Interview – Mark Manantan

https://www.e-ir.info/2022/02/19/interview-mark-manantan/

E-INTERNATIONAL RELATIONS, FEB 19 2022

This interview is part of a series of interviews with academics and practitioners at an early stage of their career. The interviews discuss current research and projects, as well as advice for other early career scholars.

Mark Bryan Manantan is the resident Vasey Fellow at Pacific Forum, Hawaii and an AI Research and Policy consultant at the Asia Society Policy Institute in Washington D.C. Concurrently he is also a research fellow at the AI Asia Pacific Institute in Singapore and a non-resident fellow at the Center for Southeast Asian Studies at the National Chengchi University in Taiwan. Prior to that, he also held visiting fellowships at the Center for Rule-Making Strategies, Tama University; the Japan Foundation in Tokyo, Japan, and the East-West Center in Washington D.C. His current research examines the nexus of cybersecurity, artificial intelligence, and critical technologies in the Indo-Pacific. Mr. Manantan's research and policy-relevant work has been published by the Australian Journal of International Affairs, the Cyber Defense Review, Asian Politics and Policy, Issues and Studies, the East Asia Forum, the Diplomat, the Asia Pacific Bulletin, and the Philippine Star. He obtained his Bachelor of Arts (magna cum laude) in Broadcast Communication under the Presidential Scholarship at the University of the Philippines. A recipient of the Australia Awards Scholarship, he also holds a Master of International Relations (Advanced) with Honours from the Australian National University.

What (or who) prompted the most significant shifts in your thinking or encouraged you to pursue your area of research?

My mentor-turned-confidante and former thesis adviser, Professor Elizabeth Enriquez, Ph.D. from the Department of Broadcast Communication, College of Mass Communication, University of the Philippines Diliman was the very first person who opened my eyes to the world of research. During my third year, I enrolled in her course Broadcast Communication 180: The Political Economy of Broadcasting where I learned about critical media and cultural studies. Although Broadcast Communication was a very production-heavy course where we write scripts, produce shows and documentaries, and edit videos, the political economy class provided me with a distinct lens on how to frame the stories or narratives we produce. I gained a better sense of my responsibility as a storyteller to highlight underlying tensions between power, ideological proclivities, and structural conditions through our production in broadcast and digital media.

How do you think your background in Communication informs the way you analyze International Relations? What new perspective does it give you as a policy analyst?

International Relations and media communication are very interrelated. Stories on geopolitics, economy, trade, diplomacy, and culture are very much reflected in current events or news cycles. With my media background, especially in writing and producing news, I can critically analyze how news articles, editorials, commentaries, or interviews are framed to suit a particular narrative. My affinity with media allows me to keep track of past and latest developments unfolding at the national, regional, or international level which is highly crucial in conducting policy-relevant research. With this grasp, it gives me the capability to quickly analyze trends based on existing and historical data to forecast outcomes or even formulate several future scenarios. In my work in cybersecurity, particularly on threat intelligence, communication is fundamental in researching open-source channels or platforms to provide the

Interview – Mark Manantan

Written by E-International Relations

strategic context to triangulate other sources of information. Writing or communications, in general, is also a very undervalued asset in cybersecurity. Through my communication skills, I can bridge the policy and the technical side of cybersecurity, producing important briefs for key decision-makers or media articles that inform the man on the street.

In your article, you describe an increasingly uncertain international landscape of cybersecurity cooperation. Why is this so and what are some emerging trends that would indicate otherwise?

Undoubtedly, the US and China's strategic rivalry is putting too much strain on global internet governance. But aside from the growing tensions between US and China, the rise of non-state actors such as Information and Communications Technology giants and the hacker-for-hire industry are also exerting equal if not too much influence on the strategic, operational, and normative dynamics in cyberspace. Their growing influence has profound consequences in cybersecurity and geopolitics. States no longer have a monopoly on the overall physical, information, and digital dimensions of the cyber domain. For instance, cybersecurity firms like FireEye/Mandiant and Trend Micro are at the forefront of collecting cyber data and generating analyses given their special access to both public and private infrastructures. They have unparalleled access to data breaches and cyber intrusions. States may invoke national security to obtain access to such pertinent data, but they do not possess timely and direct visibility of such information. Companies like Microsoft have also proposed initiatives like the Digital Geneva Convention that reinforces or supports discussions of cyber norms on the international stage. Although, there is the obvious commercial interest at play, inevitably, they are becoming key players in shaping the strategic and normative contours of cyberspace alongside state actors.

The proliferation of spyware such as Pegasus, most notably from groups like NSO, also raises further questions on the extent, reach, and influence of non-state actors—private and commercial entities in particular—while the hacker-for-hire industry will continue to gain traction due to the growing low cost and accessibility of hacking tools. On the other hand, we will also see the mobilization of potentially more citizen journalists from Bellingcat and Co-FACTS based in Taiwan who are using open-source intelligence resources and social media to uncover conflict, crime, human rights abuse as well as fact-checking and potentially detecting computational propaganda tactics like deep fakes.

How would you differentiate the cybersecurity strategies of the United States vis-à-vis that of the European Union's in the Indo-Pacific region? Would you say that these two approaches are compatible?

The United States is gradually rolling out more laser focus initiatives to counter the growing threats in cyberspace. Last year, the US Persistent Engagement Strategy has become an important concept on how to confront adversaries operating in the gray zone. Under the Biden Administration, the US is also reviving its cyber diplomacy efforts, especially in Southeast Asia. The EU has also been proactive in engaging countries in the region through capacity-building, particularly through ASEAN. With the advent of Artificial Intelligence (AI), and rapid digital transformation in Southeast Asia, the EU's General Data Protection Regulation is becoming an important reference framework on data governance in the region, especially with the ongoing debates on data localization. Given the US' current tenor on cyber diplomacy and the EU's emphasis on cyber capacity-building and the promotion of cyber norms in Southeast Asia, I would argue that there are areas of convergence they can explore especially in strengthening the region's adoption of international standards, risk-management approaches, and threat-information sharing.

In what ways is cyber diplomacy being pursued among Indo-Pacific states? How can cyber diplomacy help balance out the differences in countries' maturity and capacity?

Cyber diplomacy engagements cut across bilateral, minilateral, plurilateral to multilateral levels in the Indo-Pacific. Through capacity-building, advanced economies provide the necessary resources and expertise to help developing economies improve their technological competitiveness in the data-driven economy. Although advanced economies often invest resources to undertake cyber diplomacy initiatives, I would argue that it plays even more to their advantage given the vast number of Western companies operating in Southeast Asia.

Interview – Mark Manantan
Written by E-International Relations

Fundamentally, cyber diplomacy eases asymmetries because it recognizes that no country no matter how technologically advanced is immune from the borderless nature of cyberattacks. Regular and constant dialogue, training, and exercises allow countries to take stock of best practices and lessons learned from known cyberattacks and incidents regardless of their maturity or tech capacity. Cyber diplomacy also supports Global South-to-South cooperation. Developing economies can learn from their peers given their shared experiences and conditions. Such a dynamic can unlock potential solutions that generate a more localized or tailor-fit intervention to cyber threats rather than exporting frameworks or models that were applied elsewhere or simply do not match their technological and cultural context.

What are you currently working on?

I am currently working on several tech-related projects that are due to launch this 2022. I am also watching key tech trends in geopolitics that includes the proliferation of ransomware as a service, the commodification of cyber capabilities, the inherent risks of the Internet of Things, adversarial AI, and computational propaganda.

What is the most important advice you could give to young scholars?

The field of foreign policy and international affairs can be very intimidating especially to young scholars from the Global South. As a young scholar myself, I always go back to my unique story. This means tapping into my core and asking the following questions: who you are, what inspires or motivates you, and most importantly what you believe or stand for. From there, you will be clear with your intention and what you can contribute to the conversation, which then moves into solid action. Going back to your story will help you navigate the challenges in our industry, and make you realize the power and influence you hold in your hands in shaping the course of your country or the world's history in the years or decades ahead!