FTCN Replay: Cybersecurity Expert Warns of Government Vulnerabilities Following Salt Typhoon Attack

A leading cybersecurity expert is warning that government mandates designed to assist law enforcement investigations are creating dangerous vulnerabilities that foreign adversaries can exploit, citing the recent Salt Typhoon cyber attack as a prime example of these risks.

In a recent episode of the **From the Crows' Nest** podcast, host and AOC's Director of Outreach and Advocacy Ken Miller talked with Dr. Susan Landau, professor of cybersecurity and policy at Tufts University. Landau recently testified before the House Judiciary Committee about the intersection of cybersecurity threats and government access requirements, emphasizing how policies intended to help domestic law enforcement can inadvertently weaken national security.

Salt Typhoon Reveals Systemic Vulnerabilities

The Salt Typhoon attack, revealed in late 2024, saw Chinese hackers infiltrate U.S. telecommunications networks and compromise sensitive information from senior members of both the Trump and Harris campaigns. According to Landau, the attack exploited vulnerabilities that stem directly from the Communications Assistance for Law Enforcement Act (CALEA), passed in the mid-1990s.

The law required all digital switching systems to be built with wiretapping capabilities, a requirement that many technologists warned against at the time. "If you stop and think about security for a moment, you're now saying any

switching technology has to be built with a wiretap capability in. It sounds sort of crazy if you're thinking security," she said.

The Chinese hackers were able to access not only text messages and voice communications but also "the database of wiretap targets," Landau noted. "What that meant is the Chinese then knew, the Chinese government then knew which of their spies we had found out and which ones we hadn't. They found out not only those, they found out which Russian spies, which Iranian spies, which North Korean spies."

Landau characterized the breach as "a Kim Philby type of catastrophe for the US" – a reference to the British intelligence officer who secretly worked as a double agent for the Soviet Union for decades.

Government Response Highlights Policy Tensions

In response to Salt Typhoon, four of the Five Eyes intelligence alliance members – Australia, Canada, New Zealand, and the United States – issued guidance recommending the use of end-to-end encryption wherever possible. Notably, the FBI, which has historically opposed widespread encryption, was among the signatories.

"That's striking for a number of reasons, including the fact that the FBI was one of the signatories or agreeers to this set of guidance. Even though the FBI itself has been fighting the use of end-to-end encryption for at least three decades now," Landau said.

The fifth member, the United Kingdom, notably did not sign on to the guidance, instead pursuing a different approach through its Technical Capability Notice (TCN) under the Investigatory Powers Act.

UK Policy Creates International Friction

The UK's TCN policy requires service providers to provide unencrypted content when requested by the government and prohibits companies from publicly disclosing such notices. Apple received such a notice and was required to disable its Advanced Data Protection feature for UK users.

"What this means is essentially you can't do end-to-end encryption because end-to-end encryption makes that impossible," Landau explained.

Landau testified earlier this summer for the House Judiciary Committee 's Subcommittee on Crime and Federal Government Surveillance.

"The hearing that I and my colleagues participated in June had bipartisan support that end-to-end encryption is important, that the UK response is inappropriate because essentially the UK is legislating what companies in the United States can do and whether companies in the United States can put in security protections that they deem appropriate," she said.

Recommendations for Moving Forward

Landau argues that the cybersecurity challenge requires viewing encryption not as a privacy versus security issue, but as "a battle between security versus security." She advocates for several key changes:

- **Enhanced law enforcement training**: Current FBI training on technical surveillance consists of just "45 minutes every two years" for all agents. "I can't learn how to use one tool properly in 45 minutes — and I'm a techie," Landau said.
- **Stronger cybersecurity requirements**: She called for moving away from checklist-based approaches toward "red teaming and ensuring that your system is secure against attacks."
- **Data minimization**: "I think what we need to do, among other things, is make data a lot less available. Yes,

> that will make law enforcement's job somewhat more difficult, just like it will make national security's job difficult in one way and easier in another."

The Congressional hearing on "Foreign Influence on Americans' Data through the CLOUD Act" demonstrated rare bipartisan agreement on these issues, with both Democratic and Republican members expressing concern about the UK's approach.

The Broader Context

Landau emphasized that modern cyber threats require a fundamental shift in how law enforcement operates. "90% of investigations have a digital component," she said, yet many agencies remain unprepared for 21st-century challenges.

Landau also warned that cyber attacks bring the front lines of conflict directly to American citizens. Unlike traditional warfare, "there is no distance, geographic distance, when you're talking cyber operations," making domestic cybersecurity a critical national security priority.

As policymakers continue to grapple with balancing law enforcement needs, privacy rights, and national security, Landau's testimony underscores the complex technical and policy challenges that lie ahead in securing America's digital infrastructure against increasingly sophisticated adversaries.

READ SUSAN LANDAU'S CONGRESSIONAL TESTIMONY

Landau testified June 5 for the House Judiciary Committee on "Foreign Influence on Americans' Data Through the CLOUD Act." **Read her full statement to Congress.**