CENTER FOR
APPLIED CYBERSECURITY RESEARCH

2016–2017
Speaker Series

Authoritarian Soft Power?

Russia, International Cyber Conflict, and the Rise of "Information Warfare"

Jaclyn Kerr

April 27 | 12pm | Ostrom Workshop
Tocqueville Rm, 513 N. Park Ave. *(lunch provided)*

Cosponsored by
OSTROM WORKSHOP PROGRAM
ON CYBERSECURITY AND INTERNET GOVERNANCE

In the lead-up to the November 2016 U.S. presidential election, the American media audience was barraged by a surprising display of confidential information and correspondence stemming from hacked private and organizational emails and other records, most notably from the Democratic National Committee (DNC). After months of speculation concerning Russian involvement in the hacking which led to the release of private documents and data on the sites WikiLeaks, DCLeaks, and Guccifer 2.0, in early October the Obama administration formally announced its belief that the Russian Federation was behind the disclosures and that these were intended to interfere with the United States election cycle. Reporting around these incidents swiftly resorted to labels of "cyber-attack" to describe the purported Russian involvement. The administration also indicated its consideration of a "proportional" response.

For those familiar with Russian politics, such strategic release of "compromising material" concerning political rivals does not appear so unusual, with so-called "kompromat" having been utilized to tarnish reputations and undermine opponent messages for years. Recent Russian examples have included leaked recordings of private phone conversations by opposition leaders and video footage of prominent critics in bed with prostitutes. The international deployment of such a tactic to influence the domestic politics of another country is a little more novel, however.

This talk examines Russia's evolving information strategy abroad, examining the variety of different tools now being used to try to influence the domestic political discourse and media space of other countries. From online trolls and bots to DDoS attacks, hacking, kompromat, deception, and targeted propagandistic media outlets, the talk outlines current Russian tactics of information manipulation and "information warfare" recently deployed in settings from Ukraine and Georgia to Syria and the United States. The analysis discusses how many of these techniques – aimed at shaping the narrative in a complex information space – have long been utilized at home to manage Russia's own public discourse and media space, but only recently emerged as tools in the country's strategic playbook to exert its influence in international affairs.

Dr. Jaclyn Kerr is a Postdoctoral Research Fellow at the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory. She is also an Affiliate at the Center for International Security and Cooperation (CISAC) at Stanford University. Her research examines cybersecurity and information security strategy, Internet governance, and the Internet policies of non-democratic regimes. Areas of interest also include risk and governance in relation to emerging technologies, and the relationships between security, privacy, and freedom of expression in Internet policy. She was a Science, Technology, and Public Policy (STPP) Pre-Doctoral Fellow with the Cyber Security Project at the Belfer Center for Science and International Affairs and Visiting Scholar at the Davis Center for Russian and Eurasian Studies at Harvard University in 2015-2016 and a Cybersecurity Predoctoral Fellow at Stanford's CISAC in 2014-2015. Jackie holds a PhD and MA in Government from Georgetown University, and an MA in Russian, East European, and Eurasian Studies and a BAS in Mathematics and Slavic Languages and Literatures from Stanford University. She has held research fellowships in Russia, Kazakhstan, and Qatar, and has previous professional experience as a software engineer.