An Argument for Linguistic Expertise in Cyber Threat Analysis: LOLSec in Russian Language eCrime Landscape

DECISION: accept

AUTHORS: Dalyapraz Manatova, L Jean Camp, Julia R Fox, Sandra Kuebler, Maria A Shardakova and Inna Kouper

Summary of Reviews

- Review 1: -1 (5)
- Review 2: 3 (5)
- Review 3: 2 (4)

Reviews

Review 1

TOTAL SCORE: -1 (weak reject)
Overall evaluation: -1 (weak reject)
Reviewer's confidence: 5 (expert)

This is a position paper arguing for the need to combine linguistic capability with NLP methods in order to better understand e-crime landscape.

The authors provide examples from Conti leak data where the machine translation was incorrect or lost original meaning. I agree with these examples.

I also agree with the need to combine local expertise with computer-assisted tools. This is what cybersecurity companies and intelligence agencies are doing.

However, where is the research in this?

NB. There could be promising new methods such as generative adversarial networks that may assist in crossing the language barriers. However, they would still miss on the broader context. See for example Ebrahimi et al 2022. CROSS-LINGUAL CYBERSECURITY ANALYTICS IN THE INTERNATIONAL DARK WEB WITH ADVERSARIAL DEEP REPRESENTATION LEARNING. MIS Quarterly, 46(2), pp. 1209-1226.

Review 2

TOTAL SCORE: 3 (strong accept)
Overall evaluation: 3 (strong accept)
Reviewer's confidence: 5 (expert)

Summary
This work presents a position paper offering arguments supporting the need for linguistic expertise in Cyber Threat Analysis. In particular, the authors study the discourse of the Conti ransomware group in the context of the Russian invasion of Ukraine. The paper takes the recent Conti leaks and performs a qualitative comparison of the quality of

machine translation (MT) using DeepL and a translation from a native speaker. Results show important distinctions.

Strengths
+ Problem formulation
+ Engaging discussions
+ Clear takeaways
+ Novel case study
+ Well written

Detailed Comments
I would like to thank the authors for putting on the spotlight the importance of sociotechnical approaches to understanding eCrime. It is undeniable that studying the current landscape requires combining linguistic, regional, professional, and technical expertise.

I have enjoyed reading the paper and I am positive the WACCO community will learn a valuable lesson. The paper is not only very well written, but it also offers a good motivation for the problem and empirical evidence of the challenges behind studying cybercriminal conversations in the Russian language.

I found it very interesting to see how the meaning of some common words (e.g., email or wallet address) is misrepresented in the presence of dark jargon. Arguably, some readers may find the statement "the meaning of it may be *completely* lost in automated translations" slightly unfair. Judging by the difference between MT and native translations in Tables I and II, I could infer from the context the meaning of most of the incorrections without speaking Russian.

On another note, Table II has translations from either DeepL or Google Translate. However, the rationale for the choice is unclear. The quality of the paper would improve if the authors were to offer more details on whether there are differences between the two MT models.

I would've liked to see more engaging discussions on how multidisciplinary approaches can start offering headway into addressing the shortcomings discussed in the paper. I found it relevant and insightful the references pointing to prior work on media studios studying humor-related changes, and I wonder if the authors could extend their discussions and cover works like [R1] (just a quick example).

[R1] Seyler, D., Liu, W., Wang, X., & Zhai, C. (2021). Towards dark jargon interpretation in underground forums. In Advances in Information Retrieval: 43rd European Conference on IR Research, ECIR 2021, Virtual Event, March 28–April 1, 2021, Proceedings, Part II 43 (pp. 393-400). Springer International Publishing.

Review 3

TOTAL SCORE: 2 (accept)
Overall evaluation: 2 (accept)
Reviewer's confidence: 4 (high)

This paper presents a simple but important idea: the specifics of language matters when translating text from cybercrime groups. It is well suited as a position paper, given its focus is on presenting this idea, rather than offering a detailed analysis. The paper is well written on the whole.

There are some ways it could be improved:

1) It seems as if there are three elements of importance, in relation to translation: 1) the language (e.g. Russian); 2) cybercrime tech terms/slang/symbols; 3) jokes/humour. These elements appear in the paper, but the emphasis is put on language, with a secondary emphasis on humour. It might work better to acknowledge the overall issue of

translation but then break this issue down into these three points, which can be flagged in the introduction and then discussed in the main body. At the moment, humour at first appears somewhat of an aside in the introduction, with its relevance only realised later in the paper. Language and tech terms are conflated, but they are really separate points.

2) The authors could explain more pointedly that the Russian underground is really important to cybercrime as a whole (e.g. Holt, Chua, Smirnova 2013; McCombie, Pieprzyk, P Watters, 2009; Lusthaus 2018; Goncharov 2012). I don't think this point is made clearly enough and this is one of the key reasons why paying attention to Russian language text matters (the key argument of the paper). If many researchers are operating in English, but leading cybercriminals are operating in Russian, there is a mismatch. This should be stressed, as it strengthens the overall contribution of the paper.

3) The focus on state-sponsored or state-aligned eCrime groups (e.g. in the abstract) does not seem appropriate. Surely the insight around language would be important for cyber threat analysis of any group where Russian or another non-English language is used? The case study might be of a group with state links (Conti), but the application is much wider. Why limit this potential contribution?

4) This paper fits with a broader argument for the value of qualitative analysis of small amounts of data, in addition to any macro level analysis of big data, which is likely to be done through statistical methods. Again, this extends the potential contribution of this paper, by hooking it onto bigger debates within cybersecurity and scholarship more generally.