The Name of the Title is Hope

BEN TROVATO* and G.K.M. TOBIN*, Institute for Clarity in Documentation
LARS THØRVÄLD, The Thørväld Group, Iceland

A clear and well-documented LaTeX document is presented as an article formatted for publication by ACM in a conference proceedings or journal publication. Based on the "acmart" document class, this article presents and explains many of the common variations, as well as many of the formatting elements an author may use in the preparation of the documentation of their work.

CCS Concepts: • **Computer systems organization** → **Embedded systems**; *Redundancy*; Robotics; • **Networks** → Network reliability.

Additional Key Words and Phrases: datasets, neural networks, gaze detection, text tagging

ACM Reference Format:
Ben Trovato, G.K.M. Tobin, and Lars Thørväld. 2018. The Name of the Title is Hope. *J. ACM* 37, 4, Article 111 (August 2018), 3 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

ACM's consolidated article template, introduced in 2017, provides a consistent LaTeX style for use across ACM publications, and incorporates accessibility and metadata-extraction functionality necessary for future Digital Library endeavors. Numerous ACM and SIG-specific LaTeX templates have been examined, and their unique features incorporated into this single new template.

If you are new to publishing with ACM, this document is a valuable guide to the process of preparing your work for publication. If you have published with ACM before, this document provides insight and instruction into more recent changes to the article template.

The "`acmart`" document class can be used to prepare articles for any ACM publication — conference or journal, and for any stage of publication, from review to final "camera-ready" copy, to the author's own version, with *very* few changes to the source.

[1]

2 REVIEW PROCEDURE

This section describes the inclusion criterions for the review, the method used to identify the relevant literature, the elements extracted from the literature and process of extracting this information.

*Both authors contributed equally to this research.

Authors' addresses: Ben Trovato, trovato@corporation.com; G.K.M. Tobin, webmaster@marysville-ohio.com, Institute for Clarity in Documentation, P.O. Box 1212, Dublin, Ohio, 43017-6221; Lars Thørväld, The Thørväld Group, 1 Thørväld Circle, Hekla, Iceland, larst@affiliation.org.

0004-5411/2018/8-ART111 $15.00
https://doi.org/10.1145/1122445.1122456

2.1 Research questions

2.2 Inclusion Criterion

As noted above, the issue predicting adversarial cyber operations involves both straightforward cases were a known threat is to be recognized and more or less impossible cases where previously unknown attacks performed by professionals should be predicted. The panel and the literature search aimed at focusing on research in-between these two extremes. It was also recognized that much of the extant research on cyber security have some relation to prediction. For example, when the relationship between cyber variables are investigated in terms of statistical relationships this offers potential input to prediction models. However, as this review is mostly concerned with existing prediction models, and not surveying potential building blocks of new ones, such research was excluded. Thus, the primary inclusion criteria was that the papers should describe a model explicitly developed for predicting adversarial cyber operations. In addition, the predictions produced by the model should be able to support a decision maker within an organization to secure their cyber environment. This meant that papers listing attacks that were possible to perform against the cyber environment were excluded they did not make statements about the likelihood that the attacks would be performed within a certain time frame. For instance, most papers on attack graphs, which rarely state how likely attacks are to happen, were excluded. Similarly, papers on models producing generic predictions, such as "more attacks of type X will happen next year", were excluded unless it was possible to tune the predictions based on information related to a specific organization or cyber environment. Finally, some papers were excluded because they were too abstract and superficial. For example, papers stating basic ideas about how threat intelligence could foster prediction, without detailing what this threat intelligence comprise of, were excluded.

2.3 Literature Search

Some initial attempt with the definition of search terms that could be used to target literature related to predicting adversarial cyber operations. However, it was soon acknowledged that this literature was too diverse and scattered to be identified by a straightforward search in literature databases. Fortunately, the panel members participating in the review process was diverse set of researchers, with backgrounds in cyber security, mathematics, forensics, combat assessments, visualisation, and military intelligence . This diversity helped to identify a fifteen topics that were related. These topics included, among others, "the cyber OODA-loop", "cyber attack profiling", "data fusion approaches", "risk and incident management", "situation description methods", "the relationship between capabilities and actions", "unknown vulnerability detection", "attack probability indicators", and "multi-step attack models". Panel members were assigned to topics they had previous knowledge of and searched for literature within this topic that could match the search criterion. These searches typically started with searches in scholarly databases to identify research papers and internet searches to find "grey literature" (e.g. technical reports). Such searches were complemented by inspection of references used in papers considered relevant. The search process hardly can be described as structured. However, the range of competences and background among the panel members ensured that it covered a wide range of topics related to cyber security. A database of 36 papers had been identified and passed the inclusion criterion after the group screened the paper's title and abstract. After review of the full text XX papers were found to meet the inclusion criterion. These XX can not be said to represent an all available papers related to prediction of adversarial cyber operations, but it is the group's opinion that they are likely to indicate the state of research in this area.

2.4 Information Extraction

The literature addressed the prediction problem from a number of different angles, and at different levels of abstraction. At first, an input-output-perspective attempted to broadly characterize the data the models used. The model of STIX [REF] was used for this purpose. However, the analysis soon showed that it was that most of the models used more or less the same data objects in STIX, namely: vulnerability-information, attack patterns, indicators, intrusion sets, and other observed data. In addition, it turned out to be non-trivial to classify the data used in a reliable manner, partly because of the different levels of abstraction used in the papers. Instead, the following information was extracted to characterize the models:

(1) If a particular formalism was used or proposed.
(2) Data used as input for the prediction model.
(3) The data produced as output by the prediction model.
(4) The scalability of the solution or implementation. To further characterize the models it was extracted how they handled the following issues:
(5) Adversaries attempting to tampering with/fooling the prediction method.
(6) The time it takes to make the prediction and timing issues.
(7) Availability of data needed for analysis or model construction.
(8) Assumptions concerning knowledge of system vulnerabilities and attacks. Furthermore, information was extracted to characterize the maturity of the research in terms by assessing:
(9) If the model had been implemented in prototype and what Technology Readiness Level the model was on.
(10) If the model's its usefulness for was demonstrated, e.g. in a case study.
(11) Tests or other evaluations of accuracy of the prediction model. These nine information elements was extracted as quotes and descriptive summaries of descriptions provided in the reviewed

REFERENCES

[1] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A Ghorbani. 2009. A detailed analysis of the KDD CUP 99 data set. In *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*. IEEE, 1–6.