Internet Intelligence & Investigations Guidance

III Covert Profiles

Security classification: OFFICIAL
Disclosable under FOIA 2000: YES
Author: Peter Lloyd, Capability Advisor
Force/organisation: NPCC, Internet Intelligence & Investigations Working Group

Owner	CC Carl Foulkes / III Working Group
Version Number	V 0.2
Date Published	Draft

Compliance Record

Version Control Table

Version	History of Amendments	Approval Date
0.1	First draft	
0.2	Minor amendments made after feedback	
0.3		
04.		
0.5		

Table of Contents

1. Purpose

1.1 The purpose of this document is to provide guidance and clarity with regard to the creation, deployment and recording of Internet Intelligence & Investigations (III) Covert Profiles. This guidance should be read in conjunction with the NPCC III Strategy Document and any local policy or guidance. **Local policy and guidance will always take precedence.**

2. Introduction

2.1. The NPCC III Strategy Document sets out a clear Capability Delivery Model which sets out three capability descriptors;

- Core Internet Use
- Internet Investigations, and
- Covert Internet Investigations

2.2. The use of III Covert Profiles sit firmly with the Covert Internet Investigations capability descriptor. Covert Internet Investigations is defined as;

- A structured, methodical, task driven and planned approach to covert online research, conducted by a suitably trained (and current) individual. When authorised, activities which fall into this capability descriptor include but are not limited to;
  - Facilitate covert access to closed and private group and areas
  - Covertly gather evidence and intelligence
  - Conduct online surveillance of a known subject or group
  - Facilitate the deployment of additional on line covert tactics

2.3 Covert Internet Investigations incorporate a wide range of tactics and capabilities which allow practitioners to add significant value to many enquiries. A small part of this is the research and analysis of Social Media and Social Networking platforms. Although the option to deploy III Covert Profiles is open to those that are suitably trained, there are a number of considerations which will impact on the selection of an appropriate strategy and the use of specific tactics and tradecraft, before it is deployed.

2.4 Whilst there are numerous Social Media and Social Networking platforms each with their own configuration and security settings, this document will highlight key points for consideration prior to deploying an III Covert Profile, and providing guidance on the creation and management of such profiles. This document will not provide a detailed step by step instruction on the creation of profiles for every relevant platform.

2.5 The use of III Covert Profiles is only one tactic available to a trained 'Covert Internet Investigations' practitioner. Prior to commencing any covert online investigation it is imperative that an investigative strategy is created and decision log maintained. The agreed tactics, use of III Covert Profiles, rationale and risks considered should be recorded accordingly.

2.6 The use of any covert tactics will require consideration with regards to the requirement for specific activity to be authorised. The creation and deployment of III Covert Profiles will not automatically necessitate an authority, under the Regulation of Investigatory Powers Act (2000), to be in place. This document will outline general accepted practice in this area however practitioners should **always be aware of, and follow, local policy, guidance and instruction.**

2.7 The III Strategy utilises a definition for covert which is derived from that used in the Regulation of investigatory Power Act 2000 (Part II, Section 26 (9)).

> Online activity is covert if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the online investigation are unaware that it is or may be taking place.

3. Internet Intelligence & Investigations Covert Profiles

3.1. Although overt and covert are binary terms, covert itself covers a spectrum of efforts, tradecraft and processes to conceal, obfuscate or otherwise misattribute activity. Historically the terms false persona, grey, ghost, platform access accounts and many others have been used to distance practitioners from the term covert and the subsequent rigour that operating covertly requires.

3.2. The III Strategy provides a simple and all-encompassing definition for III Covert Accounts which acknowledges that any activity carried out in a manner calculated to be covert, is covert. The definition of an III Covert Profile is provided below;

> **III Covert Profile** – Any profile designed or created to obfuscate the fact it is being used for a policing purpose. This includes accounts which have minimum details, with obvious fictitious names, such John Doe etc.

3.2 To avoid confusion, and recognise the considerable implications of using covert profiles, any terms other than III Overt Profile or III Covert Profile are discouraged.

4. Creation of III Covert Profiles

4.1 The nature of the enquiry, capability of the subject of interest and the impact of any compromise, will have a significant impact on the efforts and length take to create an III Covert Profile.

4.2 An III Covert Profiles can range from merely using a fictitious username or vanity name to a supporting a full covert legend [1]with multiple synchronised profiles across numerous platforms, utilising dedicated devices and internet connections which all reflect and uphold a detailed back story.

4.3 The practitioner should have a thorough understanding of the nature of the investigation, the potential capability of subject of the investigation, and have completed assessment of potential risk prior to creating an III Covert Profile for a specific investigation. This risk assessment, and the professional judgement of the practitioner, will inform the level of effort required for the creation and subsequent maintenance of an III Covert Profile.

4.4 This section will examine some of the areas to be considered when creating an III Covert Profile. This list is not exhaustive and practitioners must consider all aspects, potential risk and options when creating an III Covert Profile.

4.5 As previously mentioned the nature of an III Covert Account can range significantly from a simple anonymised user name to a full covert legend. It also important to note that III Covert Profiles can portray people, businesses, groups etc. This guidance will focus on the creation and maintenance of a covert legend. Practitioners should scale their effort to meet the needs of the investigation.

5. Pen Picture

5.1 A credible covert legend will require a number of profiles on different online platforms which appear to reflect the personal likes, beliefs and interests of a real person. To ensure a covert legend is consistent and as realistic as possible it is important to create a pen picture of the entity you are creating.

5.2 By creating a detailed pen picture of the entity you are creating you can ensure that there are consistencies, or engineered inconstancies, across the various platforms and III Covert Profiles. The pen picture should include basic details such as full name and nicknames used, date of birth and area of residence, gender etc. The pen picture can however extended to many other aspects, such as sexual orientation, political or religious beliefs, hobbies etc.

5.3 It is advisable to maintain and update the pen picture through the life of the legend.

5.4 Although there may be an operational reason to develop a legend which has extremist or controversial views or beliefs. Wherever possible it is advisable to keep the legend and their associate profiles, as bland and uncommitted as possible. This will allow the practitioner to flex the legend as required by the operation.

6. Profile Creation

[1] A Covert Legend is a synchronised group of covert profiles which all support and portray a single entity.

6.1 **Profile Names & Vanity Names** – There are few hard and fast rules about selecting a username or vanity name for an III Covert. Generally a profile should not reflect the persona of a real person either alive or dead. After selecting a profile or vanity name it is always good practice to undertake some online research to ensure there are no obvious issues with selected name. Controversial, funny or otherwise notable names should be avoided unless they are used deliberately as part of the covert legend or investigative strategy.

6.2 **Email Addresses / Telephone Numbers** – Where the practitioner wants to create a simple anonymised profile, a basic email address from a free email provider will almost certainly suffice. The reuse of email addresses and phone numbers across a number of simple anonymised profiles will normally not raise any issues.

6.3 Where the practitioner is creating a profile to support a Covert Legend then additional steps should be considered. Email addresses and telephone numbers should not be shared across profiles, from different legends, unless this part of the investigative strategy.

6.4 **Bio and Descriptions** – Where biographies and descriptions feature within a platform, where applicable, they should be completed in line with the associated legend. As a rule, unless the investigative strategy, directs otherwise it is usually better to avoid providing additional unnecessary information. If additional information is used, consideration should be taken that any information could easily be checked or verified online by a subject of interest or third party.

6.5 **Security Settings –** With regard to a simple anonymised profile, it is advisable to secure the account as much as possible. The security setting for a profile linked to a Covert Legend will be directed by the nature of the legend and investigative strategy. Security settings can change on platforms without knowledge, they should be reviewed on a periodic basis. Accounts should also be looked at from an external perspective to see what information can be determined or extracted.

6.6 **Communications** – A simple anonymised profile should not be used for any form of communication or interaction. A fully developed covert account can be used for minimal communication however extreme care should be taken not to stray into the realms of a Covert Human Intelligence Source (CHIS). **Local policy and guidance will always take precedence.**

6.7 **Account maintenance** – On some platforms to maintain a profile, it must engage with other users, pages, groups or risk being deleted. If this is required, then it can be deemed acceptable to like and share routine posts that fit with the pen picture of the profile. The liking and sharing of extreme or controversial content should be avoided unless it is in support of an investigative strategy. Comments on content can be made, in line with the Covert Legend however care should be taken not to stray into direct communication and the forming of any form of relationship. Any activity of this nature should be recorded and the rationale of use be justified.

6.8 **Friends / Following / Connections –** Covert Profiles can be used to send and accepted connection requests. However caution should be used to avoid stepping over the thresholds of Directed Surveillance, Covert Human Intelligence and Undercover Online activity.

6.9 When a connection is being made simply to build and maintain a profile then the 3rd party profile should be selected carefully. Although the nature of the Covert Profile and the Investigative Strategy should provide some guidance in relation to 3rd party profile selection, in general it is usually better to select a 3rd party account which already has large number of connections.

6.10 Selecting a 3rd party account which has some synergy with the Covert Legend may reduce the potential for 3rd party to instigate a conversation. Any attempt at a conversation must be closed down, to avoid straying into the remit of Undercover Online activity. Where the likelihood of a subject attempting to engage in conversation is deemed high then it may be advisable utilise a trained UCOL officer to conduct this activity. An Authorising Officer should always be consulted, even where a CHIS authority is not deemed necessary.

6.11 A Covert Profile can be used to make connections, in line with the Investigative Strategy, to facilitate the gathering of information, intelligence or evidence which would otherwise not be available. Please note that such activity may require a Directed Surveillance Authority. See Section 10, below.

6.12 When a connection is being made to progress the Investigative Strategy, it is often advisable to connect with a number of associates of the subject, prior to considering connecting with the subject themselves. Subject to appropriate authority, consideration should also be given to deploying more than one Covert Legend, for any covert enquiry. Approaching the subject with multiple accounts, from different routes, will provide resilience to operation and gives an increase likelihood of success.

7. Recording

7.1 The deployment of an III Covert Profile with often require a Directed Surveillance Authority to be in place. The specific information and detail required to be recorded as a result of a DSA will be dealt with separately.

7.2 The appropriate recording of activity in relation to the creation, deployment and maintenance of III Covert Accounts is critical. Although there is no legal requirement it is advisable that forces (or agencies) have a method of approving and recording the creation and maintenance of III Covert Accounts.

7.2 Although not exhaustive it is advisable the following information is recorded in relation to III Covert Profiles;

- Details of creation
    - Approved by
    - Approved date
    - Details of Profile / Legend
- Details of deployment
    - Date of deployment
    - Deployed by
    - Subject of deployment
    - Details of deployment
    - Any risks identified or compromise
    - Record of activity
- Details of maintenance
    - Approved maintenance activity
    - Record of activity
- Details of deletion
    - Deletion instructed / approved by
    - Deletion conducted by
    - Record of deletion

8. Compromise

8.1 Despite a practitioner taking all possible precautions and mitigating risks wherever possible, the potential for an account to become compromised will always exist.

8.2 Whilst it is important to record and report all compromises it is equally important that a practitioners actions do not confirm or further exacerbate the situation.

8.3 It is relatively common that new online accounts, which enter a closed area or group, are accused of being utilised by Law Enforcement. The practitioner's response to such accusation is key to a compromise either being confirmed or avoided.

8.4 A response, in character with the established legend, to refute, ridicule or otherwise divert the accusation will often placate or dismiss the comment. Care should be taken, with regard to the response not to enter into a conversation or in any way create a relationship.

8.5 The deployment of multiple profiles can sometimes be utilised to provide support when refuting such allegations, however extreme caution should be taken that such a strategy does not result in additional profiles also being compromised.

8.6 Alternatively, subject to appropriate authority, additional profiles can be utilised to monitor any discussion about the suspect compromised profile.

8.7 Where the practitioner believes that a compromised, has occurred there are various action that are open to them.

- Withdrawing and closing the profile will only confirm what could be a speculative accusation.
- Leaving the account in place could be used to disrupt the online criminal activity
- Withdrawing the account from the group or page or the compromise and continuing to maintain the account could be seen as the most likely actions of a genuine account.

8.8 All compromises should be recorded in line with force or agency procedures.

9. Risks & Considerations

9.1 It should always be noted that the practitioner has a duty of care to any 3rd parties which they connect with. The impact and safety of a 3rd party must be considered at all times. Connecting with a subject can potentially poses a risk to the Covert Profiles 3rd party connections, by way of introducing them to SAOC that they wouldn't otherwise be exposed or through retribution if the Covert Profile is compromised.

9.2 Although this list is not exhaustive, the risk to 3rd parties can be mitigated by:

- Ensuring the Covert Profile has sufficient 3rd party connections for no connection to be singled out for retribution
- Selecting 3rd party connections who are geographically and demographically diverse from the subject
- Selecting 3rd party connection who have numerous (1000+) and varied connections

9.3 On completion of a deployment consideration should be given to reviewing and potential removing connections.

9.4 There is nothing to prevent an III Covert Profile being deploy on a series of unconnected operations. However care should be taken not continue surveillance on unauthorised subjects or create a link between subjects that wouldn't otherwise exist. It is always good practice to have a period of time between deployments, where a covert legend can be simply maintained, and kept current.

9.5 To assist with managing collateral intrusion consideration should be given to utilising a platforms security setting to reduce the number of updates from those not subject of the investigation. Some platforms allow updates from specific connections to be blocked whilst retaining the connection.

10. RIPA Guidance

10.1 This guidance should be read in conjunction with the Home Office Codes of Practice and any local policy or guidance. All online covert activity must be conducted in accordance with the directions included in any relevant authorisation.

10.2 All practitioners who conduct Covert Internet Investigations must be familiar with the content of the following;

- The Regulation of Investigatory Powers Act 2000 (RIPA)[2]
- Covert surveillance and property interference code of practice
- Covert human intelligence sources code of practice

10.3 Both codes of practice, mentioned above, contain specific guidance in relation to online activity, however the documents must read and guidance applied in full.

10.4 It can be helpful to view RIPA as a tool to provide protection to the practitioner, rather than an instrument that provides permission.

10.5 The key points for any practitioner to consider in relation to the application of authorities – What am I doing and why and I doing it?

10.6 The initial research of social media to identify a potential threat, establish facts, confirm the availability of goods or services; or corroborate an intelligence picture is unlikely to require an authorisation for directed surveillance; whereas repeated visits, building up a profile of a person's life style or the nature of a group's activities would do so.

10.7 Each case must be considered on its individual circumstances and early discussion between the investigator, the RIPA Co-ordinator and the Authorising Officer is advised to determine whether activity should be conducted with or without the protection of an authorisation. If the aim is to gathering evidence/intelligence against specific individuals from the outset, then it may be appropriate to have a DSA before any activity is commenced.

10.8 It should be noted that the systematic monitoring of a personal profile, even where the profile is open and an Overt III Profile is used, will be considered to be directed surveillance, if it is not clear to the subject that such activity is taking place. Due to the requirement for Regulation of Investigatory Powers Act 2000 (RIPA) authorisation this activity falls within Covert Internet Intelligence & Investigations.

10.9 The use of III Covert Profile will not automatically require a DSA, however consideration must always be given to what activity is planned and what the objective of the activity is.

10.10 As previously mentioned the use of a connection requests does not automatically amount to directed surveillance but is another step forward towards the trigger of consideration. Using a friends request to join a large selling group on Facebook with 100's or 1000's of followers to assess the availability of illegal money lending would unlikely need a DSA. If your research had identified a very tight closed group offering loans where you believed the principle only had a handful of trusted and referenced in members, the requirement for the protection of a DSA is much more likely.

[2] The Regulation of Investigatory Powers (Scotland) Act (RIP(S)A) 2000 in Scotland

10.11 The practitioner, and supervisor must always be alert to the risk that such a connection can, if not managed properly, develop into a relationship requiring CHIS Authorisation.

11. Summary

11.1 The creation and deployment of III Covert Profiles is one tactics which fall into the capability descriptor 'Covert Internet Investigations'. This work should only be conducted by suitably trained individuals and in accordance with any local policy and guidance.

11.2 Online platforms can change security settings and information visibility on an ad hoc basis, so any covert profile created should be checked periodically to ensure it is still valid and has the same settings in place to support its use.

11.3 The nature and effort required to create and maintain an III Covert Profile will range significant and should be driven by the relevant risk assessment and investigative strategy.

11.4 This document provides some general guidance on the creation, maintenance and deployment of III Covert Profiles.