Cyber Threat Intelligence (CTI) for Security Operation Centres (SOCs) and Surveillance Technology: A literature review

Author: Mikko Luomala, Research Scientist, Doctoral Student

Introduction

Cyberattacks can be targeted any connected technology and the security operation centre and centres surveillance technology is not immune from cyberattacks.

Research questions

RQ1: What research has been done on the role of cyber-attacks in hybrid threats or inter-state conflicts?

RQ2: What methods can be used to prioritise, filter and classify CTI?

RQ3: Are there ways to classify CTI or existing classifications that can be used by authorities to combat cyber threats against SOCS and surveillance technology?

Research methods

Artificial intelligence (AI) assisted literature review methodology can used to conduct "Preferred Reporting Items for Systematic Reviews and Meta-Analyses" (PRISMA) based systematic literature review [1].

Hypothetical results

Technical methods and procedures to prioritise, filter and classify CTI and mitigate cybersecurity issues.

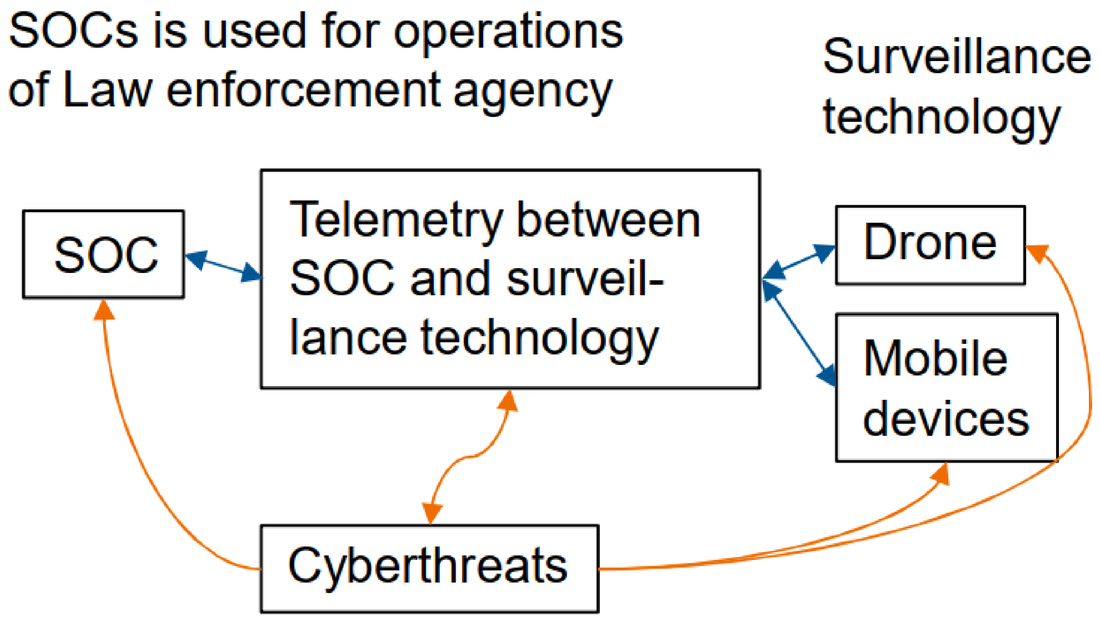

Figure 2. Attack layer against SOC and surveillance technology.

Highlights

- CTI is required to secure the SOCs and surveillance technology
- Systematic reviews are credible ways to gain knowledge of previous studies [2].
- AI assisted methodology has a potential, thus it is hypothetical currently

Acknowledgements: Business Finland for funding this research and honourable regards to Jani Suomalainen and Jarkko Kuusijärvi for comments

References

[1] Page, M.J., McKenzie, J.E., Bossuyt, P.M. *et al.* The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *Syst Rev* **10**, 89 (2021). https://doi.org/10.1136/bmj.n71

[2] Guillaume Lamé. Systematic Literature Reviews: An Introduction. International Conference on Engineering Design 2019, Aug 2019, Delft, Netherlands. pp.1633-1642, 10.1017/dsi.2019.169

Contact: Mikko Luomala, Research Scientist
Tel. +358505954771, mikko.luomala@vtt.fi