Trusting Smart Cities: Risk Factors and Implications

Margaret L. Loper, Ph.D.
Chief Scientist, Information & Communications Lab
margaret.loper@gtri.gatech.edu

June 19, 2018
Rise of Smart Cities

Surrounded by billions of sensors, devices and machines

- Next-generation Vehicle Center (Op Center)
- Intelligent Transportation System (ITS)
- Multi-energy Station
- EV Car Sharing
- Smart House
- Solar Panel
- Offshore Wind Farm
- Battery Storage Systems
- Environment-friendly Design Buildings
- Smart Buildings Linked Through Regional EMS
- Regional EMS (Control Center)
- Wind Farm
- MegaSolar
- Smart House
- Biomass Fuels
- EV Car Sharing
- Electric Bus
- Small/Medium-scale Smart Buildings
- Multi-energy Station

Improve quality of life, efficiency of urban operation and services, and competitiveness

**The idea of a smart city can be applied to smart military installations, smart compounds, and smart campuses**
Commercial Smart City Technologies

- **Smart Waste Collection**
- **Security:** Video, License Plate Recognition, Gunshot Detection
- **Efficient Buildings**
- **Transportation:** Parking, Charging, Routing
- **Wi-Fi Kiosks**
- **Smart Streets:** Light posts Monitoring Pollution, Noise, Traffic
Can We Trust Smart Cities?

• So many definitions of Trust....
  - “... the competence of an entity to act dependably, securely and reliably within a specified context.”
  - “...the extent to which one party is willing to depend on somebody, or something, in a given situation ... even though negative consequences are possible.”
  - “Trustworthiness is the demonstrable likelihood that the system performs according to designed behavior under any set of conditions as evidenced by characteristics including, ... security, privacy, reliability and resilience.” - NIST

• Risk and trust have an inverse relationship

The lower the risk associated with the city, the more we can trust it!
Smart City Risk Factors

**Non-Technical:** aspects where humans are involved
- Management
- Training & education
- Governance and security practices

**Technical:** aspects where technology is involved
- Hardware
- Software
- Cyber-physical systems

**Complexity:** a city is a complex multi-dimensional interconnection of human and technology systems
- Cascade effects
- Normal accident theory
Risk Factor: Non-Technical

Smart cities represent a fundamental change to the way that services are delivered, focusing on processes and people - how to make a city smart and who manages it.

1. Management
   - Performance depends on effective management of the systems and infrastructure
   - IT deployment is complex - 85% of all IT projects fail due to non-technical aspects of innovation

2. Training and Education
   - Shortfall of as many as 1.5 million security experts by 2020
   - Shortage worse in public sector
   - Preventable human errors account for a large number of data breaches

3. Best Practices
   - Hardware and software released without security, and governments release it without testing
   - 200,000 vulnerable and insecure traffic control sensors were discovered in cities such as Washington D.C., New York, Seattle, San Francisco and London
Risk Factor: Technical

Technology is the enabler of a smart city, which includes hardware, software and cyber physical systems

1. Software Development
   - "We don't know how to write software without bugs. We've been trying for 70 years." – Vint Cerf
   - In a city running 100’s of systems for critical services, a software bug in the alarm system had huge impact due to a chain reaction of events
   - Affected almost 10M people in Ontario, Canada and 45M people in 8 U.S. states

2. Trusting Data and Devices
   - IoT sensors can be hacked and fed fake data
   - Devices may misrepresent themselves - intentionally programmed to cheat
   - Delegating more control and decision making to devices can create more temptation to cheat
   - Growing need to validate, regulate and trust IoT devices
Risk Factor: Technical

3. Cyber Attacks
- Attack surface for smart cities is huge: wireless sensors will control everything from traffic lights to water management
- 2013 Symantec Security Threat Report: 22% of attacks are aimed at governments and energy/utilities companies; 24% of identity breaches are governments and healthcare institutions

2012 Hackers breached Canadian software company
2014 Researchers black out city using smart meters
2015 Hackers remotely kill a Jeep on the highway
2018 City of Atlanta Ransomware attack
1. Cascade Effects
   - City systems for critical services are interdependent - a bug or attack can cause chain reactions
   - What would commuting look like with non-functional traffic systems, no streetlights, and no public transportation?

2. Normal Accident Theory
   - Framework for characterizing complex systems according to risk
   - Accidents are presumed unavoidable because seemingly unrelated events accumulate to create major malfunctions
   - Three conditions make a system susceptible:
     • the system is complex
     • the system is tightly coupled
     • the system has catastrophic potential

Smart cities are not discrete – they are complex multi-dimensional interconnection of diverse systems that promise unique services and optimum performance
Evaluating the Trustworthiness of Cities

• Group threats into four categories
  - Imminent (current)
  - Not persistent (sometime)
  - Can recover from (tolerable)
  - Black swan (intolerable)

• Grade how well a City can respond to the threats
  - Risk Score (low risk = high trust)

<table>
<thead>
<tr>
<th>Threat (current)</th>
<th>Threat (sometime)</th>
<th>Threat (tolerable)</th>
<th>Threat (intolerable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Score</td>
<td>Risk Score</td>
<td>Risk Score</td>
<td>Risk Score</td>
</tr>
<tr>
<td>Risk Score</td>
<td>Risk Score</td>
<td>Risk Score</td>
<td>Risk Score</td>
</tr>
<tr>
<td>Risk Score</td>
<td>Risk Score</td>
<td>Risk Score</td>
<td>Risk Score</td>
</tr>
</tbody>
</table>

Threats to Cities
• Traffic Control Systems
• Smart Street Lighting
• City Management Systems
• Sensors
• Public Data
• Mobile Applications

• Cloud and SaaS Solutions
• Smart Grid
• Public Transportation
• Cameras
• Social Media
• Location-based Services
Are We Overplaying the Cyber Risk to Cities?

“...the IoT links individuals’ daily lives to that of the internet. This interconnectedness between people and cyberspace gives criminals, extremists, and adversary nation-states a vector to target individuals, private and governmental organizations, and U.S. civil society as a whole, and, in the process, it has inspired a fear of the unknown. In short, cyber is the new weapon of mass destruction threat, and addressing it will require marshalling the resources of the entire interagency.”

U.S. Army Major Quan Hai T. Lu, Deputy Chief of Systems Vulnerability & Assessment at the Defense Threat Reduction Agency 2015
Conclusions

• Combination, connection and integration of systems and infrastructures are fundamental to a city being smart
  - Greater possibility that things can go wrong
  - More vulnerable it is to different types of risk

• Technology alone won’t solve trust problems
  - Technology: change and upgrade technological tools to improve services and create conditions where the tools can be better used
  - Organization: managerial and organizational capabilities for effective use of technological tools and conditions for their use
  - Policy: address institutional and non-technical urban problems and create conditions that enable a smart city

• Need a holistic approach to smart city security to overcome the adverse impact of siloed organizational structures