Standards v Open Source

Applied to Critical National Infrastructures

Standards

Pros

- Common foundation specifications referenced globally
- Community learning by sharing rationale & debate
- Enables backwards compatibility
- Discourages lock-in to a single implementation
- Recognized / persistent governance authority
- Clear licensing model (typically FRAND)
- Facilitates "Security by Design"
- Implementation diversity reduces global vulnerability

Cons

- Time to analyze technical feasibility and develop consensus
- Potential for over-specification constraining innovation
- Vulnerable to blocking behaviors
- Implementation ⇔ feedback cycle too long
- Difficult to align domain-specific standards organizations to create compatible specs
- Barriers to participation by smaller players
- Entrenched culture resistant to change
- Poor participation by IT players

Open Source

Pros

- Bypasses consensus reducing time to implementation
- Fast bug fixes and improvements
- Community development of core functionality
- Low barrier to participation by smaller players
- Strong participation by IT players

Cons

- Reduced implementation diversity increases vulnerability
- Lacks recognized / persistent governance authority – who determines priorities for releases?
- Unconstrained code contributions leading to bloat / bugs
- Feature persistence from release to release -- what constitutes "normative" in open source code?
- Risk of lock-in through forking
- Uncertain licensing implications
- Difficult to ensure "Security by Design"
- Culture: hard to manage individual developer contributions
- Vulnerable to fragmentation into multiple communities
- Stretches developer resources
- Poor / non-existent documentation on what the code does