Drexel Hamilton

A Service-Disabled Veteran Owned & Operated Business

Drexel GPS – "Outside the Wire"

Protecting U.S. Critical Infrastructure from Cyberattacks – Time for a Second Internet?

Photo Credit: Kelsey McClellan – SciTech Daily

The $1 trillion infrastructure bill has finally passed. While it has provisions for improving many areas of this country's infrastructure a glaring issue remains- cyberattacks on infrastructure will continue to increase. The United States has identified 16 sectors of the economy as "CNI" (Critical National Infrastructure) assets for the nation. The Cybersecurity and Infrastructure Agency (CISA) defines critical infrastructure as follows: *"Critical infrastructure describes the physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety."*

The same agency has issued alerts to operators of these sectors to take action to defend against malicious acts and activity. However, this is easier said than done as there are a variety of barriers that complicate and prevent this from happening in an organized fashion. The CNI sectors are a combination of public, private and government entities that lack a national standardized cybersecurity protocol. This complicates the approach taken towards securing our critical infrastructure from cyberattacks. So what can be done?

Building a separate internet strictly for use by select critical CNI operators could be the solution. *Select* is the operative word in this scenario since the residents of this second internet would only be granted access by determination on a graded scale of the residents' association with a critical CNI sector and the perceived impact on national security a compromise of their systems would exploit.

The creation of this "CNI-Internet" would be by no means simple or cheap to implement however, the benefits when viewed from the aspect of national security and the mitigation of the available attack surface for malicious actors to plan and execute cyberattacks would at least make further investigation worthwhile.

There would be many benefits in designing the legal and regulatory framework of this second internet from scratch. We already have the advantage of advancements in technologies such as blockchain, 5G and AI, and (artificial intelligence), and what has been learned in the almost four decades of the current internet's existence. The "hindsight being 20/20" advantages of this would be many. A hypothetical scenario for what this might look like this:

Government entities (incl state & local) operating the selected critical infrastructure would be onboarded. Private companies wishing to continue providing service to CNI assets would be required to migrate only the segments of their operations considered to be vulnerable to attack which could result in interruption of primary functions that would be deemed "critical" to the actual output of the good or services they provide.

For example, a powerplant operator might not be required, or would perhaps not even be allowed to migrate their HR information and payroll activities to the "new internet". However, operations which directly correlate with the function of power generation, distribution, and all **SCADA** (Supervisory Control and Data Systems) would be relocated onto the new "CNI-Internet". A key component of this would be to eliminate "bridging" of legacy connections and IPs from the existing internet. From a regulatory standpoint this would require a new and presumably highly intrusive federal act upon private companies. This would be similar to, but much more focused in scope as the 1996 Federal Communications Act.

The creation of the new "CNI-Internet" would improve upon on what our current system already does in the administration of regulation once legislation is passed. Obviously, there can be improvements and the age-old argument that "regulation kills new businesses/innovation" will always exist. However, businesses always find a way to adapt and more importantly, adhere to new regulations when they are properly structured and enabled with the proper oversight and enforcement tools. Willingness to utilize the enforcement tools by lawmakers would be key to businesses abiding by them.

The current model we utilize for cybersecurity is flawed. An analogy to our current approach can be viewed like this- we are looking to protect vehicles (CNI's) on a road (the internet) that was not originally created with security in mind. The series of patches and protocols being applied to address cybersecurity on the internet are much like taking a family sedan and attempting to transform it into a tank for military use. You can only add so much armor plating before slowing the sedan's performance down, and eventually the suspension will simply fail due to the constant addition of weight.

Public and private partnership in the creation/building of a new internet would in the long run create greater, and more efficient cooperation between these entities. This may not only help provide a more stable platform from which to defend critical infrastructure from cyberattacks but may also provide an environment which would allow many of the entrenched leaders in these industries, who are not currently incentivized to change the operational status quos of their businesses. Considering the increasing cyber threat from current and future adversaries, the implementation of a second internet for the military should be explored to determine additional geopolitical advantages.