lawfareblog.com

Cybersecurity: Time for a New Definition

Susan Landau

6-8 minutes

Or maybe we need a new definition of *cyberinsecurity*. Whatever it is, the current U.S. government definition is outdated. But I should start at the beginning …

As you may have noticed, over the last week Paul Rosenzweig and Herb Lin have disagreed about election hacking being a cybersecurity issue. It's likely not the first time they disagreed; it won't be the last. Paul pointed out there is a serious danger of hacking of U.S. voting systems. Herb observed the voting systems weren't hacked, writing that the real cyber issue of the 2016 election was the influence operation that Russia ran. While the voting platforms do not appear to have been hacked this time, there are serious cybersecurity concerns over the technology we use for voting. And the disinformation campaign the Russians ran during the 2016 U.S. presidential election was highly disruptive. In this case, though Herb and Paul disagree, they're both right. But someone else is wrong.

Herb cited the NSPD-54 definition of cybersecurity, which is:

> Prevention of damage to, protection of, and restoration of

> computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation

Herb concluded that the Russian influence operation was not a cybersecurity concern. Under the NSPD-54 definition, Herb's right. But the definition is wrong; it's outdated and should be replaced.

If there is anything we've learned from the Russian cyber activity during the Brexit campaign and the 2016 U.S. and 2017 French presidential campaigns, it's that our cybersecurity protections are completely unprepared to cope with a disinformation campaign. They, and our policies, were focused on protecting computer systems and their data, not on protecting people's minds from misinformation planted on networks users relied upon.

Combating information warfare is complicated. The first step requires letting people who were the targets of the disinformation campaign know they were manipulated. Roger McNamee, who has written an excellent article on the Russian attacks, says this requires major tech companies—Facebook, Google, Twitter, and others—to explicitly inform the targets of the Russian campaign that they were subject to Russian manipulation. (Currently, such information is available through a relatively buried portal

McMamee suggests prohibiting the use of digital bots to impersonate people. That would certainly damp down on the amplification of disinformation. Now there are policy and legal questions to be debated here. Bots have proved useful in making

certain interactions with automated systems more efficient, and a complete ban might be the wrong approach. But banning or controlling their use is certainly within the policy capabilities of Internet companies.

The technical capabilities are a different question. Some bots are easily identifiable: they might have highly periodic or automatic behavior, urls that can identify them as bots, etc. But three decades of history of cyberexploits and cyberattacks shows that attackers only grow more sophisticated. The automated tools that work today to identify bots will be less successful in the future as bot designers discover new ways to fool site defenders. Put another way, we will need new technical tools to defend against bots spreading disinformation.

The same is true about another of McNamee's suggestions, namely requiring transparency about who is behind political *and* issue-based communications. This one is hard. Defining a political ad is relatively easy; defining an issue-based communication is far more complex. And determining attribution—where that communication really comes from—more difficult still. Some of the capability to do this will come from analysis of network traffic, some from sentiment analysis—and some likely from the intelligence agencies. There will be social science and technical research and tools to uncover attribution, which will, in the end, likely only be partially successful.

McNamee also wants Internet companies to clarify *for users* how algorithms like news feeds and search engines work; that is, how certain items are at the top of lists. This is for the user to understand, "Why am I seeing this now?" One can imagine

companies objecting to exposing the secret sauce of their algorithms—the tools of their trade. But let's think for a moment not about the legal and policy issues here, but the technical ones. Done right, enabling users to learn why they are seeing what they're seeing is a fascinating learning tool, and one that will have implications well beyond disarming information warfare. Or as the techie in me says, "Cool."

These are all *technical* aspects to combating information warfare. The psychological aspects (e.g., teaching people how to assess reliability and how to discern fact from fiction) are critical to develop. As machine learning algorithms improve, training people will be insufficient to counter disinformation campaigns. We also need technical tools to disrupt the efforts.

Here's where the U.S. government's definition of cybersecurity is wrong: It was written with the idea that the enemy would attack virtual and physical infrastructure—it did not include psychological warfare. We are now well aware that information warfare is a significant part of the picture. And thus a new definition of cybersecurity needs to be crafted.

We don’t need the new definition to acknowledge that, yes, indeed, the information warfare attacks during the campaigns were cyber tools that used weaknesses in cyber infrastructure to work. And we don't need to wait for the updated definition of cybersecurity to start developing cyber—and other—tools to prevent such attacks in future.

That's separate from the other, extremely important, issue Herb raised, which is healing the sharp political divide that exists in the United States. That is crucial, but it will take considerably more

than fixing buffer overflows to repair that one.