SECURING INFRASTRUCTURE IN 2030

Botan Osman *looks into his crystal ball as he explores the evolution of technology for the future*

Looking ahead to the year 2030 and even beyond, in terms of advances in technology and securing our infrastructure, leads us to ask several additional questions; what might our infrastructure look like by 2030? How exactly will technology have evolved? And more importantly, how will the good guys and the bad guys be using it?

As we contemplate the next 10-15 years, we should remember that the rate of change is difficult to imagine and we will likely underestimate it. While considering how our industry will evolve, it's important to remember the likely changes in several interrelated technology capabilities as well as the transformation of our infrastructure and cities, and the evolving threat.

To answer the question "what are we securing", we first must imagine the world in 2030. What will infrastructure look like and what types of transportation will be in place? How will businesses be operated, and what will be the priorities of people and governments? The list of questions is seemingly endless.

IT'S GOOD TO TALK

No doubt there will still be cities, highways, railways, airports and ports, but the components of these will be communicating with each other. We will know more about the people within the infrastructure in real-time. There will be an increased number of sensors on infrastructure, devices and people. The Internet of Things (IOT) is already upon us; in 2012 the number of connected devices reached 8.7billion, surpassing the number of people in the world. It is now estimated to have reached a staggering 30 billion devices, and is set to grow to an estimated 50 billion devices by 2020. That's a lot of IP addresses vulnerable to attack, and with every device added, the risk of attack increases.

All of these devices and sensors create a lot of data about our world, almost like a global nervous system. In addition, data connectivity will be cheaper and further reaching, and there will have been incredible advances in AI, Robotics, Big Data and Automation; enabling us to make more sense of our environment.

More data provides a bigger opportunity to gain insights and act on them, to better secure our built environment and infrastructure. However, exploiting the data with analysis and acting on the information learned will be the key. Data alone is not enough.

The threat of physical attacks is unlikely to subside, but cyber is already becoming increasingly attractive to criminals due to the fact that these types of attacks are easier and cheaper to execute. Geography represents no hurdles for a cyber attack, with a perpetrator based on one side of the world able to breach the defences (or lack thereof) of an organisation on the opposite side of the world. Over recent years, we've seen an increase in the number of cyber attacks and the devastating impact that they can have on organisations and the general public.

By way of example, earlier this year a strain of ransomware called WannaCry spread around the world, breaching the defences of hundreds of thousands of targets, including public utilities and large corporations. Notably, the attack temporarily crippled National Health Service hospitals and facilities in the United Kingdom, disabling emergency rooms, delaying vital medical procedures and creating chaos for many British patients.

DETECTION, PREDICTION AND REACTION MIGHT BE CONDUCTED BY CONNECTED DEVICES

In our increasingly competitive world, we are already seeing pressure on businesses mounting to increase their performance and profitability by introducing new technology, and as such, we can expect a wider adoption of Industrial IoT to emerge in the future. This reliance on technology will only lead to a growth in the severity and damage caused by a potential cyber attack.

Kinetic attacks are always changing, and perpetrators seemingly gravitate towards the simplest and cheapest solution available for causing devastation; will we see the convergence of kinetic and cyber attacks in the future? Imagine a time when all cars are connected to the Internet of Things. During rush hour, a terrorist could hack the system that links these vehicles, and at random hit the emergency brake on multiple cars. This could cause traffic accidents across the country at the touch of a button.

It's not all doom and gloom. As the potential for attack changes, the security industry will also see an increase in the sophistication of our own technology, and how it can be applied to securing infrastructure.

Data connectivity will be cheaper and further reaching

Some of the key technology trends we expect to create transformation in our industry will be: Artificial Intelligence, Machine Learning, Drones, Facial Recognition, IoT, Autonomous Vehicles, Big Data Analytics, Cloud Connectivity, Mass Mobile Connectivity and Block Chain Technology.

As these technologies mature, their respective capabilities and the interrelation of these technologies solidify, facilitating security solutions we simply cannot imagine possible right now, and fundamentally changing the way we secure people, assets and infrastructure.

This month, Apple announced that the iPhone 10 will be equipped with facial recognition. It is estimated that the accuracy of Face ID will be 1 in 1,000,000 when compared to the 1 in 50,000 of TouchID fingerprints. The TrueDepth camera uses 30,000 infrared dots harmlessly projected onto the face for depth mapping. This is held in a tiny area within the top of the phone. Technology that was unthinkable in the past is now part of a phone you will buy this year.

And this is 2017 – imagine how much more accurate the technology will be in 2030. Consider how this type of technology could be integrated into a security solution to recognise known criminals within a crowded space. What if the facial recognition could go beyond simply identifying a person, but when combined with machine learning begins to recognise emotions and behaviours, identifying a likely perpetrator and even delivering the relevant automated emergency response?

How will we achieve situational awareness in the new world? It has already been highlighted that cities will be smarter, buildings will be communicating with each other, granting us more knowledge about the people within the infrastructure in real-time.

With every device connected, we see exponential growth of situational data at volumes currently unimaginable. These provide a major opportunity for real-time insights that will put the emphasis on detection and prevention rather than response and retrospective investigation, and will over time reduce the need for human intervention altogether.

The world's nervous system will spread and grow, with advances in data processing, AI and machine learning, allowing us to better understand our environment, and consequently improve building

security tactics and strategies.

The buildings themselves will become smarter – no longer relying on individual cameras and sensors to feed into a screen in an isolated control room, and connected cars across cities will provide the data required to understand movement and vehicle trends that no longer depend purely on ANPR cameras dotted around a city. We've seen a rise in the use of vehicles as weapons in terrorist attacks in recent years, and if this trend continues to grow, it may force the introduction of legislation whereby every car is tracked as standard.

The global impact of the non-state based actors carrying out cyber attacks will mean increased international cooperation over data sharing and the identification of possible attackers. Cyber attacks are changing the geopolitical risk vectors that previously shaped our thinking around security. Where you are, no longer determines where you can harm.

As an industry, security professionals must constantly challenge themselves to think ahead, considering how infrastructure and the built environment will evolve in the future, and consequently, how this might affect the way we secure this infrastructure.

THE NUMBER OF CONNECTED DEVICES IS SET TO GROW TO 50 BILLION BY 2020

Keeping up to date with new technology and how it impacts infrastructure and organisations is also important. We must also consider the potential changes in the threat landscape; how might the bad guys use new technology, data and connected systems against us? This knowledge will enable us to design today, with an eye on tomorrow.

With technology, we sometimes can't comprehend the future. In our own lifetimes we have seen the development and creation of communications beyond our wildest imagination. We can't always predict what advancements might be on the horizon. It was only 20 years ago that most people thought the internet was a fad that wouldn't catch on.

In short, we don't know what we don't know. In the film *Minority Report*, technology advanced to a point that the level of situational awareness was absolute, and crime could be predicted before it even happened. In this scenario, emergency response as we know it would be effectively defunct. In 2030, Detection, Prediction and Reaction may be automated and conducted by connected devices with the brain in the cloud.

Beyond the advancements in technology, there will be other changes we can't anticipate. What or who will we be protecting? Where will the conflict zones be? Will the goals of terrorists change? Will government legislation have changed fast enough? The answers to these questions will shape the development of technology and the way we integrate it into security solutions.

BLURRED LINES

We can never forget the kinetic threat and as such, the requirement for physical security measures will no doubt remain, but it will be the style of attack and thus the solutions that will change, with the lines between cyber and physical attacks and security blurring and possibly even merging.

Security will be data lead, distributed, intelligent and proactive with physical drones and robots reacting to decisions being made by machine-learning algorithms improving at an unimaginable pace while we sleep.

The demand for connectivity will continue to be driven by businesses wanting to increase efficiency and profitability, and it is likely that security will be an afterthought in this transformation. As an industry, we must strive to encourage organisations to keep safety and security at the forefront of their minds, as once the technology and connectivity spreads, it may be too late to fix the gaps.

Technology advancement is accelerating; this applies as much to the bad guy as the good guy. As the good guys, we must endeavour to stay one step ahead. As Bill Gates once said: "We always overestimate the change that will occur in the next two years, and underestimate the change that will occur in the next 10. Don't let yourself be lulled into inaction" ●

Botan Osman – Managing Director at Restrata – originally joined the company in 2013 as Country Manager of Kurdistan. Prior to this he served as the Head of the KRG Department of IT and Advisor to the Prime Minister.

Cities will be smarter as buildings communicate with each one another