THE OSINTER CENSUS²

PROJECT DESCRIPTION

Since the 2010s, Twitter/X has emerged as a crucial platform for Open Source Intelligence (OSINT) practitioners to share their analyses and insights on global events, conflicts, crime, and corruption. The nature of OSINT, which does not require formal qualifications, has led to a largely unorganized online community. However, the rapid growth of OSINT and the concurrent rise in misinformation and disinformation on social media have underscored the critical need to differentiate between reliable and unreliable OSINT content. Addressing this challenge, our project has developed a comprehensive matrix encompassing 23 distinct categories. This matrix aims to systematically evaluate the credibility of posts made by OSINT accounts on Twitter/X, thereby enhancing the accuracy and trustworthiness of information disseminated on these platforms.

RESEARCH QUESTION

There were several research questions leading to different stages of the research project.
We wanted to find unreliable OSINT accounts and their accompanying tweets in order for us to analyze them along the lines of indicators like language use, brevity, signs of bias, and others. By analyzing and iteratively categorizing them, we could in the future, give this data to an AI model that will be able to identify unreliable OSINT accounts and less trustworthy tweets. Our main research question was: What indicators make an OSINTER tweet unreliable?

In order to find means to identify reliable and unreliable OSINT, we developed the following categories in an iterative way to create a matrix: (1) Data, information, and sources, (2) Argumentation quality, (3) Style of communication, and (4) Community

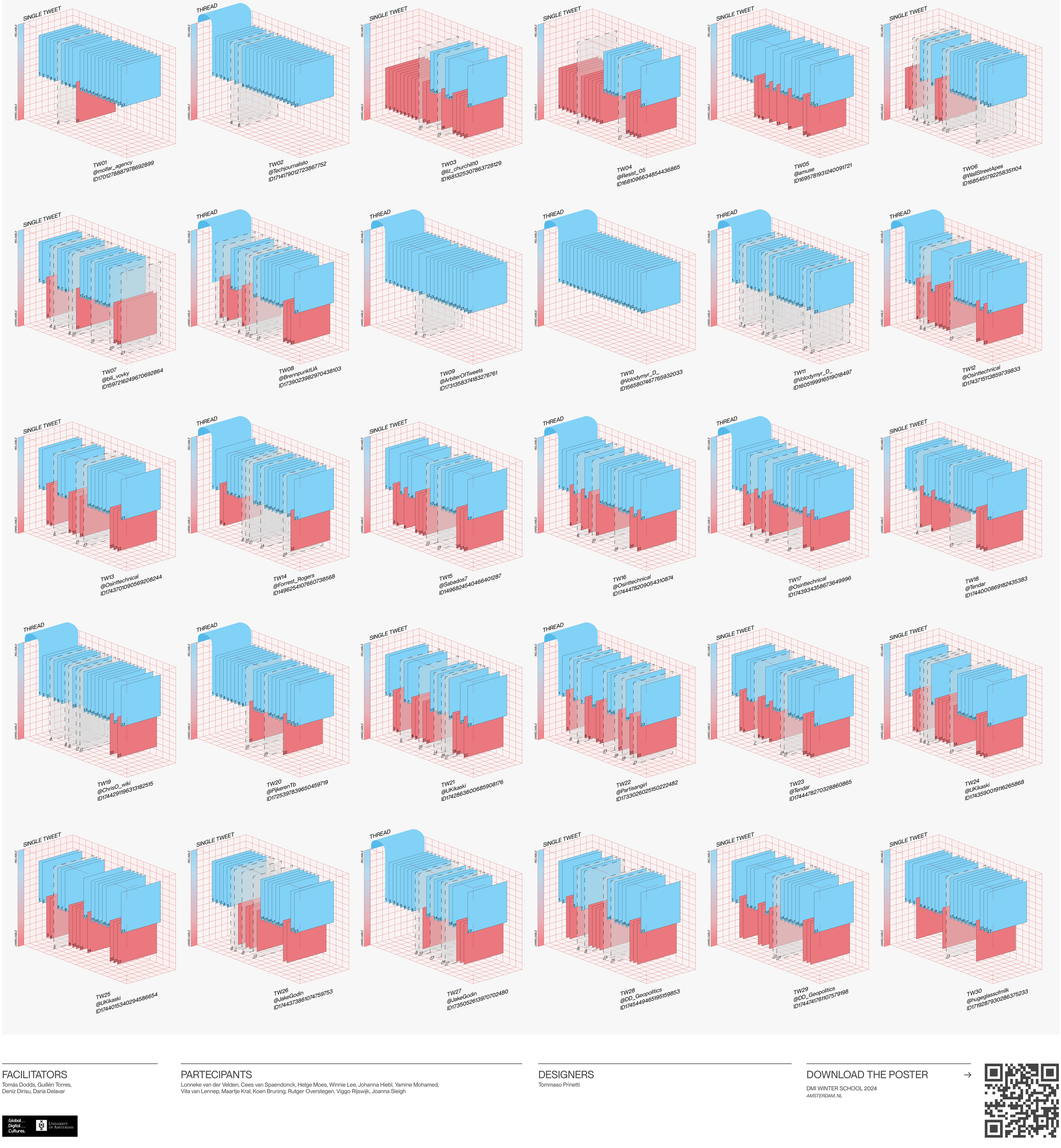
The questions guiding each of these categories were:

1. What is the type of information that is incorporated in the tweet?
2. How are the argumentative techniques mobilized in the tweet?
3. What is the style of communication that the author uses in the text of the tweet?
4. To what extent are characteristics of the OSINT community present in the tweet?

BACKGROUND: WHAT'S OSINT?

Open Source Intelligence (OSINT) refers to the practice of collecting and analyzing open-source information to produce valuable insights and intelligence for various uses. Traditionally, OSINT was considered a branch of military intelligence. However, with the advent of widespread social media, internet access, and technological advancements in the 2010s, its application expanded significantly. OSINT has since become integral to investigative journalism, news reporting, and international justice, complementing conventional investigative methods. Currently, OSINT is undergoing a transformation, increasingly becoming the primary means of information gathering and investigation, reflecting its growing importance and effectiveness in the digital age. This definition is built on the content as presented in the Berkeley Protocol (2022).

**Why we use OSINT instead of Open Source Investigation: "Bellingcat uses open sources to conduct investigations, just like OSINT professionals, but the INT in the acronym suggests that only intelligence agencies do this. Bellingcat is emphatically not an intelligence agency." (source) The use of the word OSINT, according to our project group of OSINT specialists, academics and journalists, does not indicate that it is solely in the realm of intelligence agencies. Intelligence is no longer in the domain of the government/military. Therefore, the definition of Intelligence that it is solely "information collection for political/military use" is no longer accurate. Information that is collected can provide actionable insights and intelligence to the public, such as NGOs, civic action platforms, investigative outlets and more.*



FACILITATORS
Tomás Dodds, Guillén Torres,
Deniz Dirisu, Daria Delavar

PARTECIPANTS
Lonneke van der Velden, Cees van Spaendonck, Helge Moes, Winnie Lee, Johanna Hiebl, Yamine Mohamed,
Vita van Lennep, Maartje Kral, Koen Bruning, Rutger Overstegen, Viggo Rijswijk, Joanna Sleigh

DESIGNERS
Tommaso Prinetti

DOWNLOAD THE POSTER →

DMI WINTER SCHOOL 2024
AMSTERDAM, NL

Global Digital Cultures · University of Amsterdam

THE OSINTER CENSUS[1]

RESEARCH METHODOLOGY

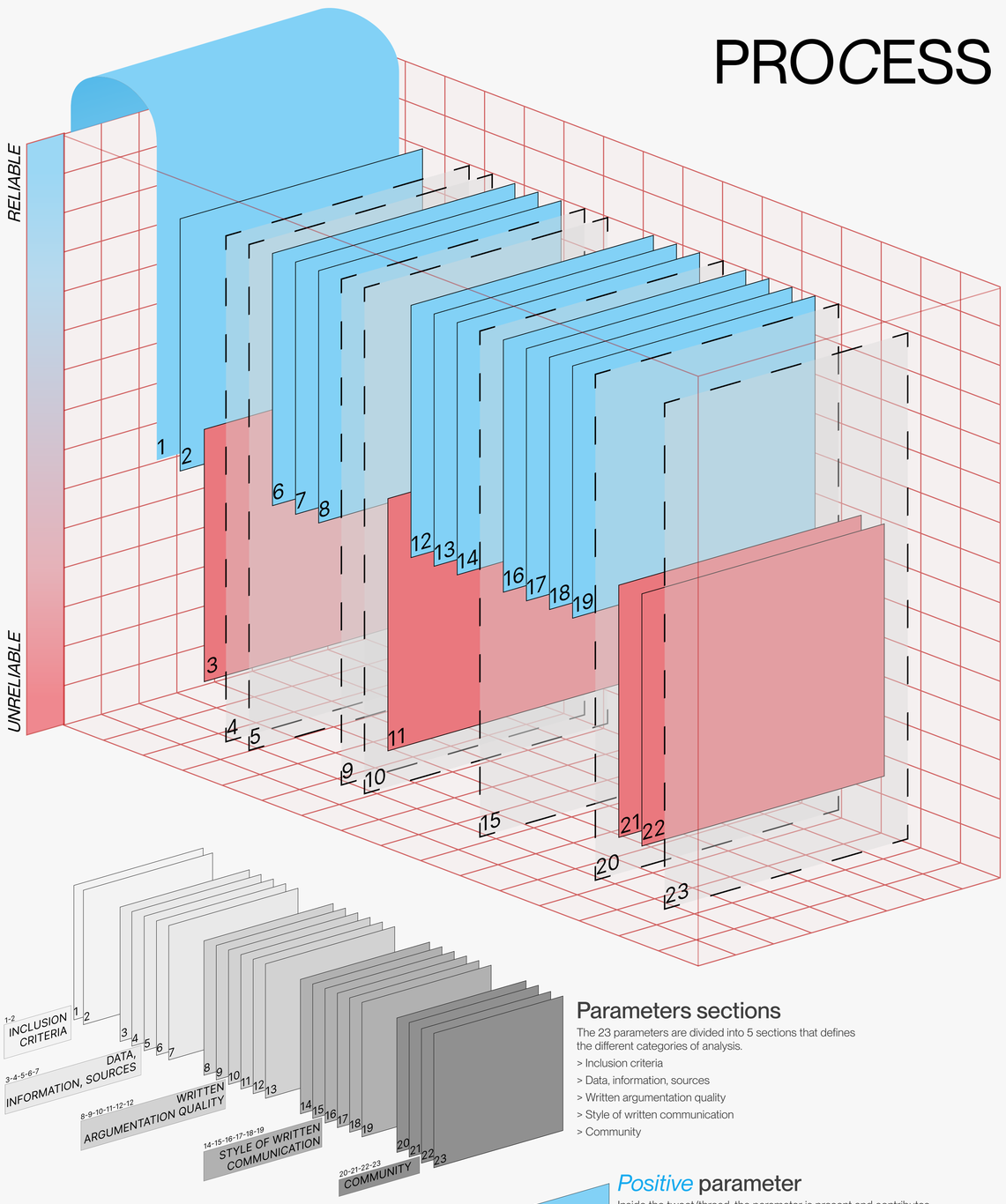
A systematic, multi-step approach was employed to classify tweets and Twitter accounts engaged in the Open Source Intelligence (OSINT) practices. In the initial step, the group familiarized themselves with OSINT tweets and accounts. Some members explored a pre-collected database of tweets with the hashtag #OSINT provided by the 4CAT tool, while others examined tweets from OSINT accounts pre-identified as either problematic or trustworthy. Moving to the second step, the group dissected the anatomy of OSINT tweets by identifying variables within the tweet or account that signaled degrees of trustworthiness (e.g., use of AI images, excessive hashtags, and source links). These variables were collectively discussed and led to the creation of a matrix, which was iteratively tested on a sample in Step 3. In Step 4, the matrix underwent validation through intercoder reliability testing, with any discrepancies resolved through group discussion. The refined matrix was then applied in Step 5 to code a dataset of OSINT tweets collected through snowball sampling. Finally, in Step 6, accounts with OSINT tweets were analyzed based on induced variables.

RESULTS OF THE RESEARCH

Our research reveals that the trustworthiness of an OSINT tweet cannot be pinned down to a single characteristic; a holistic and nuanced approach is crucial. Interestingly, there was no link between style of communication and trustworthiness. We also found that it is difficult to present reliable OSINT on Twitter without resorting to threads or external links to sources. Furthermore, the mere credibility of an author does ntot suffice to establish the trustworthiness of OSINT accounts. Finally, the use of artificial intelligence in OSINT tweets often serves as a red flag, signaling the need for extra scrutiny. The research process itself highlighted the importance of iterative coding in helping define the boundaries of OSINT practice.

- Not link between style of communication in the tweet and the quality
- Not determine reliability on one single characteristic
- Holistic and nuance
- Hashtags osint not part of the community vernacular - reliable
- Boundary work
- The importance of iterative coding / help us define boundaries for the practice
- We can determine that something is not OSINT
- We determine what OSINT is
- Entering the field of OSINTERS - Having a better understanding, from a social media environment
- Difficult to present reliability on Twitter without using threads or external links to sources
- Author credibility is not enough to justify reliability of OSINT accounts
- Ai being a red flag.

PROCESS & *RE*ADING



Parameters sections

The 23 parameters are divided into 5 sections that defines the different categories of analysis.

> Inclusion criteria
> Data, information, sources
> Written argumentation quality
> Style of written communication
> Community

Reliable tweet

Inside the tweet/thread, the parameter is present and contributes negatively to the realiability of the tweet.

Unreliable tweet

Inside the tweet/thread, the parameter is present and contributes negatively to the realiability of the tweet.

Positive parameter

Inside the tweet/thread, the parameter is present and contributes to the realiability of the tweet in a positive way.

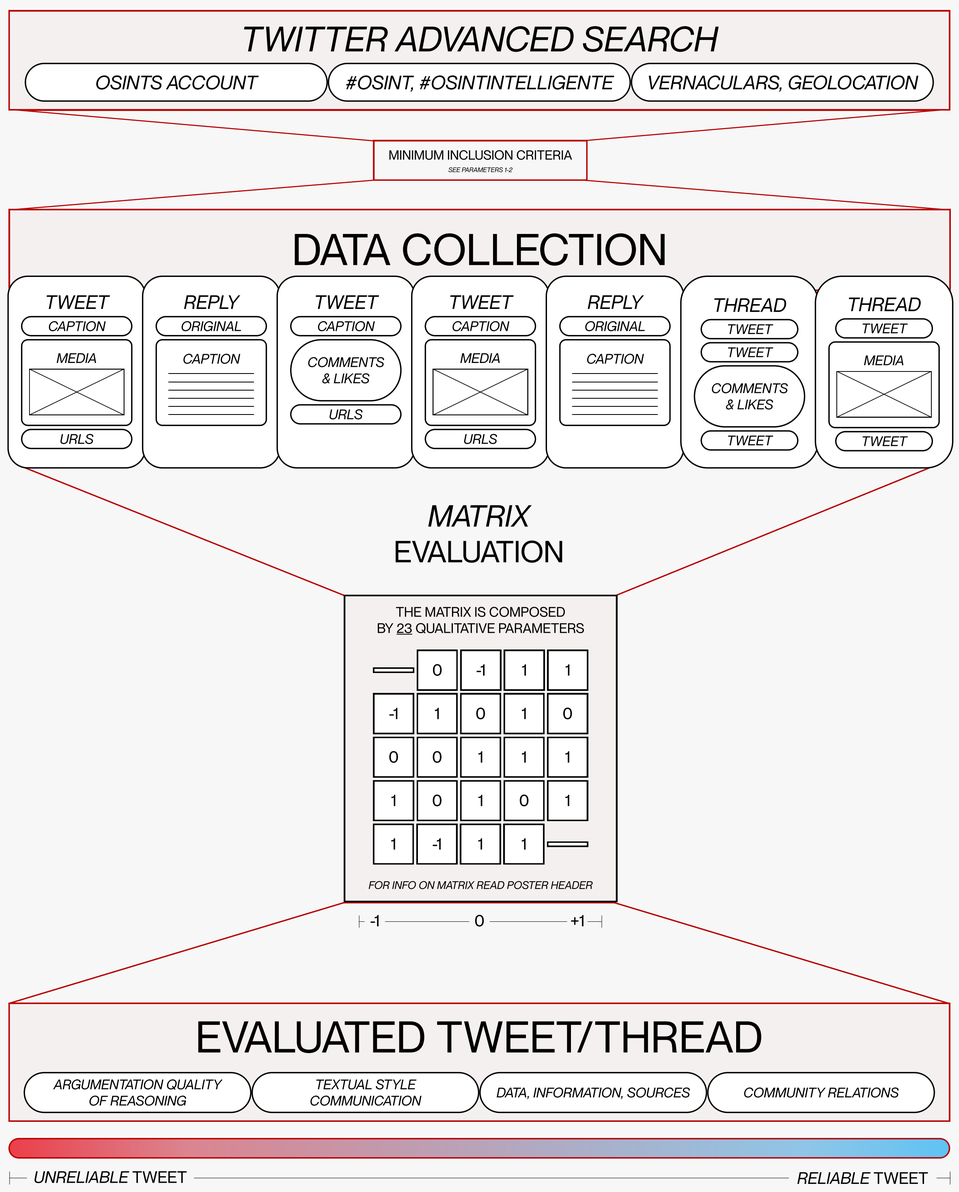
Negative parameter

Inside the tweet/thread, the parameter is present and contributes negatively to the realiability of the tweet.

Incomplete parameter

Inside the tweet/thread, the parameter is present in an incomplete way and it's hard to evaluate.

22 Parameter *number*



MA*TRI*X'S PA*RAME*T*ERS*

1
STATUS OF DATA AND/OR INFORMATION
Trustworthy OSINT provides data and/or information that relates to the claim/s made. For example GPS location is given in relation to a photo. If this is not the case, it is untrustworthy.

2
ADDS AN INSIGHT
An insight to the data and/or information is provided, one that is more than a repetition of the information. For example, a verification could be considered an insight. If this is not the case, it is untrustworthy.

3
LINKS TO SOURCES
A source (hyperlink) is provided that takes the viewer to the source of information and/or data. If not, it is untrustworthy.

4
PRESENCE OF CREDITS
References a source (not a hyperlink but an explicit statement that clarifies where the information and/or data comes from). If there is no credit, it is untrustworthy.

5
ANNOTATED CONTENT
Media (photo or video) is annotated by the author with the goal to support the claims made about the data and/or information. If not there, or if it is distracting, it is untrustworthy.

6
MANIPULATION
Potential signs of media manipulation with the intention of deceiving lead to untrustworthiness.

7
NOISE
The addition of elements or non relevant content, that could be distracting for the user, or that do not support the claim/s. For example, the use of text, emoticons, media, AI, or watermarks.

8
SPECIALIZED KNOWLEDGE
Provides specific information such as geolocation, a weapon, or a vehicle, which suggests that the person has expertise in a specific domain.

9
METHOD COMMUNICATION
A method is provided and described, or referenced in a link. If not, it is untrustworthy.

10
LOGICAL ARGUMENTATION
The conclusion follows logically from the claims and the provision of data and/or information. No logical fallacies. It is untrustworthy if there is no logic to the argument.

11
GAPS IN INFORMATION
Trustworthy OSINT would acknowledge potential gaps in the argumentation, data, and or information.

12
RESULT IS REPLICABLE
Trustworthy OSINT provides enough information for another person to redo the investigation and make the same claim. Untrustworthy OSINT does not provide such info or info that leads to other conclusions.

13
SELF- AFFIRMATION AS ARGUMENT
Over-emphasis on the author's credibility as a means to justify or persuade the reader of the argument or claim should not be trusted. For example using terms such as "trust me".

14
EXCESSIVE USE OF HASHTAGS
The overuse hashtags and ones that do not relate to the content, or that do not support the content or its consumption, is problematic.

15
LOGICAL STRUCTURE
Trustworthy OSINT structures sentences and presents information so that the argument is clear to follow. If not, it is untrustworthy.

16
EMOTIVE LANGUAGE
Language appeals to the emotions of the reader is untrustworthy. This is because the overuse of emotions can hinder or distract from the argumentation or the conclusions.

17
VICTIM LITERATURE
If the communication style falls into victimisation styles primarily, we tag it as untrustworthy. For example, emphasising the suffering of children or the opression by colonialists... etc.

18
HARMFUL LANGUAGE
Language that incites violence on groups or individuals, any racist or sexist undertones etc, indicates untrustworthiness.

19
SARCASM
Too much use of irony or sarcastic language distracts from the conclusion or argument and should not to be trusted, especially if this is the main tone of the tweet.

20
SHARES OSINT TOOLS/TECHNOLOGIES
Trustworthy OSINT provides links or references to tools and technologies that other OSINTers can use for investigations.

21
COMMUNITY VERNACULAR USAGE
Trustworthy OSINT correctly uses community vernacular, which refers to the language or dialect spoken by a community, that outsiders won't necessarily understand. This refers to terms related to OSINT and does not include specialized knowledge. Untrustworthy tweets lack or wrongly apply vernacular.

22
TAGGING THIRD PARTIES
Tagging third parties on twitter using a handle (@) is a good thing, as the user opens themselve up to scrutiny, which is a sign that the information can be validated or reviewed. For example, tagging reputable sources such as @GeoConfirmed.

23
ENGAGEMENT (LIKES, RETWEETS)
Trustworthy tweets receive feedback through likes and retweets, and the retweets and or likes are not simply from the same author.

FACILITATORS
Tomás Dodds, Guillén Torres, Deniz Dirisu, Daria Delavar

PARTECIPANTS
Lonneke van der Velden, Cees van Spaendonck, Helge Moes, Winnie Lee, Johanna Hiebl, Yamine Mohamed, Vita van Lennep, Maartje Kral, Koen Bruning, Rutger Overstegen, Viggo Rijswijk, Joanna Sleigh

DESIGNERS
Tommaso Prinetti

DOWNLOAD THE POSTER →
DMI WINTER SCHOOL 2024
AMSTERDAM, NL

.Global_ .Digital_ .Cultures. | University of Amsterdam