

# **SECURITY, RESILIENCE & SUSTAINABILITY**

The benefits and challenges  
brought by SDR

Dr James Irvine  
Dr Greig Paul  
University of Strathclyde

# THE CHALLENGE

Current wireless networks lack sufficient

Security

Resilience

Sustainability

in particular for CNI applications

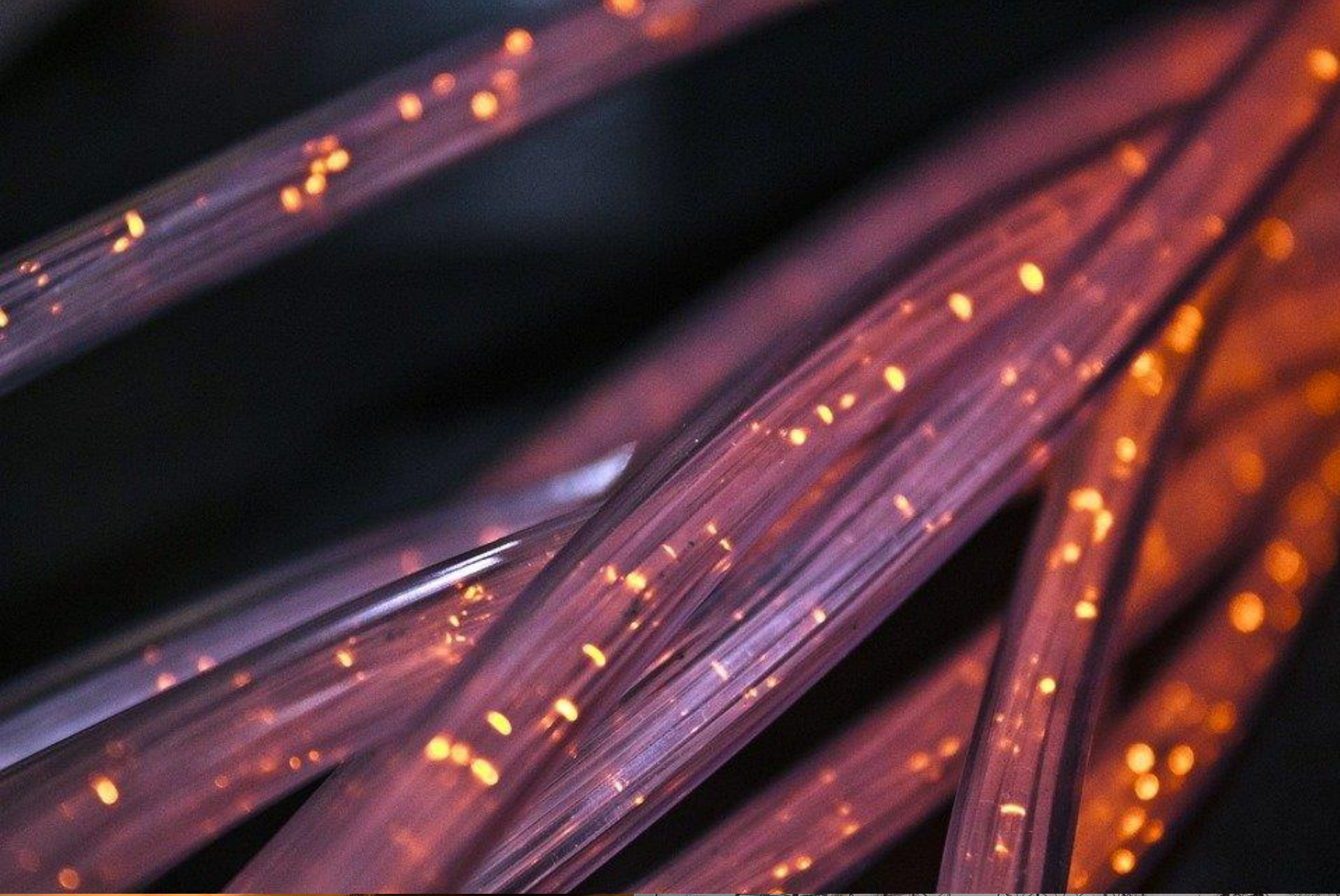


5G has enhanced expectations, not necessarily delivery

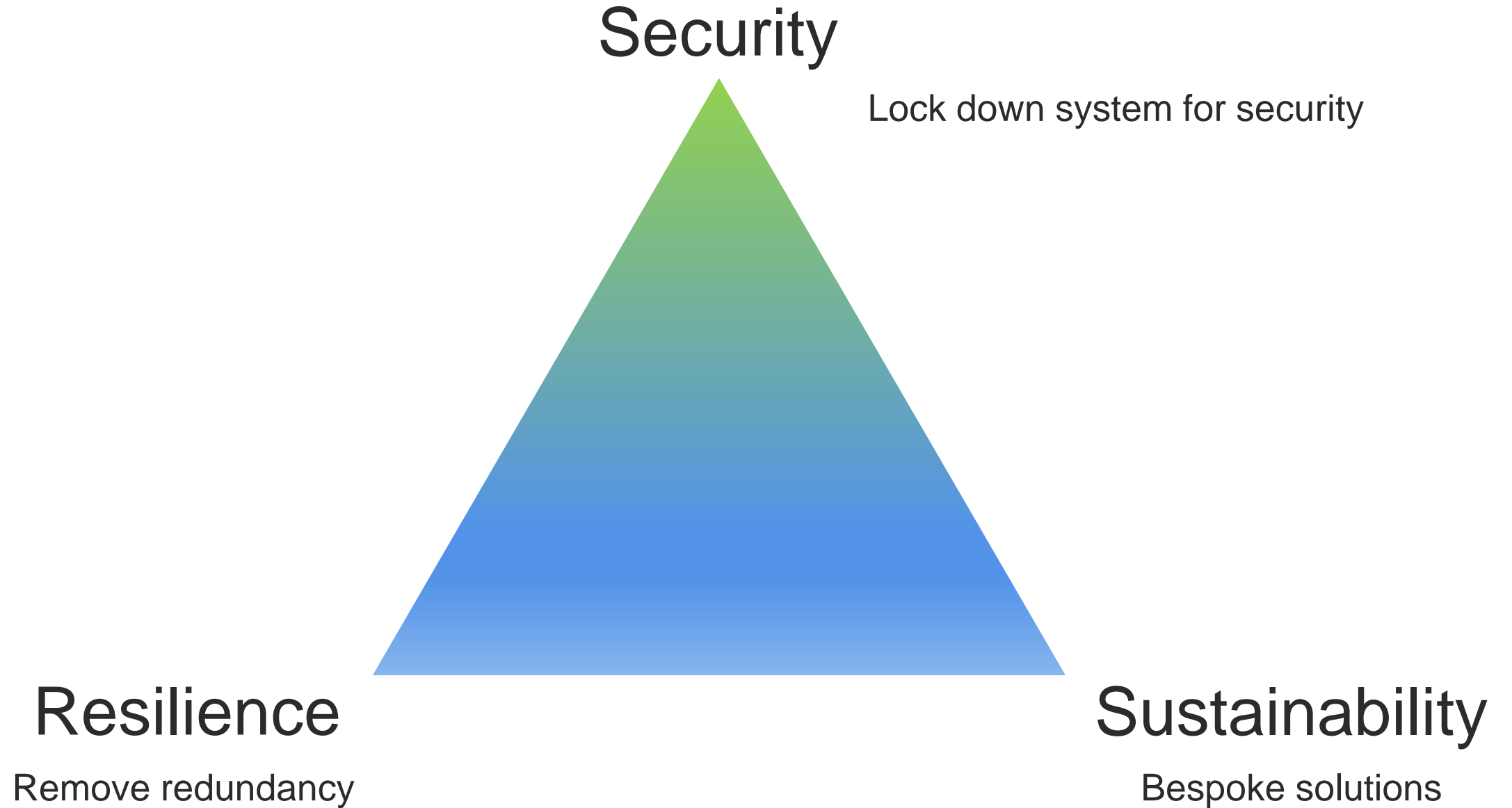
# REAL-WORLD RESILIENCE?

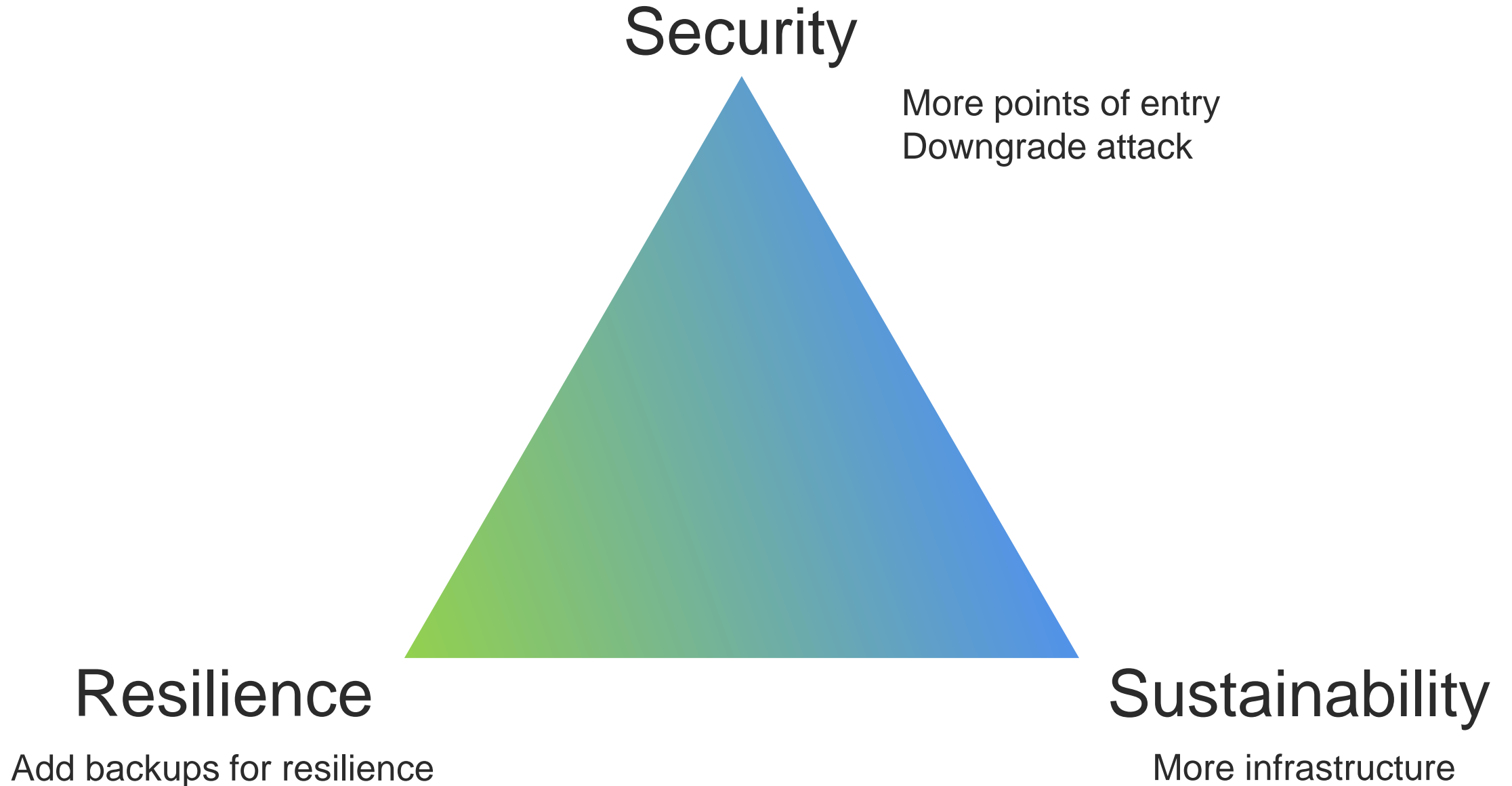
Network	% of network (approx.)	Power Autonomy
EE & 3	~3%	~6 hours
EE & 3	~4%	5+ days (ESN EAS sites)
EE & 3	<b>~93%</b>	<b>None</b>
Vodafone (Beacon)	~50%	4 hours
Vodafone (Beacon)	~50%	1-2 hours
O2 (Beacon)	~5%	4 hours
O2 (Beacon)	Few large coverage area sites	10 mins
O2 (Beacon)	<b>~95%</b>	<b>None</b>

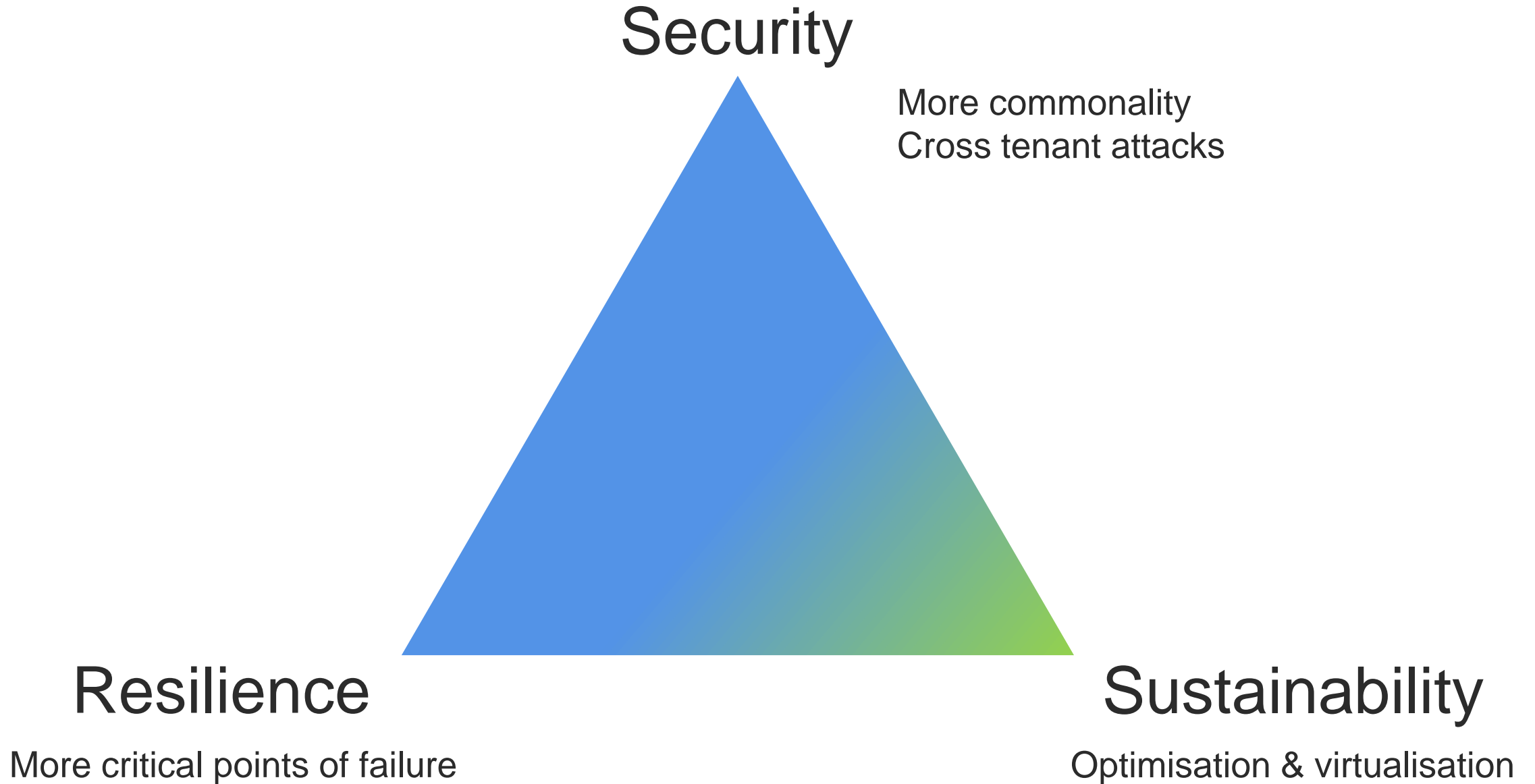
Is mobile in your disaster recovery plan?

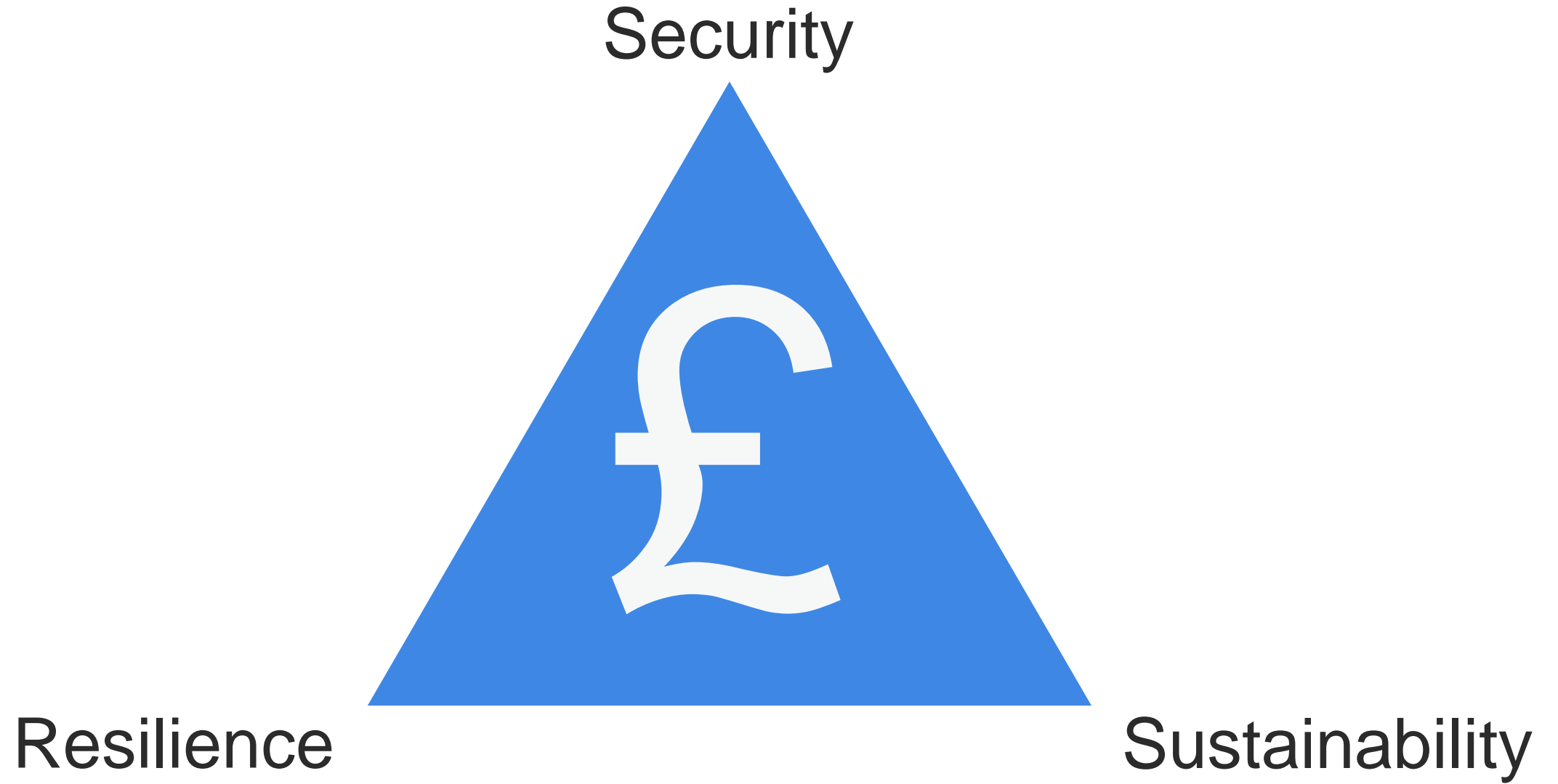


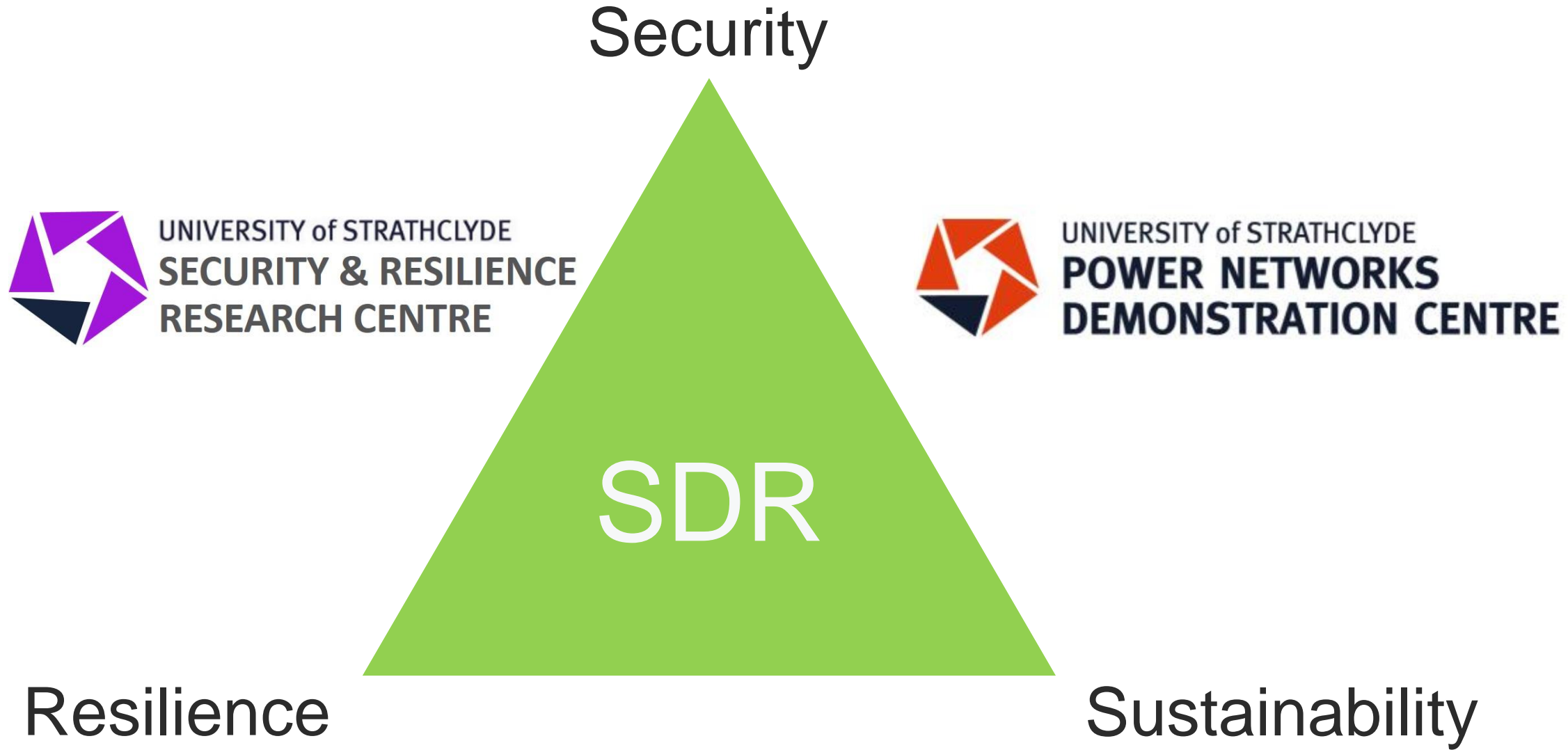
# THE TENSION







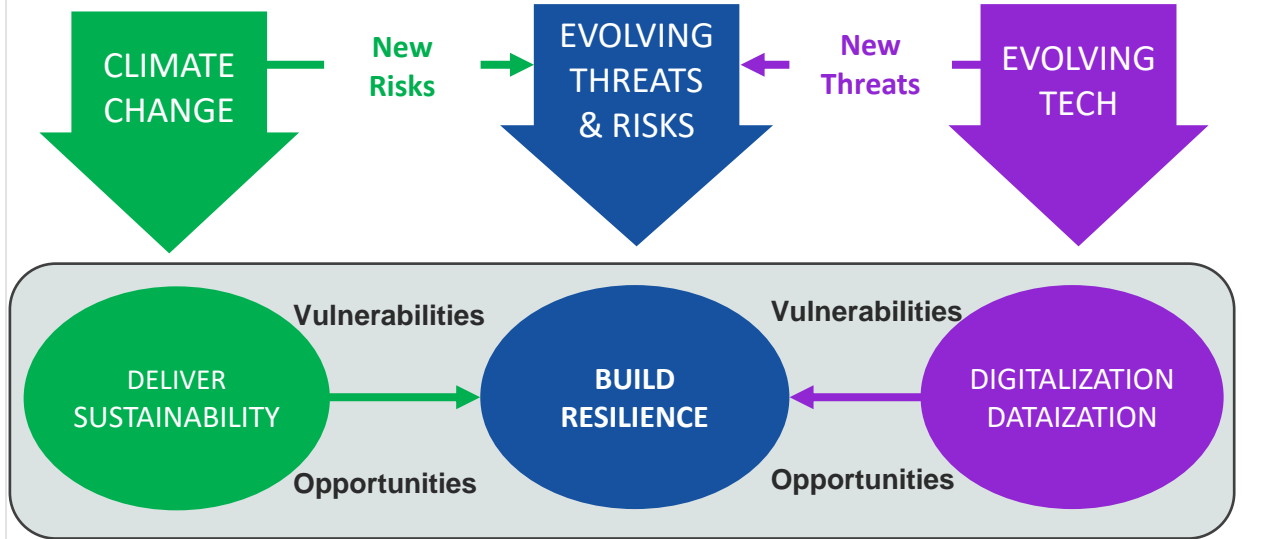






# UNIVERSITY of STRATHCLYDE SECURITY & RESILIENCE RESEARCH CENTRE

Change to survive and thrive in an ever-changing world

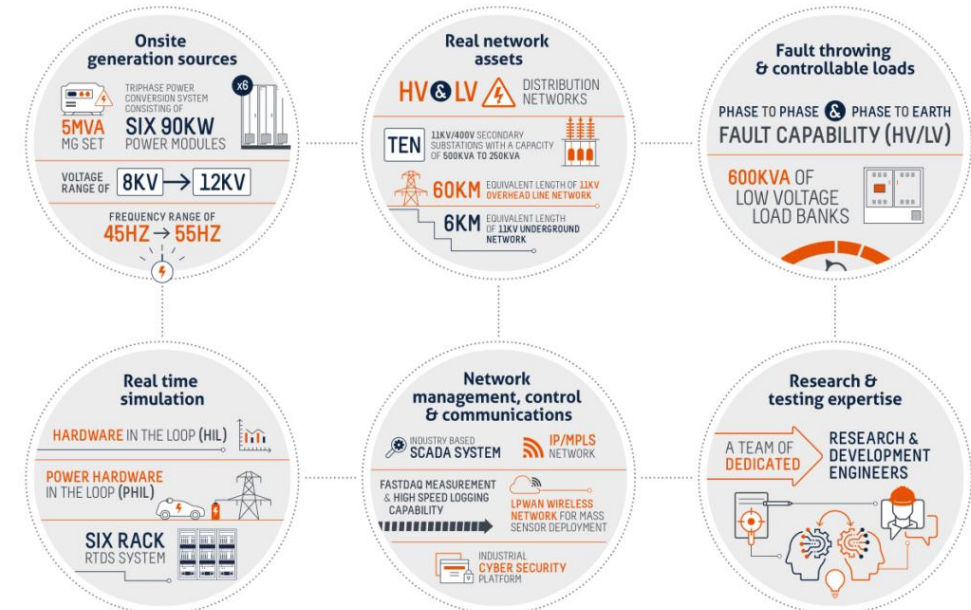
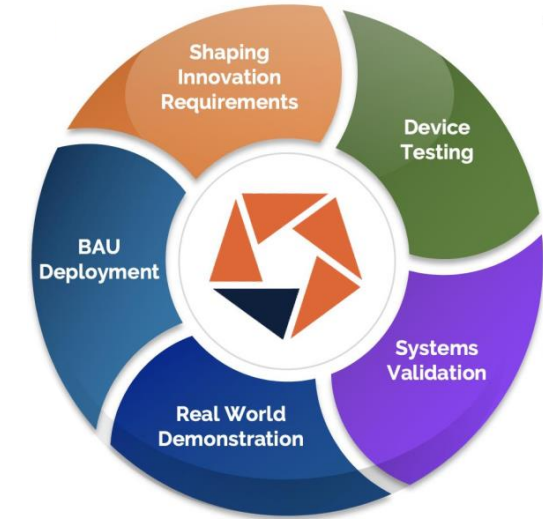


## Common and achievable enablers

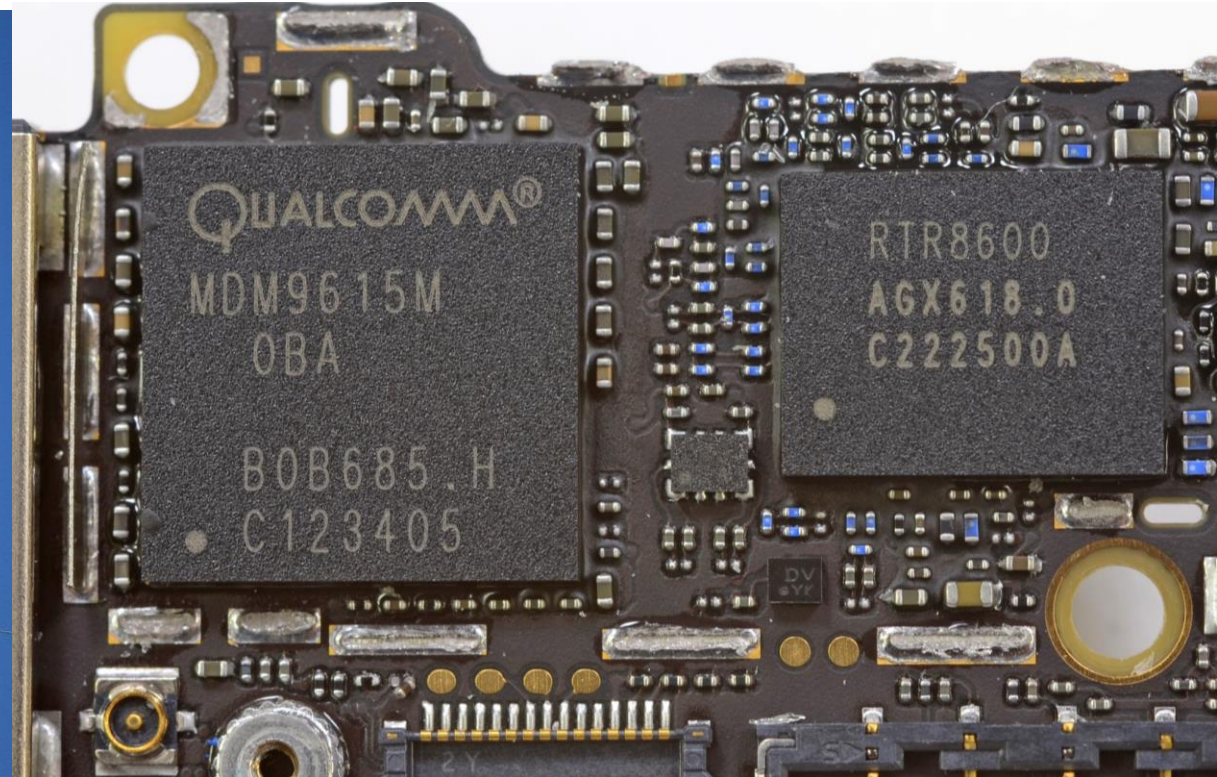
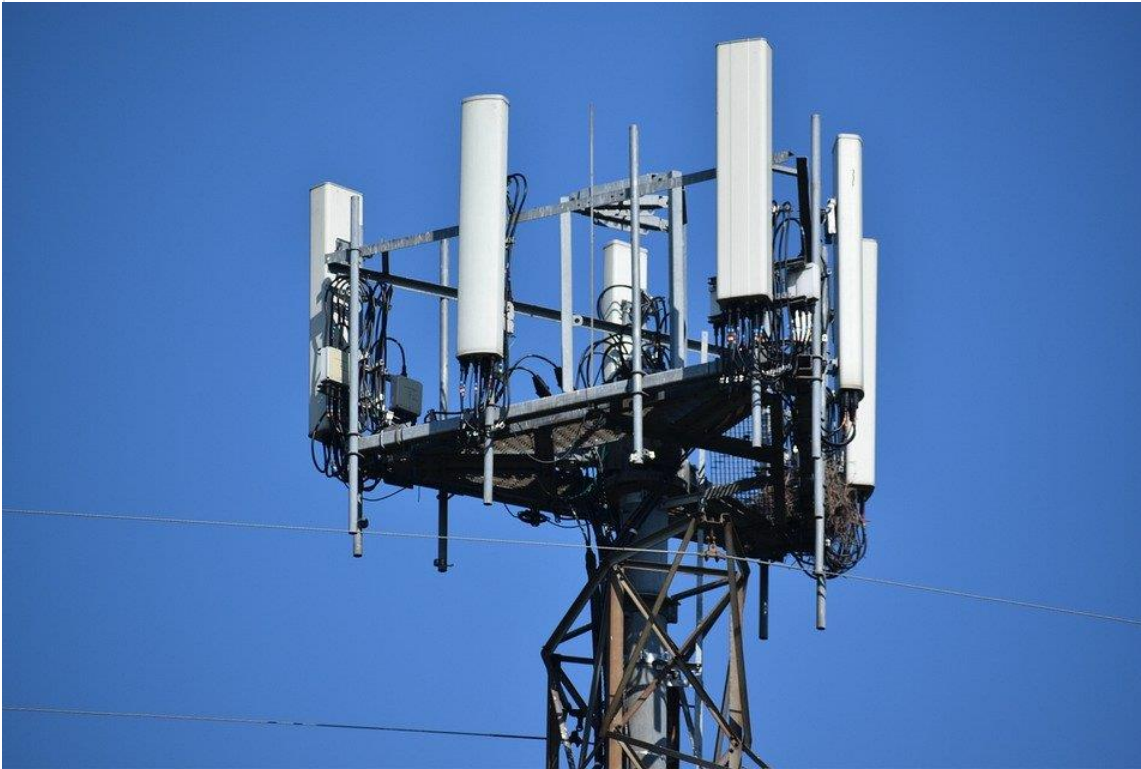
- Policy, regulation and corporate governance that values and drives for these outcomes
- Leaders who understand the potential costs of not acting and invest accordingly
- Active risk awareness, risk management and a risk culture
- Real-time monitoring, data-driven decisions and a data culture



# UNIVERSITY of STRATHCLYDE POWER NETWORKS DEMONSTRATION CENTRE



# SDR IN MOBILE?



# THE SECURITY CHALLENGE OF WIRELESS

The air interface is exposed (to everyone)

Programmable logic is a possible exploitation route

The supply chain?

But...

A fixed implementation becomes useless

When, not if, it becomes vulnerable

# THE RESILIENCE OPPORTUNITY OF WIRELESS

Redundancy of systems often gives us resilience

A phone can “do” 2G, 3G, 4G (and maybe 5G)

As transport, but the service must be supported

Graceful fallback to lower generations

Most G’s can be delivered over the same bands

Adapting the service as required – what do you **need**?

# ANSWERING THE SECURITY CHALLENGE

We cannot “freeze” our security stack at the RF layer

Security **framework** needs to be built in from the start

Post-quantum encryption/signature standards inbound!


Ensure the logic update mechanism is robust and securely built

Try to make as much logic updateable as possible

Vulnerabilities **will** be found

# SIGINT: Few advances in GSM security



European network operators are taking their time updating their networks to close known security vulnerabilities, cryptography experts reported at the Chaos Computer Club's [SIGINT 12](#)  conference in Cologne, Germany. An analysis of 105 networks showed that only very few providers have taken effective steps against security vulnerabilities that allow third parties to, for example, pinpoint the location of mobile phones, listen to messages, and misappropriate someone else's identity. Plans are now in the works to further evaluate the gathered data with better software.



At the [CCC conference 28C3](#) in late 2011, Karsten Nohl and his team demonstrated new security vulnerabilities affecting GSM, and launched the [GSMMMap](#) project, where volunteers can submit data on the state of network operators' security in various countries. The Osmocom software serves as the foundation, collecting data on network communication with the help of a cheap mobile phone. An interactive map shows the results of the crowdsourcing project.

The results are sobering. At this point, only seven of the network providers included have implemented the A5/3 encryption standard, which fixes the [problems](#) known since 2009 to be present in the previous A5/1 standard. On other networks, these vulnerabilities can still be used to intercept GSM data and decode it almost in real time. For example, according to GSMMMap project's data, none of the German network operators have switched to A5/3 yet. In Cologne, Sam May pointed out that very few mobile phones in western Europe can even handle the new standard. The figure is between 10 and 25 per cent in Germany, but over 75 per cent in Iran, Slovenia and Egypt, May said.

Downgrade attacks

Standards set in stone

Very hard to upgrade clients in-the-field

More software means more ability to patch!

# REALISING THE RESILIENCE OPPORTUNITY

Fallback can give us resilience for “almost free”

But in CNI we can't fall back to something insecure

De-coupling the PHY at both ends is highly versatile

If we sort out the commercial challenges

For resilience, adapt the network for reduced power usage, etc.

Graceful degradation, longer run-times

# **BUILDING NETWORKS FOR RESILIENCE**

SDR gives huge flexibility across systems

Within band/power amp constraints, can deploy a more appropriate technology if needed

For example, to EC-GSM-IoT (Rel-13) or TETRA

Longevity

CNI expects/requires far longer lifespans than telcos

60 year-old assets in many substations!

# SOFTWARE CHALLENGES/OPPORTUNITIES

Software supply chain complexity is increasing exponentially

Solarwinds, Kaseya – 2 notable recent examples

Software logic can be compromised “after shipping”

Chain of trust – today’s update controls tomorrow’s

How do you validate/assure updates before deploying?

How can we validate & assure SDR FPGA bitstreams?

More complex orchestration/platforms for software a risk too...

{\* SECURITY \*}

# Microsoft fixes flaw that could leak data between users of Azure container services

No data went awry, Cosmos DB had a similar bug just two weeks ago

Simon Sharwood, APAC Editor

Thu 9 Sep 2021 // 02:56 UTC

3 



Microsoft today revealed it fixed a vulnerability in its Azure Container Instances services that could have been exploited by a malicious user "to access other customers' information."

**Azure Container Instances** (ACI) is a serverless container environment. Microsoft says it offers the flexibility of containers and the security of VMs running atop a hypervisor.

No technical details of the flaw have been revealed, **save that** users should "revoke any privileged credentials that were deployed to the platform before August 31, 2021," and that rotating privileged credentials would be "an effective precautionary measure" – perhaps suggesting an authentication issue. Microsoft has also reminded users that credentials can be found in environment variables, secret volumes, and even in Azure file shares – so there may be a bit of tidying up to do.

# Reflections on Trusting Trust

*To what extent should one trust a statement that a program is free of Trojan horses? Perhaps it is more important to trust the people who wrote the software.*

**KEN THOMPSON**

---

<sup>1</sup> UNIX is a trademark of AT&T Bell Laboratories.

---

© 1984 0001-0782/84/0800-0761 75¢

**August 1984** Volume 27 Number 8



# University of **Strathclyde** Glasgow