Politecnico di Torino
Dipartimento di Automatica e Informatica

PhD in Computer and Control Engineering
XXXV cycle

CYBERSECURITY NATIONAL LAB

Supervisor
Prof. Paolo Prinetto

Methodologies and tools to support Vulnerability Assessment and Cyber Risk Analysis activities within the Italian Cybersecurity Perimeter

PhD Candidate: Nicolò Maunero nicolo.maunero@polito.it

1. Introduction

In 2019 the Italian National Cybersecurity Perimeter (PSNC) was established, defining critical service for the State. Providers of these services are required to (I) create and maintain a *description of their infrastructure*, and (II) periodically perform *cyber risk assessment*.

NIST defines risk assessment as: "*the process of identifying risk to organizational operations, assets, and individuals*"[1]. Risk can be evaluated using the following formula:

$$\boldsymbol{Risk} = \boldsymbol{Likelihood} \times \boldsymbol{Impact}$$

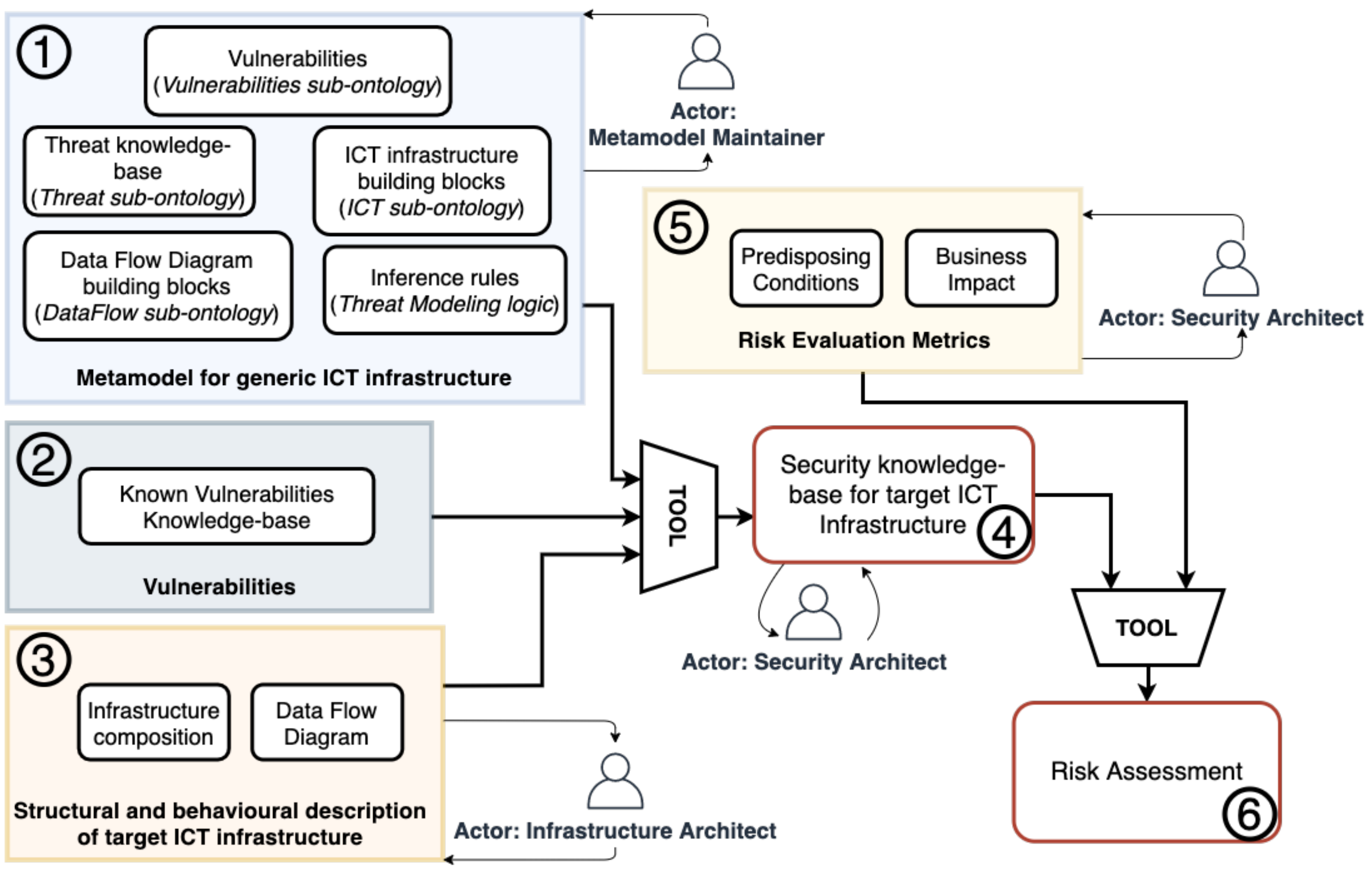
where *likelihood* expresses the possibility of an incident happening while *impact* quantifies business consequences.

2. Goal

The goal is to provide methodologies and tools to support organization in the activities defined by the PSNC legislation. The focus was to provide automation to risk assessment and cybersecurity knowledge-base management. Activities that are still mainly manual.

In particular, is provided a *formal vocabulary* for a generic ICT infrastructure description, tightly linked to *cyber threats and vulnerability*[2], in addition to well defined *inference rules* to support the automated reasoning tasks[3].

3. Methodology


①
Vulnerabilities
(Vulnerabilities sub-ontology)
Threat knowledge-base
(Threat sub-ontology)
ICT infrastructure building blocks
(ICT sub-ontology)
Data Flow Diagram building blocks
(DataFlow sub-ontology)
Inference rules
(Threat Modeling logic)
Metamodel for generic ICT infrastructure
Actor: Metamodel Maintainer
②
Known Vulnerabilities Knowledge-base
Vulnerabilities
③
Infrastructure composition
Data Flow Diagram
Structural and behavioural description of target ICT infrastructure
Actor: Infrastructure Architect
TOOL
Security knowledge-base for target ICT Infrastructure ④
Actor: Security Architect
⑤
Predisposing Conditions
Business Impact
Risk Evaluation Metrics
Actor: Security Architect
TOOL
Risk Assessment ⑥

1. An ontology defining the ***formal vocabulary*** for modeling a generic ICT infrastructure and vulnerabilities; the ***threat knowledge-base*** and ***inference rules*** necessary for threat modeling automation.
2. Known vulnerabilities databases: CVE, CWS and NVD.
3. Information and composition of the target infrastructure: list of assets, behavioral interaction and data exchanges.
4. Through ***automation*** threats are linked to assets by applying the defined inference rules. Known vulnerabilities are gathered from external databases.
5. Metrics required for cyber risk evaluation. ***Predisposing conditions*** evaluate attackers' capabilities and vulnerabilities exploitability. ***Business impact*** evaluate the consequences of a given threat
6. After providing the required information ***risk evaluation*** is automatically computed and threat identified are ranked based on severity level.

4. References

[1] Al Fikri, M., Putra, F.A., Suryanto, Y. and Ramli, K., 2019. Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency. Procedia Computer Science, 161, pp.1206-1215.
[2] De Rosa, F., Maunero, N., Prinetto, P., Talentino, F., Trussoni, M., 2022. ThreMA: Ontology-based Automated Threat Modelling for ICT Infrastructures. In: IEEE Access, pp. 1-13.
[3] De Rosa, F., Maunero, N., Nicoletti, N., Prinetto, P., Trussoni, M., 2022. Ontology for Cybersecurity Governance of ICT Systems. In: ITASEC22 – Italian Conference on Cybersecurity, June 20th-23rd, pp. 1-12.