Cyber Challenges to International Human Rights

Title: Doxfare – Election Hacking as Prohibited Intervention

Name: Ido Kilovaty

Institution: Yale Law School

Abstract:
Alleged Russian digital interference during the 2016 U.S. presidential election presented international law with the challenge of characterizing the phenomenon of politically motivated leaks by foreign actors, carried out in cyberspace. Traditionally, international law's norm of nonintervention applies only to acts that are coercive in nature, leaving disruptive acts outside the scope of prohibited intervention. This notion raises a host of questions on the relevancy and limited flexibility of traditional international law in relation to new threats and challenges emanating from the use of cyberspace capabilities. The discourse on transnational cyberspace operations highlights how it has become increasingly difficult to deal with nuanced activities that cause unprecedented harms, such as the Democratic National Committee hack, as well as disinformation campaigns on social media, online propaganda, and leaking of sensitive information.

This article argues that foreign actors meddling with a legitimate political process in another State through cyberspace ought to be in violation of the norm of non-intervention. Although seemingly the constitutive coercion element is absent, international law should adapt to the digital era's threats, and consider non-coercive interferences that constitute "doxfare" – the public release of sensitive documents – with the intent of disrupting legitimate domestic processes, as violations of the norm. As this paper contends, cyberspace operations are distinct in their effects from their physical counterparts, and a traditional standard of coercion for the norm on non-intervention is outdated and requires the introduction of a more nuanced approach, that takes into account interventions that are non-coercive in nature.

Keywords: cyber warfare, information warfare, doxing, international law, non-intervention, cyber security, cyber intervention, international relations