9 November 2020

Memo for: Biden-Harris Transition Team

From: Jason Healey

Subject: A One-Page Cyber Strategy

Summary: Past Federal cyber efforts have failed because there has never been a simple, unifying strategy. Just as the Cold War strategy was simple (containment), as was the Army's COIN strategy (roughly, to win hearts and minds), **the US cyber strategy should be to get defense the advantage over offense.**

Background: Past US cyber strategies have been just lists of actions, with no connection between them or tradeoffs, and few ways to decide between competing priorities.

Quotes from as far back as 1979 show the attackers in cyberspace have the advantage over defenders. Over those four decades, through the hundreds of billions of dollars spent, the patents, and all the missed kids' birthdays, we have not changed that fundamental dynamic.

Discussion: **The US strategy must be to reverse this trend, so that the defense has the edge over the offense**. In short, D>O.

The New York Cyber Task Force examined decades of defensive innovations, in technology, operations and policy, and found D>O is possible but only if we work with **leverage**.

- We overinvest in technologies inside enterprises (e.g. firewalls) rather than those that operate across all of cyberspace (e.g. end-to-end encryption or automated updates). The USG must incentive this through every means.
- We overlook process and organizational innovations. We had to invent CERTs after 1988, CISOs after 1995, and ISACs after 1998. We are ripe for new innovations here, such as organizations built to collaborate on each kind of major cyber incident (counter-DDoS, counter-APT, etc.).

The most **leverage at scale comes from the private sector** – especially the main cybersecurity providers that can act at scale – not the Federal government. This requires three elements:

- *Engage*: Use the bully pulpit to set major goals and enroll traditional and non-traditional allies
- *Empower*: Find ways to better align incentives at scale for the least cost and most minimal government intervention
- *Enforce*: As Beau Woods has put it, rational market choice requires the ability to distinguish between security in market alternatives (patchability, downtime per year), the transaction cost, and a recourse in case of harm. We work across all three. Accordingly when we must regulate, favor *regulation for transparency* not security (like SEC guidance on board responsibility).

Simply put then, the US approach should be (1) getting defense better than offense (2) using leverage, (3) especially engaging, empowering, and enforcing (4) the private sector.

What About US Adversaries? "Engage, empower, enforce" is all well and good, but our adversaries are increasingly audacious. We must continue USCYBER defending forward but only with close NSC scrutiny over metrics of success on whether their actions are working toward D>O.