Making Democracy Harder to Hack

A Collaborative Research Workshop

Australian National University-Indiana University

Washington, D.C., Sept. 6-7, 2018

Abstract

In the wake of the 2016 U.S. elections, a debate is brewing about how to mitigate the risk of hackers who are now not only targeting individuals, firms, and governmental secrets, but who are also now going after the election machinery upon which U.S. democratic society is built. Beyond political parties, vulnerabilities are replete across the myriad locally managed systems that together comprise the U.S. election infrastructure, including voting machines that in some cases—such as in the case of many Pennsylvania counties—have “zero paper trails” and are often running “severely outdated operating systems like Windows XP,” which has not been patched since 2014. Although the decision to classify elections as critical infrastructure in January 2017 has helped speed progress on this issue, much more remains to be done. And securing election infrastructure is not just a problem for the United States. Developing nations, emerging markets, and advanced democracies around the world, including Australia, are grappling with the best ways to manage cyber risk and build trust in diverse voting systems. This gathering of academics, civil society groups, private-sector representatives, and policymakers is designed to foster the bilateral dialogue between the U.S. and Australia by deepening scholarly ties, highlighting gaps in our current knowledge, along with areas of policy convergence and divergence with the goal of making both U.S. and Australian democracies—along with our strategic partners and friends around the world—harder to hack.

Link to Collaborative Spreadsheet:

https://docs.google.com/spreadsheets/d/1h9HvRd35A43skbNwP2K3LDOLcurfVvc3jm53AzFOin4/edit#gid=0

Link to RSVP list:

https://goo.gl/forms/SIQrk2ymYTjYmoXh2