In this episode, I interview Rob Knake, Senior Fellow at the Council on Foreign Relations, about his recent report, “Weaponizing Digital Trade – Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity.” The theme of the report is what the US can salvage from the wreckage of the 1990s Magaziner Consensus about the democratizing and beneficent influence of Silicon Valley. I suggest that it really ought to be called “Digital Dunkirk,” rather than invoking a swaggering “weaponization” theme. Rob and I disagree about the details but not the broad outlines of his proposal.

In the news roundup, we finally have a Google antitrust complaint to pore over, and I bring Steptoe’s Michael Weiner on to explain what the complaint means. Bottom line: it’s a minimalist stub of a case, unlikely to frighten Google or produce structural changes in the market. Unless a new administration (or a newly incentivized Trump Justice Department) keeps adding charge after charge as the investigation goes on.

Speaking of Justice Department filings that may serve up less than meets the eye, DOJ has indicted GRU hackers for practically every bad thing that has happened on the internet in the last five years, other than the DNC hack. (In fact, I lost an unsaved Word document in 2017 that I’m hoping will be added to the charges soon.) The problem, of course, is that filing the charges is the easy part; bringing these state hackers to justice is unlikely in the extreme. If so, one wonders whether a policy that requires an indictment for all the cyberattacks on the US and its allies is a wise use of resources. Maury Shenk thinks it might be, at least in demonstrating US attribution capabilities, which are indeed impressive.

While we are covering questionably effective US retaliation for cyberattacks, Maury also notes that the Treasury Department has imposed sanctions on the truly unpronounceable TsNIKhM, a Russian institute that seems to have developed industrial control malware that caused massive outages in Saudi Arabia and may have been planted in US energy systems as well. Again, no one doubts that heavy penalties should be imposed; the doubt is about whether these penalties will actually reach TsNIKhM.

Nick Weaver celebrates the German government’s dawn raid on spyware exporter, FinFisher. Maury expresses modest hope for Facebook’s Oversight Board now that it has started reviewing content moderation cases. Color me skeptical.

Now that we’ve seen the actual complaint, Nick has his doubts about the Microsoft attack on Trickbot. It may be working, he says, but why is Microsoft doing something that the FBI could have done? I pile on, raising questions about the most recent legal theory Microsoft has rolled out in support of its proposed remedies.

Finally, in quick hits: I hum a few bars from “John Henry” in response to a Bloomberg story suggesting that CEOs are successfully beating the AI engines parsing their analyst calls and trading on the results. Maury debunks the parts of the story that made it fun, but not before I’ve asked whether Spinal Tap was decades ahead of its time in repackaging failure. Maury also notes the ho-hum upcoming Judiciary Committee testimony of Twitter and Facebook CEOs about their suppression of the New York Post “laptop from hell” Hunter Biden story. I’m much more interested in the Commerce Committee’s subpoenaing of contacts between the campaigns and those companies. Because you just know the campaigns have a whole strategy for working the speech refs, and it would be an education to see how they do it. Nick and I congratulate Edward Snowden on the confirmation that he’ll be in Russia forever. And I mock the Portland City Council as well as all the journalists who tried to make face recognition toxic – until it turned out that face recognition might help antifa dox the police. Suddenly we can’t expect to stop the march of technology.

And more!
As always, The Cyberlaw Podcast is open to feedback. Be sure to engage with @stewartbaker on Twitter. Send your questions, comments, and suggestions for topics or interviewees to CyberlawPodcast@steptoe.com. Remember: If your suggested guest appears on the show, we will send you a highly coveted Cyberlaw Podcast mug!

*The views expressed in this podcast are those of the speakers and do not reflect the opinions of their institutions, clients, friends, families, or pets.*

Practices
Privacy & Cybersecurity