Cyber Challenges to International Human Rights

Title: State Operated Hackings: Human Rights in the Cyber Era

Name:

- Prof. Amnon Reichman
- Adv. Ido Rosenzweig

Institution: The Minerva Center for the Rule of Law under Extreme Conditions University of Haifa

Abstract:
What happens when a state hacked a computer placed abroad and gained access to private information that is completely irrelevant or necessary for its activity? What are its obligations towards that information? Towards the owner of that information? Would it make a difference whether it was a case of one computer, several or many computers?
The fact that states take advantage of extraterritorial cyber hacking abilities should not come as surprise. While in many states, the internal use of hacking activity has been subjected to both domestic legislation and international human rights law (IHRL), the situation has not been so clear with regard to extraterritorial hacking. In fact, in the recently published Tallinn 2.0 the group of experts failed to reach a consensus over the applicability of IHRL over such operations.
Our research starts with the basic premise that when hacking to a computer one gains some level of control over it and the information with in, and combine it with the extraterritorial applicability of IHRL when the state has gained sufficient control. Thus we address the state's obligations to respect, protect and fulfill relevant human rights requirement and obligations towards any information obtained from the hacked computer(s)..