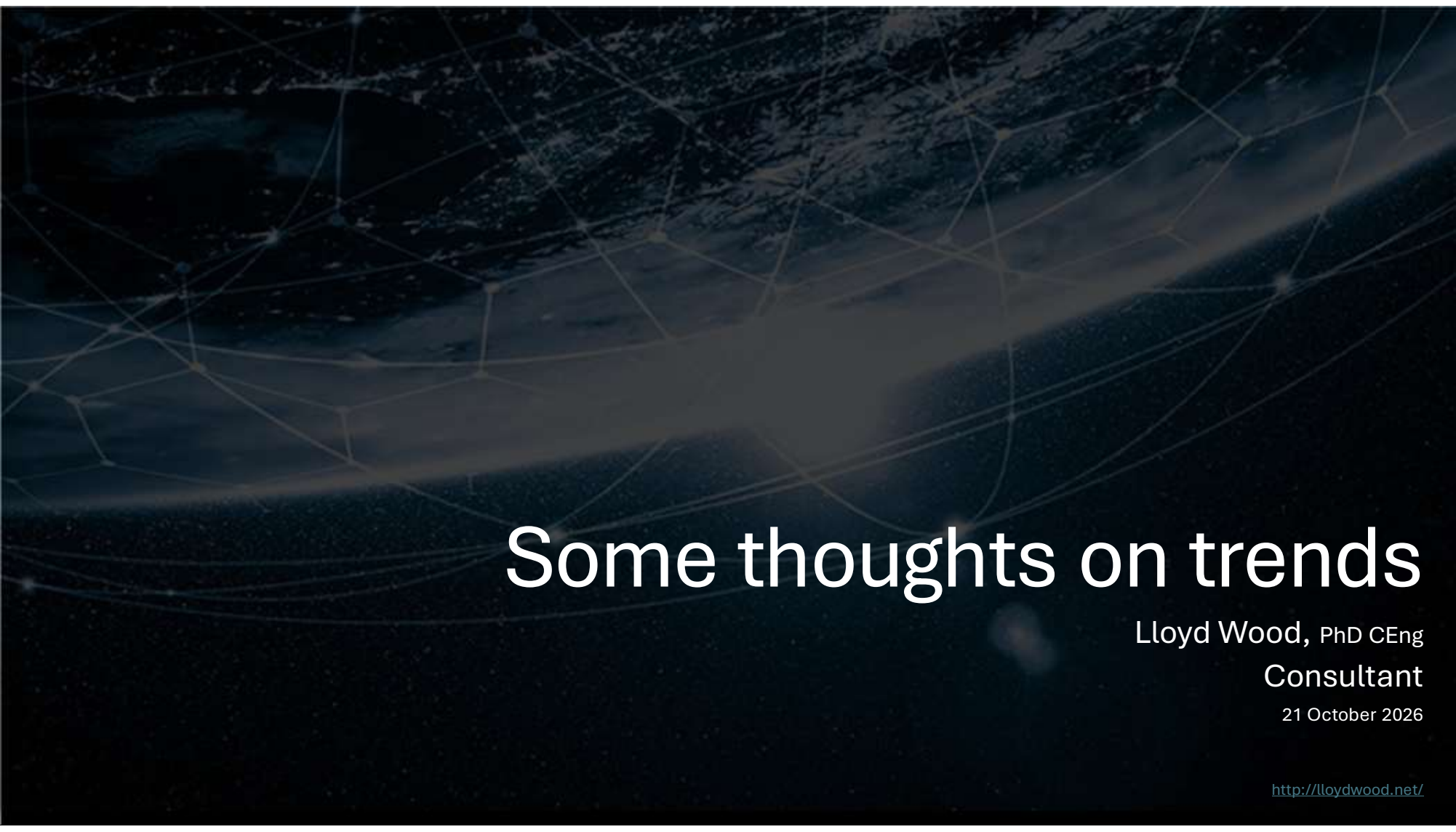


Some thoughts on trends

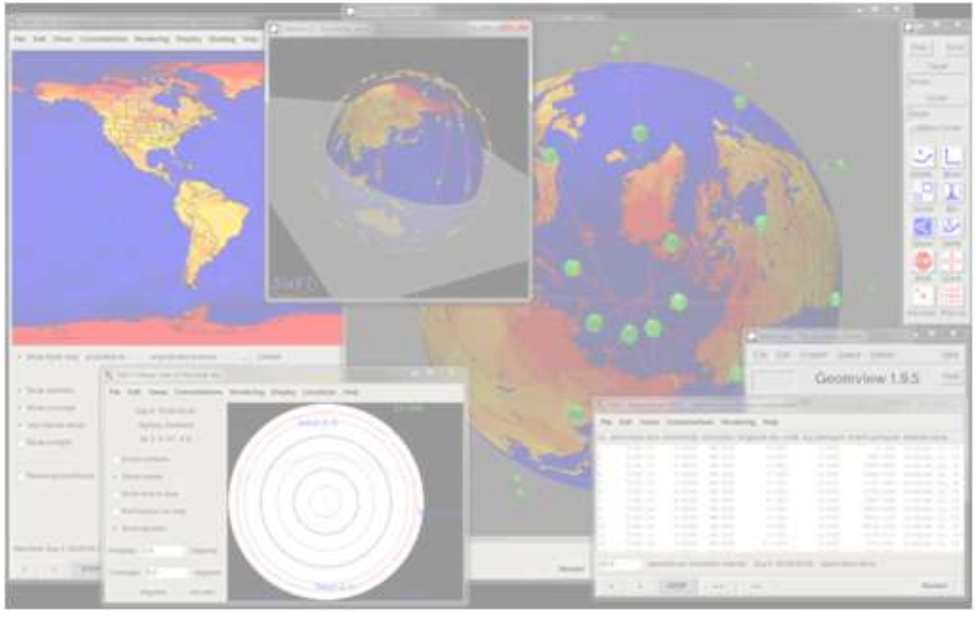
Lloyd Wood, PhD CEng
Consultant

21 October 2026

http://lloydwood.net/

My perspective

- **Offering opinions** and speaking solely in a personal capacity.
- **My viewpoint** is informed by my experience as an engineer.

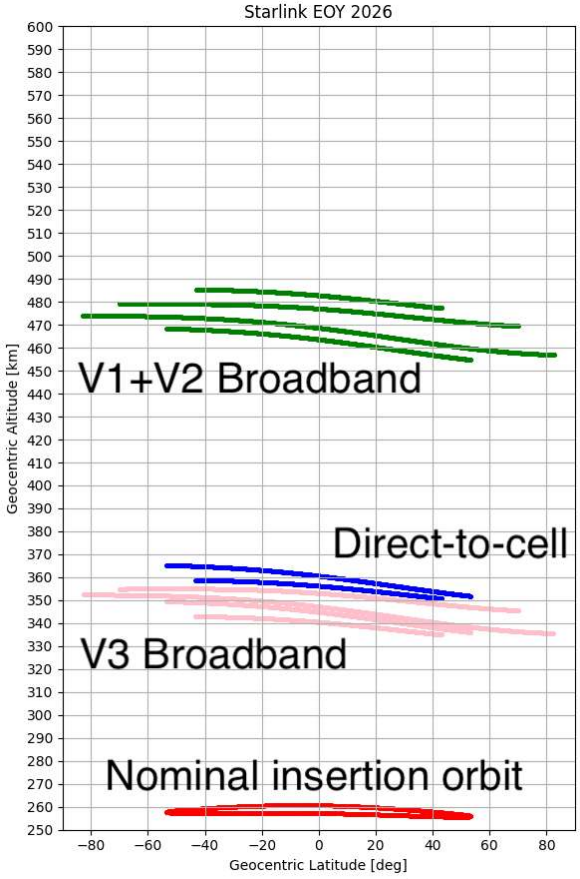


http://savi.sf.net/

- I have **design and operational experience** in:
  Enterprise security – previously worked in that space.
  Internet – contributed to various IETF RFCs, including for TCP.
  Satellites – flew payloads and code in orbit, managed GEO beam use.
  …and used to research satellite constellations, using SaVi

Satellites, constellations and shells

- How many satellites is enough satellites? (lower altitude: more for same coverage)
- Do data centres in orbit even make sense? (radiating heat, event upsets, built-in obsolescence)
- Another constellation shell simply means that there's not enough capacity in a single shell – to serve the busy *spots of peak demand*. Other areas remain idle, or are occasionally used when needed.



https://space-safety.starlink.com/

Choice and control of a LEO constellation

- You're subscribing to a global service, subsidising eternal replacement of capacity flying mostly over… well, nowhere. You have no control over the system. Harnessing MoUs, assurances, contracts, SLAs…
- Contrast with single geostationary satellites with shaped, targeted coverage. GEO satellites can now be refuelled in orbit – potentially giving decades *vs* low-latency LEO replaced after a few years.
- GEO can give an increased degree of *operational control*.
- but that's still not reaching we-built-it-ourselves we-can-rebuild-it capability and *sovereignty*. Few nations have that.
- Maybe hedge your bets, diversify, and go multi-orbit?

How much security is considered enough?

- We all know *regulatory capture*: a government agency serves the interests of an industry it is meant to oversee, over the needs of the public that it is intended to serve. *(*the *revolving door)*
- *Security capture*: an organisation's security function serves the interests of the security sector it is meant to use, over the needs of the business that it is intended to serve. (Just maturing as a profession?)
- Security issues capture the attention of the board. Threats are articulated, and must be responded to. Difficult to argue with the concerns advocated for, or with the budget requested.
- Security protects and preserves the *status quo*. It doesn't build new business. But security does work to protect business *sovereignty*. **Budget spent on security is not spent elsewhere: a zero-sum game.**

Examples of more than enough security?

- **ASD Essential Eight/Essentials** : Level 1 is achievable, maintaining levels 2/3 takes considerable extra effort and expense. Not always worthwhile.
- Vulnerabilities: there are so many vulns! So, we must triage, and choose what should be addressed. But this choice requires domain-specific knowledge; saying “we’ll address every CVSS over 9.0” is an ambitious approach. Infinite technical debt, tying up testbeds and engineers.
- A CVSS score is a choice, describing a threat that may not be relevant to you.
- Does closing vulns to meet a compliance checklist and scorecard add any protection to the organisation, if those vulns would never have been exploited?
- State actors may really *not* be interested in your network. (But security says you can’t take that risk. And then there’s the growing threat of AI…)

Accepting your level of security is a choice

- Security is an ongoing investment, at a level the business should be comfortable with.
- Best practice must be bought and paid for. Continually.

- Scope creep: how much security is sufficient for business needs?
- Does the business really have any say here?

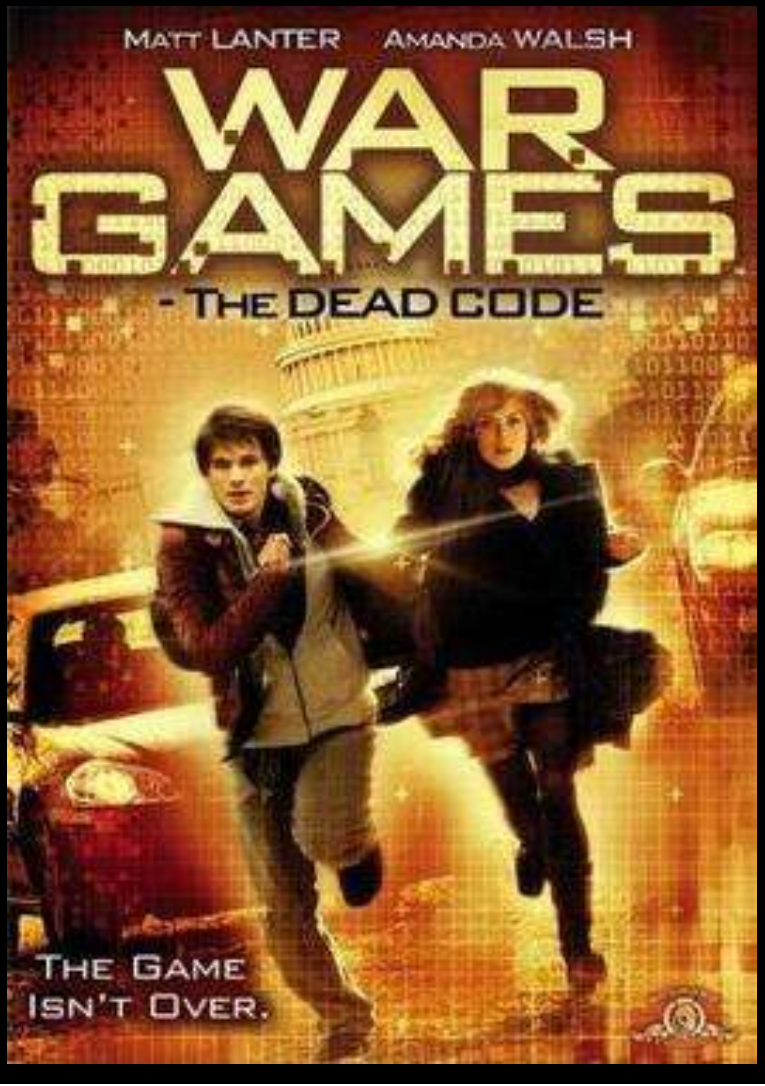
Security capture in standards processes

- I've observed that conversations about design can often become conversations about *security design*. Two examples:
- The interplanetary internet: the bundle protocol (IRTF DTNRG, now IETF DTNWG). Designed with security in it from the get-go.
- IETF tiptop (Taking IP to other planets) group. Now derailed into discussion of reliance on QUIC, and on adjusting security protocols for deep space.
- 'How will we talk to other planets' is now 'how do we deal with certificate expiry and key rotation at large distances with large delays?' when security wants faster-expiring certificates for forward secrecy, quantum resistance.
- How do we ensure control of our distant deployments.. *securely*?

Security's strength: it fails hard

- **Also security's biggest *weakness*: it fails hard.**
- "Everything is an attack!"
- But to be fair, *everything* can fail hard, given half a chance.
- Degradation is often not handled gracefully.

- **Security contains its own manifold denials of service.**
- When a certificate expires, the systems that depend on use of that key can fail too. A problem gets amplified.
- Doesn't matter if it's a key permitting use of vendor software, or…
- Oh, no, *printers*.



"A STRANGE GAME. THE ONLY WINNING MOVE IS NOT TO PLAY"

- WAR GAMES (1983) MOVIE

Consider the Telstra GPS outage in July 2026

- An internal clock rollback in time due to a lack of software upgrades, exposing misset stratum levels, caused timing issues that cascaded through the network. (Not actually an attack on security!)
- Nothing said ‘wait a minute, time just changed a lot? Is that right?’
- Why can functionality be made to fail so easily?
- Who still understands the brittle systems that we have built?
- Emergent behaviour is unanticipated. Our complexity will doom us all.
- Timing was called out as one of the *sovereign functions*.

Findings Report on the July 8th Telstra Outage, Technology Audit Partners, 24 August 2026. (Raymond Owen, Partner at TAP)
Failures and Resilience in the IP Era: Navigating the Fragility of Modern Telecommunications Networks—The Sovereign Functions,
R. Owen, A. Bryant, L. Finch, D. Franklin, M. Abdollahi and M. Abolhasan, IEEE Access, 25 August 2025, http://dx.doi.org/10.1109/ACCESS.2025.3602054.

Humans look to authority

- We build systems containing single authoritative points of failure, *e.g.* Active Directory servers, BitLocker servers, GPS for NTP. Locally redundant, but providing single, trusted, sources of truth. Until they don't.
- We build big centralised systems. Then we try to defend them. Shore them up.
- When a centralised piece of control fails, the effects are widespread.
- A single flaw can bring down a network.
- Why don't we design distributed systems, which fail differently? Gradually? Gracefully? Why *can't* we? (Complexity? Cost?)
- Lock-in to existing dogma? Limits to human imagination and psychology?
- Calling something *sovereign* calls it *important*. Says it has to be *protected*.
- But that won't fix flaws in the architecture around it. **Where is the resilience?**


STAR WARS, STARGATE,
OBLIVION, EDGE OF TOMORROW,
THE LORD OF THE RINGS, GAME OF THRONES,
THE AVENGERS, INDEPENDENCE DAY, PACIFIC RIM...

Sovereignty

- Our society's entire reliance on positioning (GPS/Glonass/Galileo) shows some of the limits to our sovereignty. How much independence do we really have?
- Technical sovereignty? We're placed at the mercy of vendors – mostly outside Australia – and the way that their industries have chosen to do things.
- This is the nature of the globalised world.
- How much sovereignty do you have over your household appliances?
- **Make procurement choices carefully** – in satellites, in submarines, in vendors or in anything else. That will ultimately dictate what and how much you can control…
- …but even your best-practice architecture can still contain the dormant seeds of your destruction.
- Sovereignty isn't ***resilience***.


“TAKE WHAT YOU CAN. GIVE NOTHING BACK.”
- PIRATES OF THE CARIBBEAN