www.pipelinepub.com
Volume 17, Issue 1

Smart City Cyber War Games

By: Mark Cummings, Ph.D., Bill Yeack

Economic, social, and technological pressures are moving us to smart cities. If the world follows a common technology implementation path of focusing on capability, and only on security as an afterthought, the world could get into serious trouble. People in Australia recognized the potential for this possibility and have started an interesting approach, a cooperative effort between government and industry to model and test smart cities.

The Australian experience is very instructive. There may be other approaches developed to plan and test smart city use cases (applications, devices, and more). However, any effort to develop plans and tests for smart cities should integrate the results of the Australian experience.

The pressures are real. Cities around the world are growing at a rapid pace. Today 55 percent of the world's population lives in urban areas. By 2050, this proportion is forecast to jump to 68 percent. As urbanization rises, the demand for resources and services to support cities grows. We see this reflected in the major areas of social contention today:

- Energy management to control global warming
- Disease monitoring and control
- Maintaining social – order policing, social services, and so on
- Social equity – such as reducing quality of life gaps

Cities have to deal with these environmental, economic and social challenges. At the same time, wireless technology has evolved from smartphones for people to networking devices (IoT or Internet of Things). One of IoT's earliest big pushes was into the 'smart home.' Unfortunately, this initiative followed the old pattern of capability first. The result has been a large installed base of insecure devices with no clear path for how to secure them.

Smart cities and the security stakes

This convergence of urbanization and technology evolution is creating pressure for the development of smart cities as a way to increase efficiency while deploying innovative services that can resolve the areas of social contention. Many experts wonder whether smart cities will follow the path of smart homes to great capabilities with little security. If so, this will be a real problem. It is not good when the security of a home is compromised, but the damage is relatively contained. For a fully interconnected city with large arrays of sensors and actuators affecting all aspects of life, the consequences of compromise are much greater. It can become a survival issue for substantial portions of society.

This raises the question of whether we can make smart cities safe. It is important that we ask and answer this question now, before we end up with large deployments with no clear path to safety.

Australia: leading the way

Australia has emerged as a leader in this area. The country has created a unique partnership between public, private and classified agencies. The premise of its work is that good intentions are necessary but not sufficient. It is not enough to try to design safe deployments; they must be tested, retested, and then tested again. The leaders of Australia's effort have even gone one step further: they have decided they need to train the defenders in the testing phase.

Their focus is to aggressively train the defenders. As part of this organized effort, the Australian government hosts an invitation-only Cyber War Games to test the current state of smart cities. These are live fire tests against a synthetic city with kinetic properties.

To be effective, it has to be 'live fire' testing. But using a real city is dangerous. The use of a synthetic city for testing is important. The experience at Fort Bragg in North Carolina shows that unintended consequences are too likely and too severe to test on real cities. In this case, the military felt they needed to test the base's infrastructure. In the process, they inadvertently brought down the local community for 12 hours. As William Ratcliffe, former member of the Australian Navy and current CEO TLR Communications Australia says, "You absolutely need to test, but in a controlled environment. Crashing a real city is the worst case."

Here is how this live cyber war game works. On an annual basis, one of the core government agencies creates a new synthetic city code named Shell Cove. This city is created out of a massive number of LEGO pieces (yes, LEGO for the city elements). Then, the electronic infrastructure is developed to represent a model smart city. For example, the police station has the electronic elements of a working police station. There is an airport as well as mass transit trains, water works, and so forth. The result is a complete electronic-kinetic model city where the impact of attacks can be seen.

This combination of kinetic and simulated is very important. It makes the exercise more real in the minds of the participants. It creates a much better sense of what is at stake. But there are also important interrelationships that might not appear if the city were only computer simulated. Some examples from past war games can illustrate this. It was discovered that if an attacker

compromised the electrical system, the fire department couldn't respond to fires; firefighters could not open the firehouse doors. When the water distribution system in the city wasn't able to distribute water, dams creating reservoirs serving the city failed and created a flood in the city.

These are important and interesting findings. But the real goal is to take cybersecurity experts that are defending the smart cities and teach them to be attackers. Once they understand how an attacker thinks and their methods and mannerisms, they can become much stronger defenders. A key lesson learned in the recent War Games of 2019 was the importance of knowledge sharing between all sides of the cybersecurity problem. One team simply cannot do it all. This is already understood, but it becomes clear during these types of exercises.

With these insights, the Australian government has taken an interesting hybrid approach. By partnering with industry and sharing all the tricks and approaches, leadership is not only hardening the skills of government employees but also carefully selected private company employees too. Or in the words of Stuart Robert, Minister for Government Services Australia, DHS Senior Minister, "We have found that the public-private partnership is a very powerful way to harden our people's skills and build new methods of defense."

Measuring "smartness"

The smartness of a city is measured by six characteristics: smart economy, smart people, smart governance, smart mobility, smart environment, and smart living. The three layers that make up the smartness of the city are based on ICT structures such as IoT, Big Data, the Internet, and so on. But is a good ICT infrastructure enough to build a smart city? Technological interconnectivity is key: all smart devices and virtual data should be linked to the infrastructure and analyzed in order to achieve the goal of a sustainable and smart city.

What about safety? While each element may be safe, this may not result in safety in combination. Also, as Bill Ratcliffe asks, "How many of the key characteristics can be lost before chaos reigns? What is the threshold where the city becomes unstable? If you introduce a global pandemic to a smart city, what happens?" Finally, Diana Neuman from Bace Cybersecurity Institute, which focuses on resilience analysis, says, "Today's technologies are so complex no amount of theoretical review will find all the issues." You only know if you test!

Over the years, the cyber war game sponsors have created a significant body of knowledge, tricks and techniques. Many countries have asked about this, and while nothing is final, the Australian government is considering partnering with another country or group of countries. For example, the Abu Dhabi government has created Masdar City, a pioneer in sustainability and a hub for research and development. The city is home to a rapidly growing clean-tech cluster, business-free zone, and residential neighborhood with restaurants, shops, and public green spaces. The government recognizes the importance of security for Masdar City. As Mohammad Al Ramahi, CEO of Masdar says, "Secure growth is a challenge and an opportunity."

Learning by Example

This article should be considered as only an introduction to the Australian and possible follow-on efforts. Others dealing with the economic, social, and technological pressures moving us to smart cities may develop other ways to plan and test to avoid the path of focusing on capability and only focusing on security as an afterthought. However, any such effort should include outreach to the Australian project to incorporate what its leaders have learned.