POLICY TOPICS

DHS has the lead for most cybersecurity issues yet has been generally ineffective, especially next to DoD. Analyze and propose new ideas on what the White House and Congress should do next.

The US government has ultimate authority to defend the nation and its citizens from external threats. Yet it is the private sector companies – especially those in the IT, telecommunication, and cybersecurity sectors – which have most of the actual power to protect and defend. Analyze and propose new ideas on how to bridge this gap.

There are several projects underway to improve relations in cyberspace with Russia. Yet given the general antagonism on each side, tied to competition and conflict in and through the net, perhaps there is not much point. Analyze and propose options reasonable to the geopolitical situation.

LEGAL TOPICS

What was the main problem(s) that the Cybersecurity Information Sharing Act of 2015 was intended to address, how did it do so, and what are some major limits to its effectiveness?

Discuss the significance and implications of the case *FTC v. Wyndham Worldwide Corporation* (3d Circuit, 2015): http://www2.ca3.uscourts.gov/opinarch/143514p.pdf

What is the Wassennaar Arrangement and what are a few of the major challenge to regulating the export of cyber technologies under it?

TECHNICAL TOPICS

The NSA is the greatest repository of cryptographic expertise in the country and probably the world. As such, it is called upon to render advice to NIST, a civilian agency, that (among other things) sets all non-military government cryptographic standards. In fact, by law NIST is required to consult with them (15 U.S.C. §278g-3). However, the NSA is also charged with breaking encryption systems, and has been known to sabotage standards; consequently, many people, especially abroad, distrust the NSA and hence its advice. Analyze and propose options for resolving this dilemma.

The FBI, the NSA, and probably other government agencies are known to possess some stockpile of “0-days”—security holes for which no patches exist. Some suggest that these agencies should be required to report these holes to vendors, to protect American systems; others say that these are necessarily kept secret to preserve the agencies’ ability to lawfully hack into computers belonging to criminals and hostile governments. A scheme known as the Vulnerabilities Equities Process is supposed to resolve this issue for each 0-day. Is this working well? Should more or fewer holes be disclosed?

By design, the Internet puts control in the hands of end-systems. ISPs can thus do little to protect users from over-the-wire attacks (as opposed, to, say, phishing emails, which can be detected on mail servers—another type of end-system). The benefit, of course, is that end-systems can innovate, without having to consult or coordinate with the ISPs. In today’s world, it isn’t clear that this tradeoff is correct. How can we redesign the Internet to reconcile the two?