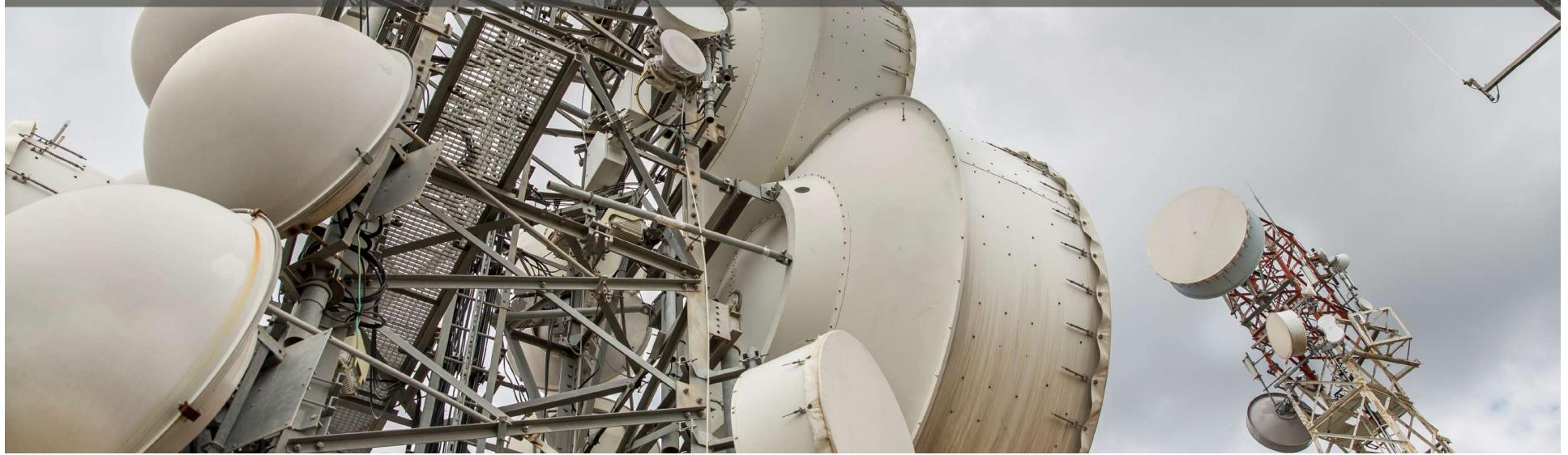


SECURING 4G LTE NETWORKS AND DEVICES

Critical Infrastructure Resilience Institute (CIRI) at the University of Illinois



The homeland security challenge

By 2020, the number of 4G LTE connections is expected to reach 2.8 billion, due to higher communications capabilities and a growing appetite for online services and resources. Because everything from toothbrushes to automobiles to mobile phones are part of the Internet of Things (IoT), a hacked device can be used to attack other systems and create extensive damage. Because the security of these devices and the networks that connect them haven't evolved as quickly as their proliferation, these devices pose a significant threat to multiple aspects of critical infrastructure across a wide range of industries.

The COE solution

Dr. Guanhua Yan is creating a new methodology that would help make 4G LTE networks—which are embedded in the daily operation of everything from healthcare to transportation—more secure and reliable. His goal is to learn more about 4G LTE mobile communication networks and device vulnerabilities in an effort to prevent complications arising from failures or attacks on device and network vulnerabilities. This project is process oriented and targeted, which will result in the development of new software that can be leveraged by mobile telecommunications network providers and device developers.