The genre of threat reports

Emma.Moreton@liverpool.ac.uk

Research questions

- How, exactly, do we communicate cyber threats? What words, phrases and metaphors are typically used to communicate threats and how is this information organised and presented?

- How do linguistic markers of threats correspond to perceived and actual threats?

- What impact does the language of threats have on different stakeholder groups in terms of their decision-making?

- And, finally, what are the most effective (language) strategies for communicating cyber threats?

The communication of threats from two perspectives

- Challenges faced by cyber practitioners and cyber security training and awareness specialists in communicating risks and threats, prioritising information and explaining technical issues to non-expert audiences.

- Challenges faced by non-expert audiences (including policy makers, the Board, employees and the general public) in understanding, interpreting and evaluating information relating to cyber threats.

NCSC Weekly Threat Reports

- Threat Report Corpus (TRC)
- 231 weekly threat reports
- 23rd September 2016 – 28th May 2021

Readership groups

Readership	Frequency
Cyber security professionals	157
Individuals and families	237
Large organizations	268
The public sector	265
The self-employed and sole traders	250

Legitimising strategies

- The extent to which the text, and the propositions contained therein, are accepted as 'true and accurate representations of reality' (Hart 2010: 10).

This is achieved through…

- Internal coherence: logical relations between clauses, sentences and text sections.

- External coherence: the use of linguistic expressions which persuade the readership to accept the writer's claim (Hunston 1993: 116).

Legitimising strategies

- The extent to which the text, and the propositions contained therein, are accepted as 'true and accurate representations of reality' (Hart 2010: 10).

This is achieved through…

- Internal coherence: logical relations between clauses, sentences and text sections.

- External coherence: the use of linguistic expressions which persuade the readership to accept the writer's claim (Hunston 1993: 116).

Genre: what are the different stages (Martin 1992) or moves (Swales 1990) in the texts?

Overarching structure of the threat reports

- Each threat report contains different sections (an average of 2.85 sections p/report)

- Each section represents a specific threat (a total of 658 threats)

- Within each section there are different stages (an average of 4.51 stages per section)

Stages within the threat report sections

Stage		Definition
Heading	\<H\>\</H\>	A one-line summary of the what the text section is about.
Problem	\<P\>\</P\>	An outline of the threat being discussed.
Background	\<B\>\</B\>	Further contextual information relating to the 'Problem' / threat.
Response	\<Resp\>\</Resp\>	A summary of any response made (either verbal or physical) by a person, government body or organisation in relation to the threat.
Recommendation	\<Rec\>\</Rec\>	Advice or suggestions on what action the reader might take in relation to the threat.
Resolution	\<Reso\>\</Reso\>	Details of how the threat/problem was resolved (i.e. what action was taken).

Most frequent patterns

Genre pattern	Frequency
H^P^B^Rec	202
H^P^B	49
H^P^B^Resp^Rec	26
H^B^Rec	21
H^P^B^Reso^Rec	20
H^P^Rec	20
H^B^P^B^Rec	17
H^B^P^Rec	15
H^P^B^Reso^B^Rec	13
H^P^B^Resp^B^Rec	12
H^P^Resp^B^Rec	12
H^P^B^Resp	10

Most typical pattern:
Heading^Problem^Background^Recommendation

Heading
WannaCry ransomware attack illustrates risk of using unlicensed software

Problem

The WannaCry international ransomware attack has highlighted the risks of relying on unpatched software.

Background

The scale of the outbreak has been blamed in part on the widespread use of unlicensed software. Pirated software is often insecure as it does not benefit from manufacturers' updates to fix vulnerabilities. Several of the countries reported by cyber security companies to be worst affected are also amongst the countries where unlicensed software is most widely used. This incident illustrates that while using unlicensed software might be seen as a way of saving money in the short term, it can put cyber security at serious risk and may potentially lead to losses far outweighing any savings.

Recommendation

The NCSC's guidance on protecting your organisation from ransomware can be found here. Further guidance for home users and small businesses as well as enterprise administrators is also available.

Some general observations

- 160 patterns identified

- 131 contain a *Problem* stage and 133 contain a *Background* stage

- The *Recommendation*, *Response*, *Resolution* stages are less consistent

- Just over 70% of the reports contain a *Recommendation* stage, 50% contain a *Response* stage, 30% contain a *Resolution* stage

What next?

- What impact do these different structures have in terms of how the information is received by the text-consumer? (This can be explored in lots of ways through focus group studies with the different readership groups, for e.g.)

- Rather than using a Heading^Problem^Background^Recommendation structure, would a narrative structure be more effective?

- Speculative futures, hypothetical scenarios, fantastical events?

- A closer look at the language of the different stages.