utopia. Therefore, states often identify potential threats in cyberspace and respond accordingly to prevent and mitigate the adverse impacts. **However, accountability and responsibility remain fundamental in international relations.** Without it, the anarchy becomes chaos. In other words, states should attempt to define when will sovereignty cross the line? Therefore, international community should aim to develop binding and non-binding norms for responsible state behaviour in cyberspace.

	➢ In this regard, the UN Cyber OEWG has recently adopted the Final Report through consensus. Other multilateral efforts are seen via the ARF, GGE, OSCE, Interpol's ASPWP on IT Crime, etc. The 2015 U.S.-China Cyber Agreement also marked a vital bilateral effort for the two sides. Cyber Diplomacy should be based on several factors, as follows: ▪ **International order and norms**: Regardless of the side they are on, states have to abide by international norms as the basis of their engagement. After all, CD and international law have some objectives in common, namely order, stability and security. ▪ **Reciprocal trust**: Easier said than done, but this will **prevent grave threats or tension** escalation, as it would provide time and space for concerned parties to engage in dialogue, despite fierce disagreement. ▪ **Collective action and mutual benefits**: This will **concretise partnership, interdependence** and thus ensures **sustainability**. It should follow economic integration model, where costs of disengagement/dispute/conflict/war are high. States may make a political decision to accept some economic cost to gain the benefit of security and privacy, but none will decide on actions that lead to major fracturing. E.g. Almost 80 countries (including the EU) have passed laws that restrict the flow of data across borders. ➢ E.g. states to collectively safeguard internet cables to avoid disruption of data flows, which affect e-commerce, e-banking, etc. Or they could cooperate to bolster deterrence, respond to threats, uphold human rights online and advance fair economic access.

	▪ **Innovation and growth**: The very existence of the internet exemplifies these. Cyber diplomats and policymakers must prioritise these over their disagreement and/or confrontation. Suggest Areas of Cooperation and Way Forward for Cyber State-Actors ▪ Create a **glossary of cyber terminologies** to enhance common international understanding; ▪ Endorse **proactive engagement by private sector and tech companies** to guarantee the integrity of the products they produce and the supply chain supporting them; ▪ Develop **regional/international mechanisms to protecting online rights** and the interests of their citizens and companies; ▪ Arrange **diplomatic efforts for cyberspace** (e.g. appoint of digital/cyber diplomats); ▪ Exercise **self-restraint** in certain cyberspace operations to ensure stability and security; ▪ Enhance **mechanisms and channels of communications** to avoid misunderstanding or miscalculation especially in emergency and/or military activities; ▪ The **UN SG's Roadmap to Digital Cooperation**: Connectivity, digital public goods, digital inclusion, digital capacity building, digital human rights, digital trust and security, critical infrastructure, and global digital cooperation;

	▪ The **EU approaches**: cyber dialogues, capacity building and technical assistance, engagement, outreach and awareness campaigns, diplomatic demarches, statements and declarations, restrictive measures. In an era where cyberspace becomes a core interest for politicians and policymakers, on top to mere experts and engineers, CD is more relevant than ever to bridge the two leading outlooks on cyber governance. As cyber diplomats are navigating through these challenges, it is critical to note that any desire to spread universal values must also answer to sovereignty. There must be a point of equilibrium where both models can coexist. But until then, strong political wills and compromise are the decisive factors.

Informant **#3**	
Question 1	How do we define sovereignty in cyberspace or "Cyber Sovereignty"?
Response	"Sovereignty" is a concept in traditional Western political theory. As human development and scientific and technological advancement pushes forward our frontiers of knowledge and experience, it may be necessary to reconsider our concepts and theories. Instead of asking how might a traditional theory guide us in the changing environment, we may find it necessary to ask what kind of theory is necessary to hold together our understanding of the human condition and the human world. "Sovereignty" is commonly understood as the monopoly of supreme legitimate power within a territory. But what is power, and what is territory? Power is not just coercive force such as military might or legal sanction, it can also take the form of money and information. Globalization as the free flow of capital around the world leads to the existence of mega-size corporations which dwarf countries and governments, in terms of influential power, both in providing incentive and penalty. Such cross-border mega-size corporations have great bargaining power against local governments, and they make important decisions without being held accountable by the electors or citizens of the local countries. Likewise, the all-penetrating cyberspace creates a "territory" that is uncontrollable by border petrol or customs control. It is not territory in the traditional physical sense, but it is territory in the sense that it provides room for human activities and interactions, causing substantial gain and loss. Traditional theory places sovereignty in each state, which has supreme legitimate use of coercive power over its territory. However, as the territory on which it can exercise its power is blurred, it is unclear whether it can still be assumed that there is or has to be a sovereign power,

	whether it is based on authoritative leadership or democratic election. The question is: Should there be a sovereignty to regulate all these kinds of human activities and interactions? The question is not just whether it can be done or not, but also whether it is good to have such kind of supreme power all in one body. Traditional theory holds each sovereign state has supreme legitimate power over its territory and people, conflict between states is resolved through diplomacy or war, and it is always wrong to intervene in the internal affairs of another sovereign state. Such a theory has quite a number of difficulties: How to rectify the wrongs done within a sovereign state? How to resolve competing claims of sovereignty by separatists or unificationists? How to resolve conflicts between two sovereign states except by might and real politics? These problems cannot be answered satisfactorily if it is assumed that there is a supreme power not subject to challenge within the territory that is under its rule. In the few decades before the end of the Twentieth Century, there has been a trend to redefine the role of the government, releasing some of its power to other sectors, such as the market and the non-government public sector. Privatization of some of the functions previously taken by the government has led to the rolling back of the state. Some regulatory functions have also been transferred to international organizations, which can set standards, formulate policies, and monitor implementations. Globalization, as signified by the free flow of capital around the world and the prevalence of global companies in different parts of the world, gives rise to mega-size companies that can hardly be controlled by local governments. It is questionable how useful the traditional

	concept of sovereignty can be in this changing environment. The traditional concept of sovereignty is closely tied to the concept of territory. There can be no sovereignty without territory, and when a new territory is claimed, a new sovereignty can be founded. In the case of cyberspace, the space is not something that exists objectively, and unlike physical territory, it is not of limited supply, and can be created out of nothing. The existence of cyberspace is defined more by the networking, not less than the storage space of the relevant systems. In a nutshell, the concept of sovereignty has limited validity in the new globalized environment, and it has greater problems when applied to the domain of cyberspace.
Question 2	How can we use diplomacy in cyberspace or "Cyber Diplomacy" to reconcile two opposing views (US – Internet Freedom, China – Internet Sovereignty) on international cyberspace governance?
Response	Both of the two opposing views have their own problems. The kind of freedom of speech in our social life is executed under some conditions. First, there is some kind of self-moderation, as our identity is known to others, and we may have to bear the consequences of our speech. Second, there are established mechanisms, such as those related to slander, sexual harassment, such that legal sanction is available against unacceptable behaviors. Third, in order to have access to a wide audience, one has to rely on mass media such as newspapers, which can serve as a third party doing regulatory works. However, such kinds of conditions are hardly obtained in the case of internet freedom. This problem is made more serious with hidden identity on the internet, and real-time cross-border interactions. Human beings are psychological and emotional animals.

	Misdirection, provocation, manipulation done in a virtual setting can be no less harmful than physical or financial harm. The lack of good governance on the internet is indeed a problem. The lack of government control does not mean that everyone is equally free. Those who are in command of mega-size social media corporations actually have a lot of political power, in the sense that they can influence the political scenarios as they are in control of the platform of communication, including banning users and screening contents, even in the case of presidential or parliamentary elections. They are, however, profit-making companies, and they have such power not because they have secured the support of those who confer such power to them, but just because they are entrepreneurs and they own the resources and technologies. On the other hand, the exercise of strong government control also seems to have a lot of problems. The China model has its advantages. For example, in the case of city lockdown during the COVID-19 pandemic, the monitoring of citizen mobility has been very successful in controlling the spread of the disease. The strong control of giant internet companies in China has also stopped them from becoming a separate source of power from the government. However, the price is also high. The highly centralized political power together with an information technology that can penetrate all aspects of daily life including shopping, transportation, social networking, means that the power of the government is able to extend to the mundane details of its citizens on an individualized basis. This raises the issues of check and balance of the power of the government, and the effective protection of the privacy and freedom of the individuals. These issues are alarming, especially when the country concerned is rising to become

	a world power, in that case the power is even more far reaching, and may be put into good as well as bad uses. Could diplomacy in cyberspace or “Cyber Diplomacy” be used to reconcile the two opposing views on international cyberspace governance? As I understand it, such kind of “Cyber Diplomacy” operates like a kind of international institution, which gains its authority from the voluntary participation and agreement of individual states. It still assumes the idea of state sovereignty, and it only gets the power as agreed or authorized by the individual states. As such, it is difficult for the institution to make a case against the views of its member states. Such a kind of cyber diplomacy may be preferred to cyber anarchy or cyber dictatorship, but it may also be a kind of cyber League of Nations that lacks claws and teeth, and weak in coherence and coordination. One step forward from such kind of “Cyber Diplomacy” may be something like the European Council. It seems to involve a revision of the concept of sovereignty. There is no absolute and supreme power that resides in one single entity, but definition and moderation of power at different levels. The final appeal is not to the real power, but to principles which are spelt out in Constitutions.

Informant **#4**	
Question 1	How do we define sovereignty in cyberspace or "Cyber Sovereignty"?
Response	As a diplomat, cyber sovereignty – capacity of states to align states with international laws and norms. Rights, freedom, ability, to determine affairs related to global phenomenon of internet.
Question 2	How can we use diplomacy in cyberspace or "Cyber Diplomacy" to reconcile two opposing views (US – Internet Freedom, China – Internet Sovereignty) on international cyberspace governance?
Response	International cyberspace governance is key, international laws coherent, new norms to match new technologies, consistent with existing laws and norms, interaction of states and human rights. Australia voted against establishment of UN cybercrime convention, as states involved did not seem to match international norms. Respect the decision but voted against it. Working constructively to build on existing norms and human rights, established practices. Build stability between states. Diplomacy plays important role to ensure international coherence, bilateral (frank exchanges between diplomats and government officials). In SEA, Australia frank dialogue occurs in private, for the majority, as opposed to public statements. Multilateral and regional cooperation, leader summits, follow-up forums. Capacity building and training, technical knowledge, for diplomacy. Mechanisms for developing norms and holding states accountable to them. Emphasis on human rights in cyber governance, serve people. People-centered approach, not one-size-fits-all. UN declaration of human rights, article 19, people right to obtain information. Applied in ways that make sense.

Informant **#5**	
Question 1	How do we define sovereignty in cyberspace or "Cyber Sovereignty"?
Response	Sovereignty is related to territorial authority and it implies the right to territorial integrity and authority but also the responsibility of States towards international order or external sovereignty. Each State is bound to respect the authority of other States. Cyber sovereignty is the ability of State to control internet within its borders. This means controlling e-activates in many areas including political, economics, and technological activities. The question one can ask: is this possible? Knowing that cyberspace has no boundaries, no territories. It is in fact controlled by the Global technological corporations e.g. Google or Facebook. I think the Cyber sovereignty of state can be applied on infrastructure and on persons within its territory.
Question 2	How can we use diplomacy in cyberspace or "Cyber Diplomacy" to reconcile two opposing views (US – Internet Freedom, China – Internet Sovereignty) on international cyberspace governance?
Response	The digital revolution is here to stay, it's changing the world's commerce, communication, politics, but it also presents risks related to safety and security. China and US have different approach to cyber sovereignty, but both consider it as a priority. However, China seems to have a defensive and seems supportive to the concept of cyber sovereignty while US consider an expandible approach to cyber sovereignty and has long been opposed to the idea. The question is can we find a balance between the two approaches?

	Countries have to confront cyber security threats without violating citizen's freedom and rights. Internet shutdown has become a frequent solution against protests. We need legal approaches on how to manage data flow and enforced regulations against terrorism propaganda and other issue such as child pornography and many other practices that are unacceptable in democracies. I think defending a net neutrality is not a possible solution in now days and we should find an in between diplomatic solution to the issue of: "too much cyber sovereignty". We need an open debate on internet regulation and on to what extend we can accept cyber sovereignty. Diplomats should engage with the geopolitics and foreign policy.

Informant **#6**	
Question 1	How do we define sovereignty in cyberspace or "Cyber Sovereignty"?
Response	It is not an easy to term to define sovereignty in Cyberspace. As of today, there is no consensus definition of sovereignty. Therefore, the understanding of this term depends on the professionalism of each group. ▪ Politician: the right of the state to left alone and conduct it affair without the interference from outsiders that International Law refers the prohibition of intervention ▪ Lawyer: more focus on territorial integrity of a nation state ▪ Diplomacy: as we are aware that in UNGGE report in 2015, the word sovereignty appeared quiet often and that mean every nation state inside the report giving the weigh to sovereignty depside of controversial in general discussion. In International Law, two components of sovereignty: ▪ Territoriality: any significant cyber effect occurs on territorial of the state that sometime can be violated the sovereignty of the state, for example the physical damage due to cyber operation. ▪ Jurisdiction: There are 3 key principles: Legal, Judicial and Enforcement Sovereignty: Rule of international law Vs. a Principle of international law. We need to have a view of these views. Usually, it is left to the country to define it. However, the state that doesn't define it clearly will find it troublesome when there is an assessment of cyber-attack on the state.

Question 2	How can we use diplomacy in cyberspace or "Cyber Diplomacy" to reconcile two opposing views (US – Internet Freedom, China – Internet Sovereignty) on international cyberspace governance?
Response	Confident Building Measures (CBM) is one of important tools as we did in the past during the cold war (the red telephone line between US and Russia) Agree on actionable Norms: Consensus of implementation of Norms on cyberspace. UN Mechanism: We should work on the existing platform, OEWG (Open-Ended Working Group) to drive through the mis-understanding issues. In terms of methodology, the research conducted for this thesis will be split into 80% for literature review and 20% for interviews. This literature review will explore the concepts and theories of traditional sovereignty and diplomacy – extrapolating their reach into cyberspace and identifying their emerging challenges. The informants selected for the interview will be both from Cambodia and around the world. They do not need to possess any expertise in cyberspace. They may be scholars or practitioners (public or private sector) with expertise in sovereignty, diplomacy, philosophy, and beyond. Throughout their careers, the informants have used Internet technology or telecommunications tools (computers and smartphones) for their everyday work. The interview results will then be integrated with the literature review to give a more complete understanding of cyberspace, not only from an academic perspective, but from an implementation perspective as well.

Informant **#7**	
Question 1	How do we define sovereignty in cyberspace or "Cyber Sovereignty"?
Response	I am able to elaborate on the historical concept of sovereignty. But your questions are about cyber sovereignty. I have no expertise on cyber matters. I am able to express opinion only. I would like to start by recalling the evolution of the concept of sovereignty. Sovereignty has not always been linked to the notion of territory. Thus, before the colonial period, alongside essentially European territorial sovereignty, we observe a tributary sovereignty which dominates in Africa and Asia. In the latter case, the relationship of subordination of a people to a state authority is linked to the payment of a tribe. It was colonization which extended the assimilation of sovereignty to a given territory and generalized the concept of nation-state (Etat-nation). This concept is based on two practices that we have gradually tried to codify: a) the fate of arms and b) international recognition. a) The border line which limits territorial sovereignty has most often been the result of armed conflicts, the emergence of nation-states putting an end to feudal practices where matrimonial alliances led to transfers of sovereignty. Four examples: 1. After having ceded to Annam, by written agreement signed in December 1845, the territory of Kampuchea Krom, King Ang Duong denounced this agreement and launched a military operation to retake this territory. Having failed, this territory remained in Annam.

	2. It is the fate of arms that allows France, on behalf of Cambodia, to recover the three northern provinces in 1907. 3.During World War II, in the name of Free France, Gl de Gaulle declared that the final line of the border between France and Germany "is left to the fate of arms". 4. Convinced that international law would not allow them to reclaim Kampuchea Krom, the leaders of Democratic Kampuchea have deliberately chosen the armed option. b) Seeking to reduce conflicts linked to questions of territorial limits, international diplomacy has endeavored to have several successive principles adopted. 1. The first principle is mutual recognition. A state only exists if it is recognized by others. Thus, the People's Republic of Kampuchea (which became the State of Cambodia in 1989) had no official existence in the eyes of the majority of states between 1979 and 1991. This principle stabilizes the existence of the components of the international community. But its application depends on eminently political choices, as Cambodia has experienced (since other States, born from similar circumstances, have been recognized before and after 1979). 2. The codification of relations between States has increased: example: Vienna Convention on the Law of Treaties, Convention on Diplomatic Relations, Law on the Sea, etc. The creation of the Permanent Court of Arbitration (1913) and the International Court of Justice (1921) were significant steps. This culminated, in 1945, with the United Nations Charter which was founded on the recognition of the sovereignty of States.

	Since 1948 and the adoption of the Universal Declaration of Human Rights, the sovereignty of individuals has been asserted almost parallel to the sovereignty of States. The right of peoples to self-determination has undergone an evolution which has, little by little, called into question the absolute sovereignty of States. This evolution has gone through several stages: a) The increasing affirmation of the universal character of human rights and the inclusion in international law of the notion of the right to interfere (for humanitarian purposes, but in fact for policial reasons as we saw in Irak and Lybia) have reinforced this development. The creation of ad hoc international criminal tribunals and then of the International Criminal Court (2002) were important steps in this questioning of the sovereignty of States as far as mass crimes are concerned (violation of Geneva Accords, crimes against humanity and genocide). b) Globalization, that is to say the internationalization of the rules relating to trade following the WTO Agreements and the creation of the latter (1995), has been another major challenge to the sovereignty of states. Because the great novelty of the WTO agreements and many free trade treaties that followed is that they challenge also what are called non-tariff barriers (and not only tariff barriers like before). Non-tariff barriers are the laws and regulations specific to each State considered as "obstacles to trade". It can be social, health, environmental legislation, rules relating to public services, culture, intellectual property rights. In fact, the WTO agreements represent the strongest limitation ever placed on state sovereignty. Only the WTO has a power to sanction the states that fail to comply with the WTO agreements. All the other institutions in the UN system (with the exception of the UN Security Council

	when it agrees to implement Chapter 7 of the Charter) do not enjoy such power. c) Scientific discoveries and their technological achievements have called into question the sovereignty of States. The observation of territories by satellites, the capture capacities of all types of communication, geolocation, social networks, ... make very difficult the political will of states to preserve total sovereignty, that is to say a total ability to control their territory and the flow of people and ideas. d) The destruction of the land and marine environment, the significant degradation of biodiversity and climate change are phenomena which know no borders and which illustrate the interdependence of peoples. Once again, national sovereignty is limited by the required cooperation between countries in this vital issue. The old national sovereignty, in the sense of the sovereignty of states, is clearly called into question by the phenomena mentioned above.
Question 2	How can we use diplomacy in cyberspace or "Cyber Diplomacy" to reconcile two opposing views (US – Internet Freedom, China – Internet Sovereignty) on international cyberspace governance?
Response	The proposal of a world governance cannot be retained as a credible hypothesis for the decades to come. It is crystal clear when we see the power of the WTO now clearly challenged by many states. An international governance is only a long-term solution. The sense of responsibility in the face of the emergency forces us to recognize that the states are the only framework to face the challenges of this century. Regional groupings can be a step forward to the extent that the degree of integration is sufficient to adopt common

	solutions. But, in the last resort, the decision will come from the states. It is the mission of the diplomacy of the 21st century to seek new balances in the face of the multiple attacks on the sovereignty of states whose current pandemic shows that this institution remains relevant. If our world is a huge village, if it is the seat of a common destiny for all humanity, it is also made up of inescapable realities that are nations, the competing interests of peoples and above all the deep inequalities that endure century after century.

Informant **#8**	
Question 1	How do we define sovereignty in cyberspace or "Cyber Sovereignty"?
Response	In principle, traditionally when we are dealing with the international relations, the term "sovereignty" will normally refer to the sovereignty of states. It dealt with the territorial jurisdiction and autonomy of each state. However, in cyberspace the thing might be different as cyberspace is borderless and it crosses every domain i.e. land, air and maritime. As for me, cyber sovereignty could be defined as the way where each sovereign state not only protect their cyber environment or ecosystem through a good and structured governance, but how they control their cyber environment. For instance, having a well-defined national legislation, rules, policies, strategies and standards in cybersecurity. By having an effective governance and management, it will help the state to coordinate and response to cyber threats, define clear roles and responsibilities of agencies and build the capability to safeguard their cyberspace since cybersecurity is a shared responsibility. It does not only the sole responsibility of the government, but it is everyone responsibility including private sectors, businesses, industries and public citizens.
Question 2	How can we use diplomacy in cyberspace or "Cyber Diplomacy" to reconcile two opposing views (US – Internet Freedom, China – Internet Sovereignty) on international cyberspace governance?
Response	In diplomacy including cyber diplomacy, the main objective is to reduce conflict and friction between the international society. Since the world is moving towards the digital era, cybersecurity has now become one of the fastest growing fields. A lot of cyber activities either by state or non-state actors if not well-governed may lead to conflict due to its nature of pseudonymity and anonymity.

	Sometimes, a technical issue could become a political or geopolitical matter. Thus, cyber diplomacy plays an important role in maintaining the peace and stability of cyber domain. Cyber diplomacy could be a soft channel to response and settle the disputes between states. It could be developed in various terms. For instance, having a regular dialogue and discussion with multi-stakeholders on cybersecurity could also consider as part of cyber diplomacy. It will help the states to create a common understanding, reconcile opposing views and sharing information. Apart from that, cyber diplomacy could further strengthen the international collaboration and cooperation to build trust and confidence among cyber community since cyberspace is trans-border issues and there are still many grey mutable areas that has not been addressed. Further, the element of cyber diplomacy could also be a useful channel to promote common norms and values in cyberspace for both regional and international peace and security as well as political, economic and social stability of the states. The implications of malicious use of information and communication technologies (ICTs) by states could cause a dominos effect not only to the specific state but to other parts of the world as well. For instance, any damages or threats to critical information infrastructures that support core services to the public like medical, financial, transportation, electric and water services will create chaos to both public and government as most of it are interconnected and interrelated or operated across different states. By having common norms and values, states would be able to promote transparency and develop confidence building measures to enhance the understanding of the states in the

	cyber environment. Among the existing initiatives are the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UNGGE) Report 2015 11 voluntary and non-binding norms, rules and principles of responsible behaviour of state to strengthen common understandings and reduce risks to international peace, security and stability in the global ICT environment. In fact, the current Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) as well has reaffirmed the importance of having common understanding between multi-stakeholders in reducing the risk of misperception, miscalculation and escalation of tension leading to conflict. Then, at the regional level, in 2018, all the ASEAN Leaders has agreed to reaffirm the promotion of the voluntary non-binding cyber norms among the ASEAN Member States in the ASEAN Leaders' Statement on Cybersecurity Cooperation. Later, the Third ASEAN Ministerial Conference on Cybersecurity (AMCC) has agreed to subscribe in principle the 11 norms and to focus on regional capacity building in implementing these norms. In 2019, the Fourth AMCC has agreed to establish a working-level committee to consider the development of a long-term regional action plan to ensure effective and practical implementation of the norms and agreed to recommend the establishment of ASEAN Cross-Sectoral Coordinating Committee with representatives from relevant sectoral bodies to strengthen cross-sectoral coordination on cybersecurity.

Informant **#9**	
Question 1	How do we define sovereignty in Cyberspace or "Cyber Sovereignty"?
Response	The International Organization for Standardization (ISO) defines Cyberspace as a complex environment resulting from the interaction of people, software, and services on the Internet through technology devices and networks connected to it, which does not exist in any physical form. Therefore, the term cyber sovereignty comes from the internet governance and usually means creating and implementing rules in Cyberspace through state governance. States attempt to control, monitor, and protect the Internet sections within their borders or sovereignty. Cyber sovereignty does not necessarily have to mean governance by a state. One of the essential elements of achieving this is that the states can create a law to keep the system in check. Or in other words, the government can interpret and apply the law toward Cyberspace, i.e., having jurisdiction in Cyberspace. In today's global Cyberspace, developing countries mainly serve as users while developed countries specifically provide infrastructures and critical applications. Such a new north—south structure, or some would argue it is neocolonialism which has already emerged, and this cause asymmetry of power or many handicaps the developing state's ability. Usually, it revolves around politics, security, and the military, therefore, with this threat emerging some states are opting for sovereignty in cyberspace other than freedom in cyberspace.
Question 2	How can we use diplomacy in Cyberspace or "Cyber Diplomacy" to reconcile two opposing views (US – Internet Freedom, China – Internet Sovereignty) on international cyberspace governance?

Response	Cyber-diplomacy can be defined as diplomacy in the cyber domain or, in other words, the use of diplomatic resources and the performance of diplomatic functions to secure national interests concerning Cyberspace. Such claims are generally identified in national Cyberspace or cybersecurity strategies, often including references to the diplomatic agenda. It contains cyber-diplomacy plans such as cybersecurity, cybercrime, confidence-building, internet freedom, and internet governance. Diplomacy is the way forward to reconcile the two opposition views. Moreover, it can be gapped when considering that the Cyberspace included a wide range of stakeholders. It is a global domain connecting nations and citizens worldwide in various manners, generating interactions and conflict between them. Furthermore, Cyberspace is usually considered a "global common" as it is hard to have clear-cut management. All these characteristics make both international cyber relations and the governance of Cyberspace extraordinarily complex and fragile, but at the same time make diplomacy all the more necessary, particularly concerning confidence-building mechanisms and the development of international norms and values. Cyber-diplomacy aims to progressively shift those behaviors and attitudes towards a space of peaceful co-existence, defined by clear rules and principles: from a system of interactive units to a society of states. More importantly, diplomacy can enhance cooperation, collective action, incident response, and capacity building**.** Diplomacy plays a vital role in directly responding to specific cyber threats and laying the groundwork for better cooperation and action against future threats., especially in cybercrime, cyber-attack, and other threats.

	At the same time, with Multinational Cooperation plays an essential role in the commercialization of Cyberspace, states should work together through diplomacy and benefit mutually from the commercial transaction. On the other hand, the two blocks can also benefited through sharing or transferring knowledge of cyber technology can help a world be better for all human kinds. All can be done with the work of diplomacy.

Informant **#10**	
Question 1	How do we define sovereignty in cyberspace or "Cyber Sovereignty"?
Response	"Cyber Sovereignty": A Shortened Form of "Cyberspace Sovereignty" Cyberspace is a man-made electromagnetic space within the Internet, various telecommunication networks and communication systems, various transmission systems and radio and television networks, various computer systems, and ICT infrastructures such as embedded processors and controllers in key industrial facilities, as the carrier, over which people create, store, change, transmit, use, and display data and do other things with data to accomplish specific communication technology activities. In an early stage, the constitution of sovereignty emphasizes three elements including people, territory (resources) and regime. The Basic Elements of Cyberspace Sovereignty. "Cyberspace sovereignty is a natural extension of state sovereignty in the cyberspace hosted by the ICT infrastructure located in the territory of a state; namely, a state has jurisdiction (right to interfere in data operation) over ICT activities (in respect of cyber roles and operations) present in cyberspace, ICT systems per se (in respect of facilities), and data carried by the ICT systems (virtual assets)." In the above description, the ICT activities relate to cyber roles which are equivalent to "network population"; the ICT systems per se relate to facilities which are the platforms carrying the cyberspace and are equivalent to "territorial cyberspace"; the data carried by the ICT systems is similar to "cyber assets"; and jurisdiction refers to the right to interfere in facilities, data and data operation, which is equivalent to "cyber regime".

	The above description directly points out that cyberspace sovereignty inherits all four elements of state sovereignty, clarifies the "regime" attribute of cyberspace sovereignty, namely, a regime controls the "territorial cyberspace", the "cyber resources" carried by the "territorial cyberspace", and the population and operations in cyberspace. Basic rights of cyberspace sovereignty - The basic rights of cyberspace sovereignty also directly come from state sovereignty, namely, the right of cyberspace independence, the right of cyberspace equality, the right of cyberspace self-defense and the right of cyberspace jurisdiction. Basic Principles of Cyberspace Sovereignty - The basic principles of cyberspace sovereignty also come from state sovereignty. Respect for cyberspace sovereignty means that the right of cyberspace independence shall be respected, and conduct causing sovereign cyberspace to be unable to autonomously operate shall not be adopted; mutual non-aggression means that cyber attacks shall not be carried out on other states' cyberspace; mutual non-interference in internal cyber affairs means indiscreet remarks or criticisms shall not be made on the jurisdiction over sovereign cyberspace; equal cyberspace sovereignty means that sovereign states have equal rights to co-govern cyberspace, rather than relying on the "stakeholder" model that causes some states to lose their right to participate in co-governance of network, while the others dominate the global cyberspace. Definition of Cyberspace Sovereignty: Taking account of the above-mentioned three aspects, namely, the four basic elements including territory, resources, population and regime; the four basic rights including the right of independence, the right of equality,

	the right of self-defense and the right of jurisdiction; and the four basic principles including respect for sovereignty, mutual non- aggression, mutual non-interference in internal affairs and equal sovereignty, we can give a definition of cyberspace sovereignty as follows: "Cyberspace sovereignty of a state is based on the ICT systems under the state's own jurisdiction; the boundaries thereof consist of a collection of the state's own network device ports directly connected to the network devices of other states; cyberspace sovereignty is exercised for protection of various operations of data bycyber roles. The constituting facilities of cyberspace, the carried data and the operation of data are subject to judicial and administrative jurisdiction of the state to which they belong; each state can equally participate in the governance of international network interconnection; operations of the information and communication infrastructure located in the territory of a state shall not be interfered in by other states; a state has the right to protect its own cyberspace from aggression and to maintain corresponding military capabilities. States shall show mutual respect for cyberspace sovereignty; one state shall not invade the cyberspace of another state; one state shall not interfere in another state's cyberspace management affairs; the cyberspace sovereignty of each state has equal status in international cyberspace governance activities." In short, cyberspace sovereignty, originating and extending from the state sovereignty, inherits many attributes of the national sovereignty, including the four basic elements of territory, population, resources and regime, the four basic rights of the right of independence, equality, self-defense, jurisdiction, and the four basic principles of respecting national sovereignty, mutual non-aggression, mutual non-interference in internal affairs and sovereignty equality. Cyberspace has different forms of

	expression, and people hold different views on the sovereignty issues in different forms of cyberspace.
Question 2	How can we use diplomacy in cyberspace or "Cyber Diplomacy" to reconcile two opposing views (US – Internet Freedom, China – Internet Sovereignty) on international cyberspace governance?"
Response	In the case of telecommunication networks, the international community has effectively carried out sovereign state-based co-governance of international telecommunication networks using the International Telecommunication Union (ITU) as a platform for global governance of telecommunication networks. The reason why the international community reached a consensus on co-governance of telecom space derived from the evolution of telecommunication networks. However, such a mode, in which telecommunication networks is managed, did not find a replication in the Internet space. The reason is that the evolution of the Internet makes it difficult for the fairness of co-governance thereof to benefit all the nations. In the case of telecommunication networks, some countries first built their own telecommunication networks and then linked their respective networks to each other on agreements, thereby forming a sovereign state-led management mode. For the Internet, the United States first built it, and then other countries were allowed to get access to it, thereby forming a US-led centralized management mode. In other words, it is the US that has the right to speak in the management of the Internet. US cyberspace security coordinator, Michelle admitted, "cyberspace is carried by a series of servers that are facilities located in a country, so cyberspace is not an independent existence." Since a country has sovereignty over ICT facilities, it is derivable that the country has

	sovereignty over cyberspace carried by the facilities located in its territory. If there is no cyberspace sovereignty, there is no basis for cyberspace legislation; if there is no cyberspace sovereignty, there is no way to combat cybercrime; if there is no cyberspace sovereignty, there is no right to clear harmful information such as child pornography on the Internet; and so on. Those legal and administrative acts that have been incorporated into individual countries' administration systems showcase the objective existence of cyberspace sovereignty. Therefore, the principle of Cyber Sovereignty should reflect the country sovereignty in Global Internet Governance Sovereign countries should participate in the governance of the Internet on an equal footing, combat in concert cybercrime, and jointly promote the construction, utilization, and development of cyberspace by abiding by the principle of respecting other nations' cyber sovereignty, the principle of cyber sovereign equality among nations, the principle of noninterference in other nations' internal affairs of cyberspace and the principle of all nations being equal and benefiting each other in cyberspace. In short, after we make clear the objectiveness and necessity of the existence of cyberspace sovereignty, the next thing is to manage the Internet based on the sovereignty principle. The international community should deepen its commitment to international cooperation in cyberspace and work together to build a cyberspace destined community, make proper use of, promote the development of, and govern the Internet. An international organization similar to the ITU should be built to govern the Internet in a "multi-stakeholder" mode. When it comes to Internet policies, they should be made by sovereign countries, and for technology innovation, the stakeholders should play a greater role.

	Informant **#11**
Question 1	How do we define sovereignty in cyberspace or "Cyber Sovereignty"?
Response	It would be extremely difficult to establish an exact definition for "cyber sovereignty". Even the term "sovereignty" has different interpretations within international law. It will be up to states and stakeholders to construct their own meaning of cyber sovereignty as society moves forward and technology advances. On this note, the difficulty of defining this term also lies upon the extent of the reach of the cyber realm, which has caused various legal issues including jurisdiction, ownership of data, and rights to usage. While certain organizations or groups may have a clear definition for it, states will interpret it differently. Nevertheless, a general sense of the term can be laid out. The concept of sovereignty can be traced to the absolute power of monarchs. Accordingly, sovereignty generally refers to the state's power and control over its territory, people, and affairs. Cyber sovereignty would essentially mean the state's power and control over data, information, and everything cyber. One of the simplest ways a state can claim cyber sovereignty is the exercise of control and at times ownership over data and information that traverses across its territory.
Question 2	How can we use diplomacy in cyberspace or "Cyber Diplomacy" to reconcile two opposing views (US – Internet Freedom, China – Internet Sovereignty) on international cyberspace governance?
Response	First, these two states' views are not absolute in practice. While these states may lean towards one view or the other, it is important to note that the US does not have absolute internet freedom and China does not have absolute internet sovereignty either. The US has expressed its desire to control and limit the freedom to access the internet on equal terms in the past through net neutrality regulations.

	The US also has issues with the consolidation of power to only a few internet services providers and news networks that influences the extent of its internet freedom. China, on the other hand, has not been able to absolutely control the flow of data and information its citizens receive and transmit, especially when they use VPNs. It is not in the nature of states to relinquish total control. Every state will express some sort of level of cyber or internet sovereignty. This is mainly for national security purposes and political and economic competition. For this reason, the only way cyber diplomacy may have a chance of working is through the constant engagement and dialogue of all stakeholders on the establishment of international cyberspace governance principles. This is integral and must be coordinated in parallel to other important foreign policy and geopolitical issues. It is not a standalone issue. Successful diplomacy will have a chance only if the stakeholders and mediators have a comprehensive understanding of the dynamics of foreign relations and integrates cyber diplomacy into the mix. All of this is easier said than done because, as with any type of diplomacy, it is complex, relational to other issues, and takes years of trust- building and political willingness to cooperate.

Informant #12	
Question 1	How do we define sovereignty in cyberspace or "Cyber Sovereignty"?
Response	Impossible to define, create firewall, national system to control flow of data and information. Internet, cross-border networking. Digital service tax, but not complete sovereignty in cyberspace – only financial transactions, digital services, control to some extent.
Question 2	How can we use diplomacy in cyberspace or "Cyber Diplomacy" to reconcile two opposing views (US – Internet Freedom, China – Internet Sovereignty) on international cyberspace governance?
Response	▪ No absolute internet freedom or sovereignty. ▪ US still has control and censorship, politicized private data. Contradictory to "freedom. Private data manipulated for commercial/political purposes. ▪ Cannot control sovereignty completely in China. Still have VPN and other ways around Great Wall. ▪ In between freedom and sovereignty, cyber diplomacy requires rules and regulations. Development of posts and telecommunication, role model for cyber governance. ▪ Role of cybersecurity – negotiation of rules and norms, diffuse conflict and settlement in cyberspace.

- **Annexe 2: Podcast Transcription**

Title: “Siriwat Chhem on What Makes for an Inclusive Digital Economy”

Podcast Name: Between the Binary: Tech and the Global South

Date: 30 March 2022

Length: 34 minutes and 10 seconds

Podcast Host: Elina Noor, Director of Political-Security Affairs, Asia Society Policy Institute

Podcast Guest: Siriwat Chhem, Director of Centre for Inclusive Digital Economy, Asian Vision Institute.

Transcripts

- **Elina**: Welcome to “Between the Binary”, a limited series podcast highlighting the priorities, prospects, and challenges of technology in the Global South through the voices of experts in and from the Global South. This podcast is curated for the John H. McArthur fellowship program in cooperation with the Asia Pacific Foundation of Canada. I am Elina Noor, one of the two inaugural McArthur fellows, and the host for the series. I’m joined by Siriwat Chhem, who is Director of the Centre for Inclusive Digital Economy at the Asia Vision Institute in Cambodia. Siriwat is also a digital business consultant at Phnom Penh Commercial Bank and Jobify. He’s also a visiting professor at Kirirom Institute of Technology, as well as a member of the World Economic Forum’s Global Shapers Community, Phnom Penh Hub. So, Cambodia with a population of about 17 million, (you can tell if I’m wrong, Siriwat), is one of the smaller countries in Southeast Asia. But the country is steep in rich civilizational history, famous with beautiful and intricate temples like Angkor Wat and Bayon, but also perhaps infamous for a tragic past not so long ago. These days geopolitical headlines in Cambodia are merely about Phnom Penh's relations with China, on the one hand, and

with the United State and its partners and allies on the other. This year, Cambodia holds a rotating chair of ASEAN and so there will be great to spotlight on your country, Siriwat. There is very little that is reported about Cambodia's drive for digitalization in the international media and yet there is really interesting below-the-radar development of Cambodia adopting Big Data and AI, for example, for agriculture innovation, financial inclusion, and even for historical education such as the Virtual Angkor Project which created and reconstructed the ancient city of Angkor at the height of the Khmer Empire at the 14th century.

Siriwat, your educational background and current professional role embody promise in the vibrancy of Southeast Asia's digital future. And yet we both know that there are many challenges related to technological access, capacity, and development in Cambodia and Southeast Asia writ large, both within the 10 ASEAN member states as well as among them. So tell us, What are Cambodia's most pressing technology priorities beyond these stories that we read about and hear about in the news?

- **Siriwat**: Yes, first of all, thank you for having me. It is a great honor and pleasure. I just like to share some of my personal perspectives today based on my research, based on my study in international relations and digital technology management. I think regarding the case of Cambodia in the context of today's modern age where we see rapid digitalization, especially over the past two years, which has been accelerated by the situation of the pandemic. There are certain sectors or components of the Cambodian economy and society, which have been focusing in terms of technology. If we look at the new established Ministry of Industry, Science, Technology, and Innovation of Cambodia, recently you could say re-branded and re-focused on STI (Science, Technology, Innovation). They lay out their national STI policy framework and Roadmap for the next few years to be focusing on three main technology

priorities. So, those three priorities consist of Health Technology (Health tech), Agriculture Technology (Agri tech), and, finally, Education Technology (Edu tech). So, we could say that those 3 of Edu tech, Health tech, and Agri tech are some of the technology priorities for Cambodia for the next few years.

Another important factor or to keep is that, in terms of the economic sector in Cambodia before the COVID-19 era, we could say that the garment industry along with tourism, agriculture, and construction consist and makeup of, we could say, driving sector of the Cambodian economy for the last one or two decades, where in the last 20 years, Cambodia has experienced above 7% GDP growth annually. So, in terms of economic growth and development, this is quite remarkable, not just in the case of Cambodia or ASEAN, but really around the world. So as you correctly mentioned before, the population of Cambodia is around 16-17 million. In terms of population and size, perhaps one of the smaller countries in the ASEAN region but based on past data and evidence, we can see that Cambodia is indeed quite a rapidly developing country for many factors, some of which may be, first of all, a very young population. I believe a median age in Cambodia is around 26 years old with more than 2/3 of the population or around 70% under the age of 30. So, having a young population compared to the rest of the ASEAN nations or around the world, it's a quite competitive age in terms of contributing towards the bright future. Another important factor in terms of technology priorities and overall digital adoption and tech savviness in the nation has been quite affordable mobile data. So, we see that through the local telecom sector providing quite affordable and accessible mobile data in addition to internet service, we pay around 8 USD per month, which essentially just to have unlimited mobile data or anything upwards from 20 gigabytes. So, these are just small factors which do in the long run accumulated towards access to the internet, our ability to utilize and navigate digital platforms and applications, and all of these in the

context of the digital era. So for now, I just keep my answer to that but those are the 3 main technology priorities, which are Health tech, Agri tech, and Edu tech. And we can once again put that in the context that there are 4 main economic sectors driving the nation are related to the garment industry, agriculture, tourism, and construction.

- **Elina**: Great, Thanks! And I wonder If you could unpack some of the approaches or policies that are to meet these priorities that you outline. I also would like to get your thoughts on what makes for an inclusive digital economy for Cambodia's younger generation given that you are from the Centre for Inclusive Digital Economy after all.

- **Siriwat**: Yeah, thank you for the question. So, in terms of unpacking or maybe diving a little bit deeper into the respective policy and framework that will drive those 3 technology priorities are reaching those goals and accomplishments. I would say that, it's definitely a collective effort inter-ministerial, meaning that, not only this specific ministry that I mentioned but others as well, whether it be from Post and Telecommunications aspect or from Economy and Finance or any other ministry or institution with some sort of technical capability or support are all starting to come into play. So, we can see that, regionally, in terms of cyber security we see that most of the ASEAN countries over the last few years or decades have adopted their respective cyber security/cybercrime laws. Certain countries put them separately and certain countries have them all in one and we see that now Cambodia is also catching up to that now with a formulation of their own, let say, the whole legislation process for cyber security law, that's a one-way important aspect. I think all around the world regardless of where you are, and what kind of technology priority or sectors that you're trying to accomplish, having a very robust policy framework for cyber security will indeed protect citizens but also organizations, and of course the critical information infrastructure, which

is essential to all effective operations of nations, whether they be from the banking sector, from the water supply, electricity and so on. So all of these are very interlinked, there are many policy frameworks and legislation that are in process. We could say that another key component or important policy framework that is in play is from the Ministry of Economy and Finance, where they will lay out their Digital Economy and Society Policy framework. It's quite extensive but again we show the collective effort from the different ministries in Cambodia. So, the first being the national STI Roadmaps from the Ministry of Industry, Science, Technology and Innovation. Another one would be this particular Digital Economy and Society Policy framework for the Ministry of Economy and Finance and so on. The list goes on. So, we do see these big-picture policy frameworks being taken very seriously and in consideration from all sectors across Cambodia and we do see more technically capable ministries who are providing very important and effective laws such as cyber security and so on from these efforts. All of these together, I believe that, in terms of moving towards an inclusive digital economy, it is quite a goal to reach but really to be inclusive, just implies that of course becoming a digital economy or transforming into one, it implies increased connectivity between people, between businesses, organizations looking at the demand and supply sides, so I'm using third party application of platform that are either centralized or not that brings together really all of our daily needs operation, whether being in personal life or in professional. And so all of these are really taking into account how rapidly are we moving forward in terms of development through digitalization. We see it every day here in Cambodia to give you very on-the-ground evidence which is less as a shake.

In the last two years, we have seen a huge increase in e-commerce, food delivery, and financial payments through mobile applications, not that these did not already exist before, but it really came out of the necessity during the

context where we're working from home and lockdowns were quite apparent throughout the past year that there has really been an emergence and really a recognition of these applications and platforms to help the economy, help the society. So I think my final point would just be that, in other to keep in mind inclusiveness, it's definitely a challenging path simply because development is not always equal or growth at equal rates or speeds but it really is starting of at the center of the development or innovation and then has to gradually spread outwards or beyond from urban to rural. That's quite natural in terms of development and even more so when it comes to technology and to anything that is related to the digital economy because, at the end of the day, it does rely on very key pillars of infrastructure, which are traditional. You have your electricity poles and then, therefore, that extends into access to the internet. So all of these components really play a very important role and are all interlinked.

- **Elina**: Yeah, I'm glad you mentioned context because I wanted to bring up this issue of language. In one of the things I've heard coming from countries that don't have English as their first language, has very different scripts to be romanized alphabets. I've heard that sometimes this is the problem, particularly in rural areas and this goes to the point about inclusion. Is it something that is the challenge in Cambodia as well?

- **Siriwat**: Definitely, inclusion is a challenge just like around the world, but you could say, in the context of Cambodia, naturally because Cambodia had a bit of a late start, given its historical context. What Cambodia did in the past years is truly remarkable. In terms of a leapfrogging and going towards Industry 4.0 and really rising up the ranks very quickly in terms of how we went from the very basic of production towards the garment sector and now more into the manufacturing sector. We have really seen a lot of growth. And does it has some implications on inclusive? Definitely. The disparity between

urban and rural areas, these are very common concepts according to the digital devices, how that truly be applied digital applications and platforms in our everyday uses and throughout society. It will create some sort of gap or digital device where those in the urban area will benefit with full access to the internet and reliable infrastructure will continue to grow and forward and advance technologically, but then those are the rural areas either have limited or no access to the internet or smartphone and mobile devices. But to be completely honest, these are the kind of hiccups or obstacles that sometimes have to be dealt with from different approaches because there is not one solution to fix all these at the same time and it would be two ideal to think that development could be laid out in certain time without some sort of implications on the divider gap, but on the more positive note, we do see that in Cambodia, despite the rapid growth and despite the fast-growing technological infrastructure, moving out throughout the country and from urban-rural, there are many initiatives as well as by do taking to account digital divide and trying raise awareness on digital literacy and so on. So, it's quite an interesting topic to discuss, but we can go more into that into the next few questions.

- **Elina**: Yeah, I know that's great and as you pointed out, this is the issue that digital devices it's true across the regions. It's true in developed economies and it's not one often. But there is a lot of capacity building that is trying to be initiated in our region and Southeast Asia. And very often, we tend to the more developed economy of the Global North with technological advancement and matured infrastructure to help the South. I wonder though, what you think of more inter-regional cooperation among countries in the Global South that face a number of common challenges such as the one that we've talked about already. Do you think there are more prospects that need to be explored in South-South cooperation?

- **Siriwat**: Yes, it is a great question. But before I'm answering, I just want to clarify. So, we can be on the same page. I mean what exactly do you imply by Global South or which nations consist of the region and the same for global?

- **Elina**: So, this podcast takes a very broad interpretation of the Global South. We are talking about countries that are below the equatorial line. Geographically, that's the Global South. But we are also considering communities in the Global South context, meaning marginalized, underrepresented communities, and even developed economies in the Global North. So, it's more of an abstract concept but it's also one that is rooted in geography. So, hopefully, that help somewhat.

- **Siriwat**: Yes, thank you for your explanation. It's good, just to be on the same page before I start answering. So, I think if your question is related to really hardest digital cooperation and collaboration, effective technology advancement moving forward, most definitely. I mean, it can happen in many ways. First of which is certain countries that are wanting to adopt new legislation or policy framework and so on, can definitely learn from more advanced and established nations from around the world. In a global perspective, they don't always work because we all understand that different nations and different regions have different contexts in terms of culture, and because of that it is sometimes quite beneficial to look at regional partners. Why do we look at partners? Because they have at least slightly more similar characteristics to the nation of interest and we do see certain similarities sometimes in that context. So, I think it does help to understand both the similarities and the differences of the nation that we are comparing.

  If we take more concrete example. I mean Singapore is a very technologically advanced country at the very early start. I studied 10 years in Singapore, so I really lived through what was going on during that time and the evolution, and

then to see my home country in Cambodia, I wouldn't say it's on the same path or similar path, but it just two parallel paths that each nation has to go through. So every story is really different. But in terms of what we can learn, we can go really many ways and sometimes in both directions. If we look at Singapore in terms of their robustness and really what they have been able to do with technology, given smaller populations and smaller country size is truly internationally recognized. This is why it becomes one of the global technology and financial hubs in the world, very well-known and respected. But at the same time, it has pros and cons. If you go attend any international cyber security conference or you can read and feel the cyber security, they often bring up Singapore as a prime example of being one of the most technologically advanced countries in the world, which is truly amazing. But at the same time. Even though they rank number one in cyber security index or preparedness, they still are being attacked the most or experiencing the most cyber-attacks. So, all of these indexes and matrixes, which are formed to act as the criteria to see who is more advanced or who is more established, it's quite really a grey area sometimes. But regardless, as I mentioned before, I think each nation follows their own path and, for Cambodia, there is much to be learned from our regional partners and friends from around the world. I think the best approach is really just to be to explore what the different nations are doing and at the same time contextualize that for our very own case or situation.

- **Elina**: Yes, personally, I think there are a lot of opportunities for exchanges between Southeast Asia and the African continent. For example, sub-Saharan Africa is such a dynamic part of the world and if you consider how most of the world's population lives outside the US, lives outside Europe recently a lot of these types of exchanges that need to be taking place, given where we're at socio-economically. Most of us are on par or there about, so I think there

are lessons to be learned even outside the ASEAN region. We have also often heard in Southeast Asia that the region doesn't want to be squeezed and there is a technological rivalry between the US and China. Where does Cambodia stand on this? Does it take a similar position? And how does the technological fissure that is being entrenched now bear upon Cambodia's priority and technological prospect in the next few, say 10-20 years?

- **Siriwat**: Yes, so the question you ask is definitely very hard one, a very hard topic. I'd like to answer this from more a scholarly perspective simply because my master's degree in international Relation, I did focus a lot on sovereignty and diplomacy in cyberspace, looking into technology rivalry that is happening all around the world. It's definitely an interesting topic, so I would say that if ASEAN does not want to be squeezed within a rivalry or some sort or at least that's what the narrative is, sometimes that is inevitable. It can't really be avoided simply because if we look at this from a more technical perspective and less political, okay. For example, one key component or aspect would be, for example, rare earth elements. Rare earth elements are extremely key materials essential for creating semiconductors and we know that semiconductors are used in all of our essential mobile devices or electronical devices, especially with the emergence of smart technology. So you could say that this is really the building block of almost everything we use today in digital era because everything is done online. Everything is done electronically, digitally throughout smartphone, throughout laptop. It become an extension of the human body because although they do remain separately physically, I think it is very difficult for anyone to let go of their phone or laptop at any certain point. So, we see that it's become so deeply ingrained into our bodies not just, as I mentioned, not yet physically but mentally, psychologically. All of that is happening and so going back to rare earth elements, which is just one very key aspect, we see that whichever nation, not

to name any, but whichever nation has the monopoly on the rare earth elements market, whichever countries are related to them in terms of international trade and the global supply chain for the manufacturing and developing these smart devices or electronic goods and services that are related to them this really does create some tension in the arena of international relations, whether or not you want to be stuck in some sort of rivalry. So I think just to put all of that in the big picture, it's very interesting to see how the world is increasingly becoming globalized, not just through diplomacy or travel and entry but really a key components that build up everything around us and this new infrastructure that is in place is not only tools. If we think about it in a very traditional manner, every country has their raw materials to build their houses, to build roads and so on but now that we become much more technical in cyberspace, all of these infrastructure, a lot of these components come from around the world and moving around, they make up what is cyberspace which it truly an additional layer of existence on top of where we already live, which is in reality. So I think all of these components between the physical and the cyber and how it affects our individual behaviour as humans, as organizations, as nations. All of this creates a natural tension through a very dynamic nature how things are interlinked, how things are interacting between human and machine, so I think it is very hard to avoid any stimulating change. That's just the natural path that it would follow.

- **Elina**: You brought out rare earth, which is, of course, a controversial topic right now. And as you pointed out, it’s one of the foundational elements of the devices that we have today but there are also a lot of talks about things like algorithms, and the logic layer of technology that maybe countries in Southeast Asia and other parts of the developing world need to be more part of. Can you talk a little bit about where you see Cambodia future in these? Should we rethink how technology design is constructed, even deployed?

Because for the most part, we in southeast Asia are consumers of new technologies. Sure, we have unicorns. We have Grab. We have GoJek, Tokopedia and all that. But at the widest scale, we are not producers. We are not innovators of technology right at scale. Is that something that should change, given the demographic of the world? Given what the region can bring? Given Cambodia young generation? Should this change?

- **Siriwat**: Thank you for the question. It really sparked my interest and now I remember that finally the point I forgot before, so I quickly move on to that. So you did mention that Cambodia and ASEAN, we are not yet producers of these technologies in the field of data and algorithms and so on. All this is key in the field of AI ethics. We talk about ethics because although we can simply put this into man and machine, there's always a man behind the machine and if all algorithms and programs applications and platforms are being produced from a certain part of the world, they will naturally result in something that's called algorithm bias, because the data that is being fed to it, the people who are collecting the data, people who are really structuring the program and the codes all create bias. So just in parallel, the point that I wanted to mention before, Cambodia and ASEAN countries, yes, we are huge consumers of this technology and applications, not just in terms of the population but even per capita, I mean, I would say that based on recent data statistics we see that ASEAN is most definitely one of the dynamic economic regions in the world and for many good reasons. Firstly, as I mentioned, which is similar to Cambodia as in the whole region, is the young population. Overall, they are very tech-savvy.

  I recently read an article that really caught me by surprise because when you live in a certain country or certain context, you don't realize what is normal and not normal. Basically, this article said that I don't remember the statistic exactly but I remember that Facebook. So using Facebook voice function or

the voice recording function in the entire world, Cambodia takes up more than 50% of that voice recording function on Facebook. So when you think about it's very very strange. It is very specific and for Cambodia to have over 50% or very large majority of the entire world, the usage of this voice function is quite remarkable. I look more into this article and did more research and I did realize that it's to the point that you mentioned before. The Khmer language is very complicated. Therefore, we can't use it in Google Translate. It is very difficult to type even for a native speaker, a native Cambodian person. It is very difficult to type because of the structure of the alphabet and the Grammar and the formulation of sentences. So, Cambodia does what most countries do. Just like in Chinese, you have pinyin and then just like another foreign languages apply the Roman alphabet to it. That's what we do in our Khmer language as well for typing. And because it's been so complicated, Cambodian have sort of gone through their own paradigm shift, where they use voice recording for everything. We use it on WhatsApp, on Telegram, on Facebook. It's just become the new way of operation. Whether it's for work, for e-commerce, delivery services. It has really taken on an unexpected role that has had such a huge impact on people's lives in Cambodia, the economy, the society. As I mentioned before, having lived here for the past two years, I didn't even notice to what extent until an outside perspective was given on this. I like this day scientific and evidence-based as possible but when you see an article like this and really hits the point home that Cambodia really has this sort of a different mindset and impact. So it's not to say whether one certain nation is more technology advanced but just that every nation has their different contacts. We use technology in different ways, and sometimes these functions are unintended but, in the long run, they do contribute in and put that in the right direction. To just finally answer that last point, should we re-design technology and how its applications and platforms are being consumed or being supplied to citizens and organizations and nations. Definitely, there

should be more consideration in terms of the design. We do have to take into account ethics. The more rapidly growing the technology world and field becomes, the more we have to rely on the humanities and ethics and philosophy behind it to really keep us grounded, because if we go too far into this advancement, it can really take away from what we as humans should be doing the right thing, the good thing, the ethical thing. All of these are very general but, in technology, it really does extend, and you can say amplify. Whatever we put in will amplify it, whether it's good or whether it's bad. Finally, in terms of the actual redesigning of how we see technology applications and platforms, it is extremely hard to say if we could create an ideal or perfect product or service. Just like in the video game. Putting everything to 100 like in terms of efficiency, speed, use case. For it to be ethical, non-harmful or lethal or be able to affect bias and in political attention, that would be great. But of course, that is not possible. As we mentioned before that, sometimes even if we redesign our technology in a certain way, there will always be another way that was unintended for it to be useful and the same could be that there's always going to be another way that somebody with malicious intent or bad intentions to misuse it or abused it in a way that would not be beneficial but would be harmful. With all of this in mind, I think it's quite difficult to have everything ideal, whether it's development to be growing at the right time equally among the urban and rural, especially with technology, and the same goes with in terms of redesigning for this purpose and for the functionality. But it is important to keep in mind all these factors and I think moving on into the future, Cambodia, ASEAN, and Asian countries and so on will continue to develop very rapidly and contribute towards the more global digital economy, where we will start to produce our own applications and platforms, which have already been seen. But hopefully they will add to the diversity in the market and, overall, this will create some sort

of the digital equality among the world and then hopefully that might ease some tensions and understanding between nation. Thank you.

- **Elina**: I'm so glad you brought up that point about the Khmer language because I was trying to get at that but I clearly could not articulate it eloquently, and so that was the exact anecdotes that I've heard about the Khmer language so thank you so much for bringing that up. Siriwat, I started off in my introduction of you by saying that your experience, your educational background embodies the promise and vibrancy of Cambodia in particular but also Southeast Asia in general. And I think the insights that you shared have only emphasized and highlighted that. So it's been such a pleasure speaking to you and listening to your perspective. Thank you so much for joining us.

- **Siriwat**: Thank you so much. It's been a great pleasure and great honor, and I wish you all the best.

- **Annexe 3: Concept Notes and Agendas of the "Regional Capacity Building in Cyberdiplomacy" Project implemented by NIDIR**

MINISTRY OF FOREIGN AFFAIRS AND INTERNATIONAL COOPERATION

NATIONAL INSTITUTE OF DIPLOMACY AND INTERNATIONAL RELATIONS

Concept Note

"Cybersecurity and Cybercrimes: Challenges and Solutions"

Wednesday, 12 August 2020

Background

With the proliferation of Information and Communication Technologies (ICTs) and the emergence of the "Internet of Things" (IoT) projected to attract an exponential number of devices being connected to the network, cyberspace and ICTs carry enormous potential for economic and social development across societies. However, their all-encompassing, ubiquitous natureand their growing political application pose increasingly significant risks to global economicvalue and to international peace, stability, and security. Cybersecurity has reached head-of-state-level attention and has become a major source of concern for policymakers, as it has been considered the fifth domain of warfare after land, sea, air and space.

Considered one of the fastest growing economies, with annual GDP growth of about 7% for several consecutive years, Cambodia also comes along with the rapidly expandinguse of technology. The number of connected users and devices in the country has been increasing at a frenetic pace, from 4.9 million in 2017 to 8.4 million users in 2019. While promising circumstances augur well for Cambodia, rapid technological advancement could put the country at a high risk of cyberattacks. Studies reveal that Cambodia is still facing problems with cyber awareness and infrastructure. Following the cyberattack incidents in Cambodia, the Anti-Cybercrime Department, a specialised unit under theNational Police of

Cambodia, and Cambodia's national computer emergency response team, known as CamCERT, were established subsequently. In addition, to enhance cybersecurity, Cambodia has advanced its ICT infrastructure, including hardware and software.

Objectives

Considering the importance of cybersecurity and the growing incidents of cybercrimes, the National Institute of Diplomacy and International Relations (NIDIR) is hosting a seminar underthe theme "Cybersecurity and Cybercrimes: Challenges and Solutions". The main objectivesof the seminar are to:

- Raise awareness and spark meaningful discussion on cybersecurity strategy launched by the Royal Government of Cambodia and on crimes in the cyberspace
- Identify key challenges, opportunities and needs in support of strengthening cybersecurity and cyber governance within MFA-IC officials
- Share the confidence-building measures to reduce the risks stemming from the use ofICTs

Expected Outputs

Participants can expect to learn about:

- ICT development and its opportunities and challenges
- Promoting self-awareness of the cybersecurity content
- Lessons learnt of cybersecurity issues, cybercrimes, management, preventive measuresand recommendations from professionals and practitioners.

Date and Venue of the Seminar

- Conducted in two separate sessions, the seminar will be held on **12 August 2020** at Mebon Room, 2nd floor, NIDIR, Ministry of Foreign Affairs and International Cooperation.
- Targeted Participants: MFA-IC officials: From Directors of Departments up to Secretaries of State.

Moderators and Guest Speakers

Session 1: Moderator: H.E. Dr Chhem Kieth Rethy, Minister Attached to the Prime Minister

Guest Speaker:

- H.E. Dr Chhem Kieth Rethy, Minister Attached to the Prime Minister, Council of Ministers
- Mr Ou Phannarith, Director of ICT Security, Ministry of Post and Telecommunications, Cambodia
- Mr Chhem Siriwat, Director of the Centre for Inclusive Digital Economy, Asian Vision Institute and Digital Business Consultant, Phnom Penh Commercial Bank

Session 2: Moderator: Dr Chem Phalla, Vice President of NIDIR

Guest Speaker:

- H.E. Prak Phalla, Advisor to Samdech Techo Prime Minister and Head of Data Digitization Program and ICT Management, Ministry of Foreign Affairs and International Cooperation
- H.E. Chea Peou, Director of Anti-Cybercrime Department, General Commissariat of National Police
- Mr Sorn Chanrithy, Focal Point for Cybersecurity, Ministry of Foreign Affairs and International Cooperation

Next Seminar

The next seminar will be targeting mainly MFA-IC officials up to Deputy Director s of Departments the **First Week of September 2020** at NIDIR.

Tentative Program

Seminar: "Cybersecurity and Cybercrimes: Challenges and Solution"

12 August 2020

8:20-9:00	**Guest Arrival and Registration**
	Arrival and registration of guests and participants
9:00-09:15	**Opening Remarks**
	H.E. Dr Chhiv Yiseang Secretary of State, Ministry of Foreign Affairs and International Cooperation
09:15-10:15	**Session 1: Security in the Cyberspace**
Moderator:	**H.E. Dr Chhem Kieth Rethy** Minister Attached to the Prime Minister, Council of Ministers
Speakers:	**H.E. Dr Chhem Kieth Rethy** Minister Attached to the Prime Minister, Council of Ministers **Mr Ou Phannarith** Director of Department of ICT Security, Ministry of Post and Telecommunications **Mr Chhem Siriwat** Director of Centre for Inclusive Digital Economy, Asian Vision Institute and Digital Business Consultant, Phnom Penh Commercial Bank. Q & A
10:15-10:30	**Coffee Break**
10:30-11:30	**Session 2: Crimes in the Cyberspace**
Moderator:	**Dr Chem Phalla** Vice President of National Institute of Diplomacy and International Relations, MFA-IC
Speakers:	**H.E. Mr Prak Phalla** Advisor to Samdech Techo Hun Sen and Head of Data Digitization Program and ICT Management, MFA-IC **H.E. Mr Chea Peou** Director of Anti-Cybercrime Unite, General Commissariat of National Police **Mr Sorn Chanrithy** Focal Point for Cybersecurity, MFA-IC

11:30-11:35	**Closing Remarks**
	H.E. Mr Tean Samnang President of National Institute of Diplomacy and International Relations, MFA-IC
12:00	**Lunch for speakers hosted by President of NIDIR**

*Note: This program is subject to change with prior notice.

MINISTRY OF FOREIGN AFFAIRS AND INTERNATIONAL COOPERATION

NATIONAL INSTITUTE OF DIPLOMACY AND INTERNATIONAL RELATIONS

Concept Note

Kick-off Workshop of Building Capacity in Cyber Diplomacy Project

Geopolitics in Cyber Diplomacy

The Ministry of Foreign Affairs and International Cooperation (MFA-IC) implements a project on "Building Capacity in Cyber Diplomacy" under the Mekong-Lancang Cooperation (MLC), a special fund, from now until mid-2022. As an institute of MFA-IC, with this fund, the National Institute of Diplomacy and International Relations (NIDIR) leads this project's coordination and implementation process. As part of the project objectives, NIDIR is organizing a "Kick-Off Workshop of Building Capacity in Cyber Diplomacy Project" under the theme "Geopolitics in Cyber Diplomacy.

The advancement of Information and Communication Technologies (ICTs), along with the use of the "Internet of Things" (IoT), has expanded the number of connected devices to the online network. Although the development brings about benefits and modernizations, technological innovations are also associated with risks, uncertainties, and threats, including cyber espionage, cyber-attacks, identity theft, among others, posed by state and non-state actors. These emerging cyber issues have become unconventional threats that endanger international peace, stability, and security. To alleviate such problems, cooperation is required among international actors in this uncharted territory. As a result, "Cyber Diplomacy" – a term that refers to the use of the internet

and digital tools in diplomatic activities – has enabled the rampant flow of information, leading to tremendous changes in the conductof modern diplomacy worldwide, especially to enhance trust and transparency. Digital devices and the internet have thus become critical instruments for the advancement of diplomatic means of communication. In other words, Cyberdiplomacy embodies a new discipline of diplomatic practicesfor the 21st century in pursuit of more cohesive global governance, where states can engage and seekways to address cyber-related issues peacefully.

Cyberdiplomacy has gained momentum, showing an even more stark appearance following the emergence of COVID-19, where digital technology has been an integral part of states. It has become a key topic for countries' foreign policies and a necessity for governments to formulate national cyber strategies to deter the proliferation of cyber-attacks and sustain the peaceful use of digital technology. However, given the mounting challenges of cybersecurity coupled with the non-existenceof universally-agreed cyberspace governance, the cyber-related issues have led to geopolitical rivalriesamong major powers. The world is currently being faced with two conflicting and incompatible ideologies between the multi-stakeholders-led initiative represented by the United States and Europe andthe state-led initiative by China and Russia. The competition amongst big states may have severe consequences for smaller states, such as Cambodia. Thus, a holistic approach with a collective response is necessary for actors to monitor and govern cyberspace in the conduct of Cyberdiplomacy to effectively address cyber-related issues peacefully and ensure the safety and security of users.

The project aims to build qualified diplomats' cyberdiplomacy capacity to contribute to regional peacebuilding, a shared future, and economic development prosperity. Though in the face of the COVID-19 pandemic, the team can implement it progressively, with some delayed activities:

1. We review the literature to explore conceptual theories and local, regional, and globalinitiatives and practices of cyberdiplomacy.
2. We conduct a needs assessment of Cambodia's current cyberdiplomacy human resource capacity to propose a regional cyberdiplomacy training curriculum.
3. We develop a training curriculum and deliver a regional training course on cyberdiplomacy.

The purpose of the consultation workshop includes:

- The introduction of a research framework to stakeholders,
- Disseminating and getting insight into the need for training in cyberdiplomacy,
- Seeking more advice from partners on cyberdiplomacy issues, and
- Discussing the way forward to strengthen regional collaboration in cyberdiplomacy.

Kingdom of Cambodia

Nation Religion King

Ministry of Foreign Affairs and International Cooperation

National Institute of Diplomacy and International Relations

Mekong-Lancang Cooperation

Tentative Agenda

Kick-off Workshop of Building Capacity in Cyber Diplomacy Project

"The Geopolitics of Cyberspace"

September 30, 2021

Zoom Meeting

September	**Kick-off Workshop**
8:00-8:30	Registration and seating
8:30-9:00	**Opening remarks** 1. **H.E. Mr Sok Soken**, Secretary of State of MFA-IC, and Vice Chairman of National Secretariat of Cambodia for Mekong-Lancang Cooperation 2. **H.E. Mr Wang Wentian**, Ambassador of the Republic of China to the Kingdom of Cambodia
9:00-9:15	Brief on Building Capacity in Cyber Diplomacy Project by **H.E. Mr Tean Samnang**, President of NIDIR
9:15-9:45	Cyber Diplomacy in the Context of Geopolitics Rivalries Keynote address by **Dr Chheang Vannarith**, President of Asian Vision Institute
9:45-11:15	Discussion: "Sovereignty, Global Security and the emergence of Cyber Diplomacy" Moderator: **H.E. Dr Chhem Kieth Rethy**, Minister Attached to the Prime Minister and Secretary of State of MISTI 1. Sovereignty and Diplomacy in Cyberspace by **Mr Chhem Siriwat**,Director of Center for Inclusive Digital Economy, AVI 2. Global Security and Cyber Diplomacy by **Dr Tat Puthsodary**,Freelance Researcher 3. Cybersecurity and International Relations

	by **Mr Ou Phanarith**, Director of ICT Security Department, MPTC
11:15-11:40	Wrap-up and closing remark **H.E. Mr Tean Samnang**, President of NIDIR

MINISTRY OF FOREIGN AFFAIRS AND INTERNATIONAL COOPERATION

NATIONAL INSTITUTE OF DIPLOMACY AND INTERNATIONAL RELATIONS

Concept Note

"Cyber Diplomacy: Enhancing Cybersecurity and Tackling Cybercrimes"

Wednesday, 23 March 2022

Background

With the proliferation of Information and Communication Technologies (ICTs) and the emergence of the "Internet of Things" (IoT) projected to attract an exponential number of devices being connected to the network, cyberspace and ICTs carry enormous potential for economic and social development across societies. However, their all-encompassing, ubiquitous nature and their growing political application pose increasingly significant risks to global economic value and to international peace, stability, and security. Cybersecurity has reached head-of-state-level attention and has become a major source of concern for policymakers, as it has been considered the fifth domain of warfare after land, sea, air and space.

"Cyber Diplomacy" – a term that refers to the use of the internet and digital tools in diplomatic activities – embodies a new discipline of diplomatic practices for the 21st century in pursuit of more cohesive global governance, where states can engage and seek ways to address cyber-related issues peacefully. Although Cyber Diplomacy provides states with opportunities to enhance communication, it also makes them more vulnerable to cyber threats such as hacking and data breaches. Since cybersecurity is borderless, no individual state can combat its challenges alone. A holistic approach coupled with a collective response is

necessary for states to monitor and govern cyberspace and conduct ICTs to ensure Cyber Diplomacy's safety and security effectively.

Considered one of the fastest growing economies, with annual GDP growth of about 7% for several consecutive years, Cambodia also comes along with the rapidly expandinguse of technology. The number of connected users and devices in the country has been increasing at a frenetic pace, from 4.9 million in 2017 to 8.4 million users in 2019. While promising circumstances augur well for Cambodia, rapid technological advancement could put the country at a high risk of cyberattacks. Studies reveal that Cambodia is still facing problems with cyber awareness and infrastructure. Following the cyberattack incidents in Cambodia, the Anti-Cybercrime Department, a specialised unit under theNational Police of Cambodia, and Cambodia's national computer emergency response team, known as CamCERT, were established subsequently. In addition, to enhance cybersecurity, Cambodia has advanced its ICT infrastructure, including hardware and software and launched a Sub-Decree on a National Internet Gateway on February 16th, 2021, to regulate online traffic in the interest of protecting national security and maintaining social order.

Objectives

Considering the importance of cybersecurity and the growing incidents of cybercrimes, the National Institute of Diplomacy and International Relations (NIDIR) is hosting a seminar under the theme "Cyber Diplomacy: Enhancing Cybersecurity and Tackling Cybercrimes". The main objectives of the seminar are to:

- Raise awareness and spark meaningful discussion on cyber diplomacy, cybersecurity strategy and laws launched by the Royal Government of Cambodia and on crimes in the cyberspace
- Identify key challenges, opportunities and needs in support of strengthening

cybersecurity andcyber governance within MFA-IC officials

- Share the confidence-building measures to reduce the risks stemming from the use of ICTs

Expected Outcomes

- Participants can expect to learn about:
- ICT development, with its opportunities and challenges
- Promoting self-awareness of the cybersecurity content to be considered in the augmented ear of science, technology and innovation
- Lessons learnt of cybersecurity issues, cybercrimes, management, preventive measures and recommendations from professionals and practitioners.

Date and Venue of the Seminar

- Conducted in two separate sessions, the seminar will be virtually held on **23 March 2022**.
- Targeted Participants: Union Youth Federation of Cambodia (UYFC)

Kingdom of Cambodia

Nation Religion King

Ministry of Foreign Affairs and International Cooperation

National Institute of Diplomacy and International Relations

Mekong-Lancang Cooperation

Tentative Agenda

Kick-off Workshop of Building Capacity in Cyber Diplomacy Project

"Cyber Diplomacy: Enhancing Cybersecurity and Tackling Cybercrimes"

March 23, 2022

Zoom Meeting

September	**Kick-off Workshop**
8:30-9:00	Registration and Seating
9:00-09:10	**Opening Remarks** **H.E. Mr Tean Samnang,** President of National Institute of Diplomacy and International Relations
09:00-09:15	Photo Session
9:15-10:45	**Presentations by** 1. **H.E. Lieutenant General Chea Peou**, Director of Anti-Cybercrime Department, General Commisiariate of National Police 2. **Mr Ou Phannarith**, Director of ICT Security, MPTC 3. **H.E. Mr San Chanrithy**, Senior Officer in charge of Cybersecurity and Director of Finance and Accounting Department, MFA-IC. 4. **Dr Alamgir Hossain**, Professor of Artificial Intelligence and Vice President of Academic Affairs and Research, CamTech University 5. **Mr Touch Ra**, Cybersecurity Trainer, Proseth Solutions 6. **Mr Bong Chansambath**, Deputy Director of Centre for Inclusive Digital Economy, Asian Vision Institute
10:45-11:15	Q & A Session
11:15-11:25	Wrap-up and closing remarks **H.E. Mr Tean Samnang,** President of NIDIR

MINISTRY OF FOREIGN AFFAIRS AND INTERNATIONAL COOPERATION
NATIONAL INSTITUTE OF DIPLOMACY AND INTERNATIONAL RELATIONS

Concept Note

"Diplomacy in Cyberspace: Thriving through Geopolitical Storms"

24 August 2022

At Hyatt Regency Phnom Penh

With the proliferation of Information and Communication Technologies (ICTs) and the emergence of the "Internet of Things" (IoT) projected to attract an exponential number of devices being connected to the network, cyberspace and ICTs carry enormous potential for economic and social development across societies. However, their all-encompassing, ubiquitous nature and their growing political application pose increasingly significant risks to global economic value and to international peace, stability, and security. Cybersecurity has reached head-of-state-level attention and has become a major source of concern for policymakers, as it has been considered the fifth domain of warfare after land, sea, air and space.

"Cyber Diplomacy" – a term that refers to the use of the internet and digital tools in diplomatic activities – embodies a new discipline of diplomatic practices for the 21st century in pursuit of more cohesive global governance, where states can engage and seek ways to address cyber-related issues peacefully. However, rapid digitization increases the attack surface at a pace that is not matched by efforts to secure it or by the international community as a whole to showcase responsible behaviour in cyberspace, so the diplomatic community is left to grapple with these issues. It is also a domain of not only strategic importance but one that touches and influences the everyday lives, socially and economically, of

individuals at every level. Since cybersecurity is borderless, no individual state can combat its challenges alone. A holistic approach coupled with a collective response is thus necessary for states to monitor and govern cyberspace and conduct ICTs to ensure Cyber Diplomacy's safety and security effectively.

Given that cyber diplomacy is a relatively new discipline, the field itself remains underexplored from the perspective of International Relations. The reason was that cyber issues were first considered technical matters to be predominantly addressed by experts. It has been recognised as a key topic for countries' foreign policies and has become a necessity for governments to formulate national cyber strategies to deter the proliferation of cyber attacks and sustain the peaceful use of digital technology. To further complicate the matters, cyber governance, one of the main components of cyber diplomacy, has yet to have a universal body and law to govern this domain. The ongoing issue concerning 'freedom of the internet' and 'sovereignty of the internet' has divided the international community. The United Nations (UN) has yet to find a way to mend the gap. Due to the differences in interests and application of internet norms, there remains a politically contentious sphere of how cyberspace should be regulated and governed. With the consideration above, although this seminar is about cyber diplomacy, the benefits and risks of using digital technologies in diplomatic endeavours should be discussed. Hence, the challenges of digital diplomacy should be addressed alongside those of cyber diplomacy.

Objectives

Considering the growing importance of cyber domain-related issues, the National Institute of Diplomacy and International Relations (NIDIR) is hosting a seminar titled "Global Governance in Cyberspace: Its Impact on Geopolitics and Socio-Economy". The main objectives of the seminar are two folds:

- Addressing the challenges of digital diplomacy and identifying strategies to optimize the use of ICT and social media technologies in diplomacy while minimizing their risks.
- Addressing the challenges of global governance of the Internet in the broader spectrum of cyber diplomacy

Date and Venue of the Seminar

- The seminar will be held 24 August 2022 at Hyatt Regency Phnom Penh.
- Targeted Participants: Ministry of Foreign Affairs and International Cooperation, Cooperation Partners from Laos and Myanmar.

Kingdom of Cambodia

Nation Religion King

Ministry of Foreign Affairs and International Cooperation

National Institute of Diplomacy and International Relations

Mekong-Lancang Cooperation

Tentative Agenda

Cyber Diplomacy Seminar on

"Diplomacy in Cyberspace: Thriving through Geopolitical Storms"

24 August 2022

At Hyatt Regency Phnom Penh

Time	Event
7:30-8:30	Registration and Seating
8:30-8:35	**Opening Remarks by** **H.E Chhem Kieth Rethy,** Minister Attached to the Prime Minister
08:50-09:05	Keynote Address by **H.E. Mrs Yentieng Puthirasmey**, Secretary of State Ministry of Foreign Affairs and International Cooperation
9:05-9:10	Book launching of "Cambodia in Cyberspace" Introduced by **H.E. Chhem Siriwat**, Advisor to the Council for the Development of Cambodia and Director of Centre for Inclusive Digital Economy, Asian Vision Institute
9:15-9:55	**Panel 1:** Digital Diplomacy: The Challenges of Using Internet in Diplomacy Activities **Moderator**: **H.E Dr Chhem Kieth Rethy,** Minister Attached to the Prime Minister **Panelists**: ▪ **H.E. Dr Hing Vutha**, Advisor to the Ministry of Industry, Science, Technology and Innovation; Institute for International Trade, University of Adelaide, Australia ▪ **Mr Ou Phannarith**, Director of ICT Security, Ministry of Post and Telecommunications ▪ **Mr Bong Chansmbath**, Deputy Director of Centre for Inclusive Digital Economy, Asian Vision Institute ▪ Panelist from Lao PDR

9:55-10:25	Q & A Session
10:25-10:40	**Panel 2:** Cyber Diplomacy: The Challenges of Global Governance of Internet **Moderator**: **Dr Chheng Kimlong**, Vice President of Asian Vision Institute **Panelists**: ▪ **H.E. Mr Tean Samnag**, President of NIDIR ▪ **H.E. Mr Chhem Siriwat**, Advisor to the Council for the Development of Cambodia and Director of Centre for Inclusive Digital Economy, Asian Vision Institute ▪ **H.E. Dr Tat Puthsodary**, Advisor to the Ministry of Commerce
11:15-11:55	Q & A Session
11:55-12:10	Closing Remarks **H.E. Mr Tean Samnang**, President of NIDIR