Collection

Users can Collect posts into a printable, sortable format. Collections are a good way to organize posts for quick reading. A Collection must be created to tag posts. More Help

Thread: Approach on Cyber-policy and infrastructure
Posted Date: November 24, 2019 10:13 PM
Status: Published
Post: RE: Approach on Cyber-policy and infrastructure
Author: LEAH DREW

Kianna,

I agree that we need to be prepared to make changes to our policies based on the way technology changes. I also think we need to not only be prepared for the possibility of irregularities but to expect them and accept them as inevitable. In my opinion, the "short-arm" is neither a good nor a bad thing. It's a byproduct of living in a society that always changes, which is normally good but leaves opportunities for bad things to happen. That's why it's so important to keep up with the times in terms of cyber-policy– so we can make sure the changes remain ones that benefit us.

(Post is Read)

Thread: Cyber-policy and Infrastructure in a Changing World
Posted Date: November 24, 2019 9:37 PM
Status: Published
Post: Cyber-policy and Infrastructure in a Changing World
Author: LEAH DREW

Cybersecurity is a field that changes much more rapidly than most others. Given the rate at which we develop new technology, it’s incredibly difficult to predict what the future will be like. This means that the “short-arm” of predictive knowledge is magnified in cybersecurity and related disciplines.

In the past, regulations involving security have been longstanding and could remain the same for decades. The way we defined morality didn’t change because the world wasn’t changing. That is not the case for cyber-policy. We can’t predict whether the policies we develop today will be effective in the future. We certainly can’t create policies and *expect* them to work in the future. Those policies will rapidly become obsolete and need replacing or updating. The same is true for infrastructure, which becomes more and more susceptible to vulnerabilities as technology develops and attackers find new ways of getting around existing security systems. Thus, cyber-policies and infrastructure need to be flexible, with the expectation that they will need to be changed when they become out-of-date within the following few years. Adaptability is crucial; if it cannot be changed, updated, or retired and replaced, it has already failed.

As technology becomes integrated more and more into daily life, we will need to change the definitions of existing concepts. In the previous module, “Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis” discussed one of the ways our laws have become outdated. In some cases, states have tried to extend legislation involving harassment to cyber harassment by adding to existing legislation. Doing this without rewriting the definition of harassment itself provides a shaky foundation to build off. We can’t think of cyber harassment as an extension of harassment any more than we can consider the front cover of a book the extension of the back; they’re still two parts of the same whole. Furthermore, an updated definition of harassment will need to be flexible and able to be redefined every so often to keep up with the rate at which we develop new technology. In today’s world, we can't claim to know that what works today will work in the future.

(Post is Read)

← **OK**