5 Technical and Experimental Challenges

In this section, technical and experimental challenges of formalizing uncertainty within a TIHW are discussed. For each of the identified challenges, ideas are proposed to handle them.

5.1 Representing uncertainty stemming from systems, humans and situations

As discussed in Section 3.4, uncertainty within threat intelligence workflows is mainly conveyed in natural language between people. Standardized natural language formats are used in certain domains. For example, within the defence domain the standard NATO Standardization Agreement (STANAG) 2511 incorporates linguistic labels to communicate source reliability and information credibility [66]. However, such uncertainty representation is typically not suited for machine-based processing. Since these uncertainties often stem from qualitative concepts, it can be challenging to translate them into representations that quantify the uncertainty for the machine-based processing and vice versa. Furthermore, the threat intelligence workflow is hybrid. Meaning that the uncertainties themselves will not only stem from abstractions and errors in systems and data but also from the process of human decision-making. In addition, to provide a basis for accountability in the larger societal context, uncertainty information should be available along the chain of communication.

Technical Challenge 5.1: Representing and tracking uncertainty for actors in TIHW is complicated due to qualitative sources of uncertainty

Uncertainty will not only arise from abstractions and errors in systems and data but also from the process of human decision-making. The uncertainty information should be available along the chain of communication. Representing uncertainty stemming from qualitative concepts is challenging.

Uncertainty can be factorized by a plethora of elements. Due to these different factors and categories, explicitness helps in reasoning about involved uncertainties throughout the process.

A possible extension of the URREF ontology [23], introduced in Section 3.3, could serve as a basis to start representing uncertainty within the threat intelligence workflow. It provides the opportunity to explore the boundaries of the (information fusion) system that one is building. It also has the expressiveness to incorporate the current NATO-STANAG 2511 standard [9]. It should be considered a checklist, forcing any information system developer to thoroughly analyse the information fusion-pipeline and make adjustments where necessary.

For uncertainty to be used not only between two agents who are in immediate connection to one another but also along the chain of communication, it is necessary that uncertainty provenance is tracked. A second proposed framework, handling provenance tracking, is the PROV data model [40]. This model can be used to structure the information in a knowledge graph (KG), making a distinction between entities (things that contain information), activities (the process that produced the information), and agents (persons/software/machines responsible for the taken actions). If applied within a TIHW, it allows for the construction of a provenance trail of information, providing insights into origin of the information.

Idea 5.1: Making uncertainty explicit by expanding and combining existing ontologies

Uncertainty can be factorized by a plethora of elements. Due to these different factors and categories, explicitness helps in reasoning about involved uncertainties throughout the fusion

process. A possible extension of the URREF ontology [23] in combination with the PROV ontology [40] could serve as a basis of representing these uncertainties.

5.2 Formal reasoning with uncertainty

When it comes to providing explanations that agree with human understanding, uncertainty representation is not enough. A specific type of formal uncertainty reasoning that can reflect abductive inference is necessary [53].

With respect to formal reasoning, two directions can be distinguished. These directions are forward and backward reasoning, see Figure 2. Backward reasoning, in the current context, is about recreating trails and possibly gathering more information to demonstrate proof of the proportionality and subsidiarity of actions for each TIHW component and for the entire TIHW. Forward reasoning, in the current context, could be used in building an actionable strategy with minimal uncertainty. The challenge at hand is that there are no such reasoning tasks that minimise the uncertainty on process level for threat intelligence and also, with respect to proportionality and other legal and societal constraints, in a domain agnostic way.

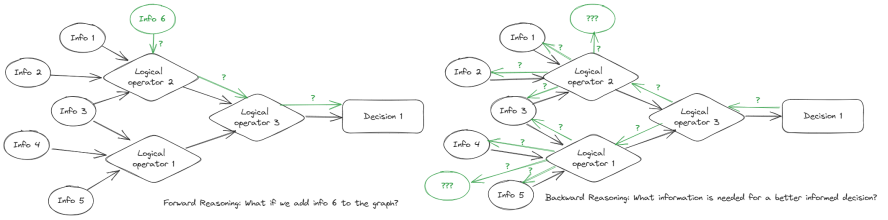

Fig. 2 Forward and Backward Reasoning. *Forward and Backward Reasoning: Forward reasoning can be thought of as a form of what-if reasoning where the reasoning starts from the information and moves forward. Backward reasoning can be thought of as an evaluation where the reasoning starts from the decision and moves backwards. The green colour represents the respective reasoning paths.*

Technical Challenge 5.2: Formalizing reasoning tasks to minimize uncertainty is challenging

How to formalise reasoning tasks that minimise the uncertainty on process level, e.g. by backward reasoning ("what-if"), or forward reasoning ("why")?

A third framework is needed. One that could unify the uncertainty overview with formalized reasoning about uncertainties. Which to choose, is not a trivial choice. This depends on the complexity of reasoning capabilities, and the richness of the uncertainty overview. The combination of uncertainty representation, provenance tracking, and reasoning/causal inference is necessary.

Past approaches in uncertainty reasoning use fuzzy logic [10], epistemic logic [5], Markov network/processes [91], probabilistic logic [41], Bayesian networks [15], and Dempster-Shafer theory [114]. However, automated reasoning over uncertainty is very complex. The choice of reasoning method is dependent on the way the uncertainty is represented (for example, in a qualitative format [107]). The combination of the URREF ontology [23] and PROV data model [40] with the intent

to reason about uncertainty, is particularly difficult. The foundations of both the URREF ontology and PROV data model are based on boolean statements; either something is true, or it is not. When dealing with uncertainties, the assigned value lies most often somewhere in the gray area in between.

Idea 5.2: Combine uncertainty representations with a provenance framework and reasoning/causal inference

To tackle provenance tracking and enable forward and backward reasoning within the workflow, the URREF ontology can be combined with the PROV framework [40] and integrated with a third framework (uncertainty reasoner), to unify the uncertainty overview with formalized reasoning about uncertainties.

5.3 Experimental methods aware of uncertainty

Designing methods to evaluate the correctness of a threat intelligence decisions regarding a course of action or event likelihood is not easy because the lack of ground truth is persistent in threat intelligence. In controlled experimentation, one possible solution is to curate the ground truth manually [94, 98] but this is not always feasible when analyzing large number of threat intelligence sources [62]. In previous work, there exists an optimal choice [56], preferences were measured [64, 47], or expert judgment was used for validation [65]. These measurements were sometimes in a qualitative format, e.g. interviews [105, 83], and in other cases they were quantitative, e.g. optimal likelihood estimations [56]. However, it is not clear how incomplete and uncertain threat intelligence information should be treated in the ground truth.

When it comes to expert judgment, the situation becomes complex. On the one hand, analysts are highly trained individuals in high-risk decision making [75]. The combination of training and experience often leads to "intuitive" decision-making. This behaviour is rarely seen in non-experts [75]. On the other hand, decisions about security risks may be affected by biased judgement [6, 49]. Uncertainty and bias are key-elements of each socio-technical system. Minimization is not the ultimate goal. However, existing experimental methods lack protocols that can effectively and systematically measure human bias in threat intelligence decision-making [96].

Technical Challenge 5.3: Existing empirical protocols for THIW validation have to be adapted to incorporate the human factor

What existing empirical protocols and measures can be adapted to quantify measures of uncertainties including human bias in TIHW?

The property of the exchanged information in the TIHW is that from an analyst's (or study participant's) point of view, the information may (or may not) be aggregated, incomplete, inaccurate, unreliable, and/or censored. And yet, a sound and convincing explanation (with at least partial traces in the model) for a minimal intervention (i.e., proportionality) must be possible. The current landscape of empirical methods does not cater for investigating such aspects of decision-support systems. Important is to measure the human effects. Qualitatively and quantitatively evaluating the entire intelligence pipeline thus calls for novel protocols, measures, and controls to be developed.

See Table 3) for an overview of methods used in recent (2018-2023) research on bias and uncertainties in cybersecurity from the perspective of the analyst/defender (for background information on the research in question, see Table 1). Internal validation of surveys, questions, and other methods were rare. External validation of these methods was most often checked with a group of

experts or participants [37], [38], [32]. These findings suggest that there is a need for more internal and external validation methods.

Validation in isolation is not insightful enough. A validation methodology has to be adapted to effectively assess heterogeneous systems with both AI, human, and unknown components.

Uncertainty/bias	Ref	Type of study	Measures
Overconfidence	[32]	Cyber game	Argumentation and self-confidence via coded transcripts of verbal discussion
Primacy bias	[37]	Vignette	Attribution via survey on confidence levels
Seizing and Freezing	[38]	Vignette	Attribution via survey on confidence levels and coded justification
False sense of validation	[109]	Vignette	Machine preference via survey on confidence levels and selecting decisions
Information-pooling bias	[84]	Synthetic task environment (i.e. less focus on realism and more on the cognitive task at hand) experiment	Team collaboration and information pooling were measured via coded transcripts of the verbal discussions

Table 3 Overview of methods used in recent (2018-2023) research on bias and uncertainties in cybersecurity from the perspective of the analyst/defender

Idea 5.3: Validating effectiveness of a human-based decision making process (such as TIHW) calls out for human-in-the-loop experimental protocols

To this aim, new experimental protocols must be specifically designed to measure human effects. For instance, similar protocols outlined in [96] could be retrofitted to the domain of threat intelligence.

5.4 Computing with objects of evaluation to measure their quality may not be possible

Since direct computation over unknown (or uncertain) values is not possible, the evaluation should take as input meta-information rather than the object of evaluation. So the key question is not whether say an AI image recognition tool works with 80% or 90% of accuracy, but rather, which representation of such uncertainty is actionable for the user. However, methodologies for threat modeling and analysis and the protocols used for their evaluation require the user to specify the sources of security relevant components and the locations where such information is not allowed to flow. Therefore, existing methodologies [45, 95, 43, 97] can not be directly carried over to evaluate the appropriateness of alternative suggestions by the TIHW, such as an alternative plan of intervention in presence of a terrorist threat by requesting input from a new source.

Technical Challenge 5.4: Measuring meta-information about objects of evaluation is necessary instead of measuring the object level

How can meta-information about objects of evaluation be measured and under what conditions are these measurements valid?

Since computation with the object of evaluation itself is not always possible, we need to make use of the meta-information that is available (e.g., timestamp, type of device, etc) to define and compute new measures of quality. As put forward in Zibak, Sauerwein, and Simpson, data quality in threat intelligence has not been properly empirically investigated [115]. To achieve this, the first step is to investigate what type of meta-information is available from the field.

Confounding factors should be balanced within these measurements. For example, a THIW relies on AI modules, which can be symbolic modules explicitly taking uncertainty into account, or sub-symbolic modules (ML-like). For the latter, several studies exist on estimating and propagating uncertainty on the output of e.g., Deep Learning models (see for instance the popular dropout method [35]) but there is no protocol to propagate the effect of hybrid errors of the next TIHW component.

Idea 5.4: Validate new measures to quantify meta-information about objects of evaluation.

Since computation with the object of evaluation itself is not always possible, we need to make use of the meta-information that is available (e.g., timestamp, type of device, etc) to define and compute new measures of quality. To achieve this the first step is to investigate what type of meta-information is available from the field.

6 The bigger picture

In this chapter, we discussed the interplay between complex conditions and trade-offs between security and legal, societal, and organizational restrictions that make decision-making under uncertainty a challenging endeavour. Table 4 shows an overview of the illustrated challenges.

In the quest to achieve efficiency and effectiveness in threat intelligence, security and intelligence agencies are implementing AI powered solutions to find actionable information to aid them in decision-making during uncertainty. However, one must remember that these AI tools to help deal with uncertainty in threat intelligence can end up being a double-edged sword. The development of a threat intelligence hybrid workflow (TIHW) is not an exception. Uncertainty will likely arise due to communication errors, ambiguity, and unknown credibility of the sources/provenance.

Challenges arise when creating a robust system that advances the embedding of regard for citizens' fundamental rights and responding to efficiency and support of user autonomy to enable intelligence agencies to arrive at the best possible decisions. Achieving this fine point is essential in a democratic society because it develops societal trust in security and intelligence operations.

Despite developing a system that meets the requirements mentioned in this paper, we also need a path forward in security and intelligence operations to transfer this knowledge within their agencies or organizations. We recommend applying a lens based on international standardized legal principles, such as proportionality and necessity, during human-AI interactions or evaluations in the absence of ground truth. Thus, the relationship between developing an AI system and having regard for societal and legal matters are not far from each other.

Uncertainty in a TIHW stems from quantitative as well as qualitative sources. This makes the formalization of uncertainty hard. In addition, uncertainty representation has to be machine-readable, as well as human understandable. Therefore, uncertainty representation should enable reasoning according to abductive inference. Representation and reasoning methods for uncertainty that capture these conditions, have not been constructed with respect to threat intelligence.

AI augmented socio-technical systems for threat intelligence must respond to relevance, timeliness, accuracy, completeness, and ingestibility. A TIHW evaluation will require investigating the persuasiveness (e.g., to the oversight body), efficiency (helps analysts make decisions faster) and debugging (helps analysts identify when something is wrong and explore 'what-if' scenarios) of the explanations, for which appropriate measures are to this day less explored.

Category	Section	Challenge	Idea
Socio-technical	4.1	It is unclear what and how legal and societal constraints can be implemented in a TIHW	Develop a framework based on international best practices and relevant laws and regulations
	4.2	Technology changes rapidly and constraints can not be satisfied at the same time	Incoming international legal frameworks and existing societal challenges should be addressed in a TIHW
	4.3	Analyzing/improving information sharing in a restricted environment is difficult	Integrating the operational, tactical and strategic levels of organizational change with a clear distinction of processes between organizations and those within organizations
Technical	5.1	Representing and tracking uncertainty for actors in TIHW is complicated due to qualitative sources of uncertainty	Making uncertainty explicit by expanding and combining existing ontologies
	5.2	Formalizing reasoning tasks to minimize uncertainty is challenging	Combine uncertainty representations with a provenance framework and reasoning/causal inference
Experimental	5.3	Existing empirical protocols for THIW validation have to be adapted to incorporate the human factor	Validating effectiveness of a human-based decision making process (such as TIHW) calls out for human-in-the-loop experimental protocols
	5.4	Measuring meta-information about objects of evaluation is necessary instead of measuring the object level	Validate new measures to quantify meta-information about objects of evaluation

Table 4 Overview of socio-technical, technical, and experimental challenges discussed in this chapter

The validation methodology for a TIHW has to holistically incorporate AI, human, and unknown components. In addition, confound-aware methods that measure the meta-level instead of the object-level of a TIHW are necessary. Validation methodologies within threat intelligence that satisfy these requirements have not been thoroughly investigated.

We hope to stimulate discussion and further research in the community by illustrating these challenges and possible ways to answer them.

References

[1] Albu OB, Flyverbom M (2019) Organizational transparency: Conceptualizations, conditions, and consequences. Business & Society 58(2):268—-297, URL https://doi.org/10.1177/0007650316659851

[2] Alexander P (2022) Exploring bias and accountability in military artificial intelligence. 7 LSE Law Review pp 396–405

[3] Ananny M, Crawford K (2018) Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. New Media & Society 20(3):973–989, DOI 10.1177/1461444816676645
[4] Argote L, Miron-Spektor E (2011) Organizational learning: From experience to knowledge. Organization Science 22(5):1123–1137, DOI 10.1287/orsc.1100.0621
[5] Banerjee M, Dubois D (2014) A simple logic for reasoning about incomplete knowledge. International Journal of Approximate Reasoning 55(2):639–653, DOI https://doi.org/10.1016/j.ijar.2013.11.003, URL https://www.sciencedirect.com/science/article/pii/S0888613X13002478
[6] Bier V (2020) The role of decision analysis in risk analysis: A retrospective. Risk Analysis 40(S1):2207–2217
[7] Bisantz AM, Cao D, Jenkins M, Pennathur PR, Farry M, Roth E, Potter SS, Pfautz J (2011) Comparing uncertainty visualizations for a dynamic decision-making task. Journal of Cognitive Engineering and Decision Making 5(3):277–293, DOI 10.1177/1555343411415793
[8] Blagden D (2018) The flawed promise of national security risk assessment: nine lessons from the british approach. Intelligence and national security 33:716–736
[9] Blasch E, Laskey K, Jousselme A, Dragos V, Costa P, Dezert J (2013) URREF reliability versus credibility in information fusion (stanag 2511). Proceedings of the 16th International Conference on Information Fusion, FUSION 2013
[10] Bobillo F, Straccia U (2008) fuzzydl: An expressive fuzzy description logic reasoner. In: 2008 IEEE International Conference on Fuzzy Systems (IEEE World Congress on Computational Intelligence), pp 923–930, DOI 10.1109/FUZZY.2008.4630480
[11] Bohanec M (2003) Decision support. In: Mladenić D, Lavrač N, Bohanec M, Moyle S (eds) Data Mining and Decision Support, vol 745, The Springer International Series in Engineering and Computer Science. Springer, https://doi.org/10.1007/978-1-4615-0286-9_3
[12] Bouwman X, Griffioen H, Egbers J, Doerr C, Klievink B, van Eeten M (2020) A different cup of TI? the added value of commercial threat intelligence. In: 29th USENIX Security Symposium (USENIX Security 20), pp 433–450
[13] Brown I, Korff D (2009) Terrorism and the proportionality of internet surveillance. European Journal of Criminology 6:119–134
[14] Carlsen L (2012) Mexico's false dilemma: Human rights or security. Nw J Hum Rts 10(3):145–135
[15] Carvalho RN, Laskey KB, Costa PCG (2017) PR-OWL – a language for defining probabilistic ontologies. International Journal of Approximate Reasoning 91:56–79, DOI https://doi.org/10.1016/j.ijar.2017.08.011, URL https://www.sciencedirect.com/science/article/pii/S0888613X17301044
[16] Catano V, Gauger J (2016) Information fusion: Intelligence centers and intelligence analysis. In: Goldenberg I, Soeters J, Dean WH (eds) Information Sharing in Military Operations, Springer International Publishing, pp 17–34, DOI 10.1007/978-3-319-42819-2_2
[17] Claver A, van de Meeberg HM (2021) Devil's advocacy within dutch military intelligence (2008-2020): an effective instrument for quality assurance? Intelligence and National Security 36(6):849–862, DOI 10.1080/02684527.2021.1946951
[18] Collins RN, Mandel DR (2019) Cultivating credibility with probability words and numbers. Judgment and Decision Making 14(6):683–695, DOI 10.1017/S1930297500005404
[19] Commission E (2021) Regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. COM(2021), 206 final, 2021/0106 (COD)
[20] Committee CTIT (2023) Introduction to stix. https://oasis-open.github.io/cti-documentation/stix/intro.html, accessed: 15-06-2023
[21] Constantino J (2022) Exploring article 14 of the eu ai proposal: Human in the loop challenges when overseeing high-risk ai systems in public service organisations. Amsterdam Law Forum 14(3):17
[22] Corporation TM (2023) Mitre att&ck. https://attack.mitre.org/, accessed: 15-06-2023

[23] Costa P, Jousselme AL, Laskey KB, Blasch E, Dragos V, Ziegler J, de Villiers P, Pavlin G (2018) Urref: Uncertainty representation and reasoning evaluation framework for information fusion. Journal of Advances in Information Fusion 13(2):137–157
[24] Court THD (2020) Njcm et al. v. the dutch state (2020). https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBDHA:2020:865, eCLI: NL: RBDHA: 2020:865 (NL) and ECLI:NL:RBDHA:2020:1878 (EN) (SyRI): [6.5]
[25] Dagar D, Vishwakarma DK (2022) A literature review and perspectives in deepfakes: generation, detection, and application. Int J Multimed Info Retr 11:219–289, URL https://doi-org.vu-nl.idm.oclc.org/10.1007/s13735-022-00241-w
[26] Dalvi A, Siddavatam I, Patel A, Panchal A, Kazi F, Bhirud S (2021) Predicting attribute effectiveness using biased databases. 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON) pp 1–8, DOI 10.1109/SMARTGENCON51891.2021.9645789
[27] Dhami MK, Mandel DR (2021) Words or numbers? communicating probability in intelligence analysis. American Psychologist 76(3):549–560, https://doi.org/10.1037/amp0000637
[28] Dias LC, Morton A, Quigley J (2018) Elicitation. The Science and Art of Structuring Judgement, International Series in Operations Research & Management Science, vol 261. Springer
[29] Durbach IN, Stewart TJ (2011) An experimental study of the effect of uncertainty representation on decision making. European Journal of Operational Research 214:380–392, https://doi.org/10.1016/j.ejor.2011.04.021
[30] of Europe C (1981) The convention for the protection of individuals with regard to automatic processing of personal data (cets no. 108). https://www.coe.int/en/web/data-protection/convention108-and-protocol, accessed: 18-06-2023
[31] Fischhoff B, Davis AL (2014) Communicating scientific uncertainty. Proceedings of the National Academy of Sciences 111(supplement_4):13664–13671, DOI 10.1073/pnas.1317504111, URL https://www.pnas.org/doi/abs/10.1073/pnas.1317504111, https://www.pnas.org/doi/pdf/10.1073/pnas.1317504111
[32] Frey S, Rashid A, Anthonysamy P, Pinto-Albuquerque M, Naqvi SA (2019) The good, the bad and the ugly: A study of security decisions in a cyber-physical systems game. IEEE Transactions on Software Engineering 45(5):521–536, DOI 10.1109/TSE.2017.2782813
[33] Friedman JA, Zeckhauser R (2012) Uncertainty in intelligence. Intelligence and National Security 27(6):824–847, DOI 10.1080/02684527.2012.708275
[34] Friedman JA, Lerner JS, Zeckhauser R (2017) Behavioral consequences of probabilistic precision: Experimental evidence from national security professionals. International Organization 71(4):803–826, DOI 10.1017/S0020818317000352
[35] Gal Y, Ghahramani Z (2016) Dropout as a bayesian approximation: Representing model uncertainty in deep learning. In: Proceedings of the 33rd International Conference on International Conference on Machine Learning - Volume 48, JMLR.org, ICML'16, p 1050–1059
[36] Garae J, Ko R (2017) Visualization and data provenance trends in decision support for cybersecurity. In: Carrascosa IP, Kalutarage H, Huang Y (eds) Data Analytics and Decision Support for Cybersecurity, Springer, https://doi.org/10.1007/978-3-319-59439-2_9
[37] Gomez M (2019) Sound the alarm! updating beliefs and degradative cyber operations. European Journal of International Security 4(2):190–208, DOI 10.1017/eis.2019.2
[38] Gomez MA (2019) Past behavior and future judgements: seizing and freezing in response to cyber operations. Journal of Cybersecurity 5, DOI 10.1093/cybsec/tyz012
[39] Gonin M, Palazzo G, Hoffrage U (2012) Neither bad apple nor bad barrel: how the societal context impacts unethical behavior in organizations. Business Ethics: A European Review 21(1):31–46, DOI https://doi.org/10.1111/j.1467-8608.2011.01643.x
[40] Groth P, Moreau L (2013) An overview of the prov family of documents. W3C Working Group Note Http://www.w3.org/TR/2013/NOTE-prov-overview-20130430/
[41] Henderson TC, Simmons R, Sacharny D, Mitiche A, Fan X (2017) A probabilistic logic for multi-source heterogeneous information fusion. 2017 IEEE International Conference on

Multisensor Fusion and Integration for Intelligent Systems (MFI), Daegu, Korea (South) pp 530–535, DOI 10.1109/MFI.2017.8170375

[42] Holzinger A, Saranti A, Molnar C, Biecek P, Samek W (2022) Explainable ai methods – a brief overview. In: Holzinger A, Goebel R, Fong R, Moon T, Müller KR, Samek W (eds) xxAI - Beyond Explainable AI. xxAI 2020. Lecture Notes in Computer Science, vol 13200, Springer, Cham, https://doi.org/10.1007/978-3-031-04083-2_2

[43] Hong JB, Kim DS, C J Chung CJ, Huang D (2017) A survey on the usability and practical applications of graphical security models. Computer Science Review 26:1–16

[44] Hüllermeier E, Waegeman W (2021) Aleatoric and epistemic uncertainty in machine learning: an introduction to concepts and methods. Machine Learning 110:457–506

[45] III HE, Gadyatskaya O (2020) Graphical models for security. 7th International Workshop, GraMSec 2020

[46] Irwin D, Mandel DR (2019) Improving information evaluation for intelligence production. Intelligence and National Security 34(4):503–525, DOI 10.1080/02684527.2019.1569343

[47] Irwin D, Mandel DR (2022) Communicating uncertainty in national security intelligence: Expert and nonexpert interpretations of and preferences for verbal and numeric formats. Risk Analysis URL https://doi.org/10.1111/risa.14009

[48] Janssen M, der Hoven JV (2015) Big and open linked data (bold) in government: A challenge to transparency and privacy? Government Information Quarterly 32:363–368

[49] Jaspersen JG, Montibeller G (2015) Probability elicitation under severe time pressure: A rank-based method. Risk Analysis 35(7):1317–1335

[50] Jensen MA (2012) Intelligence failures: What are they really and what do we do about them? Intelligence and National Security 27(2):261–282, DOI 10.1080/02684527.2012.661646

[51] Johnson CK, Gutzwiller RS, Ferguson-Walter KJ, Fugate SJ (2020) A cyber-relevant table of decision making biases and their definitions. Technical Report DOI 10.13140/RG.2.2.14891.87846

[52] Johnson SGB, Merchant T, Keil FC (2020) Belief digitization: Do we treat uncertainty as probabilities or as bits? Journal of Experimental Psychology: General 149:1417–1434, DOI 10.1037/xge0000720

[53] K M, A-V P (2022) On explainable ai and abductive inference. Philosophies 7(2):35, https://doi.org/10.3390/philosophies7020035

[54] Kahneman D, Klein G (2009) Conditions for intuitive expertise: A failure to disagree. American Psychologist 64(6):515–526, https://doi.org/10.1037/a0016755

[55] Kahneman D, Slovic P, Tversky A (eds) (1982) Judgment under Uncertainty: Heuristics and Biases. Cambridge: Cambridge University Press, DOI 10.1017/CBO9780511809477

[56] Karvetski CW, Mandel DR, Irwin D (2020) Improving probability judgment in intelligence analysis: From structured analysis to statistical aggregation. Risk Analysis 40(5):1040–1057, https://doi.org/10.1111/risa.13443

[57] Keith AJ, Ahner DK (2021) A survey of decision making and optimization under uncertainty. Annals of Operations Research 300:319–353, URL https://doi.org/10.1007/s10479-019-03431-8

[58] Korff D, Wagner B, Powles JE, Avila R, Buermeyer U (2017) Boundaries of law: Exploring transparency, accountability, and oversight of government surveillance regimes. Cybersecurity

[59] Kowalski M (2017) Ethics of counterterrorism. Boom uitgevers Amsterdam

[60] Labunets K, Massacci F, Paci F (2017) On the equivalence between graphical and tabular representations for security risk assessment. Proc of REFSQ'2016 p 191–208

[61] Laskey KJ, Laskey KB, Costa PCG, Kokar MM, Martin T, Lukasiewicz T (2008) Uncertainty reasoning for the world wide web. W3C Incubator Group Report Https://www.w3.org/2005/Incubator/urw3/XGR-urw3-20080331/

[62] Li VG, Dunn M, Pearce P, McCoy D, Voelker GM, Savage S (2019) Reading the tea leaves: A comparative analysis of threat intelligence. In: 28th USENIX Security Symposium (USENIX Security 19), USENIX Association, Santa Clara, CA, pp 851–867, URL https://www.usenix.org/conference/usenixsecurity19/presentation/li

[63] Li Y, Chen J, Feng L (2012) Dealing with uncertainty: A survey of theories and practices. IEEE Transactions on Knowledge and Data Engineering 25(11):2463–2482
[64] Logg JM, Minson JA, Moore DA (2019) Algorithm appreciation: People prefer algorithmic to human judgment. Organizational Behavior and Human Decision Processes 151:90–103, URL https://doi.org/10.1016/j.obhdp.2018.12.005
[65] Maathuis C, Pieters W, van den Berg J (2021) Decision support model for effects estimation and proportionality assessment for targeting in cyber operations. Defence Technology 17(2):352–374, URL https://doi.org/10.1016/j.dt.2020.04.007
[66] Mandel DR (2020) Assessment and communication of uncertainty in intelligence to support decision-making. NATO STO TECHNICAL REPORT, TR-SAS-114
[67] Mandel DR, Irwin D (2021) Facilitating sender-receiver agreement in communicated probabilities: Is it best to use words, numbers or both? Judgment and Decision Making 16(2):363–393, DOI 10.1017/S1930297500008603
[68] Marlin BM, Abdelzaher† T, Ciocarlie G, Cobb AD, Dennison M, Jalaian B, Kaplan L, Raber T, Raglin A, Sharma PK, Srivastava M, Trout T, Vadera MP, Wigness M (2020) On uncertainty and robustness in large-scale intelligent data fusion systems. IEEE Second International Conference on Cognitive Machine Intelligence (CogMI) pp 82–91, DOI 10.1109/CogMI50398.2020.00020
[69] Maymí FJ, Thomson R (2018) Human-machine teaming and cyberspace. In: Schmorrow D, Fidopiastis C (eds) Augmented Cognition: Intelligent Technologies, vol 10915, Springer, https://doi.org/10.1007/978-3-319-91470-1_25
[70] Menkveld C (2020) Understanding the complexity of intelligence problems. INTELLIGENCE AND NATIONAL SECURITY 36(5):621–641, URL https://doi.org/10.1080/02684527.2021.1881865
[71] Montibeller G, von Winterfeldt D (2018) Individual and group biases in value and uncertainty judgments. In: Dias LC, Morton A, Quigley J (eds) Elicitation: The Science and Art of Structuring Judgement, vol 261, Springer, Cham, pp 377–392
[72] Nauta M, Trienes J, Pathak S, Nguyen E, Peters M, Schmitt Y, Schlötterer J, van Keulen M, Seifert C (2023) From anecdotal evidence to quantitative evaluation methods: A systematic review on evaluating explainable ai. ACM Comput Surv DOI 10.1145/3583558, URL https://doi.org/10.1145/3583558
[73] Nisioti A, Loukas G, Laszka A, Panaousis E (2021) Data-driven decision support for optimizing cyber forensic investigations. IEEE Transactions on Information Forensics and Security 16:2397–2412, DOI 10.1109/TIFS.2021.3054966
[74] Nunes I, Jannach D (2017) A systematic review and taxonomy of explanations in decision support and recommender systems. User Modeling and User-Adapted Interaction 27(3):393–444
[75] Okoli JO, Weller G, Watt J (2016) Information processing and intuitive decision-making on the fireground: towards a model of expert intuition. Cogn Tech Work 18:89–103, URL https://doi.org/10.1007/s10111-015-0348-9
[76] OTAN N (2020) Automation in the intelligence cycle. https://www.sto.nato.int/Lists/STONewsArchive/displaynewsitem.aspx?ID=552 [Accessed: (11 April 2023)]
[77] Padilla L, Kay M, Hullman J (2022) Uncertainty visualization. In: Piegorsch W, Levine R, Zhang H, Lee T (eds) Computational Statistics in Data Science, Wiley, pp 405–421
[78] Pagano TP, Loureiro RB, Lisboa FVN, Cruz GOR, Peixoto RM, de Sousa Guimarães GA, dos Santos LL, Araujo MM, Cruz M, de Oliveira ELS, Winkler I, Nascimento EGS (2022) Bias and unfairness in machine learning models: a systematic literature review. 2202.08176
[79] Pagano TP, Loureiro RB, Lisboa FVN, Cruz GOR, Peixoto RM, de Sousa Guimarães GA, dos Santos LL, Araujo MM, Cruz M, de Oliveira ELS, Winkler I, Nascimento EGS (2022) Bias and unfairness in machine learning models: A systematic literature review. arXiv:220208176 Https://doi.org/10.48550/arXiv.2202.08176

[80] Pawlinski P, Jaroszewski P, Kijewski P, Siewierski L, Jacewicz P, Zielony P, Zuber R (2014) Actionable information for security incident response. European Union Agency for Network and Information Security

[81] Perry WL, McInnis B, Price CC, Smith SC, Hollywoon JS (2013) Predictive policing: The role of crime forecasting in law enforcement operations. Rand Corporation

[82] Petersen KL, Tjalve VS (2018) Intelligence expertise in the age of information sharing: public–private 'collection' and its challenges to democratic control and accountability. Intelligence and National Security 33(1):21–35, DOI 10.1080/02684527.2017.1316956

[83] Prabhudesai S, Yang L, Asthana S, Huan X, Liao QV, Banovic N (2023) Understanding uncertainty: How lay decision-makers perceive and interpret uncertainty in human-ai decision making. In: Proceedings of the 28th International Conference on Intelligent User Interfaces, Association for Computing Machinery, New York, NY, USA, p 379–396, DOI 10.1145/3581641.3584033

[84] Rajivan P, Cooke NJ (2018) Information-pooling bias in collaborative security incident correlation analysis. Human Factors 60:626–639, https://doi.org/10.1177/0018720818769249

[85] Ranade P, Piplai A, Mittal S, Joshi A, Finin T (2021) Generating fake cyber threat intelligence using transformer-based models. In: 2021 International Joint Conference on Neural Networks (IJCNN), pp 1–9, DOI 10.1109/IJCNN52387.2021.9534192

[86] Reagans R, Argote L, Brooks D (2005) Individual experience and experience working together: Predicting learning rates from knowing who knows what and knowing how to work together. Management Science 51(6):869–881, DOI 10.1287/mnsc.1050.0366

[87] Regan HM, Colyvan M, Burgman MA (2002) A taxonomy and treatment of uncertainty for ecology and conservation biology. Ecological Applications 12(2):618–628, DOI https://doi.org/10.1890/1051-0761(2002)012[0618:ATATOU]2.0.CO;2

[88] Rona-Tas A, Cornuéjols A, Blanchemanche S, Duroy A, Martin C (2019) Enlisting supervised machine learning in mapping scientific uncertainty expressed in food risk analysis. Sociological Methods & Research 48(3):608–641

[89] Russell S, Norvig P (2020) Artificial intelligence: A modern approach. Saddle River. NJ: Pearson

[90] Slayton R (2017) What is the cyber offense-defense balance? conceptions, causes, and assessment. International Security 41(3):72–109, DOI 10.1162/ISEC_a_00267

[91] Snidaro L, Visentini I, Bryan K (2015) Fusing uncertain knowledge and evidence for maritime situational awareness via markov logic networks. Information Fusion 21:159–172, DOI https://doi.org/10.1016/j.inffus.2013.03.004, URL https://www.sciencedirect.com/science/article/pii/S1566253513000523

[92] Stevens R, Votipka D, Redmiles EM, C Ahern PS, , Mazurek ML (2018) The battle for new york: a case study of applied digital threat modeling at the enterprise level. 27th USENIX Security Symposium p 621–63

[93] Tounsi W, Rais H (2018) A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & Security 72:212–233, https://doi.org/10.1016/j.cose.2017.09.001

[94] Tuma K, Scandariato R (2018) Two architectural threat analysis techniques compared. In: Software Architecture: 12th European Conference on Software Architecture, ECSA 2018, Madrid, Spain, September 24–28, 2018, Proceedings 12, Springer, pp 347–363

[95] Tuma K, Scandariato R (2018) Two architectural threat analysis techniques compared. European Conference on Software Architecture p 347–363

[96] Tuma K, Van Der Lee R (2022) The role of diversity in cybersecurity risk analysis: An experimental plan. In: 3rd Workshop on Gender Equality, Diversity, and Inclusion in Software Engineering, GEICSE 2022, Institute of Electrical and Electronics Engineers Inc., pp 12–18

[97] Tuma K, Calikli G, Scandariato R (2018) Threat analysis of software systems: A systematic literature review. Journal of Systems and Software 144:275–294

[98] Tuma K, Sion L, Scandariato R, Yskout K (2020) Automating the early detection of security design flaws. In: Proceedings of the 23rd ACM/IEEE International Conference on Model Driven Engineering Languages and Systems, pp 332–342

[99] Tuma K, Sandberg C, Thorsson U, Widman M, Herpel T, Scandariato R (2021) Finding security threats that matter: Two industrial case studies. Journal of Systems and Software
[100] van der Kleij R, Schraagen JM, Cadet B, Young H (2022) Developing decision support for cybersecurity threat and incident managers. Computers & Security 113:102535, DOI https://doi.org/10.1016/j.cose.2021.102535
[101] van der Voort H, Klievink A, Arnaboldi M, Meijer A (2019) Rationality and politics of algorithms. will the promise of big data survive the dynamics of public decision making? Government Information Quarterly 36(1):27–38, DOI https://doi.org/10.1016/j.giq.2018.10.011
[102] Villiers JPD, Laskey JP, Jousselme A, Blasch E, de Waal A, Pavlin G, Costa P (2015) Uncertainty representation, quantification and evaluation for data and information fusion. In 2015 18th International Conference on Information Fusion IEEE pp 50–57
[103] Villiers JPD, Pavlin G, Jousselme A, Maskell S, de Waal A, Laskey K, Costa P, Blasch E (2018) Uncertainty representation and evaluation for modeling and decision-making in information fusion. Journal for Advances in Information Fusion 13:198–215
[104] Vogel KM, Reid G, Kampe C, Jones P (2021) The impact of ai on intelligence analysis: tackling issues of collaboration, algorithmic transparency, accountability, and management. Intelligence and National Security 36(6):827–848, DOI 10.1080/02684527.2021.1946952
[105] Waardenburg L, Sergeeva A, Huysman M (2018) Hotspots and blind spots. In: Schultze U, Aanestad M, Mähring M, Østerlund C, Riemer K (eds) Living with Monsters? Social Implications of Algorithmic Phenomena, Hybrid Agency, and the Performativity of Technology, Springer International Publishing, pp 96–109
[106] Wagner TD, Mahbub K, Palomar E, Abdallah AE (2019) Cyber threat intelligence sharing: Survey and research directions. Computers & Security 87, https://doi.org/10.1016/j.cose.2019.101589
[107] Wei L, Du H, ain Mahesar Q, Al Ammari K, Magee DR, Clarke B, Dimitrova V, Gunn D, Entwisle D, Reeves H, Cohn AG (2020) A decision support system for urban infrastructure inter-asset management employing domain ontologies and qualitative uncertainty-based reasoning. Expert Systems with Applications 158:113461, https://doi.org/10.1016/j.eswa.2020.113461
[108] Whitesmith M (2019) The efficacy of ach in mitigating serial position effects and confirmation bias in an intelligence analysis scenario. Intelligence and National Security 34(2):225–242, URL https://doi.org/10.1080/02684527.2018.1534640
[109] Whyte C (2023) Learning to trust skynet: Interfacing with artificial intelligence in cyberspace. Contemporary Security Policy 44(2):308–344, DOI 10.1080/13523260.2023.2180882
[110] Willingham DT, Riener C (2019) Cognition : The Thinking Animal. Fourth ed. Cambridge: Cambridge University Press, URL https://doi.org/10.1017/9781316271988
[111] Wirtz JJ (2010) The sources and methods of intelligence studies. In: Johnson LK (ed) The Oxford Handbook of National Security Intelligence, Oxford University Press, URL https://doi.org/10.1093/oxfordhb/9780195375886.003.0004
[112] Wu J, Li H (2006) Uncertainty analysis in ecological studies: An overview. In: Wu J, Jones KB, Li H, Loucks OL (eds) Scaling and Uncertainty Analysis in Ecology, Springer Netherlands, Dordrecht, pp 45–66, DOI 10.1007/1-4020-4663-4_3, URL https://doi.org/10.1007/1-4020-4663-4_3
[113] Xiong W, Lagerström R (2019) Threat modeling – a systematic literature review. Computers & Security 84:53–69, URL https://doi.org/10.1016/j.cose.2019.03.010
[114] Zhao K, Li L, Chen Z, Sun R, Yuan G, Li J (2022) A survey: Optimization and applications of evidence fusion algorithm based on dempster–shafer theory. Applied Soft Computing 124:109075, URL https://www.sciencedirect.com/science/article/pii/S1568494622003696, https://doi.org/10.1016/j.asoc.2022.109075
[115] Zibak A, Sauerwein C, Simpson AC (2022) Threat intelligence quality dimensions for research and practice. Digital Threats: Research and Practice 3(4):44, https://doi.org/10.1145/3484202