Name: Ronit Singh **CDAD** **Date:** 5 September, 2021

CYBERWARFARE

Week 2 Reading Summary

"Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance"

The chapters one to three of the book by Laura DeNardis, *"Who Runs the Internet? The Global Multi-stakeholder Model of Internet Governance"* go into depth explaining the concept behind the 'Multi-stakeholderism' and 'who actually owns or governs the internet in today's technology dominated world'. It touches on the various sub-issues of the cyber world such as Privacy, Content Control, and Human Rights, which the various public and private governing bodies should take into account while creating norms, rules and regulations for internet stability and freedom. The book compares cyber issues in terms of four dimensions: depth, breadth, fabric and compliance. Taken together, these chapters bring into sharp relief the many global tensions over administrative control of the internet and the governance innovations necessary to keep the internet stable and secure in the midst of rapid technological change and rising contention.

The book states that "providing security is a classic function of government" (DeNardis, 8). With a rapidly growing population using the internet, and an easy and universal access to technology, "cyber attacks can come through several vectors, such as humans and hardware supply chains, as well as malware delivered over the network." (DeNardis, 7). That is precisely why control over the internet is more important now than it was decades ago. Taking into account the technical aspects of the internet is just one of many things to consider. The book supports this by stating, "Naming and numbering is only a small part of internet governance, and while internet governance is at the heart of cyberspace, it is only a subset of cyber governance." (DeNardis, 7). In this "era of big-data", given the increases in computing power and storage, governments are trying hard and spending huge amounts of resources to increase their privacy and security keeping in mind it's citizens. However, no system is completely safe. Hence, governments and private-sector IT security organizations should keep on evolving accordingly with technological developments taking place each second.

The book also delves deeper into the concept of 'Multi-stakeholder governance model', while also touching upon the 'Distributed internet Governance Ecosystem'. According to the book, "Multi-stakeholderism is defined here as two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature, and characterized by polyarchic authority relations constituted by procedural rules." (DeNardis, 20). However, Ideological libertarians proclaim that "information wants to be free," portraying the internet as the end of government controls. This shows the conflicting sides of internet governance. Moreover, trying to develop a treaty for the broad range of cyberspace as a whole could be counterproductive. That is why the Multi-stakeholder governance model is considered a better contender due to it's flexible nature and separation of functional areas, tasks, and internet governance responsibilities among various governmental or non-profit government-partnered private organizations such as IANA, IETF, W3C, NTIA, ISPs, network operators, software companies, registry operators etc. While the "Distributed internet Governance" being an issue-driven approach, this framework allows for collaboration between various actors and institutions that share their expertise to solve governance issues at the local and global level. Two related tools are at the centre of this framework. First, a "living database" (p. 109) facilitates data and information sharing on tried and new approaches, relevant actors and best practices. Similarly, "knowledge networks" (p. 110) allow experts to share their expertise and organize around issues within their scope of interest.

Another book by Ben Buchanan I have been reading since the past few days, *"The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations"* shows the kinds of security dilemmas that nations go through in cyberspace and how we're moving from the era of nuclear warfare to the age of cyberwarfare. This book raises some concerns on cyber espionage considering it is on the rise due to its quick operational procedures and non-risky nature on human life. Countries don't consider it illegal as of now. However, "a nation's means of securing itself threatens the security of others and risks escalating tension" (Buchanan, 2016). DeNardis's book as well touches upon this topic slightly.

What surprised me?

There was one aspect of cyber governance that surprised me i.e. offence is cheaper than defence. I could think of a few reasons behind it, but this statement made me a bit curious. I was under the impression that attacking any big corporation or a nation would require more resources and high-level skills, and hence more money. However, thinking in broad terms, I understood that defense would require continuous monitoring and upgrades in security with evolving exploits and vulnerabilities in today's world. The attackers need to get it correct once in order to penetrate a system, but the defense should be correct all the time in order to prevent the attacks from being successful.

Moreover, the book also mentioned some authoritarian countries - Russia and China - that have imposed strict measures on access to the internet. It mentions, "the Chinese government's growing efforts to suppress dissidents and control Internet content via the "Great Firewall" of China." (DeNardis, 50-51). The part about having a separate firewall for the whole country surprised me. I previously knew that China didn't allow many websites to be accessed by its people and that they had separate versions of them that abided by their rules, but I didn't know that they had a separate firewall in place for the whole country! That was good to know.

Questions?

I had a few questions in my mind that are connected to DeNardis's book.

1. How can one mitigate cyber attacks between nations and have common rules and regulations for all countries? Any possible strategies?
2. Is there an equal offence-defense balance in today's cyberspace? If not, then which one is more weighted and why?

Works Cited

GLOBAL COMMISSION ON INTERNET GOVERNANCE. *Who Runs the Internet?: The Global Multi-Stakeholder Model of Internet Governance.* Centre for International Governance Innovation, 2017, www.jstor.org/stable/resrep05243. Accessed 4 Sept. 2021.

Buchanan, Ben. The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations. : Oxford University Press, 22. Oxford Scholarship Online. Date Accessed 4 Sep. 2021 <https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780190665012.001.0001/acprof-9780190665012>.