Are Advanced Persistent Threats all that matter for a National Security Center?

An analysis of temporal and ontological alignment.

Anniek Jansen

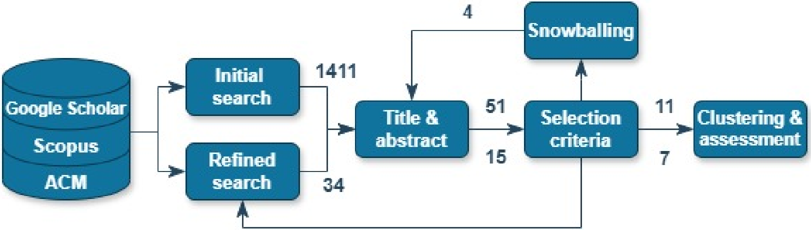
VU Amsterdam

November 6, 2024

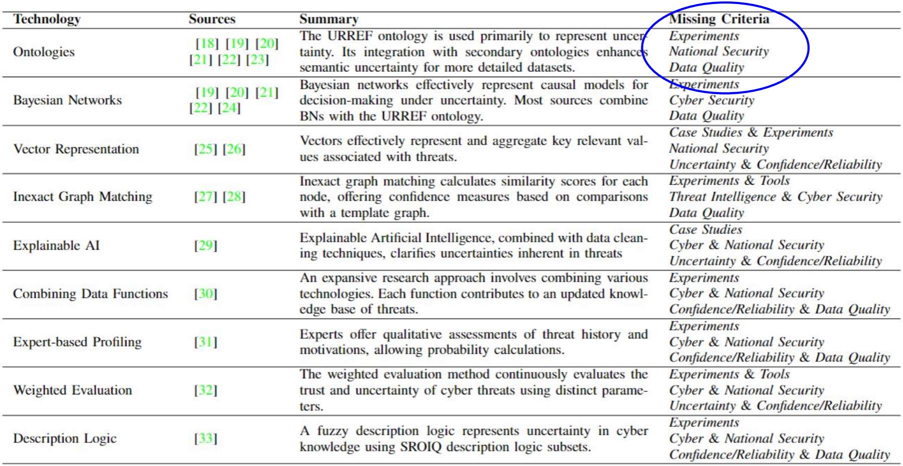
Table of Contents

1. Literature Review
2. Research Questions
3. NCSC & APT Datasets
4. RQ1: Temporal Analysis
5. RQ2: Ontological Analysis
6. Discussion
7. Conclusion

Literature Review Process



Literature Review Findings



Technology	Sources	Summary	Missing Criteria
Ontologies	[18] [19] [20] [21] [22] [23]	The URREF ontology is used primarily to represent uncertainty. Its integration with secondary ontologies enhances semantic uncertainty for more detailed datasets.	*Experiments* *National Security* *Data Quality*
Bayesian Networks	[19] [20] [21] [22] [24]	Bayesian networks effectively represent causal models for decision-making under uncertainty. Most sources combine BNs with the URREF ontology.	*Experiments* *Cyber Security* *Data Quality*
Vector Representation	[25] [26]	Vectors effectively represent and aggregate key relevant values associated with threats.	*Case Studies & Experiments* *National Security* *Uncertainty & Confidence/Reliability*
Inexact Graph Matching	[27] [28]	Inexact graph matching calculates similarity scores for each node, offering confidence measures based on comparisons with a template graph.	*Experiments & Tools* *Threat Intelligence & Cyber Security* *Data Quality*
Explainable AI	[29]	Explainable Artificial Intelligence, combined with data cleaning techniques, clarifies uncertainties inherent in threats	*Case Studies* *Cyber & National Security* *Uncertainty & Confidence/Reliability*
Combining Data Functions	[30]	An expansive research approach involves combining various technologies. Each function contributes to an updated knowledge base of threats.	*Experiments* *Cyber & National Security* *Confidence/Reliability & Data Quality*
Expert-based Profiling	[31]	Experts offer qualitative assessments of threat history and motivations, allowing probability calculations.	*Experiments* *Cyber & National Security* *Confidence/Reliability & Data Quality*
Weighted Evaluation	[32]	The weighted evaluation method continuously evaluates the trust and uncertainty of cyber threats using distinct parameters.	*Experiments & Tools* *Cyber & National Security* *Uncertainty & Confidence/Reliability*
Description Logic	[33]	A fuzzy description logic represents uncertainty in cyber knowledge using SROIQ description logic subsets.	*Experiments* *Cyber & National Security* *Confidence/Reliability & Data Quality*

Research Questions

RQ1: *How do the reserved and exploitation times of the APT align with NCSC updates, and how do the justification and likelihood classifications of vulnerabilities impact the temporal differences between the publication and exploitation of threats?*

↓

Temporal Analysis

RQ2: *How do the product, operating system, and version details of the vulnerabilities from the APT align with the data from the NCSC, and how can this alignment be evaluated using the URREF ontology to assess the consistency of threat intelligence?*

↓

Ontological Analysis

NCSC & APT Datasets

Datasets:

- National Cyber Security Centre (NCSC)
  - Dutch security advisories
- Advanced Persistent Threats (APT)
  - Prolonged and targeted cyber attacks
  - MITRE Att&ck and National Vulnerability Database (NVD)

Common Identifiers:

- `CVE-ID` = `vulnerability`
- `Uitgiftedatum` = `published_time`
- `Toepassingen` = `product`
- `Versies` = `version`
- `Platformen` = `os`

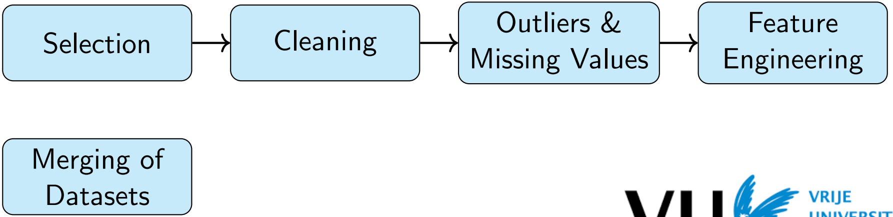
NCSC & APT Datasets

Exploratory Data Analysis:

Data Summary NCSC	
Instances	35, 684
Attributes	15
Duplicates	6, 861
Missing values	7, 639

Data Summary APT	
Instances	65, 552
Attributes	10
Duplicates	-
Missing values	1, 463

Data Pre-Processing:

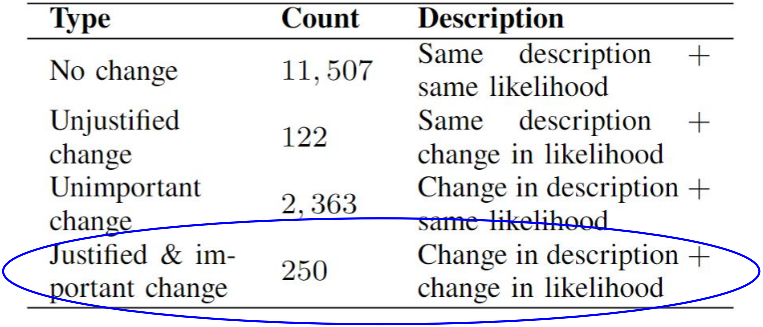


Selection → Cleaning → Outliers & Missing Values → Feature Engineering

Merging of Datasets

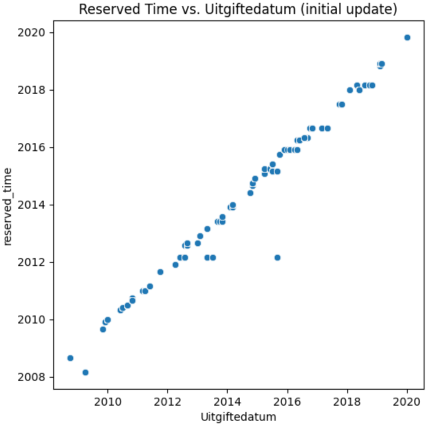
NCSC & APT Datasets

NCSC Update Justification:



Type	Count	Description
No change	11, 507	Same description + same likelihood
Unjustified change	122	Same description + change in likelihood
Unimportant change	2, 363	Change in description + same likelihood
Justified & important change	250	Change in description + change in likelihood

RQ1 - Reserved Time to Initial Release

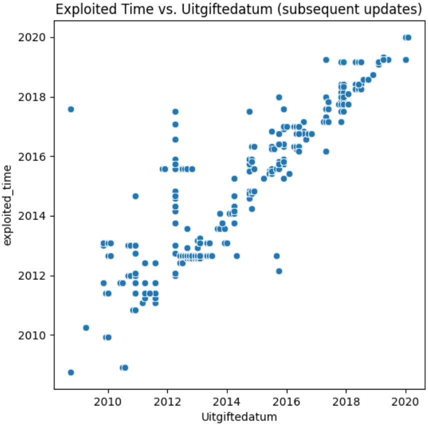


Reserved Time	
Pearson correlation	0.982***
Mean Absolute Error	1.98 months

***($p < 0.001$)

Key finding: Close alignment with an average delay of nearly two months. Defenders have difficulties keeping up with attackers.

RQ1 - Exploited Time to Subsequent Releases

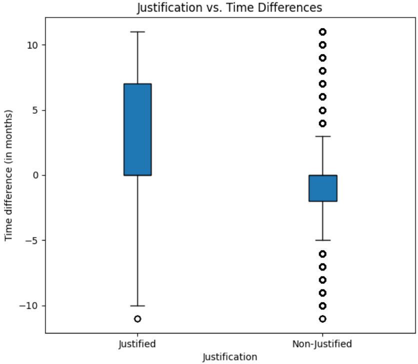


Exploited Time	
Pearson correlation	0.938***
Mean Absolute Error	2.59 months

***($p < 0.001$)

Key finding: Close alignment with more variability and increased delay. Reflects the complexity as more updates on the same threat are released.

RQ1 - Update Justification on Timing Differences

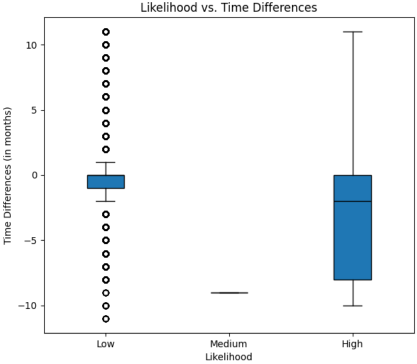


Justification	
Pearson correlation	0.067***
T-statistic	101.28***

$^{***}(p < 0.001)$

Key finding: Weak relationship. Justified updates are more consistent with fewer outliers than unjustified updates.

RQ1 - Likelihood on Timing Differences



Likelihood	
Pearson correlation	-0.438^{***}
F-statistic	247749^{***}

$^{***}(p < 0.001)$

Key finding: Moderate inverse relationship. Higher likelihood threats have smaller time gaps.

RQ2 - Vulnerability Analysis

	SPARQL Query	Total Vulnerabilities	Percentage of Total
1.1	Any product in common between NCSC and APT	86	100%
1.2	All products identical for NCSC and APT	24	27.9%
1.3	No NCSC products present in APT	45	52.3%
1.4	No APT products present in NCSC	6	7.0%
1.5	All products and any operating system in common between NCSC and APT	24	27.9%
1.6	All products and all operating systems identical for NCSC and APT	0	0%
1.7	All products and any affected version in common between NCSC and APT	24	27.9%
1.8	All products and all affected versions identical for NCSC and APT	0	0%

Key finding: All vulnerabilities share at least one affected product, but only 24 have identical products, with no common operating systems or versions.

RQ2 - Product Analysis

Top 5 most frequently shared affected products:

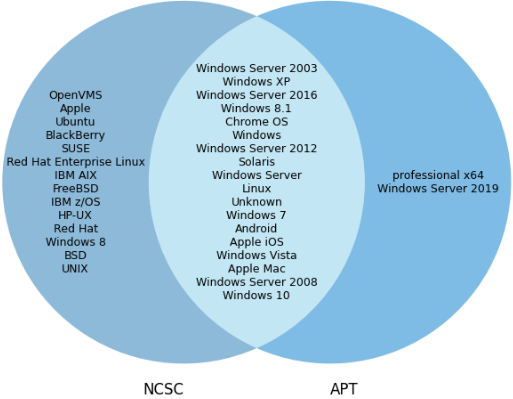
1. `Microsoft Windows` (25)
2. `Adobe Flash Player` (24)
3. `Microsoft Internet Explorer` (20)
4. `Microsoft Office` (14)
5. `Adobe AIR` (9)

Disjoint products:

- 22 of 41 products (53.6%) exclusive to NCSC
- 2 of 21 products (9.5%) exclusive to APT

Key finding: Many shared products, with NCSC covering a more extensive range of products.

RQ2 - Operating System Analysis



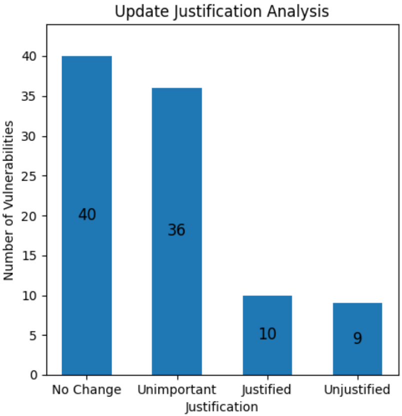
Disjoint operating systems:

- 14 of 32 operating systems (43.8%) exclusive to NCSC
- 2 of 20 operating systems (10%) exclusive to APT

Key finding: Many shared operating systems, with NCSC covering a more extensive range of systems.

RQ2 - Updates Justification Analysis

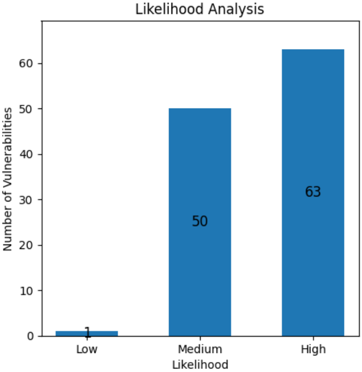
Product	Justified		Unjustified		Unimportant		No Change		Total Vulnerabilities
MS Windows	1	4%	5	20%	13	**52%**	9	36%	25
Adobe Flash Player	1	4.2%	0	0%	4	16.7%	19	**79.2%**	24
MS Internet Explorer	3	15%	1	5%	10	**50%**	6	30%	20
MS Office	2	14.3%	2	14.3%	6	42.9%	7	**50%**	14
Adobe AIR	1	11.1%	0	0%	1	11.1%	7	**77.8%**	9



Key finding: For both the vulnerabilities and products, most updates show no changes or are classified as unimportant.

RQ2 - Likelihood Analysis

Product	Low		Medium		High		Total Vulnerabilities
MS Windows	1	4%	18	**72%**	15	60%	25
Adobe Flash Player	0	0%	18	**75%**	12	50%	24
MS Internet Explorer	0	0%	10	50%	18	**90%**	20
MS Office	0	0%	10	71.4%	10	71.4%	14
Adobe AIR	0	0%	2	22.2%	9	**100%**	9



Key finding: For both the vulnerabilities and products, most are classified as medium or high likelihood.

RQ2 - Comparative Risk Analysis

Product	Justified	High Likelihood
`MS Windows`	1.69	0.54
`Adobe Flash Player`	**2.58**	2.42
`MS Internet Explorer`	1.69	1.38
`MS Office`	1.69	0.72
`Adobe AIR`	**2.58**	**3.48**

Odds Ratios Justification	
`No Change`	1.20
`Unjustified`	1.07
`Justified`	1.01
`Unimportant`	0.79

Key finding: Some products are more likely linked to vulnerabilities with justified updates and high likelihood, but none are statistically significant.

- Chi-squared p-values > 0.05: no significance.

Discussion

Key interpretations:

- Alignment of publication times
- Worrisome publication delays
- Limited novel information in updates
- Prevalence of medium and high-likelihood vulnerabilities
- Quick reporting of high-likelihood vulnerabilities
- Broader coverage in NCSC dataset
- Lack of significant product-specific risks

Threats to Validity:

- Missing likelihood data
- Manual standardization of products, operating systems and versions
- URREF ontology usage
- Small dataset of common vulnerabilities

Conclusion

Summary:

- Novel approach for representing uncertainty in threat intelligence
- Temporal and ontological analyses on alignment of NCSC and APT data

Future Work:

- Improved data integration
- NLP development for Dutch-language threat intelligence
- Predictive analytics for vulnerability assessment

Takeaway: Validation methodologies and increased collaboration can enhance the quality and effectiveness of vulnerability assessments

Q&A

Questions?