Internet Intelligence & Investigations Strategy

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

Owner	CC Carl Foulkes
Version Number	V 1.3
Date Published	17/10/2019

Compliance Record

Version Control Table

Version	History of Amendments	Approval Date
0.12	First draft	
0.13	Additional clarity around naming convention for Capability Descriptors	
1.0	Agreed version 1.0 published	27/04/2018
1.2	Downgraded protective marking to Official	10/12/2018
1.3	Addition of Principles / Doctrine Definitions of Overt and Covert Profiles Requirement for an III Investigative Strategy for Internet Investigations and Covert Internet Investigation	17/10/2019

Table of Contents

1. Purpose 4
2. Introduction 4
3. Internet Intelligence & Investigations 4
4. Principles / Doctrine 5
5. Capability Delivery Model 5
9. People 9
10. Technology 10
11. Processes 11
12. Personal Use of the Internet & Social Media Sites 11
13. Disclosure 12
14. Governance 12
11. Appendix ‘A’ 13
12. Appendix ‘B’ 14

1. Purpose

1.1 The purpose of this document is to provide clarity to the capability referred to as 'Internet Intelligence & Investigations' and outlines what activity is appropriate with regard to accessing information, on the internet, for a policing purpose.

2. Introduction

2.1. The internet, and in particular social media sites, are a rich and cost effective source of intelligence and information which can be of significant evidential value. Law enforcement agencies should actively encourage its employees to make use of the internet when conducting their enquiries, whenever it is appropriate for them to do so.

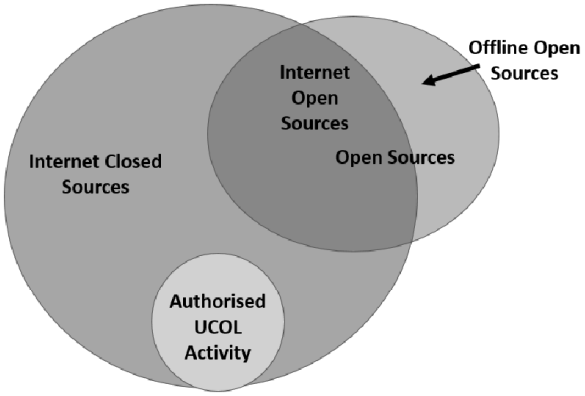
2.2. To ensure a professional, lawful and ethical approach to Internet Intelligence & Investigations a Capability Delivery Model has been devised. This delivery model groups activities into Overt or Covert tactics. The Capability Delivery Model is outlined later in this document (See para 4.1)

2.3. In providing detail about the Capability Descriptors, this paper aims to provide the necessary information to ensure officers are able to conduct internet enquiries, at an appropriate level, in a professional manner, without bringing adverse risk to their force or agency or having evidence excluded from court.

2.4. This document does not cover overt community engagement through social media or Undercover Online (UCOL) authorised activity, both fall into the remit of separate capability leads.

3. Internet Intelligence & Investigations

Figure 1. Defining the remit of Internet Intelligence & Investigations[1]



[1] *Visual representation only – Scale is not indicative of crossover

3.1. Internet Intelligence & Investigations (III) is defined as;
'The use of internet resources to gather information, intelligence and evidence.'

This includes but is not limited to, the use of overt and covert tactics to;

- Access areas which would otherwise be closed
- Gather metadata on individuals' activity through deployment of online resources
- Monitor social media or other online activity of a group, individual or relevant geographical area

3.2. As indicated in Figure 1, III includes many activities which could be considered Open Source Intelligence (OSINT) however it excludes the offline aspects of OSINT. III also includes closed sources which would not fall into the OSINT definition.

3.3. In the majority of cases, the most appropriate method for securing evidence or intelligence from social media sites, blogs and other online applications will be through internet investigations. Additionally, there is significant legislation which impacts the way Law Enforcement and other agencies are able to conduct enquiries using the internet.

3.4. Intelligence gathered from openly available information on the internet or elsewhere is often referred to as OSINT (Open Source Intelligence). Although this information is referred to as Open Source, all activity intended to gather intelligence for a policing purpose, from whatever source, must be compliant with current legislation. See Appendix A.

3.5 OSINT remains a valid and valued tool for online research however it is just one of many tools which an Internet Investigator can call upon. For clarity, and to avoid confusion, within this document all online activity is referred to as Internet Intelligence & Investigations and no further reference will be made to OSINT.

4. Principles / Doctrine

4.1 III is a core capability for all investigators involved in any form of investigation and touches on all threat areas.

4.2 Operating covertly on the internet should not be the default position. III activity will not be conduct covertly unless it is proportionate, necessary and justified.

5. Capability Delivery Model

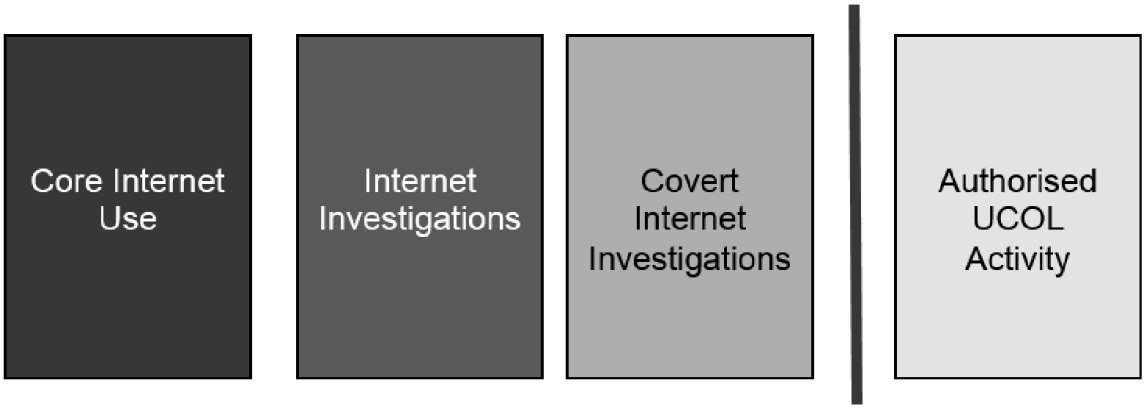
5.1 The Capability Delivery Model provides clarity around training requirements and authorisation of covert activity online. It supports both practitioners and managers providing them with a simple and straight forward framework.

5.2 The Capability has been split into Overt and Covert activity. Overt activity is further sub divided into 'Core Internet Use' and 'Internet Investigations' to distinguish between ad hoc internet use and the structured, methodical approach to internet research by suitably trained professionals. This creates the unique three Capability Descriptors displayed in figure 2;

Figure2. The Capability Delivery Model

Internet Intelligence & Investigations

Internet Intelligence & Investigations



**Note - 'Covert Internet Investigations' does not include authorised Undercover Online (UCOL). This activity falls under the remit of the UC Capability Lead.*

5.3 The skill sets which support the Capability Delivery Model and sit under each of the Capability Descriptors are outlined in the Capability Delivery Model Skill Matrix, see appendix B[2]. The Capability Delivery Model Skills Matrix is a living document and will be reviewed and update as required by the NPCC III Working Group.

5.4 All three Capability Descriptors are further defined below

6. Core Internet Use

6.1 The internet is now a fundamental part of everyday life it is accepted that all law enforcement employees should have access to the internet and in particular the World Wide Web (www). All staff should receive internet safety training to ensure their activity does not exceed their remit or risk compromise.

6.2 'Core Internet Use' is the overt and ad hoc use of online resources and search engines to provide basic information. This includes, but is not limited to;

- Capturing online evidence highlighted by a complainer or witness
- Accessing online mapping facilities in preparation for executive action.

[2] The Skill Matrix is a living document will be saved as a separate appendix

- Utilising online data sources such as 192.com, Companies House, Local Government Planning Departments etc.

6.3 Under 'Core Internet Use' individuals will not access areas of the internet which require a username and password, unless accessing an authorised site using official log in details.

7. Internet Investigations

7.1 'Internet Investigations' (Non-Covert) is a structured, methodical, task driven and planned approach to online research, conducted by a suitably trained *(and current)* individual[3]. Activities which fall into this capability descriptor include but are not limited to;

- Using overt profiles to log into and access platforms
- Utilising advanced search techniques to conduct systematic and focused research.
- Monitoring online activity in relation to pre-planned and spontaneous events
- Capturing intelligence and or evidence in support of an ongoing investigation.

7.2 No covert tactics will be used for Internet Investigations. Where a username and password is required to access an online space the credentials provided must reflect the fact that the account / profile is being utilised for a policing purpose and a record kept of all activity conducted.

7.3 No Activity requiring authorisation under Regulation of Investigatory Powers Act 2000 (RIPA), or other covert authority, will be conducted under the capability 'Internet Investigations'.

7.4 It should be noted that the systematic monitoring of a personal profile, even where the profile is open and an overt Police account 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.

7.5 Certain restrictions on the corporate web browsers, and the technical implications of utilising a fixed IP address, may mean that overt searches will need to be conducted using internet connectively out of the normal Police network and infrastructure.

7.6 Profiles created to conduct 'Internet Investigations' must clearly indicate that they are being utilised for a policing purpose. Such profiles will be referred to as **III Overt Profiles**. The definition of an III Overt Profile is provided below;

[3] The minimum knowledge, skill and competency required for each Capability Descriptor will be outlined in the Skill Matrix – Appendix B

III Overt Profile – A profile designed and created to clearly indicate it is used for a policing purpose. Such accounts should include a disclaimer to state that it is not a crime or incident reporting tool and is not monitored for public engagement.

7.7 III Overt profiles may also include a relevant crest or force logo as a profile picture. The 'vanity name' should clearly indicate its use by Law Enforcement.

7.8 It should be noted that there is no suggestion that such account should include personally identifiable information relating to the investigator using it.

7.9 Providing appropriate records are kept, these accounts can be shared between investigators.

8. Covert Internet Investigations

8.1 Covert Internet Investigations is 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

8.2 Covert Internet Investigations will only be conducted by personnel who are suitably trained *(and current)* and have been expressly authorised by the relevant force or agency.

8.3 Covert Internet Investigations tactics will only be utilised after all other reasonable, less intrusive, methods have been considered and it is proportionate and justified to do so.

8.4 As mentioned in paragraph 6.4 above, the systematic monitoring of a personal profile, even where the profile is open and an overt Police account 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 RIPA Authorisation this activity will fall within Covert Internet Intelligence & Investigations.

8.5 Covert Internet Investigations research will always require a Direct Surveillance Authority, or other covert authority, to be considered. Where an authority is deemed as not required, the rationale for this decision should be recorded.

8.6 Individuals conducting Covert Internet Intelligence & Investigations will routinely utilise covert accounts or profiles, obfuscated internet connections and suitable hardware. 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 factious names, such John Doe etc.

8.7 It is acknowledged that maintaining the covert aspect of online activity can be complex and involves a wide range of tactics and processes being employed to minimise the risk of compromise. Practitioners must be satisfied that the effort taken to maintain the covert nature of their activity meets the level necessary for the individual task, and associated risk of compromise. Measures taken to ensure the covert nature of the activity is not compromised, should be assessed against the subject's capability, the nature of the crime or event being investigated, and the impact of inadvertent compromise.

8.8 Covert Internet Investigations does not include authorised UCOL activity. Such activity falls into the remit of the Undercover Capability which has separate policy and guidance.

9. People

9.1 It is expected that all officers and staff will be provided with sufficient training to undertake 'Core Internet Use', however it is anticipated that the capability and competency of individuals will vary significantly.

9.2 A minimum standard of competency for all three capability descriptors will be identified and maintained by the Internet Intelligence & Investigations Working Group. These minimum standards will not only identify required training but will also include relevant Continuous Professional Development.

9.3 It should be noted that the Capability Descriptors are not job descriptions. Individuals trained, and competent at undertaking Covert Internet Investigations will also undertake tasks which fall into the capability descriptors for either' Internet Investigations' or 'Core Internet Use'.

9.4 As we transition from the five level model to the new Capability Delivery Model, local management will be responsible for measuring current investigators competency against the new minimum standards. Where an individual meets or exceeds competency in all the required capabilities for either 'Internet Investigations' or Cover Internet Investigations they will be considered trained to that level. Once assessed, individuals will thereafter be required to undertake the necessary CPD as outlined by the Working Group.

9.5 As mentioned in paragraph 4.3 above the Capability Delivery Model Skills Matrix sets out a minimum standard of capability and competency will be agreed for each of the three capability descriptors. The Capability Delivery Model Skills Matrix will be a living document maintained by the NPCC III Working Group, and will reflect the changing environment of online policing.

9.6 Where appropriate, individuals will be encouraged to develop their capability and competency beyond the minimum standard. The framework allows for individuals to be recognised as advanced practitioners or subject matter experts for particular skills or tradecraft.

10. Technology

10.1 Generally, all police officers and police staff have access to their force or agencies intranet through a personal login. Access to the internet on these networks is generally facilitated through an internet connection delivered by a commercial Internet Service Provider (ISP). This internet connection is, in the main, delivered using a static IP address. Freely available online resources will resolve this static address to the individual police force or agency.

10.2 Force or Agency networked computers must not be used for 'Covert Internet Investigations', unless an appropriate portal solution is provided. The portal solution allows obfuscated internet access through use of independent internet connectivity and virtualisation techniques.

10.3 Where local policy allows, Force or Agency networked computers can be utilised for 'Core Internet Use' and 'Internet Investigations' however the impact of the use of a static IP and corporate browser must be understood by the practitioner.

10.4 Those conducting Internet Intelligence & Investigations should be aware that on every occasion a computer accesses the internet it will leave a footprint. The footprint will include the IP address being used and may also include additional information such as the type of device being used, software installed on that device, and information held within the 'clipboard' of the device. Providers of websites and applications can, and will, record the IP addresses of persons using their services. For the most part this is not a threat to Law Enforcement conducting overt enquiries as the information, if gathered, is mainly used for commercial purposes etc.

10.5 Less scrupulous website providers may use this information to identify Law Enforcement Officers who are conducting enquiries on overt Police computers. Where this activity is for a lawful policing purpose and no security has been overcome, or falsehood used to enter the site, this should not limit our investigations.

10.6 Investigators should be aware that where they are identified as a Law Enforcement employee by such a site, then the possibility of being provided misinformation cannot be ruled out.

10.7 To avoid the risk of compromise, devices used to access the internet for 'Core Internet Use' and 'Internet Investigations' should not be used for 'Covert Internet Investigations'. Where the force or agency utilises a 3rd party supplier to facilitate

covert access to the internet, the force should satisfy themselves that the solution offers the appropriate level of protection.

11. Processes

11.1 All individuals conducting any online activity must be in a position to record, and bear witness to, any content which they observe. To this end no online activity should be conducted by individuals who are considered 'firewalled' from appearing at court.

11.2 Processes must be in place to allow practitioners to appropriately record and capture any online content which may contain material, both inculpatory and exculpatory, that is of evidential value[4].

11.3 The capability 'Core Internet Use' will ensure that all officers and staff can access and research the internet and may have positive impact when access is required for an ongoing incident or enquiry.

11.4 It should be noted that whilst 'Core Internet Use' may provide easy access for time critical incidents the competency of individuals at this level will vary widely. Where the threat, risk or harm associated with the incident dictates, it may be prudent to escalate the task to an individual trained to Overt or Covert Internet Intelligence & Investigations. This is particularly relevant with High Risk Missing Persons or incidents where life is at risk.

11.5 On every occasion where online research or investigations are undertaken at 'Internet Investigations' or 'Covert Internet Investigations' level an III Investigative Strategy will be agreed and a decision log maintained.

12. Personal Use of the Internet & Social Media Sites

12.1 Whilst this document is aimed at the use of the internet for a policing purpose, it is important to understand that, in order to protect the privacy and safety of officers and staff, and their family, as well as maintaining evidential and professional integrity, social media and internet accounts used for policing purposes must be separated from those used for personal social networking.

12.2 No online activity, for a Policing purpose, should be conducted on employees personally owned devices. Such activity risks compromise and risks the personal safety and privacy of the employee, their family and associates.

[4] Work is currently ongoing to establish a set of standards with regard to evidence capture and recording of online activity.

13. Disclosure

13.1 All Police officers and Police staff conducting Internet Intelligence & Investigations must be aware of their obligations with regard to disclosure. All records of activity and captures made must be stored securely, in accordance with their Force or Agency's local guidance.

14. Governance

14.1 The capability is governed by a NPCC Internet Intelligence & Investigation Working Group, chaired by the Capability Lead CC Carl Foulkes. The Working Group operates in line with the agreed Terms of Reference.

11. Appendix 'A'

List of Associated Legislation

- Police and Criminal Evidence Act 1984 (PACE)
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A)
- Computer Misuse Act 1990
- Data Protection Act 1998
- Police Act 1997
- Criminal Justice and Licensing (Scotland) Act 2010

12. Appendix ‘B’

III Skills Matrix

The III Skills Matrix is a living document and will be produced as a separate paper, the most current version will be placed on POLKA.