CYBERSECURITY SMART CITIES

Isvari Maranwe
Dweebs Global

CYBERSECURITY

SMART CITIES

Isvari Maranwe
Dweebs Global

CYBERSECURITY

SMART CITIES

Isvari Maranwe
Dweebs Global

CYBERSECURITY

SMART CITIES

Isvari Maranwe
Dweebs Global

TABLE OF CONTENTS

01

INTRO

Morocco

02

CYBERSECURITY PROBLEMS

Everything can go wrong and will.

03

SOLUTIONS

How to mitigate those problems.

04

THE FUTURE

What comes next.

MOROCCO

- Tangier Tech, 2017 launch
- Opening of large malls and creation of new developments
- Does a Smart City have to look like a Western metropolis?

MOROCCO

- Minsait won a contract to develop an urban data platform for waste collection, markets, slaughterhouses, and more.
- Saves 45% in energy, 35% in water.

02

CYBERSECURITY PROBLEMS

Everything can go wrong
and will.

CYBERSECURITY IS THE SECOND BIGGEST PROBLEM.

Data Privacy is the first!

Some other problems:

- **Loss of culture/language**
- **Slums and inequality**
- **A potential increase in harm to the planet**
- **Solar flares + other crazy things?**

CYBERSECURITY RISKS

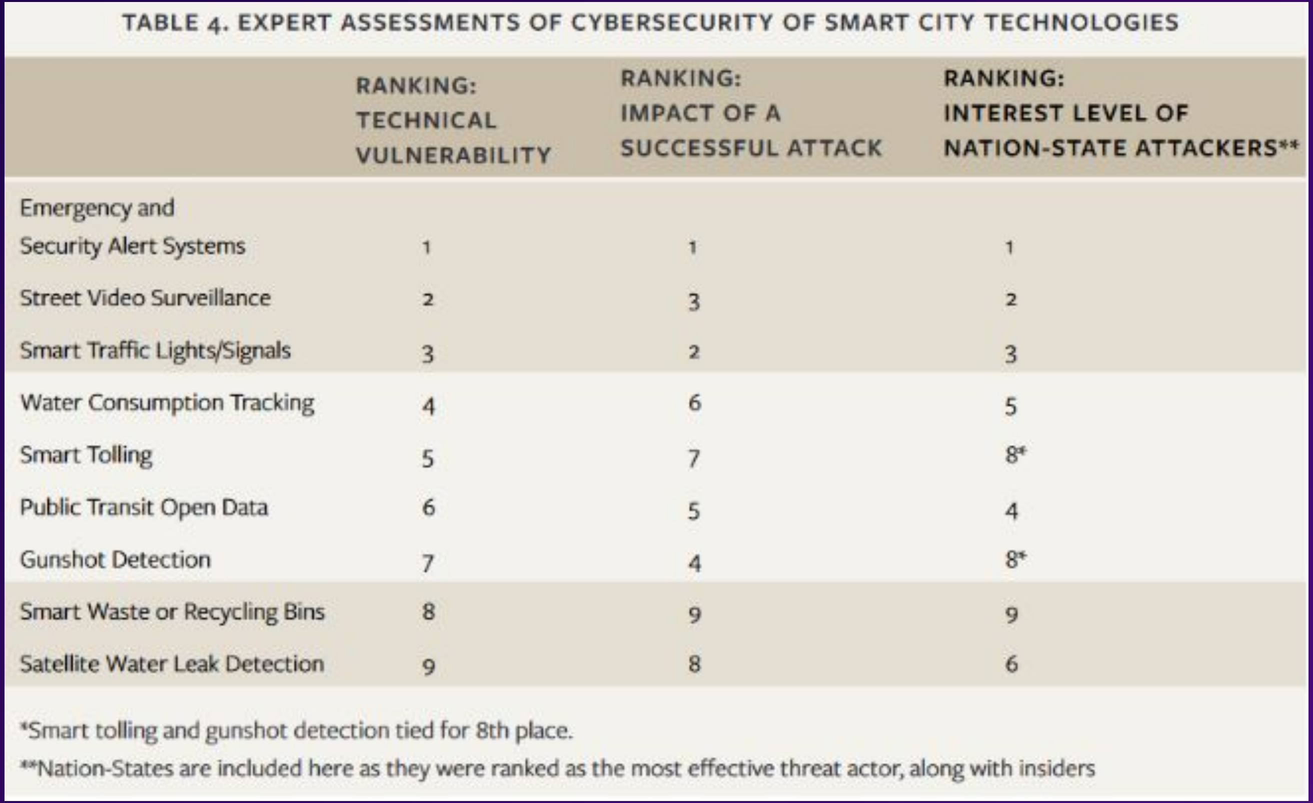


TABLE 4. EXPERT ASSESSMENTS OF CYBERSECURITY OF SMART CITY TECHNOLOGIES

	RANKING: TECHNICAL VULNERABILITY	RANKING: IMPACT OF A SUCCESSFUL ATTACK	RANKING: INTEREST LEVEL OF NATION-STATE ATTACKERS**
Emergency and Security Alert Systems	1	1	1
Street Video Surveillance	2	3	2
Smart Traffic Lights/Signals	3	2	3
Water Consumption Tracking	4	6	5
Smart Tolling	5	7	8*
Public Transit Open Data	6	5	4
Gunshot Detection	7	4	8*
Smart Waste or Recycling Bins	8	9	9
Satellite Water Leak Detection	9	8	6

*Smart tolling and gunshot detection tied for 8th place.

**Nation-States are included here as they were ranked as the most effective threat actor, along with insiders

CYBERSECURITY RISKS

- In 2017, hackers turned on 156 severe weather sirens.
- Cybercrime costs $6 trillion annually.
- Government actors and terrorists will be lured to attack. (E.g. Russia’s 2007 cyberattack on Estonia)
- There will be an estimated 1.3 billion wide-area network smart city connections by 2024.
- Despite all this, cybersecurity is often an afterthought.

SOME ATTACKS

- Data and identity theft.
- Hijacking devices.
- Man-in-the-middle attacks (posing as the sender).
- DDoS failures
- Ransomware.
- Physical destruction of networks.

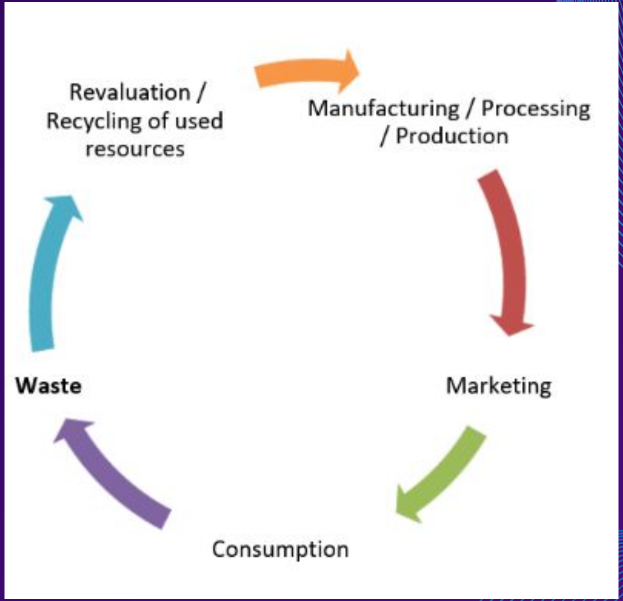
03

SOLUTIONS

How to mitigate problems.

ARE YOU READY?

- DON'T create a Smart City until you're ready.
- You need democracy, education, knowledge, and a circular economy focused on humans and ethical growth.
- Learn everything first!
- Create partnerships with nearby allies, but don't rely on foreign gov's to create your cities.



Revaluation / Recycling of used resources

Manufacturing / Processing / Production

Marketing

Consumption

Waste

HOW TO PREPARE WHEN CREATING YOUR CITY

- Start small.
- Avoid overreliance.
- Hire a dedicated security team.
- Like online banking, use security by design and default.
- Prepare for the worst.
- Mandate certification frameworks.
- Deter cybercriminals with honeypots/other processes.

HEY, TOM, I JUST REALIZED THAT I DON'T NEED TO OUTRUN THE BEAR; I ONLY NEED TO OUTRUN YOU.

WHAT TO DO ONCE YOUR SMART CITY EXISTS

- **Encrypt all your data always.**
- **Don’t collect data you don’t need to. Store the minimum.**
- **Don’t use Smart Cities for law enforcement!**
- **Have a far-reaching support platform (SaaS, IaaS, cloud, etc.)**
- **Have backups of everything.**
- **Control third party access.**
- **Protect the identity of devices cryptographically.**
- **Have white hat hackers testing ALL THE TIME!**

WHAT TO DO ONCE YOUR SMART CITY EXISTS

- **Have decentralized power grids.**
- **Follow industry standards at every step.**
- **Conduct regular audits, especially for important areas (like flood detection in flood zones).**
- **Move data for traffic control and grid systems only in one direction to networks + the cloud, so they can’t be controlled through the internet.**
- **Have physical life boats and manual overrides.**
- **Link up the absolute minimum.**

CYBER ATTACK
25315
ONLINE
4527
17563

DURING AN ATTACK

- Rely on your system: security monitoring, immediate incident response, vulnerability management, and patching.
- Monitor and assess in real-time.
- Rely on cybersecurity fighters. (We need an international cyberforce, like firefighters, and there needs to be insurance for Smart Cities.)
- If the worst happens, rely on nearby cities, countries, and partnerships.

AFTER AN ATTACK

- Share information with international partners.
- Release limited data to public, prioritizing long-term safety and ensuring a lack of panic.

INTERNATIONAL LAW NOTES

- **WE NEED AN INTERNATIONAL CYBER TREATY.**
- **WE NEED AN INTERNATIONAL CYBERSECURITY ALLIANCE.**
- **Cyber warfare against Smart Cities should be seen as a presumptive violation of international law and the Geneva Conventions.**
- **No attacking SC's, even during conflict.**

04

THE FUTURE

What comes next?

The Future

Cities that aren’t limited by borders

Happier, more productive people who waste less time

Freedom, democracy, equality

IS IT WORTH IT?

"Risk-taking is the essence of innovation."

—Herman Kahn

CONNECT WITH ME

Do you have any questions?

isvari@dweebsglobal.org
www.dweebsglobal.org

Free mentorship/mental health support!

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik**