Dealing with Russian and North Korean government hackers
Nori Katagiri, Associate Professor of Political Science, Saint Louis University

Abstract:

I present a set of policy prescriptions for governments based on an analysis of advanced persistent threats (APTs), highly clandestine cyber attack groups. APTs serve leaders of sponsoring states in the achievement of multiple purposes, including espionage and sanctions evasion. I show how the current configuration of cyberspace permits a variety of APT actions. That is, APTs thrive because state sponsors leverage their technical skills to increase national interest and extend state protection from criminal investigation and international scrutiny. APTs also thrive in a restricted yet permissive environment where information and communication technology (ICT) empowers them as cyber attackers and international law is severely restricted from applying existing principles of behavior to these groups. I show how these dynamics work in a set of case studies on the activities of Fancy Bear and Lazarus Group, APTs associated with Russia and North Korea, respectively.

Based on this analysis, I draw a set of policy prescriptions for the international community to deal with the threats posed by APTs. I will discuss what Western governments can do to deal with them by strengthening the current international legal regime and domestic law enforcement authorities. I will also incorporate in my discussion the role that emerging technologies like the blockchain technology play and how they shape and reshape APTs’ capability to carry out their missions.