Go back a hundred years and services like electricity and running water ? let alone phones ? would have all been considered luxuries. Now, we see these services as critical infrastructure that could cause a serious threat to life and societal order if they were to break down.

As the Internet of Things (IoT) is becoming a bigger part of our world, creating a marriage of software and hardware that ranges from the exceedingly useful to the overly creepy, it is also finding its way into many of the utilities that we depend on for modern living.

What we define as infrastructure is being rapidly altered by the growth of IoT and the move towards smart cities. We depend on traffic lights, security cameras and garbage removal to keep our cities livable, and we would quickly take notice if these services faltered.

As these devices and systems start to get brains, they become vulnerable to attacks like Mirai or the one that targeted the Ukrainian power grid. There is the added challenge of how to protect smart infrastructure, recognizing that it has major differences from the way that we defend power plants.

Historically, critical infrastructure projects have been tougher targets for hackers as their operational technologies (OT) relied on legacy systems that were not widely connected to the internet. As cases such as Stuxnet and more recent cyberattacks on electrical power systems have shown, these systems are vulnerable to external hackers, despite their supposedly high level of security and regulation.

[2]