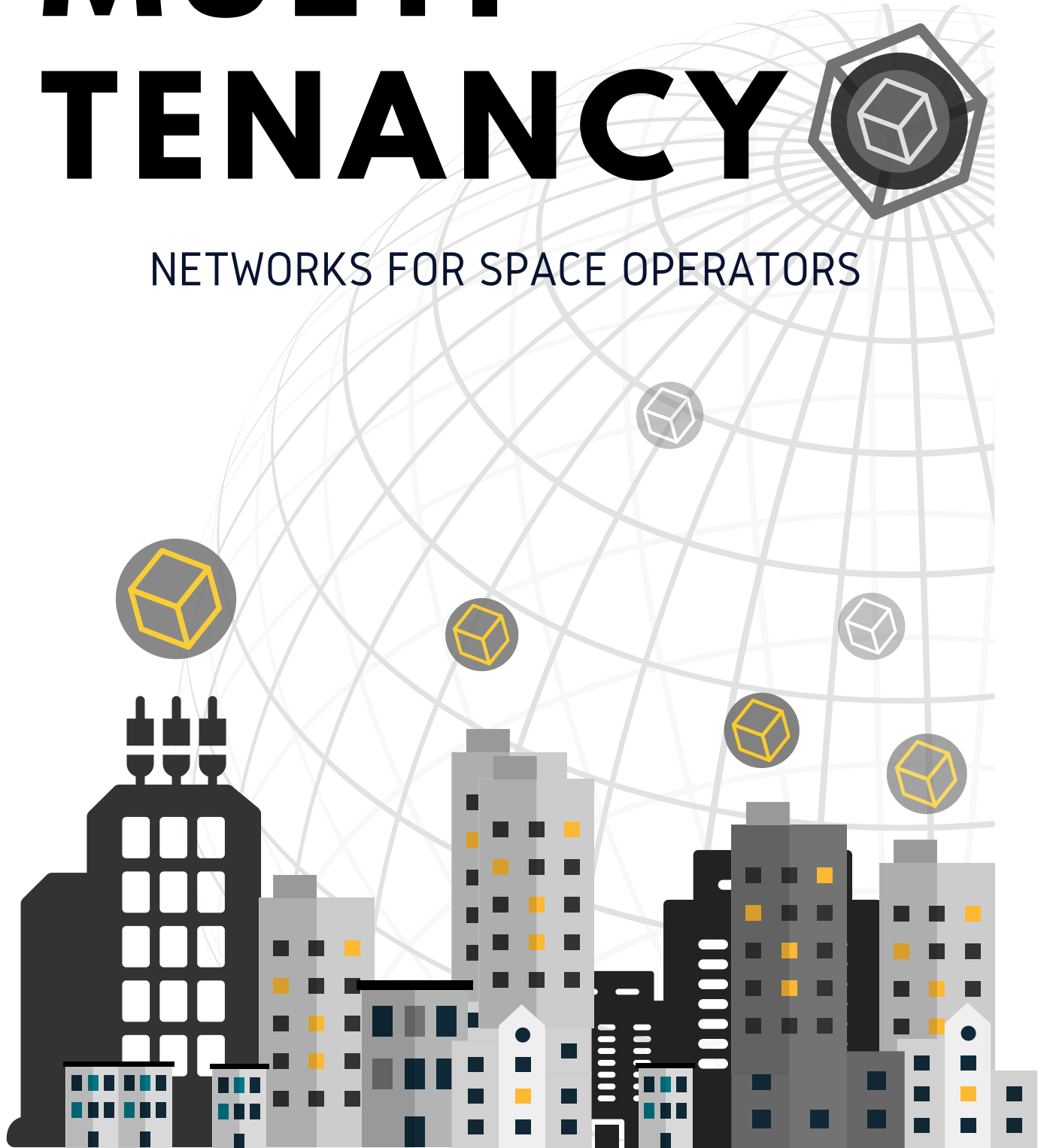SECURE

MULTI-TENANCY

NETWORKS FOR SPACE OPERATORS

Is your position defensible?

info@defensible.ie

BUSINESS AND TECHNICAL
REQUIREMENTS

- Create a **standard service offering** (versus *custom each time) inc. a* realistic **support model and engineer** service reliability.

- Define your **governance and service models** (inc. SLA/SLOs and impact of outages, **troubleshooting**, required expertise, lifecycle mgt.)

- Identify your shared **backbone** inc. **physical security**, surveillance, access control, sensors, and **Building Management Control Systems.**

LOGICAL AND PHYSICAL
BOUNDARIES

- Categorize per **building**, **tenancy**, **floor**, and user based risk profile(s). Create **zones** which define controls + **policy enforcement points**.

- Assume **bad actors** exploit the **transitive trusts** of tenants. Default all unused access ports to **isolated** 'go-nowhere' VLANs.

- Wireless (WLAN / 802.11) **bleeds** through walls and floors. Require **strong authentication**, authorisation, and accounting mechanisms.

TENANCY DATA NETWORKS
SEGREGATION MODEL

- Fully **isolated,** with **own network equipment** including **your own DIAs (Dedicated Internet Access)** rather than building shared **?**

- **Pass-through** with own equipment (core/edge) but re-brokered **ISP(Internet Service Provider)** services from space operator's **ISP ?**

- **An operator fully managed** wired/wireless **network access edge ?**

https://defensible.ie

WIRELESS EDGE

- Design WLAN **networks** for **25dB SNR**(Signal to Noise) and ensure **primary and secondary RSSI** coverage of -67dBm or less.

- **Trunk** to AP(Access Point) ports and tag **SSIDs**. Use **802.1X** when feasible to support. Design for both **horizontal and vertical** subnets to cover tenancies and any required **uninterrupted roaming**.

- Design around and minimise **CCI / ACI** (Co-channel Interference / Adjacent Channel Interference)

ALERTING AND OPERATIONS

OBSERVABILITY

- **Observe**, **Orientate**, **Decide**, **Act** is the **OODA loop.** You must empower your teams to know what's going on at all times **!**

- Configured alerts must be **actionable** and go to the **correct groups**. Historical **trending** and **capacity management** must be maintained.

- Use **sensors**, **cameras**, and **alerting thresholds** to ensure '**situational awareness**' of the operating environment.

SMARTER BUILDINGS

SENSORS AND IOT

- Design **sensor networks** in to the architecture **early** and allow for ports, zones, VLANs and horizontal or **vertical** subnets.

- **Sensors** and **IoT(Internet of Things)** devices should be zoned as **untrusted** and have their reachability heavily **restricted**.

- Measure **temperature, CO2,** and **VoC(Volatile Organic Compounds)s** to ensure a healthy environment full of productive humans and systems.

LOW VOLTAGE

Data cabling is based upon **service offerings** and tightly coupled with **network engineering** design. Mechanical, electrical engineering, and facilities **MUST collaborate with network engineering.**

Ensure **CAT5e** or **CAT6** throughout. Use fibre for **> 85m** but changes the **network engineering design** and cost structure radically **!**

All cable runs must be **tested (certified + verified) and a report provided** by cablers before 'go-live'. **Not** optional **nor** an **up-sell**.

COMMS ROOM(S) AND DISTRIBUTION

COLLAPSED CORE ?

Building or campus size and **network design** will determine the **distribution and volume** of **cabling** and **network domains/zones.**

Each **comms room** or **IT space** will require very specific working dimensions for installation, **maintenance**, HVAC(Heating Ventilation Air Conditioning), **power / UPS**, and associated cable runs.

Albeit your core data **MDF**(Main Distribution Frame) is often central, the telecommunications **MPOE**(Main Point of Entry) also factors in to many design and location decisions (especially in 'greenfields' sites).

CLOUD, ON-PREMISES, CO-LOCATION

COMPUTE

Unless you are building a datacenter, do not host client or others compute resources (if you can avoid it).

Reduce your compute footprint to a **minimum** and **leverage** co-location or **cloud** based services **for reliability** and **reduced OPEX**.

The **'cloud'** is your friend, use it, including for logging and monitoring.

https://defensible.ie

RECAP / REMINDERS

1 - Ensure business and technical requirements are defined and realistic.

2 - Governance model and risk profile(s) define the boundaries between zones.

3 - Segregate zones and tenants from each other in to separate '*failure domains*'.

4 - Wireless / WLAN helps with mobility but also bleeds in 3D. Hope is not a strategy with CCI/ACI...

5 - Use the OODA loop to manage what you measure. Detect and respond.

6 - Design sensor networks early and optimize spaces for productivity.

7 - Get certified reports on all cable runs (fiber and copper) before going live.

8 - Network engineering must drive specific requirements and outcomes.

9 - Embrace the 'cloud'.