Mapping DISARM RED to Meta's Online Operations Kill Chain

This document is intended to support analysts who intend to map Meta's Online Operations Kill Chain (MOOKC) to the DISARM Red framework. This document will be expanded as new techniques are added to the DISARM Red framework as part of our efforts to increase interoperability of the frameworks.

MOOKC framework items assert multiple things at once; for example *1.2.2. Posing as fictional journalist* implies both that an account is presenting a fabricated persona, and that they are presenting as a journalist. Based on feedback from DISARM's user community, new DISARM techniques will (as far as is possible) assert one thing at a time. This approach avoids situations where analysts feel they cannot apply a DISARM technique if the behaviour they are seeing doesn't match all criteria in a given technique. While Meta's analysts have access to detailed technical indicators which can help them confidently assert that personas are fabricated, analysts without this data are less able to discern the legitimacy of a persona without further investigation.

As such, DISARM provides separate techniques for asserting which persona an asset is presenting (*T0097: Presented Persona*'s sub-techniques), and for asserting whether the persona is legitimate (*T0143: Persona Legitimacy*'s sub-techniques). This approach gives analysts the versatility to document other types of personas, including authentic personas (*T0143.001: Authentic Persona*) and parody personas (*T0143.004: Parody Persona*).

Where MOOKC framework items assert more than one thing about an asset, there will be more than one DISARM Red technique required to make the same assertion. For example, *1.2.2. Posing as fictional journalist* maps to DISARM Red's *T0097.102: Journalist Persona* and *T0143.002: Fabricated Persona*.

The table below shows how you can use DISARM Red techniques to make the same assertions made by each MOOKC framework item.

1. Disguising Assets

MOOKC item	DISARM Red Mapping
1. Disguising assets	*Techniques contained in MOOKC's Disguising Assets are housed in DISARM Red's TA15: Establish Assets and TA16: Establish Legitimacy*
1.1. Adopting visual disguise	T0145: Establish Account Imagery
1.1.2. Copying profile pictures	T0145.001: Copy Account Imagery
1.1.3. Using profile pictures created using generative adversarial networks (GAN)	T0145.002: AI-Generated Account Imagery

1.1.4. Adopting Visual Brand	*This MOOKC item has not yet been mapped to DISARM Red*
1.1.5. Using animals as profile picture	T0145.003: Animal Account Imagery
1.1.6. Using scenery as profile picture	T0145.004: Scenery Account Imagery
1.1.7. Using cartoon as profile picture	T0145.005: Illustrated Character Account Imagery
1.2. Posing as non-existent person	T0097.100: Individual Persona and T0143.002: Fabricated Persona
1.2.1. Posing as person seeking romance	T0097.109: Romantic Suitor Persona (and, if posing as a non-existent person, T0143.002: Fabricated Persona)
1.2.2. Posing as fictional journalist	T0097.102: Journalist Persona and T0143.002: Fabricated Persona
1.2.3. Posing as fictional activist	T0097.103: Activist Persona and T0143.002: Fabricated Persona
1.2.4. Posing as fictional hacktivist	T0097.104: Hacktivist Persona and T0143.002: Fabricated Persona
1.2.5. Posing as fictional military personnel	T0097.105: Military Personnel Persona and T0143.002: Fabricated Persona
1.2.6. Posing as fictional recruiter / potential employer	T0097.106: Recruiter Persona and T0143.002: Fabricated Persona
1.2.7. Creating fictitious byline	*This MOOKC item has not yet been mapped to DISARM Red*
1.2.8. Posing as fictional person in target region	T0097.101: Local Persona and T0143.002: Fabricated Persona
1.3. Posing as non-existent institution	T0097.200: Institutional Persona and T0143.002: Fabricated Persona
1.3.1. Creating fictitious news outlet	T0097.202: News Outlet Persona and T0143.002: Fabricated Persona
1.3.2. Creating fictitious NGO	T0097.207: NGO Persona and T0143.002: Fabricated Persona
1.4. Impersonating real person	T0097.100: Individual Persona and T0143.003: Impersonated Persona
1.4.1. Impersonating researcher or think tanker	T0097.204: Think Tank Persona and T0143.003: Impersonated Persona, T0097.107: Researcher Persona and T0143.003: Impersonated Persona
1.4.2. Using duplicate accounts	*This MOOKC item has not yet been mapped to DISARM Red*
1.5. Impersonating real institution	T0097.200: Institutional Persona and T0143.003: Impersonated Persona

1.5.1. Impersonating news website	T0097.202: News Outlet Persona and T0143.003: Impersonated Persona
1.5.2. Impersonating government institution	T0097.206: Government Institution Persona and T0143.003: Impersonated Persona
1.5.3. Impersonating think tank	T0097.204: Think Tank Persona and T0143.003: Impersonated Persona
1.5.4. Impersonating commercial company	T0097.205: Business Persona and T0143.003: Impersonated Persona
1.6. Disguising malware sites [x5]	*These MOOKC items have not yet been mapped to DISARM Red*
1.7. Disguising malicious apps [x3]	*These MOOKC items have not yet been mapped to DISARM Red*
1.8. Backstopping	T0144: Persona Legitimacy Evidence
1.8.1. Backstopping fictitious individual across multiple websites	T0144.001: Persona Presented across Platforms and T0097.100: Individual Persona
1.8.2. Backstopping fictitious brand or organisation across multiple websites	T0144.001: Persona Presented across Platforms and T0097.200: Institutional Persona