Hacking the Election Conference
The Information Society Project and the Center for Global Legal Challenges
Yale Law School
Tuesday, September 20, 2016

Write up by Isabella Uría, YLS ‘19

The United States leads the world in conventional military might, maintains strategic superiority in terms of its nuclear deterrent, possesses the world’s largest economy, and promotes the ideal of democracy as a centerpiece of American values. So what happens when the integrity of the US democratic process is undermined? During a highly contentious election year, closely watched around the globe, this is a question that bears reflection.

On Tuesday, September 20, 2016, the Information Society Project and the Center for Global Legal Challenges hosted a “Hacking the Election” conference at Yale Law School. The first panel considered the impact of and potential responses to the recent targeted intrusion upon the Democratic National Committee’s computer systems, which led to the publication of thousands of emails and the subsequent resignation of the DNC’s CEO. The second panel discussed potential US electoral vulnerabilities to cyber-attacks or manipulation and considered the effects that such actions could have on the democratic process.

Panel 1 – The DNC Hack
Moderator: Scott J. Shapiro, Charles F. Southmayd Professor of Law and Professor of Philosophy at Yale Law School.
Panelists: Jack Goldsmith, Maurice R. Greenberg Visiting Professor of Law at Yale Law School and Henry L. Shattuck Professor of Law at Harvard Law School; Oona Hathaway, Gerard C. and Bernice Latrobe Smith Professor of International Law at the Yale Law School; Susan Hennessey, Fellow in National Security in Governance Studies at the Brookings Institution.

During the first panel, “The DNC Hack,” participants shared their insights on the legal, political, and security implications of the hack of the DNC computer systems. Shapiro began by reviewing the known facts. In June 2016, after detecting a possible hack and hiring Crowdstrike, a cybersecurity firm, to investigate, the Democratic National Committee was informed that two distinct hacks, conducted by APT 29 (Cozybear) and APT 29 (Fancybear) had been executed against their system. The *Washington Post* broke the story, attributing the hacks to two organizations within the Russian government. Soon thereafter, exfiltrated information was leaked until approximately 18,000 emails between officials of the DNC were published. The hacks have been attributed with some degree of certainty to the government of the Russian Federation, and the backlash against the DNC, resulting from the publication of controversial correspondence between its officials, has yielded questions as to the purpose of these hacks as well as to the appropriate response to such intrusions.

Digital theft and publication, cyber espionage, and interference in elections of foreign nations are not without precedent. Goldsmith asserted that during the Cold War, 117 elections were intervened upon by the reigning superpowers and that 69% of these were US interventions. Espionage and weaponization of information gathered is similarly not without extensive precedent. What is new, said Hathaway, is the scale of information gathered. Hathaway pointed out that while the hack on the DNC databases is unlikely to change the outcome of the election, it undermines the strength of the democratic process, of the DNC in particular, and diminishes overall trust in the election.

Hennessey emphasized that the United States is struggling to develop a comprehensive strategy for response to attacks such as this one and is currently confronted with a "paralysis of too many options." The national military, political, and economic strength of the United States leaves it particularly vulnerable to cybersecurity threats, which are idiosyncratically asymmetric. The scale of vulnerability, particularly as it relates to the nation's lack of a coordinated defense against cybersecurity threats, may yield severe consequences if not addressed. Hennessey went on to posit that traditional deterrence models of responding with unacceptable harm may not be appropriate for grappling with the new cyber threat landscape. But it is imperative that the United States establishes a cost that the adversary will need to factor into their calculus when coordinating an attack – something that will not happen if it remains paralyzed by too many options. "Just choose an option and follow through," Hennessey quipped.

Goldsmith warned that understanding the intent behind a cyber-attack is important for developing a response. While it is widely assumed that the hack may be indicative of Russian support for Republican candidate Donald Trump, he said, the cyber intrusions could also be in retaliation against the U.S.-led sanctions regime against Russia or in response to confrontation in Syria. Hathaway further cautioned that responding against attacks in kind, while potentially creating a cyber deterrent, may result instead in a "tit-for-tat" escalation. She went on to say, "If we think we can hack our way out of this problem, we are probably learning the wrong lesson."

Perhaps the most complex and ill-developed aspect of today's cybersecurity threat terrain is the, at best, nebulous and, at worst, nonexistent legal infrastructure governing it. Hathaway confirmed that while domestic law prohibits cyber intrusions and hacking, international law has little to say on this subject. Additionally, espionage, which has been widely practiced by the United States and by nations around the world, is neither explicitly permitted nor prohibited by international law. There are cases to be made for the applicability of the non-intervention norm of international law and the law of countermeasures to cases of cyber infiltration, according to Hathaway, but it is unclear whether either doctrines adequately address the nature of cyber-attacks, which do not include physical coercion nor are regulated internationally.

The appropriate response to the DNC hack may not be immediately clear, nor are remedies for the lack of international regulation of cyberspace. In the meantime, Goldsmith observed, "the United States has the most robust cyber capability in the world, but it is also the most vulnerable," due to its extensive dependence on computer systems in the public, private, and military sectors. But a normative regime in which such cyber intrusions and interference in domestic affairs from foreign entities are prohibited will not be possible to achieve, asserted Goldsmith, until the United States itself is willing to give up some of its capability or demonstrate restraint in return for reciprocal restraint. Goldsmith stated wryly, "From Sony to OPM to the DNC, there doesn't seem to be much learning that has occurred."

Panel 2 – Hacking the Election
Moderator: Jack Balkin, Knight Professor of Constitutional Law and the First Amendment at Yale Law School.
Panelists: Paul Brewer, Professor in the Department of Communication at the University of Delaware; Michael Fischer, Professor of Computer Science at Yale University, Heather Gerkin, J. Skelly Wright Professor of Law at Yale Law School.

The second panel examined points of vulnerability to hacks in the election process and the possible ramifications of such manipulation in the 2016 elections.

Fischer began with the grim statement, "Every computer can be hacked." However, the picture he painted of the diffuse US elections systems suggested that, even given that many computers in the coming elections may be hacked, the likelihood that the resulting anomalies will have a sweeping effect on the election results is low. Rather than being a federal program, elections are run by individual states, and in fact by individual localities within states. States conduct their elections distinctly, using different voting mechanisms. However, because of the efficiency of computerized voting, more and more elections are moving to computer-based – and therefore hackable – mechanisms for counting votes. Fischer pointed out that DRE machines (touch screen voting machines), in particular, have increased vulnerability to hacking and manipulation, as there are many known hacks against this software that are relatively easy to carry out. Additionally, these aging and poorly updated machines are susceptible to malfunctions, malicious or otherwise, which further undermines trust in their integrity. Other potential nodes of attack exist throughout the election process. Altering voter registrations or executing denial of service attacks on voting machines may cause sufficient chaos to increase obstacles to voting in key states or among key demographics.

Brewer cautioned against focusing solely on the vulnerabilities in the election process to hacks. Manipulating information available to voters, he said, including manipulating search result algorithms related to candidates and their campaigns or the recent DNC hack, can have equally lasting effects on the election results. Public perceptions on the legitimacy of an election process can also have a damaging impact on trust in the results. According to Brewer, in recent public surveys on perceived legitimacy of potential election results, Republicans indicated a greater lack of trust in the legitimacy of the election process in the event that Democratic candidate Hillary Clinton wins the presidential election. Brewer went on to say that, given that Donald Trump has made claims that only voter fraud will preclude him from winning the swing state of Pennsylvania, it is not unimaginable come November, should Clinton win the election, that Trump would not concede, or at the very least, that her win would be accompanied by doubt and distrust.

Unfortunately, it seems that electoral processes and state codes governing them are not adequately equipped to confront problems of voting manipulation and hacks. Gerkin discussed how the differences in recount mechanisms in each state and the lack of federal law to govern recounts enhances the difficulty of responding to election manipulation. Additionally, there is little political incentive to reform this system, Gerken stated, because "Politicians would rather fund roads, jobs, things that voters see and experience than our ramshackle electoral system." In highly political environments, particularly the deeply controversial 2016 presidential election, even if the law were equipped to address the problems resulting from voter fraud or cyber-attacks on the election process, the trust in the legitimacy of the democratic process may be irreparably harmed. Balkin highlighted that integral to the strength of the democratic system is the secure succession of power, and anything that makes succession of power insecure undermines the entire system of our nation’s democracy. Gerken asserted soberly, “By the time you get to the law, it’s already too late.”