“Huawei and Facing Up To 5G-Related Cyber Risks”

[Hersh Shefrin](https://www.forbes.com/sites/hershshefrin/)  <https://www.forbs.com/markets>

He writes about how psychology impacts financial and economic behavior and he is a professor at Santa Clara University and author of Beyond Greed & Fear.

Does it matter, that in spite of efforts by the U.S. government, and a history of cyber intrusions from China, [Germany and the U.K. are poised to allow Huawei equipment to be part of their 5G networks](https://www.cnbc.com/2019/02/19/germany-says-its-not-ready-to-bar-huawei-in-potential-us-snub.html)? The short answer is yes, and.

The “and” is that from a risk management perspective, we have yet to mitigate serious threats associated with cyber intrusions that can take control of our physical infrastructure and cause us serious disruption and damage. If 5G is as good as it is cracked up to be, 5G mobile Internet will allow **revolutionary technologies** to transform our world, greatly accelerating innovations such as self-driving automobiles and the internet of things. This revolution will bring both great benefits, but *also great risks* because the control of our “cars” and our “things” will be vulnerable to being taken over by bad actors.

From a behavioral perspective, one of the most important threats stems from availability bias, that being the tendency to attach insufficient importance to risks that are not at the forefront of our minds. Combating availability bias requires actively searching for relevant information that would typically escape our attention.

With this in mind, I have been reading a series of blog [posts by cyber security expert Joseph Weiss](https://www.controlglobal.com/blogs/unfettered/a-2018-retrospective-on-control-system-cyber-security-we-arent-as-far-along-as-many-people-think), about critical cyber risks to U.S. infrastructure which decision makers ignore at their peril, and ours. - I believe that Weiss wants us to understand that that cyber threats to infrastructure involve two separate technologies*, a first level technology and a second level technology.* The first level relates to Internet-associated information technology (IT) that *controls networks*, and the second level relates to different technology that *controls the physical devices*. Weiss' main message is that we are ignoring the vulnerabilities associated with the second level technology, because a successful breach of the IT system by an intruder can result in enormous, long-lived physical damage that will be costly, harmful, and take a long time to repair.

You may also like: --

Because Weiss’ blog posts are a bit heavy on jargon, to describe his main message I will use a simple analogy to communicate my understanding of his argument. The analogy involves the thermostat unit in my home which enables me to turn my furnace on and off.

My heating thermostat allows me both to measure the current temperature and to set the desired temperature in my home. An internal *program,* housed on a ***chip*** in the thermostat, then controls the state of the furnace, instructing it to turn on or off until the actual temperature and desired temperature are sufficiently close.

Imagine that I had an adversary who wanted to **harm me** by preventing my furnace from turning on during winter. My furnace is not connected to the Internet, and so my adversary would need to break into my home, and find a way either to damage my furnace, the thermostat, or the wires that allow the thermostat unit and furnace to communicate. The intruder would not need much more than a hammer and screw driver to cause great damage to my heating system.

*If* my heating system were part of the internet of things, I might never directly use my thermostat to control the heat in my house. I might instead use my smart phone, which communicates with my thermostat through the Internet. As beneficial as that might be, this kind of connectivity might *also* allow my adversary, were he or she sufficiently savvy, to damage my heating system without ever setting foot in my house, simply by hacking into my phone.

The intruder might not do major damage right away. She might alter the electronic settings to fool me by transmitting incorrect house temperature and desired temperature on my phone app; and unless I had some way of monitoring my thermostat directly, to double check its readings for accuracy, I might not even know I had a problem.

I think that Weiss’ main message is that the nation’s critical infrastructure, especially the ***electricity grid***, is analogous to what my home heating system would be like, were it a “thing” on the internet of things.

In respect to the analogy, the electricity grid has sensors like my home thermostat, generators like my furnace, and power lines like the wires connecting my thermostat to my furnace. Weiss is telling us that we need to monitor and protect these physical units from intruders seeking to do us great damage. He is telling us that the IT/network component is not fail safe, so that an intruder who successfully hacks into the “apps” can take control and do damage without our even knowing, until after the damage is done.

Keeping with the heating system analogy, he is warning us that we are putting too much trust in our “apps,” and that we need to double check our thermostats and keep better track of what our furnaces are actually doing. Behaviorally speaking, there is a people problem at the core of the issue.

IT people in charge of securing the network have network expertise; but they lack expertise when it comes to the physical devices. The people working to allow me to control the heat in my house by using a phone app know next to nothing about how my thermostat operates and works together with my furnace. Now there are other people who do have expertise in heating systems; and carrying the analogy further, these heating system experts need to be brought into the cyber threat battle in order to provide better security for our nation’s infrastructure.

Behaviorally speaking, availability bias is an important contribution to why we focus too much attention on securing our networks relative to our physical devices. We need to mitigate the effects of availability bias on cybersecurity. 5G is coming. ***Huawei*** will not go away. Neither will our adversaries’ interests in doing us harm, especially by using cyber tools. We need to find a way now to learn how to nudge ourselves into **paying more attention** to securing the physical components that make up our infrastructure. I am confident that we will learn, but better not to learn the hard way.

“Huawei And Facing Up To 5G-Related Cyber Risks”