Cyber Security

Panel: Session 2 (Regency Room)
Date/Time: Tuesday, April 30, 2013 / 14:00-15:15
Speakers: Eneken Tikk-Ringas, IISS-Middle East
                Richard Falkenrath, Council on Foreign Relations
                Neil Robinson, RAND Europe
                James Steinberg, Syracuse University

Rapporteur: Ardie Ermac, Korea University

The inherent complexity of cyber security and the various policy responses at the national and international level figured centrally in the discussion in this session. Dr. Eneken Tikk-Ringas, opened the session by highlighting the significance of cyber security in our contemporary understanding of the fundamental concepts of international peace and security and their implications for various policymaking processes.

There was a consensus among the speakers that the issue of cyber security makes for a complicated policymaking process, which calls for a multi-stakeholder approach. Explaining US policy on cyber security, Dr. Richard Falkenrath pointed out that the American strategy is based upon six pillars. The first relates to the US government's approach to the Internet. Dr. Falkenrath noted that the US maintains a hands-off approach to the Internet and leaves its management to private actors. As manifested in increasing government spending in the protection of ".gov" and ".mil" websites, the second pillar emphasizes safeguarding US government systems. The third pillar relates to the use of cyber-espionage by the US government, which is done not for the benefit of US-led chartered companies but strictly for strategic reasons. The fourth is concerned with the protection of non-governmental systems. He noted that there is no consensus among the US government writ large on the measures to protect non-.gov or non-.mil domains. Fifth is something that has not been done before, which relates to recent efforts from the US government to call out cyber-intrusions emanating from China. And, lastly, the sixth pillar involves the impact of

THE ASAN INSTITUTE for POLICY STUDIES

these persistent problems relating to cyber security on Chinese exporters trying to make it in the US market.

The second speaker, Mr. Neil Robinson, focused his talk on the recently published cyber security strategy of the European Union. Besides a model of economic integration, Mr. Robinson noted that there is an opportunity for the EU to model through on the issue of cyber security. The EU directive aims to set out various policies in three main areas: law enforcement and cooperation; network and information systems protection; and military and defense security capabilities. The penultimate goal of the EU directive is primarily to forge a coordinated and coherent approach to address cyber crime within the region and at the international level.

The third speaker, Mr. James Steinberg, looked into the past for inspiration on how to deal with present sources of cyber insecurity. Mr. Steinberg noted that the issues related to cyber security such as espionage, theft, and sabotage are not necessarily new and have existed before the advent of high technology and computers. He argued that we can apply the lessons learned from what has worked in the past and can develop a set of rules or strategies to deal with the current threats.

In sum, the discussions largely revolved around three fundamental issues: first, the concept of cyber security; second, the appropriate responses and/or legal instruments to deal with cyber criminals; and, finally, the relationship between cyber security and other issue areas such as economics, privacy, telecommunications, and e-commerce. In addressing all these questions, the speakers generally agreed that perhaps the overriding challenge currently facing states is how to implement a multi-stakeholder approach in the domestic and international arenas.

THE ASAN INSTITUTE for POLICY STUDIES