DISARM Decision Trees for Fact Checkers

Support with decision making for Fact Checkers when applying DISARM

Introduction

DISARM provides a framework of commonly occurring behaviours exhibited during information manipulation and interference incidents, called “DISARM Techniques”. Augmenting Fact Checks by documenting observed Techniques enables data-driven development of long-term disruption strategies, alongside vital efforts to verify veracity of viral narratives.

There are a lot of different Techniques available in DISARM. Time-pressured analysts (that is, most of them) need help prioritising which Techniques they want to apply to material they work on.

This document is designed to help Fact Checkers make such prioritisation decisions. It begins by helping analysts consider which Techniques they will consider applying to incidents. It then provides advice on applying DISARM Techniques to incidents.

Contents

DISARM Techniques as Answers to Questions 3

Is This Question Relevant to My Goals? 3

Am I Able to Answer This Question? 3

Questions Answered by DISARM 4

Asset Questions 4

Content Questions 5

Using Questions to Refine Scope of DISARM Application 7

Time-Pressured Fact Checker 7

Enforcement Action Fact Checker 7

Tell Me Everything Fact Checker 8

Applying DISARM Techniques to a Report 9

Technique Application Methods 9

Associating Techniques within a Report 11

Analysis Process for Assets 13

What type of Asset is being used? 13

What type of Identity is the Asset presenting? 14

Is the Asset’s Identity legitimate? 14

Analysis Process for Content 16

Common Issues 16

Uncommon Issues 19

Rare Issues 19

Other Metadata 20

DISARM Techniques as Answers to Questions

Techniques can be thought of as answering different questions about an incident. For example, the Sub-Techniques of T0162: Reframe Context answer the question “Has the actor reframed the context of material in such a way that its meaning is changed? How?”

Framing Techniques as answers to questions makes it easier to decide which ones you want to apply to your reports.

Is This Question Relevant to My Goals?

Why are you applying DISARM Techniques to your investigation?

For some, DISARM is a way of amplifying their work with the wider influence operation defender community. For some, it’s about informing which enforcement actions are available for a given incident. For others, it’s about converting as much of their investigation as possible into a standardised language to inform future development of interventions.

Knowing your tagging objectives helps with deciding on which questions to answer. Later in this document, we will propose which Techniques you might want to consider based on your analyst profile.

Am I Able to Answer This Question?

What capabilities do you have as a researcher?

Some Techniques require specific analyst capabilities to identify. Fact Checkers who are experts in OSINT or Geolocation will likely want to prioritise investigating issues with **Content’s*** framing, where network analysts who can identify automated **Assets*** will focus their efforts on identifying coordinated inauthentic behaviour.

Techniques identified in the **DISARM Quick Reference Guide for Fact Checkers** and the **Fact Checker Framework** have been selected with Fact Checkers’ capabilities in mind. Organisations with other capabilities may consider expanding their scope to look at more Techniques.

> ***Content:** Things like Images, Text, Video - the material people publish online*

> ***Asset:** Things like Websites, Accounts - the infrastructure people use to publish material online*

Questions Answered by DISARM

The following questions have been produced based on what is most relevant for Fact Checkers to answer using DISARM.

Asset Questions

1) What type of **Asset** is being used in this incident?	T0146: Account Asset T0152.004: Website Asset
2) What type of **Identity*** is the **Asset** presenting?	All Sub-Techniques of T0097: Present Persona, most commonly; T0097.102: Journalist Persona T0097.110: Party Official Persona T0097.111: Government Official Persona T0097.108: Expert Persona T0097.202: News Outlet Persona T0097.206: Government Institution Persona
3) Is the **Asset's Identity** legitimate?	T0143.002: Fabricated Persona T0143.003: Impersonated Persona T0143.004: Parody Persona T0143.005: Compromised Persona

Identity:* How **Assets present themselves. If it's a website, does it present as a news outlet? A government website? A fact checking outlet? If it's an account, is it an account of a journalist? A politician?

Example

1. T0146.003: Verified Account Asset
2. T0097.205: Business Persona
3. T0143.004: Parody Persona

Source: https://www.snopes.com/fact-check/eli-lilly-free-insulin/

Content Questions

Content Production Questions

4) Has the published **Content** been edited?	T0165: Edited Content
↳ 4a) Which method of editing has been used?	T0165.001: Clipped Content T0165.002: Cropped Content T0165.003: Playback Speed Altered T0165.004: Source Edited Out of Content
5) Has content been generated using AI?	T0166: AI-Generated Content
↳ 5a) Have any of these specific types of AI-Generated **Content** been used?	T0166.001: Deepfake Impersonation
6) What format does the **Content** take?	T0085: Develop Text-Based Content T0085.004: Develop Document T0086: Develop Image-Based Content T0087: Develop Video-Based Content T0088: Develop Audio-Based Content

Content Narrative Questions

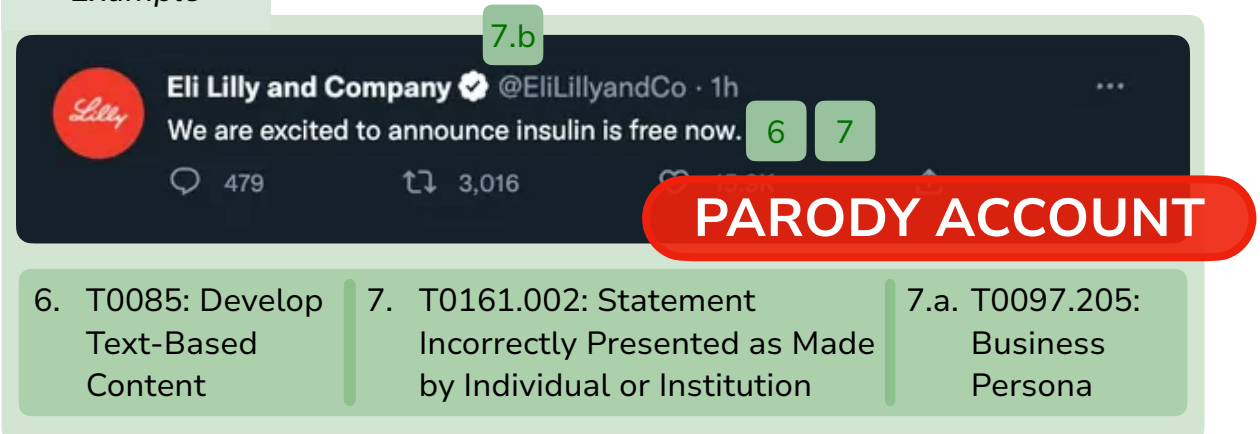
> ***Narrative:** The story that is told by the **Content** posted*

7) Have any common types of falsified **Content** been published?	T0161.001: Impersonated Content T0161.002, Statement Incorrectly Presented as Made by Individual or Institution
↳ 7a) If **Content** is incorrectly attributed, what type of **Identity** is being attributed?	All Sub-Techniques of T0097: Present Persona, most commonly; T0097.110: Party Official Persona T0097.111: Government Official Persona T0097.202: News Outlet Persona T0097.206: Government Institution Persona
8) Does **Content** recontextualise material to produce a new **Narrative**?	T0162: Reframe Context

↳ 8a) Does it use any common methods of reframing context?	T0162.001: Incorrect Subtitled Speech Reframes Context T0162.002: Edits Made to News Report which Reframe Context T0162.003: Historic Content Incorrectly Presented as Current T0162.004: Content Incorrectly Presented as Depicting Another Location T0162.005: Video Game Content Incorrectly Presented as Depicting Reality T0162.006: AI-Generated Content Incorrectly Presented as Depicting Reality T0162.008: Context Reframed by Edits to Media T0162.009: Statement Reframed by Removal from Context T0162.010: Entertainment Media Content Incorrectly Presented as Depicting Reality T0162.011: Content Originally Produced as Satire Presented as Not Satire
9) Are there any issues with cited academic research?	T0163.001: Narrative Cites Nonexistent Academic Research T0163.002: Narrative Misrepresents Findings of Cited Academic Research T0163.003: Narrative Cites Academic Research not Peer Reviewed
10) Are there any issues with cited statistics?	T0164.001: Narrative Presents Fabricated Statistics as Genuine Data T0164.002: Narrative Uses Selective Statistics to Support Claim T0164.003: Narrative Uses Misinterpreted Statistics to Support Claim
11) Are there any issues with how **Content** is titled?	T0167: Issue with Content's Headline T0167.001: Use of Clickbait T0167.002: Title Misrepresents Content
12) Has a Fact Checker assessed the claim?	T0160.006: Content Previously Fact Checked T0160.007: Claim Previously Fact Checked
13) Does the **Narrative** relate to a current event?	T0068: Respond to Breaking News Event or Active Crisis

Example

Source: https://www.snopes.com/fact-check/eli-lilly-free-insulin/



6. T0085: Develop Text-Based Content
7. T0161.002: Statement Incorrectly Presented as Made by Individual or Institution
7.a. T0097.205: Business Persona

Using Questions to Refine Scope of DISARM Application

This section contains a collection of example profiles for different analysts, and the questions they might want to answer based on this. [When able, we will also produce filtered Navigator frameworks based on these profiles].

Time-Pressured Fact Checker

Analysts who want to share their work with the DISARM community, but don't have much time to add tagging into their workflow, and just want to capture essential data about their Fact Check.

Content Questions

- Content Narrative
    - Has any of these commonly occurring types of falsified content been published?
    - Does the content reframe the context of legitimate material to produce a new narrative?
    - If the claim has been assessed by a Fact Checker, what conclusion did they come to?
    - Does the narrative relate to a current event or breaking news?
- Content Production
    - Has the published content been edited?
    - Has content been generated using AI?

Enforcement Action Fact Checker

Analysts who want to highlight information in their work which identifies incidents which are open to enforcement action (impersonation).

Asset Questions

- What type of Asset is being used?
- What type of Identity is the Asset presenting?
- Is the Asset's Identity legitimate? If not, what type of identity is observed (e.g. impersonation, or parody)?

Content Questions

- Content Narrative
    - If the content is impersonating another individual or institution, what type of identity is being impersonated?
    - If the content is incorrectly attributing a statement to an individual or institution, what type of identity is being attributed?
- Content Production
    - Has the published content been edited?
    - Have any of these specific types of AI-Generated Content been used?

Tell Me Everything Fact Checker

Analysts who want to convert all of their research into standardised data, contributing detailed information to the defender community's understanding of the kinds of information that Fact Checkers address on a daily basis. This data can be used to inform development of countermeasures which don't yet exist.

Applying DISARM Techniques to a Report

This section discusses operationalisation of DISARM Technique application; how do you take a report and apply DISARM Techniques to it.

Technique Application Methods

While some users fully embed DISARM with their analysis process, applying Techniques during their investigation, this section assumes that Fact Checkers augment their existing work with DISARM Techniques, applying them to written reports once they've been completed.

There are three different approaches which can be taken to apply DISARM to completed reports.

Summary Tagging

Summary Tagging involves an analyst identifying which DISARM Techniques appear in a report, and providing a list of those Techniques. This list could appear in a table in the report's indices, or it could be provided in metadata stored elsewhere.

This method works best for **Time-Pressured Analysts;** but provides the least detail for others looking at their work in the future.

Detailed Summary Tagging

Detailed Summary Tagging expands on Summary Tagging by providing more information for each Technique applied. It uses a table of Techniques identified in a report in the following format.

This approach provides the most possible information for why Techniques have been applied. It works well for analysts collaborating as part of remote teams, or with different organisations, for whom reducing back-and-forth questioning is of critical importance. There is no ambiguity about analysts' justifications for their tagging decisions, or the section of the report they're drawing from.

Data	Quote	Technique(s)	Justification
Data Definition	Text from the report which inspired the application of the DISARM Technique	The DISARM Technique(s) identified in the report	Why this text from the report

Data Example	On Nov. 10, 2022, a Twitter account with a "verified" checkmark badge and a display name of "Eli Lilly and Company" tweeted, "We are excited to announce insulin is free now." The account's handle was @EliLillyandCo. However, this was nothing more than a parody account, as its bio clearly said.	T0146.003: Verified Account Asset, T0097.205: Business Persona, T0143.004: Parody Persona, T0161.002: Statement Incorrectly Presented as Made by Individual or Institution	An account with a verification checkmark was used which had the name “Eli Lilly and Company”, matching the existing business Eli Lilly. Its bio claimed that it was a parody of the real Eli Lilly. It was used to make a statement which was perceived as being made by the real Eli Lilly.

Source: https://www.snopes.com/fact-check/eli-lilly-free-insulin/

However, this approach takes more time, with analysts having to draw out relevant quotes, associate Techniques with them, and provide written justifications for each tagging decision.

Inline Tagging

Inline Tagging refers to applying DISARM Techniques within a report, after relevant text. For example:

> *On Nov. 10, 2022, a Twitter account with a "verified"* **(T0146.003: Verified Account Asset)** *checkmark badge and a display name of "Eli Lilly and Company”* **(T0097.205: Business Persona)** *tweeted, "We are excited to announce insulin is free now.”* **(T0151.002: Statement Incorrectly Presented as Made by Individual or Institution)** *The account's handle was @EliLillyandCo. However, this was nothing more than a parody account, as its bio clearly said* **(T0143.004: Parody Persona)**.

This approach balances the speed of Summary Tagging with the benefit of knowing which section of the report justifies which DISARM Technique, without having to invest time in writing an explanation for each tagging decision.

However, Inline Tagging can make the report less readable for those not familiar with DISARM. To avoid confusion for the report’s wider audience, an Inline Tagged version of the report can be produced for the purpose of sharing standardised data.

Analysts will need to decide on an approach to augmenting their work which works best for them, based on the resources they have available, and their reason for using DISARM.

You can see some examples of the over 100 Inline Tagged reports produced as part of the DISARM 1.7 update in the associated document **DISARM Incidents for Fact Checkers.**

Associating Techniques within a Report

Some Techniques provide a clearer picture what a report details when associated with each other *within* a report. This section describes why that is the case, and shows how you can produce **Aggregate Techniques*** to denote that association.

> ***Aggregate Technique:** Multiple DISARM Techniques associated with each other by comma separating them in a pair of brackets*

Returning to the Asset questions which DISARM Techniques can answer (What Asset? Which Identity? What Legitimacy?), you could provide a list of three individual answers to the questions, or you can associate the answers.

For example, when documenting a verified account parodying a business, unassociated Techniques would look like:

- **T0146.003: Verified Account Asset**: There was a verified account
- **T0097.205: Business Persona**: There was an **Asset** presenting as a Business
- **T0143.004: Parody Persona**: There was an **Asset** which parodied an existing identity

Where aggregated Techniques would look like:

- (**T0146.003: Verified Account Asset**, **T0097.205: Business Persona**, **T0143.004: Parody Persona**): There was a verified account presenting as a business which parodied an existing one

Why Associate Techniques

Associating Techniques becomes more important when there are multiple topics covered in an incident. For example, BBC News published a report which discusses both the *Eli Lilly* parody shown above, and the parody of a US politician:

Example

Source: https://www.bbc.co.uk/news/technology-63599553

Documenting both in the same report using unassociated Techniques would look like:

- **T0146.003: Verified Account Asset**: There was a verified account

- **T0097.205: Business Persona**: There was an **Asset** presenting as a Business
- **T0097.110: Party Official Persona**: There was an **Asset** presenting as a Party Official
- **T0143.004: Parody Persona**: There was an **Asset** which parodied an existing identity

Because these are not aggregated, it's unclear that these were two unique parody accounts. With **Aggregate Techniques** we would instead have:

- (**T0146.003: Verified Account Asset**, **T0097.205: Business Persona**, **T0143.004: Parody Persona**): There was a verified account presenting as a business which parodied an existing one
- (**T0146.003: Verified Account Asset**, **T0097.110: Party Official Persona**, **T0143.004: Parody Persona**): There was a verified account presenting as a party official which parodied an existing one

In which case it's much more clearly defined which asset is associated with which identity, and how many there were.

Analysis Process for **Assets**

This section goes into more detail about how you can use DISARM Techniques to answer each **Asset** question identified earlier:

1) What type of **Asset** is being used in this incident?	T0146: Account Asset T0152.004: Website Asset
2) What type of **Identity** is the **Asset** presenting?	All Sub-Techniques of T0097: Present Persona, most commonly; T0097.102: Journalist Persona T0097.110: Party Official Persona T0097.111: Government Official Persona T0097.108: Expert Persona T0097.202: News Outlet Persona T0097.206: Government Institution Persona
3) Is the **Asset's Identity** legitimate?	T0143.002: Fabricated Persona T0143.003: Impersonated Persona T0143.004: Parody Persona T0143.005: Compromised Persona

What type of **Asset** is being used?

Assets used in incidents addressed by Fact Checkers commonly fall into one of two categories, a Website or an Account. Enter the matching Technique; (T0146: Account Asset), or (T0152.004: Website Asset).

You can optionally provide more information about the Account or Website, depending on your intelligence requirements and available resources.

Extra Account **Asset** questions

1a) Is the Account any one of these types of account?	T0146.003: Verified Account Asset T0146.004: Administrator Account Asset T0146.007: Automated Account Asset
1b) Does the Account ID look like another's ID?	T0146.005: Lookalike Account ID

Extra Website **Asset** questions

1c) Does the Website's domain look like another's domain?	T0149.003: Lookalike Domain

What type of **Identity** is the **Asset** presenting?

Many online **Assets** present **Identities**; i.e. that they are being controlled by a specific individual or institution, who has a specific role in society (e.g. a job for an individual, or a business for an institution).

DISARM provides a standardised list of **Identities** often presented in influence operations under the Technique T0097: Present Persona. There are many **Identities** available under T0097: Present Persona, however the following commonly appear in Fact Checks:

- T0097.102: Journalist Persona
- T0097.110: Party Official Persona
- T0097.111: Government Official Persona
- T0097.108: Expert Persona
- T0097.202: News Outlet Persona
- T0097.206: Government Institution Persona

If these don't match what you're seeing , there are other available **Identities** you can use in T0097: Present Persona [add link to navigator here].

Sub-Techniques of T0097: Present Persona with identifiers starting with a 1 (i.e. T0097.1__) are for Individuals, and those with identifiers starting 2 (i.e. T0097.2__) are for Organisations. Be sure to check the Technique's descriptions, as these detail further what the **Identity** covers, and provide examples of reports covering those **Identities**.

If there is no appropriate Persona, you can either tag nothing for this question, or enter T0097.100: Individual Persona for people, or T0097.200: Institutional Persona for organisations.

If using **Aggregate Techniques,** associate your selected **Identity** with your selected **Asset** in a pair of brackets, comma separated. For example, a news website would be represented by (T0152.004: Website Asset, T0097.202: News Outlet Persona).

Is the **Asset's Identity** legitimate?

In DISARM, **Assets**' identities have different types of legitimacy, which can be selected from the following:

T0143.003: Impersonated Persona	The **Asset** says it's owned by an existing individual or institution, but is actually controlled by somebody else.
T0143.004: Parody Persona	The **Asset** is parodies an existing individual or institution (or a genre of individuals or institutions, e.g. a parody of a non-specific politician, or a parody news site)
T0143.005: Compromised Persona	The **Asset** was previously controlled by an individual or institution, but it was compromised, and the actor now in control of the **Asset** maintained its previous persona, presenting it as still controlled by them.

If using **Aggregate Techniques,** associate whichever legitimacy matches the observed Asset to the aggregate, comma separated. For example, a compromised news website would be represented by (T0152.004: Website Asset, T0097.202: News Outlet Persona, T0143.005: Compromised Persona).

An example of a compromised news site being used to publish false information attributed to the news outlet can be found in the associated document **DISARM Incidents for Fact Checkers** under the title *Hackers publish fake story about Ukrainians attempting to assassinate Slovak president.*

Example

Source: https://www.bitdefender.com/en-gb/blog/hotforsecurity/hacker-posts-fake-story-about-ukrainians-trying-to-kill-slovak-president

Analysis Process for Content

Typically content addressed in a Fact Check has an issue which have been sorted into the following categories:

- Common Issues
- Uncommon Issues
- Rare Issues

Analysts should look through these categories to identify what issues are present in their incident, and inline tag the appropriate Technique.

Common Issues

The following are questions which cover issues most commonly addressed by Fact Checkers:

Have any common types of falsified **Content** been published?	T0161.001: Impersonated Content T0161.002, Statement Incorrectly Presented as Made by Individual or Institution
↳ If **Content** is incorrectly attributed, what type of **Identity** is being attributed?	All Sub-Techniques of T0097: Present Persona, most commonly; T0097.110: Party Official Persona T0097.111: Government Official Persona T0097.202: News Outlet Persona T0097.206: Government Institution Persona
Does **Content** recontextualise material to produce a new **Narrative**?	T0162: Reframe Context
↳ Does it use any common methods of reframing context?	T0162.001: Incorrect Subtitled Speech Reframes Context T0162.002: Edits Made to News Report which Reframe Context T0162.003: Historic Content Incorrectly Presented as Current T0162.004: Content Incorrectly Presented as Depicting Another Location T0162.005: Video Game Content Incorrectly Presented as Depicting Reality T0162.006: AI-Generated Content Incorrectly Presented as Depicting Reality T0162.008: Context Reframed by Edits to Media T0162.009: Statement Reframed by Removal from Context T0162.010: Entertainment Media Content Incorrectly Presented as Depicting Reality T0162.011: Content Originally Produced as Satire Presented as Not Satire

Below more advice is provided about specific situations which may arise with each.

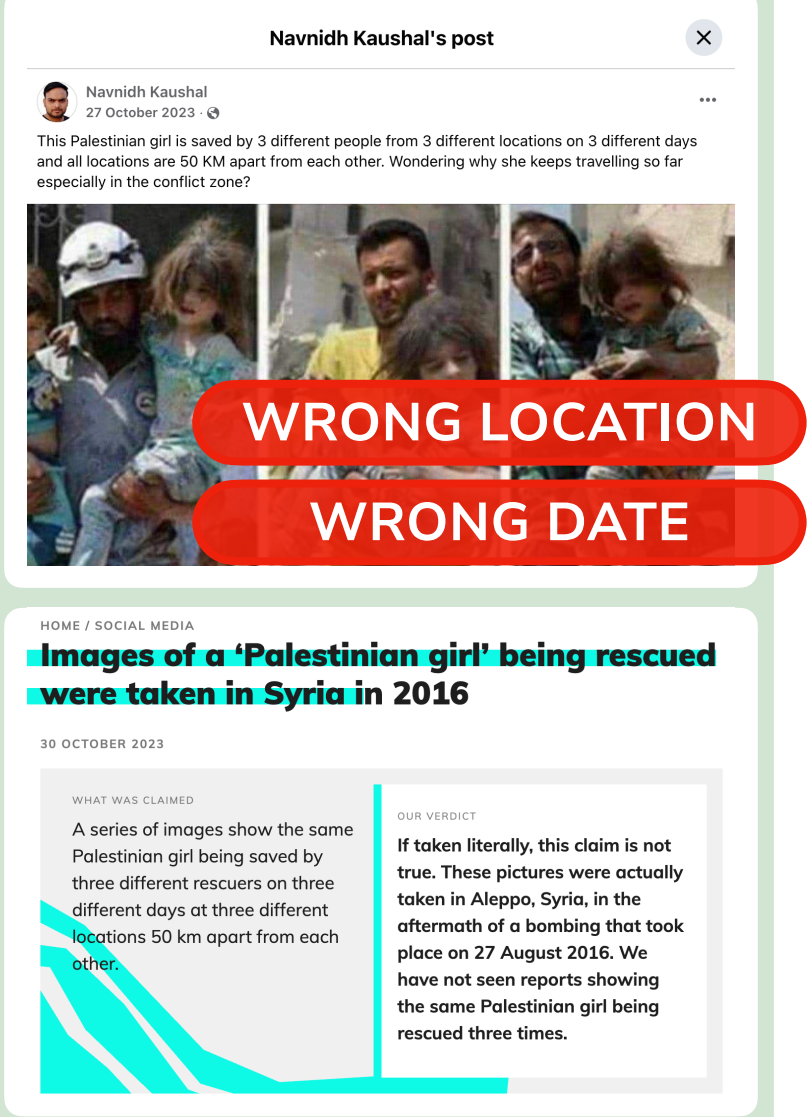
Does **Content** recontextualise material to produce a new **Narrative**?

Reframing of **Context** in Multiple Ways

Some types of context reframing commonly co-occur.

For example, historic media is often also misrepresented as depicting another location when misrepresented as showing something occurring in the present day. This can be documented using (T0162.003: Historic Content Incorrectly Presented as Current, T0162.004: Content Incorrectly Presented as Depicting Another Location).

Example



Source: https://fullfact.org/online/palestinian-girl-rescue-images/

Edited **Content**

T0162.008 Context Reframed by Edits to Media and T0162.002: Edits Made to News Report which Reframe Context may be aggregated with Sub-Techniques of T0165: Edited Content to provide more information.

For example, a video which has had its playback speed slowed to give the impression that the speaker is intoxicated can be documented using (T0162.008: Context Reframed by Edits to Media, T0165.003: Playback Speed Altered).

Deepfake Impersonation

Where T0162.006: AI-Generated Content Incorrectly Presented as Depicting Reality is a deepfake, T0166.001: Deepfake Impersonation can be aggregated with it to document this; i.e. (T0162.006: AI-Generated Content Incorrectly Presented as Depicting Reality, T0166.001: Deepfake Impersonation).

Have any common types of falsified **Content** been published?

Impersonated **Content** Attribution

T0161.001: Impersonated Content can be paired with Sub-Techniques of T0097: Present Persona to document the type of **Identity** it is presented as produced by.

For example, **Content** which falsely presents itself as being made by a news outlet can be documented using (T0161.001: Impersonated Content, T0097.202: News Outlet Persona).

Impersonated **Content** Format

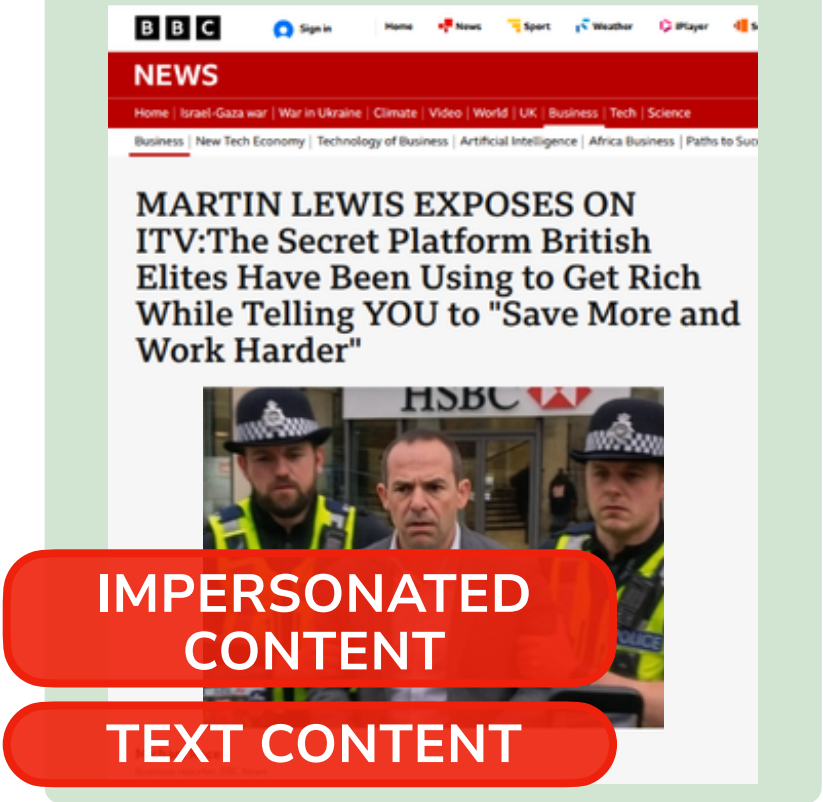
T0161.001: Impersonated Content typically comes in video format (T0087: Develop Video-Based Content) or document format (T0085.004: Develop Document).

For example, a video which impersonates a news outlet can be documented using (T0087: Develop Video-Based Content, T0161.001: Impersonated Content, T0097.202: News Outlet Persona).

Articles which are falsely presented as being produced by a news outlet can be documented using (T0085: Develop Text-Based Content, T0161.001: Impersonated Content, T0097.202: News Outlet Persona) - even if the article also contains images, it is considered text if it is primarily text based.

Example

https://fullfact.org/economy/fake-bbc-article-martin-lewis-arrested-facebook/



False Statement Attribution

T0161.001: Statement Incorrectly Presented as Made by Individual or Institution can be paired with Sub-Techniques of T0097: Present Persona to document the category of identity it is presented as made by.

For example, a statement falsely attributed to a politician can be documented using (T0161.001: Statement Incorrectly Presented as Made by Individual or Institution, T0097.110: Party Official Persona).

Uncommon Issues

Misunderstood Satirical Content

Sometimes Fact Checkers need to address or document content's origin where it was *not* falsely reframed as depicting something else, but still went on to mislead individuals. In such a case T0162.011: Content Originally Produced as Satire Presented as Not Satire would not apply - instead, T0160.005: Content Produced as Satire can be used.

Misunderstood AI-Generated Content

As above, in some cases AI-Generated content can be presented as AI-Generated and still mislead users of the internet. In such cases, T0166: AI-Generated Content or T0166.001: Deepfake Impersonation can be used instead of T0162.006: AI-Generated Content Incorrectly Presented as Depicting Reality.

Rare Issues

The following rare issues are documentable using DISARM. Analysts should use the DISARM navigator to view each Technique's description in more detail should the need arise.

- T0161.003: Falsified Graffiti or Signage
- T0163: Issues with Cited Academic Research
- T0164: Issues with Presented Statistical Evidence

Other Metadata

Analysts may aggregate other metadata alongside the issues identified above.

Content **Format***

> ***Format:** The file format content takes, i.e. Text, Image, Video, or Audio*

You can choose to identify the **Format** which content appeared in; T0085: Develop Text-Based Content, T0086: Develop Image-Based Content, T0087: Develop Video-Based Content, T0088: Develop Audio-Based Content.

News Articles may contain a combination of Text, Images and Video. Select the format which is relevant to the information you're tagging.

AI-Generated Content and Impersonated Content

Both T0166: AI-Generated Content and Impersonated Content particularly benefit from being aggregated with a **Content Format**; it's useful to know whether the T0166: AI-Generated Content or Impersonated Content is in video, audio, or image format.

For example, this allows differentiation between audio deepfakes (T0088: Develop Audio-Based Content, T0166.001: Deepfake Impersonation) and video deepfakes (T0087: Develop Video-Based Content, T0166.001: Deepfake Impersonation).

Recontextualised **Content's Format**

When observing content that has been recontextualised, the **Format** documented should refer to the **Content** which has been contextualised, rather than the **Format** that is recontextualising it. For example, if a historic *video* is posted alongside *text* presenting it as depicting current events, you would use (T0087: Develop Video-Based Content, T0162.003: Historic Content Incorrectly Presented as Current).

Relevance to Ongoing Events

Analysts have told us that it's useful to know when narratives build upon breaking news, rather than being developed outside of context of what's going on day-to-day. Analysts can add T0068: Respond to Breaking News Event or Active Crisis to an aggregate to assert that the material relates to ongoing events.

For example, a historic video recontextualised as depicting a modern conflict can be documented using (T0087: Develop Video-Based Content, T0162.003: Historic Content Incorrectly Presented as Current, T0068: Respond to Breaking News Event or Active Crisis).

Content Titling Issues

Where relevant, you can also document issues with how content has been titled:

- T0167.001: Use of Clickbait
- T0167.002: Title Misrepresents Content

Note that these Techniques don't have to apply to just news articles - videos, or even social media posts, can use deploy clickbait strategies to increase engagement.

Example

Source: https://www.rappler.com/newsbreak/fact-check/fact-check-justin-bieber-alive/

Fact Check Outcome

Incident Outcome

If your Fact Check has an assertion, you can map it to DISARM Techniques:

- T0160.001: Information is Verified
- T0160.002: Information is False
- T0160.003: Information is Misleading
- T0160.004: Information is Unverifiable

Historic Associations

You can document whether the content or claim addressed in this incident has been encountered previously with (T0160.006: Content Previously Fact Checked) and (T0160.007: Claim Previously Fact Checked) respectively.

**Claim:* The claim that is made by the content posted*