Making Democracy Harder to Hack 2.0
May 7–9, 2019 • Canberra, Australia

Collaborative Research Workshop between Indiana University & Australian National University

In the wake of the 2016 U.S. elections, along with follow-up disinformation campaigns making use of "flooding" and "confidence" attacks, a debate is brewing about how to mitigate a range of threats to democratic institutions. Beyond political parties, vulnerabilities are replete across election infrastructure, both in the United States (such as in the case of many Pennsylvania counties that have no paper trails and are often running outdated operating systems) and throughout the Indo-Pacific region. 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. But important questions remain unanswered, including: what are the main ways in which democratic nations can boost deterrence and build resilience against disinformation campaigns and cyber attacks on election infrastructure, e.g., are risk-limiting audits and paper trails enough? How can international cyber threat information sharing be made more seamless to better protect democracies against shared threats? What role can and should international norms play in this process? Ultimately, what can nations—including Australia and the US—learn from one another to help make our democracies harder to hack?