

Smart Cities Threats

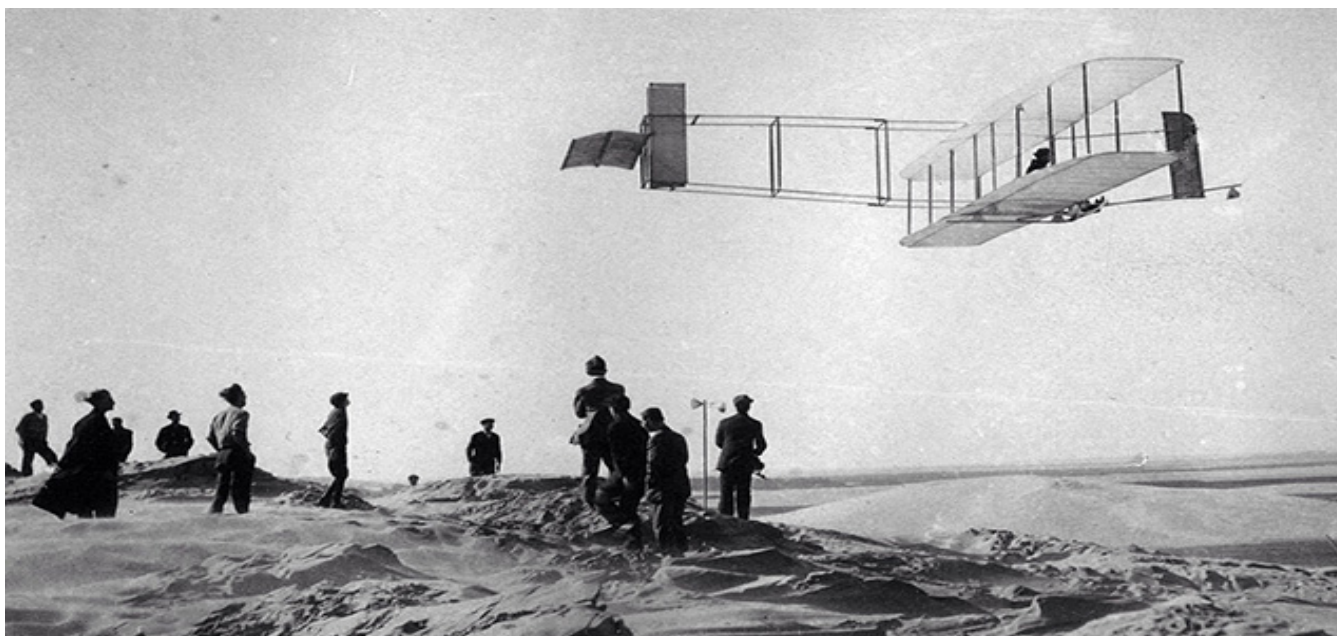
Richard Zaluski

Founder, President, CEO

Centre for Strategic Cyberspace + Security Science / CSCSS

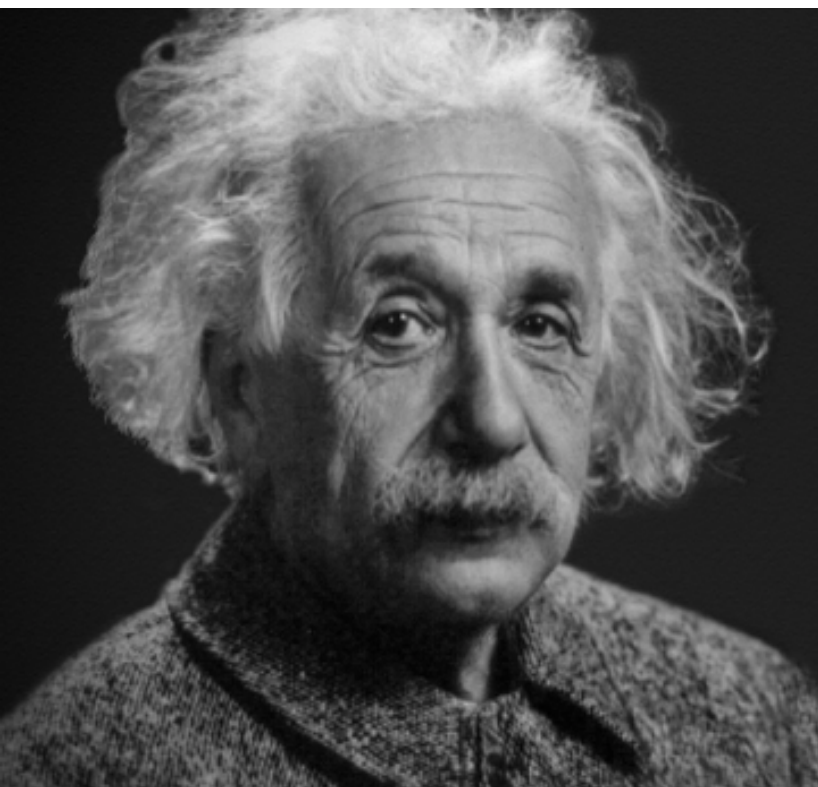


Smart Cities? Where are we now?



*We are at the dawn of the
Golden age...*

But before we go into the future



We can't solve
problems by using
the same kind of
thinking we used
when we created
them. ~ *Albert
Einstein*



Where does this leave us



With a lot of
challenges!

Smart Cities

Will change how we
~ *Live*
~ *Learn*
~ *Work*

Smart Cities

Are a an ecosystem

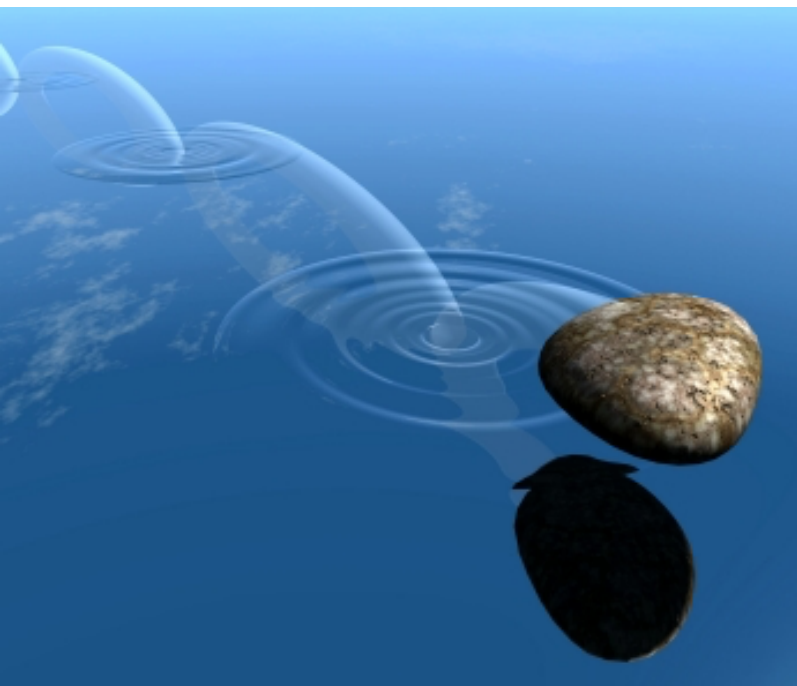
In nature : A biological community of interacting organisms and their physical environment.

In relation to smart cities : A complex network or interconnected systems of interacting “Organisms” and their physical + virtual environment.

**** An Ecosystem is extremely sensitive.



Smart city ecosystem - Ripple Effect



- The impact of natural and manmade effects on smart cities can not be minimized
- Introduction of an 'event' can have far reaching impact



Electrical “Ecosystem” - Blackout 2003



- The blackout's primary cause was a software bug in the alarm system at the control room of FirstEnergy Corporation
- Man made event
- *In terms of Smart Cities it could be catastrophic*

The Rise of Smart Cities

- It is estimated that 2050, about 70% of the world's population is expected to live in cities.
- Using the Internet of Things, analyzing lots of data, putting more services online—all herald the digital transformation of cities.
- In digital terms it means new evolving threats and the cybersecurity battles we face economically, socially and fundamentally
- Disruptive technologies and innovation breeds **ADVANCEMENT**
- Innovation also breeds the advancement of **THREATS**
- ***TRUST is a key element !***

lot Devices? in 2050?





50 Years



- In 50 years : Technology advances will make some devices we use unrecognizable
- ***What will a smart city look like in 2050??***
- ***What will the threat landscape look like in 2050??***
- We need to lay the foundation for an known future



What are we up against??

| TIME | ATTACK | SOURCE | TARGET | |
|----------|----------------------------------|--------|-----------|--|
| 23:52:09 | Dorkbot.TC.o | Japan | Sri Lanka |  Source  Target |
| 23:52:09 | Possible IRC Bot Communication.C | USA | Spain | |
| 23:52:09 | Dorkbot.TC.o | Japan | Sri Lanka | |

Cyber-attacks have transformed the risk landscape

- Cybersecurity is a city- wide issue and not just a technology risk.
- Opportunities will evolve through technological integration and collaboration
- IoT will continue to increase in complexity
- **Complexity breeds risk**

It's not looking good is it.....



75%

of respondents rate the maturity of their vulnerability identification as very low to moderate.



35%

describe their data protection policies as ad-hoc or non-existent.



12%

have no breach detection program in place.



38%

have no identity and access program or have not formally agreed such a program.

****Statistics from EY LLP GISS Survey 2017**

Smart Cities Threats

- An estimated 2.3 billion connected 'things' are deployed in smart cities across the world
- The rise of the IoT exposes a wide range of vulnerabilities that can be exploited
- Although smart cities are designed to promote productivity and efficiency, they present serious risks when cyber security is neglected
- There are an unknown number of potential vulnerabilities and methodologies



What are the threats??

- Privacy, Data & Identify Theft
- Device high jacking and compromise
- Denial of service attacks / Man in the middle attacks
- Network compromise / Device Compromise / Human Compromise
- Insider attacks (Smart city resident? / Smart City employee?)
- Zero Day Exploits

Is this anything new? No.

- All the devices and systems in place today that compromise a 'smart city' are essentially off the shelf technologies.
- All with known and unknown vulnerabilities and compromises

What are the threats??

The expansion of the attack surface

The introduction of new points of potential vulnerability such as connected and self-driving cars, drones, and the Internet of Things

- USA - 71% of local governments say IoT saves them money but 86% say they have already experienced an IoT-related security breach

A wider range of attacker motivations, including ransomware

- Motivation behind 50% of attacks in the US in 2017, with ransom payments totaling more than \$1 billion

Hactivism / Cyber Terrorism

- Drawing attention to a specific cause, adding cultural and political dimensions to cyber attacks

Cybersecurity – A Cornerstone

- A prerequisite for any smart city..
- This means pursuing and addressing physical security, cyber security, confidentiality, integrity, accountability, privacy and high-availability
- There must be by design an understanding of the persistent threats arrayed against systems there must be cyberattack recovery plan, backup plan, Business continuity / Recovery plan, associated facilities, cloud management, and manual overrides to automated systems
- Smart cities must recalibrate adjust and adapt to the requirements of the new cybersecurity landscape that will evolve rapidly.

Cybersecurity

It is critical to understand not only the threats in place, but the issues that are presented by 'innovation' and the exposure it can bring. Smart city citizens must have confidence in the infrastructure environment / ecosystem they 'live' in..

Cybersecurity is a key / cornerstone on any path forward

- With the heavy reliance on data, there is just a huge threat vector for threat that has to be met with intelligence collection, intelligent systems, and the human element for intervention



Cybersecurity must be woven
into the core social / economic
fabric of any smart city

Structured Threat Information + Action

Structured Threat Information providing a unifying diverse
Set of cyber threat information sets including:

- Cyber Observables
- Threat Vectors + Indicators
- Incidents + Response
- Threat Intelligence
- Adversary Tactics, Techniques, and Procedures
(including attack patterns, malware, exploits,
kill chains, tools, infrastructure, victim targeting,
etc.)

Structured Threat Information + Action

Structured Threat Information providing a unifying diverse Set of cyber threat information sets including:

- Exploit Targets (e.g., vulnerabilities, weaknesses or configurations)
- Courses of Action (e.g., incident response or vulnerability/weakness remedies or mitigations)
- Cyber Attack Campaigns
- Cyber Threat Actors

Smart city solutions and deliverables should be expected to comply with basic security requirements such as:

- Strong cryptography to protect data, both at rest and in transit
- Authentication capabilities / Authorization capabilities
- Automatic and secure update of software, firmware
- Auditing, alerting, and logging capabilities
- Anti-tampering capabilities
- No backdoor/undocumented/hardcoded accounts
- Non-basic functionality disabled by default
- Fail safe/close / Secure by default
- Penetration Testing of smart city devices
- Operational security verification and validation
- Hardening (Device / Application / System etc)



Smart city solutions and deliverables should be expected to comply with basic security requirements such as:

- Smart City Security Board / Leadership
- Information Sharing (CRITICAL)
- Situational Awareness (International Approach)



Conclusion

- Smart city models should boost development while not compromising on data privacy and security.
- The global smart city market is expected to reach US\$1.565 trillion in 2020 *Source: Frost and Sullivan
- Increasing smart city complexity implies increasing vulnerability, both to malicious attacks and unintentional incidents.
- A robust security and information protection framework is a must

Conclusion

To aid in implementation and governance of the smart city projects, the government can:

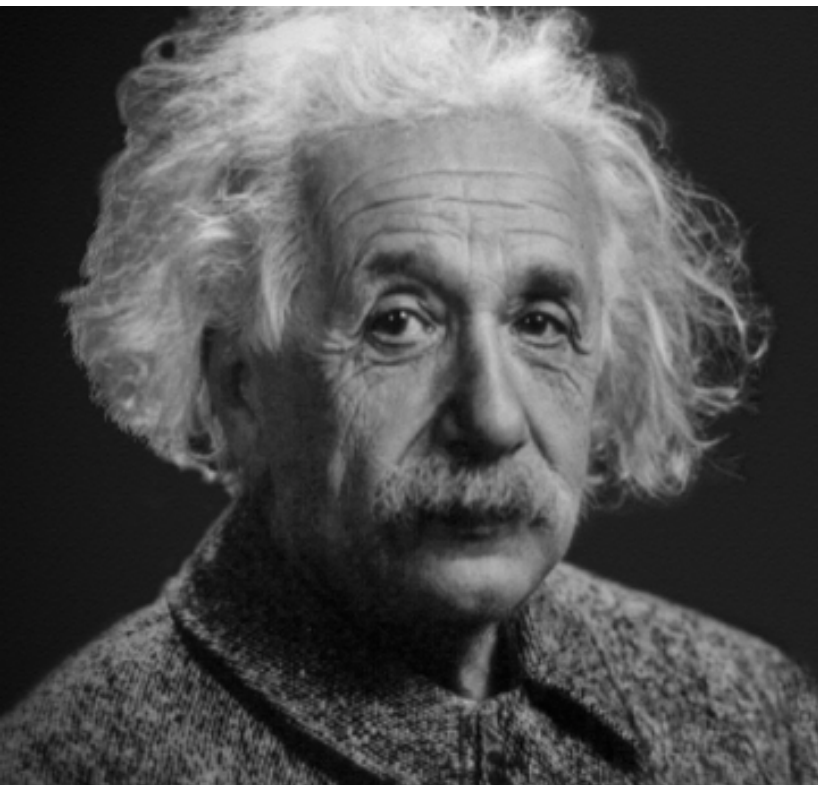
- Enter into Public Private Partnerships
- Employ the expertise of the private sector in order to deliver the benefits of smart cities efficiently
- Adaptive security is paramount
- Trust is key → tied directly into security

Final Thoughts Path Forward



- . We need to collaborate on threat mitigation
- . Globally we need to be much more proactive threat intelligence
- . Global Approach to Cyber + Smart Cities
- . Cybersecurity needs to be built into smart city architecture
- . Cybersecurity needs to be part of any project plan
- . Cybersecurity must take an active resilient approach

In closing



We can't solve problems by using the same kind of thinking we used when we created them. ~ *Albert Einstein*





RICHARD ZALUSKI



战略网络空间与安全科学中心

里查德.扎乌斯基
总裁兼首席执行官
richard.zaluski@cscss.org

Thank you!

Question & Answer

Next Steps