

ADB

Driving Digital Development across Asia and the Pacific

Cyber Security in Smart Cities

Aalok Kumar - Corporate Officer & Sr. VP

Business Head - Global Smart City



What is a Smart City?

Making a city "Smart"

Physical Infrastructure



Roads



Bridges



Airports



Hospitals



Train Stations



Electric Grids



Digital Enablement



Smart Meter



Smart Transportation



Wireless Communication



Facial Recognition



IoT Sensors



Camera



Data Synthesis



AI | ML



Integrated Command & Control center

Interconnected Smart City



Smart Economy



Smart Security



Smart Governance



Smart Public Service



Smart Health



Smart Education



Smart Transportation



Smart Infrastructure



Smart Energy

Smart Energy



Smart Logistics



Smart Sustainability

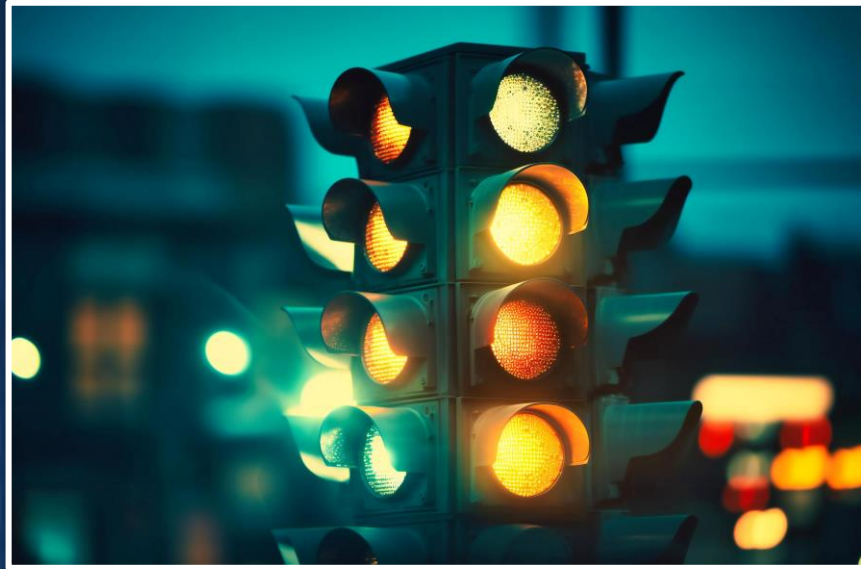




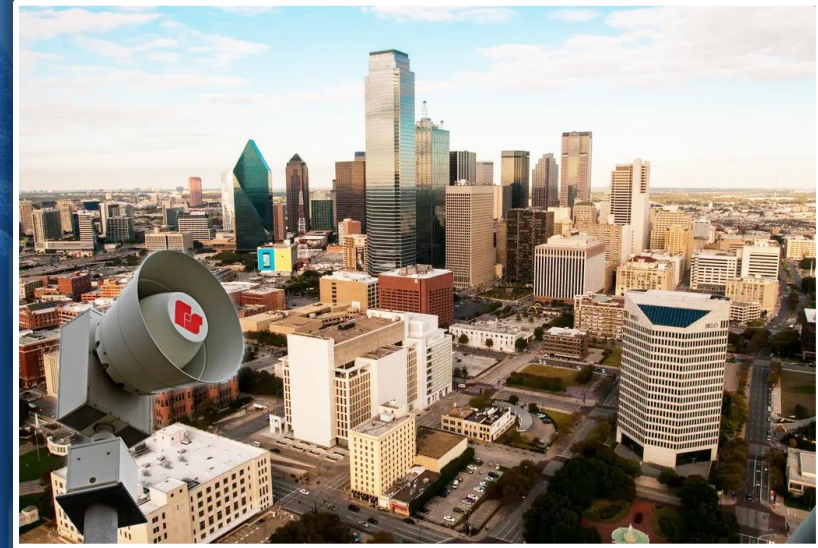
Cybersecurity Threats in Smart City

Vulnerabilities in Smart City

Sabotage of traffic signals in Los Angeles



Emergency sirens activated, resulting in widespread panic in Dallas



US

FBI - Nearly 850,000 complaints reflecting more than \$6.9 billion in losses.

\$6.9 billion



UK

30,000 cyber-complaint filings, estimated it received complaints for only about 2 percent of all incidents.

2%


Cyber Security Risks, Threats and Impact





Securing the Smart Cities

Wholistic approach to building Smarter and Safer Cities



Cyber Security Cross Functional Team

- Building Long term vision
- Driving near-term actions
- Proactively evaluate & examine cybersecurity resilience capabilities
- Determine the capabilities to be built



Master Planning and Design



Supply Chain Risk Management



Operational Resilience

Master Planning and Design



- Applying the principle of least privilege, Enforcing multifactor authentication
- Implementing zero trust architecture, managing changes to internal architecture risks
- Securely managing smart city assets its vulnerable devices, timely system & application patches
- Protecting internet-facing services
- Evaluating and managing legal and privacy risks with the deployments

Supply Chain Risk Management



- Software supply chain
- Hardware and IoT device supply chain
- Enforcing compliant cybersecurity standards for vendors
- Managed Service Providers and Cloud Service Providers
- End of life and Tech obsolescence risks mitigation

Operational Resilience



- Backup of systems and data
- Disaster recovery game plan
- Planning and conducting Periodic workforce training
- Developing incident response plans, Performing periodic Incident response & recovery exercises
- Physical Security
- Regular Security Audits

Wholistic approach to building Smarter and Safer Cities



Strategic Threat Intelligence

- Proactive threat intelligence
- Analytics to monitor industry and regional threats
- Intelligence led decision making and response plans
- Proactive response to emergent threats like ransomware or coordinated attacks



Integrated Security Approach

- Vital due to geographical and technical priorities
- Overcome stakeholder silos for better detection and response speed
- Create consistent security messages across all levels of the organization
- Design clear segregation zones between IT and OT networks



Whole-of-Industry Convergence

- Collaborate to address challenges of cyber-physical convergence
- Data driven national-level governance mechanism
- Alignment on standards and technical controls
- Balance overarching and local standards for continuous cybersecurity improvement

Conclusion



Strategic Planning to assess threat Intelligence



Policy implementation, audit and monitoring of cyber security standards



Granularity in identifying vulnerabilities to the last mile connectivity



Integration and hand shake across multiple platforms



Periodic assessment through real time drills



\Orchestrating a brighter world

NEC