By Ultan Kelly, Senior Director, Cobham Wireless

The test and measurement (T&M) industry is likely to face significant challenges in the next few years. The growth of internet of things (IoT) and machine-to-machine communication, and the introduction of new connectivity standards pose new challenges for the industry. Alongside this, cybersecurity threats are increasing every day, often with catastrophic effects. Thus, the need for high quality network validation and testing to ensure network security becomes more fundamental than ever.

IoT has already made a huge impact on industries such as healthcare and automotive. By 2021, there will be more connected devices than there are people on this planet. Further, it is clear that we will become increasingly reliant on the services that IoT provides in the not-so-distant future.

Alongside the rise of IoT, there has been a rise in cybersecurity attacks. One of the most recent global attacks was WannaCry, a form of ransomware. It brought down huge networks such as the UK's National Health Service and even impacted telecommunication providers such as Spain's Telefonica and Bell Canada. With the healthcare industry becoming more dependent on internet-connected devices, it is important to realise that IoT is vulnerable to attacks on this scale too. For instance, late last year, an MIRAI malware targeted CCTV video cameras and digital video recorders, enabling a distributed denial of service (DDoS) attack on Dyn software. This remains the largest DDoS attack recorded and brought down internet giants such as Twitter, Spotify and Reddit.

The DDoS attack on Dyn demonstrates that a threat via IoT devices is always a possibility. It is daunting to consider the impact that a security breach could have on increasingly IoT-reliant hospitals. In such a case, internet-reliant healthcare machinery could be halted and lifesaving equipment would be redundant, or attackers could even gain access, via connected devices, and disable the operating system. As IoT continues to flourish and our dependence on it increases, this possibility becomes all the more terrifying.

As IoT becomes more profitable, providers are eager to deploy new connectivity standards

ahead of the introduction of 5G, including NB-IoT, LoRa or Sigfox. All of these aim to create a more seamless IoT network ecosystem, providing low latency and high bandwidth content caching to avoid overloading backhaul and core networks. However, in the haste, they are, in fact, another aspect of IoT that could impact security. Providers are at risk of letting the security of these new modes of connectivity slip as they are rushed into deployment. As hackers become more sophisticated, the new connectivity standards are just as vulnerable as the current ones, such as long term evolution or Wi-Fi.

As such, network providers must develop a new approach to how their radio access network (RAN) and core networks are architected and validated, not just from a performance perspective, but also with security as a priority. In order to prevent and protect against future cybersecurity attacks, operators need to carry out regular vulnerability tests, re-evaluating their T&M strategy.

Testing next-generation firewalls against perceived threats to ensure network resiliency is no longer sufficient, given the sophistication of modern security attacks. Instead, operator defences must be thoroughly examined throughout the network life cycle against new hacking techniques. It is essential that this is performed against a background of emulated network application traffic to guarantee the effectiveness of infrastructure in real-world scenarios. There are solutions available to telecommunication providers that can offer unprecedented realism. Gone are the days of manual test cases; it is simply unrealistic to expect networks to be validated on this scale using outdated T&M functions.

Instead, operators now have access to preventative measures in the form of emulation and security performance solutions, which can test application services, and wired and wireless networks. Virtualised testing solutions can run anywhere, from a lab, a datacentre and even on the cloud. The flexibility of a virtualised environment enables operators to enact scalable real-world applications and threat emulation. With this approach, operators can test their networks on a global scale from almost any location.

For IoT to reach its full potential, it is essential that it is reliable. However, it is important to understand that reliability does not refer simply to function. The provision of new connectivity standards is not enough to prop up the extraordinary amount of machine-to-machine devices flooding the market. In order for IoT to truly succeed and continue to have a meaningful impact on our lives, it is fundamental for telecommunication providers to employ high quality T&M solutions. They need to address exactly how their RAN and core networks are architected and validated to ensure that the devices we are increasingly reliant on are not subject to potentially traumatic cybersecurity threats, which can now be so effectively prevented.