# Article information:

Sensors | Free Full-Text | Cybersecurity in ICT Supply Chains: Key Challenges and a Relevant Architecture
<https://www.mdpi.com/1424-8220/21/18/6057>

# Article summary:

1. The digital transformation of ICT systems has led to a greater dependence on these systems, making the resilience of ICT systems crucial in preventing disruptions and minimizing their impact.

2. Cybersecurity is a major challenge in the supply chain realm due to potential domino effects, with cyber attacks affecting all services and application domains simultaneously.

3. Challenges to achieving cyber resilience include the need for end-to-end solutions for vulnerabilities and risks management, lack of evidence-based metrics for security assurance and trust guarantees, cumbersome coordination in multi-actor and multi-vendor supply chains of ICT systems, static cybersecurity networked configurations and dynamic systems audit, and unlikely wide adoption of integrated cybersecurity solutions for composed ICT systems.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article "Cybersecurity in ICT Supply Chains: Key Challenges and a Relevant Architecture" discusses the challenges faced by organizations in securing their ICT supply chains. The article highlights the need for end-to-end solutions for vulnerabilities and risks management, lack of evidence-based metrics for security assurance and trust guarantees, cumbersome coordination in multi-actor and multi-vendor supply chains of ICT systems, static cybersecurity networked configurations, and unlikely wide adoption of integrated cybersecurity solutions for composed ICT systems.

The article provides valuable insights into the challenges faced by organizations in securing their ICT supply chains. However, it is important to note that the article may have some biases. For example, the article focuses on the challenges faced by organizations but does not provide enough information about potential solutions or best practices that can be adopted to address these challenges. Additionally, the article does not explore counterarguments or alternative perspectives on the topic.

Furthermore, while the article notes potential risks associated with cyber attacks on ICT supply chains, it does not provide enough evidence to support its claims. For instance, the article mentions that 60% of SMEs would be out of business within six months of being hit by a cyber attack but does not provide any sources or evidence to support this claim.

Overall, while the article provides valuable insights into the challenges faced by organizations in securing their ICT supply chains, it could benefit from providing more balanced reporting and exploring alternative perspectives on the topic. Additionally, providing more evidence to support its claims would make the article more credible and informative.

# Topics for further research:

* Best practices for securing ICT supply chains
* End-to-end solutions for cybersecurity in multi-vendor supply chains
* Evidence-based metrics for security assurance and trust guarantees in ICT systems
* Dynamic cybersecurity networked configurations for composed ICT systems
* Integrated cybersecurity solutions for multi-actor supply chains
* Evidence supporting the impact of cyber attacks on SMEs

# Report location:

<https://www.fullpicture.app/item/724f7c97b511b3ec9ad3eb2cd64b4509>