**Position Paper** ****

**Name of the delegate:** Divit Narang

**Country:** Cambodia

**Committee:** United Nations General Assembly

**Agenda:** Responsible state behavior in cyberspace for International Security

Cambodia is one of the fastest growing economies in the world. Companies and organizations are rapidly expanding their use of technology to accomplish impressive economic growth. The government has also promoted the use of technology by eradicating landmines with demine robots, promoting financial inclusion and improving the digital infrastructure. Technology has also eased and supported medical procedures such as mobile apps for keeping track of medical records and vaccination status during the pandemic.

Transactions and communication of illicit businesses all pass through the digital world which makes the cyberspace vulnerable to any attacks or cybercrimes. A cyber attack in 2018 to provide the Chinese government with widespread visibility into Cambodian elections and government operations was investigated by an independent team of researchers from industry leading cyber Security Company.

Cambodia is in the initial stages of establishing its own cyber governance program.

Four key gaps emerge from the analysis of Cambodia’s cyber governance efforts and underlying motivations: government transparency, human and technical resources, regional collaboration and defined goals. Although some fundamental obstacles like restriction on free expression will remain for some time, the use of international standards, frameworks and metrics can help Cambodia put an organized system in place to protect its critical infrastructure from cyber attacks, the fundamental objective.

The government must build a unified front, including the public, private and academic sectors, to provide the insight and collaboration required to develop cyber strategy and deal with complex problems. Cambodia set aggressive goals in its vision to become a fully developed country by 2050, including investing heavily in digital infrastructure, transforming Phnom Penh, Siem Reap and Battambang into smart cities, joining the ASEAN Smart Cities Network.

A large-scale cyber attack on critical ITC infrastructure before these technologies are fully implemented and secured could severely hinder their efficacy and expansion, and therefore, have direct negative consequences for Cambodia’s economic growth. It is imperative that Cambodia prioritizes a well thought out cyber governance strategy by design rather than ad hoc response to security breaches.