Priority	Priority
Date/time required by	26 March 2020 00:01

APPLICATION FOR A TARGETED EQUIPMENT INTERFERENCE WARRANT UNDER INVESTIGATORY POWERS ACT 2016

Addressee:

To	Lynne Owens
Cc	

Concurrence:

Organisation	

From:

Warrant requesting agency	NCA
Requested by	Wayne J[redacted]
Application date	24/03/2020
WRA contact details	[redacted]

Document:

Warrant type	TARGETED EQUIPMENT INTERFERENCE
Document type	NEW WARRANT APPLICATION
Document reference	91-TEI-0141-2020

Warrant details:

Warrant number	91-TEI-0141-2020
Thematic?	Yes
Operation	Project Venetic
Title	Equipment Interference
Member of legislature?	No

Statutory ground(s):

Statutory ground	Yes/No
In the interests of national security	No
For the purposes of preventing or detecting serious crime	Yes
In the interests of the economic wellbeing of the UK so far as those interests are also relevant to the interests of national security	No
For the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health.	No

Subject matter(s):

Non-thematic subject matter	No
Equipment belonging to, used by or in possession of a particular person or organisation	
Equipment in particular location	
Thematic subject matter	**Yes**
Equipment belonging to, used by or in possession of persons who form a group which shares a common purpose or who carry on, or may carry on, a particular activity	No
Equipment belonging to, used by or in possession of more than one person or organisation, where the interference is for the purpose of a single investigation or operation	Yes
Equipment in more than one location, where the interference is for the purpose of a single investigation or operation	No
Equipment which is being or may be used for the purposes of a particular activity or activities of a particular description	No
Equipment which is being or may be used to maintain or develop capabilities relating to interference with equipment	No

Subject matter details:

Ref.	Type	Subject matter detail
1	Description of Investigation	This investigation relates to the criminal use of technology in the form of the EncroChat service which is provided to the criminal fraternity.
2	Unknown Persons	Users of EncroChat devices within the UK.

Why it is not reasonably practicable to individually name or describe persons, organisations or locations:

The EncroChat service is a highly encrypted secure communication service provided to the global criminal fraternity. The NCA Strategic Threat Assessment 2019 concluded that the platform is used exclusively by criminal users via a bespoke encrypted platform that is exploited to commit serious and organised crime whilst thwarting intelligence gathering. There is an estimated UK user base of 9000 (nine thousand) and a worldwide user base in excess of 50,000 (fifty

thousand).

Users access the EncroChat service via EncroChat handsets. These are mobile devices solely used to access the encrypted EncroChat service. The registered users of this service are unknown. The inability to attribute devices to a specific individual means that the service is popular with those involved in serious and organised crime as it prevents law enforcement accessing their communications.

The registered users are provided with a randomly generated "username" which does not identify them. As a result, it is not possible to list or name all users of the EncroChat service. The NCA is aware of specific individuals using these devices who are targets of NCA operations (further details provided below under the heading "Necessity"). The NCA has been unable to attribute all EncroChat usernames to specific targets.

It is the intention of UK law enforcement to use the information obtained by this activity to conduct other investigative tactics to identify the end users of these EncroChat devices. This will maximise any disruption opportunities to the individuals and the associated Organised Crime Groups (OCGs).

Description(s) of the type of equipment to be interfered with:

EncroChat handset devices within the United Kingdom, estimated to be 9000 (nine thousand).

Conduct description:

The conduct below is being undertaken by the French Gendarmerie and Dutch law enforcement working together in a Joint Investigation Team (JIT). The NCA will not be conducting the equipment interference but will be provided with the data (collected from UK EncroChat handsets) obtained as a result of that interference. The NCA is seeking a TEI warrant pursuant to s.99(1)(a) of the Investigatory Powers Act (IPA) to authorise the interference with UK EncroChat handsets in accordance with s.99(2) of the Act and to secure the obtaining of the communications and equipment data in accordance with s. 99(3). Due to the interference being conducted by the JIT, the NCA is seeking authorisation, pursuant to s.99 (5) (b) of the IPA. This would allow the NCA to require the JIT to provide assistance by conducting the interference on the UK EncroChat handsets.

In accordance with s.126 (1) of the IPA the NCA will act with the JIT so that they can provide assistance to the NCA by conducting the interference on EncroChat UK handsets. The assistance provided by the JIT will also include the provision of the data obtained regarding UK EncroChat handsets pursuant to s.126 (4) of the IPA.

Stage 1 (Historical Data Collection)

An implant, created by the JIT, will be deployed within a digital application on all EncroChat devices worldwide. This will be placed on devices via an update from the update server, currently located in France.

On deployment this implant will collect data stored on the device and transmit it to the French Authorities. This will include all data on the devices and is expected to include identifiers (e.g. IMEI and usernames), passwords, stored chat messages, geo-location data, images and notes.

The implant will remain installed on the device to enable stage 2.

Stage 2 (Forward Facing Collection)

Communications (such as chat messages) stored on the EncroChat devices will then be collected throughout the duration that the tactic is deployed.

Once stored on the handset, messages will be collected on an on-going basis. Messages will only be collected once they are stored on the device. As a result, this is considered as being conduct that is capable of being authorised under a Thematic Equipment Interference authority.

In addition, the EncroChat handset will routinely scan for Wi-Fi access points in the vicinity of the handset. The implant will instruct the EncroChat handset to provide a list of those Wi-Fi access points (such as a Wi-Fi router) in the vicinity of the device. This command from the implant will result in the JIT receiving the MAC address which is the unique number allocated to each Wi-Fi access point and the SSID which is the human readable name given to that access point.

Duration

The period of exploitation is planned to last for up to 2 months which was originally scheduled to take place from 10 March 2020. However, there has been a delay in the commencement of this activity but it is now expected to take place imminently. After the 2 month period has concluded the JIT plans to conduct overt law enforcement activity to cause total disruption to the EncroChat service. This will include the seizure of the French based servers and a large scale media campaign.

It has been acknowledged that the Administrators of the EncroChat service could have a contingency plan in place and be in a position to re-instate their servers in another country. However, the seizure of the servers by the French Gendarmerie will likely cause significant disruption to the service in any event. The media campaign is intended to discredit the brand entirely with the intention that all users will cease using their phones immediately.

The media campaign will publicise that the EncroChat service has been infiltrated by law enforcement and will likely include any successful law enforcement activity that has occurred as a direct result of the exploitation.

It is worth noting that it is not the intention of the JIT to retrieve the implant. This is because the overt action described above is expected to effectively shut down the EncroChat service which will mean that the handsets will no longer be in use. The JIT, rather than the NCA is in control over uploading or removing the implant. Although the implant will remain on devices once the service has been shut down it will no longer be able to transmit any further data to the JIT and therefore the NCA will not be in receipt of any data.

Necessity

a. Background:

Project Venetic is the NCA's response to the UK support of a global strategic response to EncroChat devices, assessed to be used exclusively by serious and organised crime. Venetic is currently placed as number one on the NCA's High Priority Grid.

EncroChat Users

EncroChat is a bespoke, criminally dedicated, highly secure communications platform which is being utilised by criminals across the UK and internationally to facilitate criminality. This includes money laundering, class A drug trafficking and firearms trafficking. EncroChat is assessed by the NCA to be the most prolific 'criminally dedicated secure communications' platform in the UK with an estimated UK user base of 9000 (nine thousand) and a worldwide user base in excess of 50,000 (fifty thousand).

EncroChat is based on a modified version of the Android operating system. Users are supplied with a handset and SIM card (usually a Dutch data only card). The handset of choice has been the Spanish manufactured BQ Aquarius smartphone. These have now been rebranded as "VSmart" since BQ were bought out by Vietnamese company VInGroup in 2018. The device is partitioned into an open side and a secure side from where the user can access software which allows highly encrypted communications in the form of instant messaging between like devices.

Currently, encrypted communications between EncroChat devices cannot be obtained by law enforcement except via a limited forensic capability post-seizure. At present there is no ability to gather telecommunications data from the EncroChat service. Individual users set what are referred to as 'burn-times' for the messages they send and receive on the devices. This means that at the end of the 'burn-time' that has been set the messages will be deleted from the device and can no longer be viewed. The default setting is 7 days but users can set these to be as short as 1 minute. Due to these set burn times, even successful post-seizure forensic analysis will obtain only limited evidential material.

It is assessed that the use of EncroChat devices has significantly increased during 2019, from an estimated 7000 devices at the beginning of the year to 9000 at the

end of the year. They are in use by those individuals involved in criminal activities, and those who facilitate the logistical and technical support.

"EncroChat is predicted to remain the most prominent criminally dedicated secure communications provider in the UK, with the greatest market share. Used exclusively by criminals, this bespoke encrypted communications platform is exploited to commit SOC, whilst thwarting intelligence gathering." **[NCA Strategic Threat Assessment 2019]**

Due to the high costs (approx. £1500 per device) of EncroChat services and the specialist nature of the encryption employed it is assessed that these devices are used to support serious and organised crime as evidenced by their use in some of the NCA's highest priority operations mentioned below. As a result it is assessed that this fulfils the serious crime criteria as defined in Section 263 of the IPA; being offences for which a person who has attained the age of 21 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three or more years or the conduct involves the use of violence which results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.

EncroChat Administrators

[redacted]. It is assessed that EncroChat devices have been developed for and are marketed specifically for the criminal community in order to facilitate criminality in the UK. This may constitute an offence of Participating in the criminal activities of an organised crime group contrary to S.45 (Pt.III) of the Serious Crime Act 2015. Due to the volume of EncroChat users worldwide, which are either replaced or renewed every sixth month, the 'EncroChat OCG' providing the devices is also assessed to be making a substantial profit from facilitating criminality.

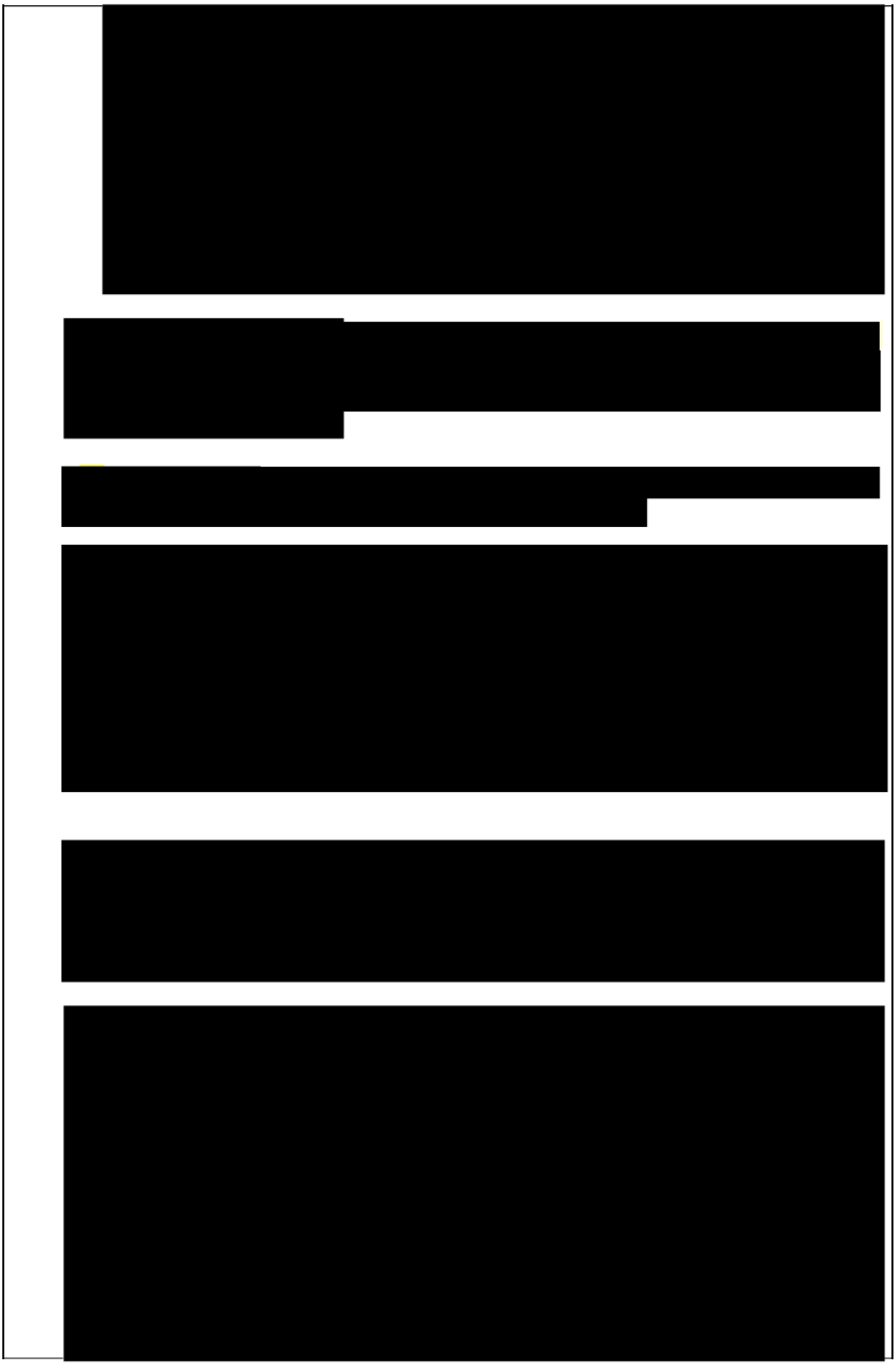
[redacted]

Evidence of EncroChat Devices in NCA Operations

The use of EncroChat devices have been reported across NCA and police operations throughout the UK. The highly encrypted nature of the EncroChat service creates a barrier to the ability of law enforcement to collect both intelligence and evidence in respect of the most serious crimes.

EncroChat handsets have featured in a number of NCA high priority operations. [redacted]

[redacted]



[redacted]

Usage is reported across the majority of high priority commodity and organised immigration crime investigations. It is assessed to be likely that EncroChat features across all of these operations but intelligence gaps remain around the use of encrypted communications.

The Joint Investigation Team

The JIT has offered to make available to interested partners, including the UK, the material being obtained under this activity. This would facilitate the disruption and dismantling of criminal networks utilising these highly encrypted communication devices.

The JIT intends to exploit EncroChat devices globally by collecting data stored on the devices, namely the IMEI details, usernames and passwords, stored chat messages, geo-location data, images and notes. The Wi-Fi scan conducted by the EncroChat handset and instructed by the implant will identify Wi-Fi access points in the vicinity of the handset. This will provide the JIT with the unique number allocated to each Wi-Fi access point and the SSID which is the human readable name given to that access point. [redacted]

[redacted]

The French authorities have obtained their legal authority permitting them to conduct this activity. However, if this activity were to take place on EncroChat handsets in the UK without lawful authority it would contravene s.1 (1) Computer Misuse Act 1990 ("CMA"). Under s. 5 (2) (b) of the CMA it is an offence if the computer interfered with is in the UK, even if the person carrying out the interference is outside the UK.

The NCA has been working with multiple international partners for a number of years on this threat and has established the [redacted] working group, which includes French and Dutch JIT partners. The NCA has been collaborating with the Gendarmerie on EncroChat for over 18 months, as the servers are hosted in France. The ultimate objective of this collaboration has been to identify and exploit any vulnerability in the service to obtain content.

[redacted]

This recent development by the Gendarmerie is in line with the objectives of the Working Group and there is a significant risk that the NCA is encouraging an offence under the CMA, which may amount to an offence under ss. 44, 45 or 46 of the Serious Crime Act 2007 (the "SCA 2007").

[redacted]

The Gendarmerie disclosed its ability to exploit EncroChat to the NCA in January 2020 and since then the NCA has been working with the JIT (including Europol) from a technical perspective to help build / improve the system that will be used to pipe, triage and filter the data before onward dissemination to the UK. This is likely to be regarded as assisting the Gendarmerie to commit the CMA offences.

As outlined above, the NCA has been liaising with the JIT in respect of this planned exploitation and will be providing some support in respect of the collection and dissemination of the data to the UK. Without lawful authority, there is a significant risk that this conduct by the NCA will facilitate the commission of the CMA offence by the JIT in the UK. The JIT will only provide this material to the NCA if it is formally requested, via a European Investigation Order, from the JIT and on the basis that the NCA provide permission for this activity to be conducted on the EncroChat handsets in the UK. The NCA considers that there is a significant risk that this amounts to an offence under the SCA 2007.

A Targeted Equipment Interference warrant would ensure that the NCA is able to provide such permission and use any material supplied by the JIT in evidence and

to resist any challenges to such use from defendants in any criminal proceedings.

The JIT will continue with their operational objectives, including targeting users of EncroChat in the UK, regardless of whether the NCA provides permission for the activity. If the NCA does not provide the permission requested and does not request the data from UK EncroChat handsets the data from those handsets will be retained by the JIT for the purposes of their operation but it will not be disseminated to the NCA.

The NCA's intention is to use the data (identified as being associated to criminals based in the UK and their organised crime groups) obtained by the JIT to facilitate current UK law enforcement activity and future criminal investigations. [redacted]

b. Reason for priority:

The JIT informed the NCA that this activity would commence on 10th March 2020. However, due to some minor issues that had to be resolved in relation to the formation and technical capabilities of the JIT that commencement date was delayed. The NCA has not been provided with an alternative commencement date but has been told that it will be prior to Tuesday 31st March 2020. The JIT has stated that they would endeavour to provide the NCA with 3 days notice of when this activity would commence although this is not guaranteed. The NCA does not have control over this implant and although the JIT will endeavour to provide 3 days notice the NCA is conscious that less notice may be provided. Consequently this application is now a priority to ensure that there is a lawful basis to obtain the data to be supplied by the JIT as soon as their activity commences.

c. Summary of what warrant is expected to produce:

The activity will produce all data stored within the device which is expected to include: IMEI details, usernames, passwords, stored chat messages, geo-location data, images and notes.

In addition, the EncroChat handset will routinely scan for Wi-Fi access points in the vicinity of the device. The implant will instruct the EncroChat handset to provide a list of those Wi-Fi access points (such as a Wi-Fi router) in the vicinity of the device. This command from the implant will result in the JIT receiving the MAC address which is the unique number allocated to each Wi-Fi access point and the SSID which is the human readable name given to that access point.

Risk assessment:

The NCA is not in control of this interference. The JIT will determine when the interference will commence, how often the data will be collected and when the interference will conclude (provided there is no compromise). As a result the NCA has no influence in respect of the use of this tactic.

If the NCA does not request this data and does not provide permission for this activity to take place on UK EncroChat handsets the data collected from those handsets will not be provided to the NCA but will be retained by the JIT. However, the JIT will not analyse the data from UK handsets. This would mean that the opportunity to disrupt the UK OCGs utilising EncroChat will be lost which would be detrimental to the reputation of the NCA in tackling serious and organised crime.

The NCA has been liaising with the JIT in respect of this planned exploitation and will be providing some support in respect of the collection and dissemination of the data to the UK. The NCA has also been requested by the JIT to provide permission for this activity to be conducted on UK EncroChat handsets and to request the data. Without lawful authority, there is a significant risk that this conduct by the NCA will facilitate the commission of the CMA offence by the JIT in the UK.

A Targeted Equipment Interference warrant would ensure that the NCA is able to provide such permission and use any material supplied by the JIT in evidence and to resist any challenges to such use from defendants in any criminal proceedings.

The JIT's media strategy is that the use of the tactic (not technical specifics) will be publicised to discredit the private and encrypted nature of EncroChat. They will also disclose the use of the tactic in any criminal proceedings that result from the activity.

Any compromise would shorten the technical activity and bring forward the planned disclosure to the public at large. A compromise would reduce the opportunity to gather valuable intelligence. This would only be detrimental to the NCA's reputation with international partners if the compromise was caused by the early disclosure of the activity by the NCA. This would unlikely be detrimental to the NCA's reputation with the public or the operational objectives as a whole.

One of the primary operational considerations, therefore, will be the protection and security of the deployment to maximise intelligence gathering opportunities and preserve future operational capability.

Although considered unlikely, as a result of the assessment regarding these devices a robust plan to minimise collateral intrusion into non-criminal communication conducted by the OCGs that operate on this platform is in place and this plan will be regularly reviewed.

Any material that is obtained and does not relate directly to criminality or criminal intelligence will be dealt with in accordance with Investigatory Powers Act 2016

(IPA), Criminal Procedure and Investigations Act 1996, and NCA guidelines.

Privileged and/or confidential information requiring additional safeguards:

Legal Privilege	**Yes/No**
The purpose (or one of the purposes) is the interference with equipment to obtain items subject to legal privilege	No
It is likely that material the obtaining of which is authorised by the warrant will include items subject to legal privilege	No
The purpose (or one of the purposes) is interference with equipment to obtain communications or other items of information that, if not created or held with the intent to further a criminal purpose, would be items subject to legal privilege	No
Confidential journalistic material	**Yes/No**
The purpose (or one of the purposes) is the interference with equipment to obtain communications or other items of information believed to contain confidential journalistic material	No
Sources of journalistic information	**Yes/No**
The purpose (or one of the purposes) is to identify or confirm a source of journalistic information	No

Details of privileged and/or confidential information, including those requiring additional safeguards:

Due to the nature and use of these devices, as described in the NCA 2019 Strategic Threat Assessment, it is considered highly unlikely that legal privilege or journalistic material will be identified in the data gathered. However, in the unlikely event that such information is inadvertently acquired the Senior Authorising Officer would be notified as soon as practicable in order to carry out an immediate review. Legal advice will be obtained so an early assessment can be made of whether it is necessary and proportionate to retain the material for one or more of the authorised purposes set out in s.129(3) of the IPA. If there is an intention to retain privilege and/or confidential material permission will be sought from the Investigatory Powers Commissioner's Office (IPCO) in compliance with the Code of Practice for Equipment Interference.

Collateral intrusion assessment:

It is assessed by the case team that there will be minimal collateral intrusion to innocent members of the public as a result of this activity. This is because this is a dedicated criminal platform. This operation is concerned with the illegal activities of criminal networks using these devices that impact across the entire UK and broader communities. However, due to the fact that the Wi-Fi scan will reveal data in respect of Wi-Fi access points in the vicinity of the handset it is possible that the implant will collect data in respect of those points belonging to a member of the public. However, the data that the implant receives as a result of this scan is minimal and the individual associated with that access point cannot be identified by that data alone. In addition, if the EncroChat handset device is located in the home address of the user the collateral intrusion would be minimal as the user would be assessed to be using EncroChat as a criminal platform. Any material that is obtained and does not relate directly to criminality or criminal intelligence will be dealt with in accordance with Investigatory Powers Act 2016 (IPA), Criminal Procedure and Investigations Act 1996, and NCA guidelines.

The development of this intelligence and the disruption of this communications network are anticipated to support successful prosecutions, resulting in the expectant lengthy custodial sentences and the confiscation of the assets of those involved in the exposed criminality. Any individuals identified as not being criminally connected will be excluded from any anticipated pro-active investigations. When balanced against what the NCA seeks to achieve, in the prevention of serious and organised crime within the UK, it is assessed that this level of intrusion is justified.

The following steps will also be taken in order to minimise collateral intrusion:

- Activity will remain focussed on the subjects wherever possible.
- All activity will be appropriately supervised.

Proportionality assessment:

It is recognised that the proposed activity is an invasive tactic, likely to engage individuals (as yet unidentified) rights to privacy under Article 8 of the Human Rights Act 1998. However, such intrusion is considered justified, proportionate and necessary when balanced against the seriousness of the offences assisted by the use of these devices. It is anticipated that the data obtained by this covert activity will be used to identify those involved and maximise the disruption to their criminal enterprise.

Due to the encryption capabilities of the devices in question, the fact that they are supplied by a recognised criminal enterprise (as explained under the “necessity” heading) and are under investigation by the NCA and international law enforcement means there is no opportunity to approach EncroChat to seek co-operation with law enforcement. Therefore, there are no other methods available to law enforcement to gather this significant and valuable data that this tactic will

undoubtedly provide.

The ability of UK law enforcement to fight serious and organised crime is consistently frustrated by the use of encrypted devices, this has meant that those involved in serious crime have been able to exploit gaps in our capability, putting the public at an unknown risk and significant unquantifiable cost to the UK.

It is acknowledged that this activity will result in the acquisition of large amounts of data. However, clear protocols and an investigative strategy have been developed in support of this operation to ensure that, once received by the NCA the material is handled correctly and shared when appropriate. This will be done in a timely manner by the NCA to UK law enforcement and partners in compliance with the safeguards contained within sections 129-131 of the IPA 2016 and duty not to make unauthorised disclosures outlined in sections 132-134 of the IPA.

The NCA has considered and precluded other methods of obtaining this information. However, due to the functionality and highly encrypted nature of the devices relied upon by the criminal providers and users of the service, this has not been possible.

There is a public interest in the integrity of telecommunications systems and to keep private information safe. It is assessed that this particular telecommunications system is used exclusively for criminality and as such there is no legitimate public interest in ensuring the integrity and security of this system.

As the system is believed to be used exclusively for the purposes of criminality, it is not anticipated there will be any implications on the privacy and security of any innocent users of the system. However, it is assessed that there may be minimal collateral intrusion in respect of the Wi-Fi scan that may reveal Wi-Fi access points belonging to members of the public who do not have an EncroChat phone and are not involved in criminality. The data obtained as a result of the Wi-Fi scan provides information outlined above that would not, by and of itself identify the owner of the Wi-Fi access point. As a result, there would be minimal intrusion in respect of the Article 8 rights of those individuals. Any material that is obtained and does not relate directly to criminality or criminal intelligence will be dealt with in accordance with Investigatory Powers Act 2016 (IPA), Criminal Procedure and Investigations Act 1996, and NCA guidelines.

Case for use of equipment interference techniques by law enforcement:

Due to the location of the servers being within France, the activity has been planned, developed and authorised by the JIT.

NCA has not been involved in the development or deployment of the implant that supports this tactic.

Assisting parties:

The French Gendarmerie and Dutch law enforcement by means of a JIT are implementing the tactics discussed. The JIT has asked the NCA for permission to conduct this activity on EncroChat handsets in the UK. They have also requested that the NCA request the material in respect of UK handsets via a European Investigation Order. The JIT will assist the NCA in accordance with s.126 (4) of the IPA by providing the data from UK EncroChat handsets. If permission is not provided the JIT will continue with the tactic. However, they will not analyse the data from the UK handsets and will not provide that data to the NCA.

Handling arrangements and safeguards:

Material from the UK EncroChat handsets that is obtained by the French authorities and shared with the NCA will take place under a memorandum of understanding (MOU).

IPA Safeguards

In accordance with s.129 (1) of the IPA the NCA, once in receipt of the data will ensure compliance with the safeguards contained in s.129- s.131 of the IPA. It is acknowledged that there will be data from UK EncroChat handsets in the possession of the JIT that the NCA is unable to control. However, the French Gendarmerie have the necessary domestic authority in place to conduct this activity and the data obtained will then be dealt with in accordance with their domestic law and data protection legislation. Consequently, it is anticipated that in terms of personal data the JIT will have the necessary safeguards in place.

Triage at Europol

Any successful application will result in a large amount of data being obtained. The material will first be triaged by Europol and will use an algorithm to identify Threats to life (TTL). NCA officers will be placed at Europol to deal with any identified TTLs.

Once the UK material (identified via IP address) reaches the NCA (likely to be daily within one day of collection) it will be triaged:

- Methods such as keyword searches will be used to identify TTLs and high risk criminality such as firearms, counter terrorism (CT) and child sexual abuse (CSA). Material relating to ongoing investigations will also be extracted and provided to those investigation teams.

- The remaining data will be exploited through keyword searches and social network analysis. The material will then be disseminated to law enforcement and other agencies by the NCA via intelligence officers with the necessary handling conditions and safeguards.

The sharing of information will be conducted in accordance with the safeguards outlined within sections 129 to 131 of the IPA and Chapter 9 of the Equipment

Interference Codes of Practice. This will be supported by means of a Memorandum of Understanding (MOU) signed by individual partner agencies.

Any overseas intelligence will only be disseminated in accordance with the safeguards described above and specified with any specific MOU.

The data provided will initially be dealt with on an intelligence only basis and disseminated accordingly. This will change once the initial two month period (planned by the JIT) has elapsed or an unforeseen compromise occurs and initiates an early disclosure of the JIT covert operational activity.

As soon as the JIT initiates their media strategy and conduct disclosure as part of criminal proceedings, the NCA will request that the JIT provide the material to an evidential standard in support of UK legal proceedings.

Unused material will be recorded, retained and reviewed in line with CPIA 1996.

Equipment Interference Supervisor's name; Lee R[redacted]	**Contact details;** [redacted]

Applicant details

Name: Andy C[redacted]	
Rank:G5	
Telephone number:[redacted]	
Signature: [redacted]	**Date and time:** **2030hours 24.03.2020**

Approving officer considerations: G3 or above

Having just read this application in detail I can confirm that the intelligence and information relied upon within is current, correctly graded, accurate and that it is recorded on NCA systems. I can confirm that this investigation has been tasked via the appropriate mechanisms; Project Venetic is a current NCA High Priority Investigation. I am fully sighted on all intelligence aspects of this investigation.

Secure Communications use by criminals is a NCA cross-cutting enabling threat due to the impact such devices are having on effective intelligence gathering and subsequent disruption of serious and organised crime. (SOC) EncroChat is currently the platform of choice among UK serious organised criminals. Although the possession of, and use of such devices and platforms is not a crime the current assessment is that EncroChat use is entirely criminal in nature.

The opportunity presented by the French activity is unprecedented in its potential.

If successful, this technique will provide time limited operational opportunities against SOC as well as the opportunity, in the longer term, to paint the strategic picture of SOC on a scale never before seen in the UK.

I have been party to the significant legal discussion and advice provided to the applicant by subject matter experts to assist with the preparation of this application. I am wholly satisfied that this application is the correct means to underpin the activity outlined. The applicant has articulated in depth, the case for necessity and proportionality which I fully support. Ultimately this authority is necessary for the NCA, on behalf of UK law enforcement to obtain the data in accordance with the correct legal framework in order to be able to exploit this valuable and rare opportunity. I believe that when weighed against the impact these devices are having on the UK's fight against serious and organised crime, the impact access to the sought information will have on SOC investigations nationwide and the inability of law enforcement to access this data any other way the sought activity is justified, necessary and proportionate.

The applicant has considered the risk of collateral intrusion occurring but articulates that EncroChat is assessed as being utilised exclusively by criminal networks. There is nonetheless a slim possibility that none criminal devices may be identified, albeit this is considered very unlikely it is acknowledged. The WiFi data that this exploitation will obtain cannot on its own identify individuals. These facts coupled with the safeguards and mitigation plan explained I believe do support the low assessment of collateral intrusion risk and impact on individuals Article 8 rights.

The nature of the user base of these devices leads one to support the assessment that there is very little likelihood of encountering confidential information or Legally Privileged Material. There is a well-practiced and sufficiently robust process that exists, and is articulated within that would be utilised in the event material is inadvertently encountered.

The applicant has fully considered the risks specific to this application. In conjunction with the detailed data triage process outlined within this investigation is subject of a whole agency response and there is specialist support staff to assist with the management of risks that can reasonably be foreseen including Threats To Life, Operational Security, Information Security and Legal / reputational considerations. There is a documented risk management plan which will be subject to detailed scrutiny through the Gold Command structure which is overseeing this activity. There is a contingency plan in place regarding the resourcing of this operation, including split site working, split teams and remote working where viable to support social distancing considerations and protect staff and the public. This is subject to daily review in a Gold Group meeting alongside the wider Agency response to this virus. There are contingencies in place to scale the NCA's response to manage and disseminate this data in the event that the COVID-19 pandemic causes significant disruption to the plans which are presently in place.

I can confirm that appropriate resources are in place to support this application, this includes specialist departments. I fully support this application.

Have all reasonable efforts been made to take account of information which may weaken the case for the warrant?	Yes

Approved by: Wayne J[redacted] – G3 Operations Manager

Approved on: 24th March 2020 – 2050hours

Approval signature: [redacted]

Senior Supervisor Considerations: DD (SAO)

This Application for a TEI Warrant is an amendment to a Warrant approved on 5 Mar 20 which authorised activity to collect all data stored within the Encrochat devices including IMEI details, usernames, passwords, stored chat messages, geo-location data, images and notes. The amendment is made to include new and enhanced activity not recorded on the original. The enhancement to the implant will allow the implant to make the EncroChat handset routinely scan for Wi-Fi access points in the vicinity of the handset. Furthermore, the implant will command the EncroChat handset to provide a list of those Wi-Fi access points (such as a Wi-Fi router) in the vicinity of the device.

This enhancement was briefed to the NCA on 24 Mar 20. It is an example of the dynamic and innovative nature of this type of TEI.

The original Warrant will be cancelled and replaced by this one, if authorised. I have acted as the SAO for both warrants and my comments from 3 Mar 20 remain extant.

I agree that this presents a unique opportunity to map and disrupt SOC within the UK. If successful, it has the potential to generate unparalleled insight into SOC, specifically the criminals, the commodities and the modus operandi. It could inform a counter SOC 4P strategy for years to come.

This application is for TEI because no communications will be captured in transmission, all the data will be collected from the devices or the server.

Although we seek to take receipt of the data gathered from c9000 handsets, there is no legitimate use for EncroChat so I am satisfied that the risk of collateral intrusion is acceptable. The NCA team are alert to this risk and have measures in place to manage this risk.

Encrochat is the preserve of those criminals seeking a high degree of operational security to protect their criminality and profits.

Since the last application measures to reduce the spread of COVID-19 have escalated considerably. In this context I note that resourcing this operation will be

accomplished through split site working, split teams and remote working where viable to support social distancing considerations and protect staff and the public. This is subject to daily review in a Gold Group meeting alongside the wider Agency response to the virus. There are contingencies in place to scale the NCA's response to manage and disseminate this data in the event that the COVID-19 pandemic causes significant disruption to the plans which are presently in place.

I recommend that the DG authorises.

NM N[redacted]
25 Mar 20 @1108hrs

Is it reasonably practicable for the Director General to authorise?	**Yes**
If no, provide reason	

Senior Supervisor: N M N[redacted]

Telephone Number:[redacted]

Authorising officer considerations:

On the 4th March 2020 I received a warrant in relation to the use of this technique and the operation that would follow. Since that date we have received information from international partners (the French) about the technical nature of the implant and, with advice from our internal legal team, we have concluded that the original terms of the warrant does not fully cover the activity to be undertaken. As a result that warrant is to be cancelled and I have considered the additional information afresh.

I have reviewed this application including the comments from those supervising it. I am fully sighted on the operation, currently sitting as a high priority for the NCA because the impact of this enabling device (phone and connected network) across all threat types, as indicated in the application, is so significant.

I remain persuaded that serious crimes are under investigation. This communications network is criminal in nature engaged in a wide variety of serious crimes, all meeting that definition, as spelt out in the application. The Public would strongly support law enforcement taking action against a network that facilitates crimes which are high harm in nature. I can see no less intrusive method of understanding the totality of those criminals availing themselves of this service. This authorised intrusion is necessary to build the case against the network providers and to take action against the wide variety of criminal enterprises using

it. The warrant seeks to conduct a remote download of stored data. However it also allows for a technical request of the device which will provide Wifi information about other encrochat handsets being at a specific location. This will allow us to understand links between the criminal users of these devices. I believe both tactics (remote download and location connected devices) are necessary tactics to identify and disrupt criminal networks engaged in serious crime.

In making the collateral intrusion assessment I have considered whether what is recorded is overly reassuring. We see evidence of these phones in organised criminal networks currently subject to active investigation (as detailed) and we assess the network is wholly criminal. It is just about possible, in my view, that phones could have been purchased for a non criminal but illicit purpose eg marital affair - this would seem extreme and perhaps even unlikely but we cannot exclude that possibility at this stage. As such I would rather we recognised that there is a slim possibility of such occurring. In the event that data gathered showed a non criminal purpose further exploitation would not occur, the material would be held securely and the SAO must be advised so that a further CI assessment could be made. In this instance IPCO would also be notified. I have also made a separate consideration in respect of the wifi intrusion. It is possible that data may be collected which links to a non criminal person or activity. At the time the intrusion is made the data that is accessed is not personal and further enquiry would be required to link it to an individual. If an innocent party is identified it can be disregarded by the case team. This warrant is proportionate to the extent of the criminality.

Warrant approved - review 1 month. To reassess use of the tactic and the operational results from it, to re examine the WIFI element of the intrusion and to be assured of progress in the context of the COVID19 outbreak,

Review Date 24/04/2020

Authorised by: DG Lynne Owens CBE QPM MA

Authorised on: 25/03/2020

INVESTIGATORY POWERS ACT 2016
Section 115(4)(b)

SCHEDULE OF CONDUCT
for a Targeted Equipment Interference Warrant

Warrant Number: **91-TEI-0141-2020**

Schedule Number: **91-TEI-0141-2020-SC-01**

Description of conduct authorised to take:

The conduct below is being undertaken by the French Gendarmerie and Dutch law enforcement working together in a Joint Investigation Team (JIT). The NCA will not be conducting the equipment interference but will be provided with the data (collected from UK EncroChat handsets) obtained as a result of that interference. The NCA is seeking a TEI warrant pursuant to s.99(1)(a) of the Investigatory Powers Act (IPA) to authorise the interference with UK EncroChat handsets in accordance with s.99(2) of the Act and to secure the obtaining of the communications and equipment data in accordance with s. 99(3). Due to the interference being conducted by the JIT, the NCA is seeking authorisation, pursuant to s.99 (5) (b) of the IPA. This would allow the NCA to require the JIT to provide assistance by conducting the interference on the UK EncroChat handsets.

In accordance with s.126 (1) of the IPA the NCA will act with the JIT so that they can provide assistance to the NCA by conducting the interference on EncroChat UK handsets. The assistance provided by the JIT will also include the provision of the data obtained regarding UK EncroChat handsets pursuant to s.126 (4) of the IPA.

Stage 1 (Historical Data Collection)

An implant, created by the JIT, will be deployed within a digital application on all EncroChat devices worldwide. This will be placed on devices via an update from the update server, currently located in France.

On deployment this implant will collect data stored on the device and transmit it to the French Authorities. This will include all data on the devices and is expected to include identifiers (e.g. IMEI and usernames), passwords, stored chat messages,

geo-location data, images and notes.

The implant will remain installed on the device to enable stage 2.

Stage 2 (Forward Facing Collection)

Communications (such as chat messages) stored on the EncroChat devices will then be collected throughout the duration that the tactic is deployed.

Once stored on the handset, messages will be collected on an on-going basis. Messages will only be collected once they are stored on the device. As a result, this is considered as being conduct that is capable of being authorised under a Thematic Equipment Interference authority.

In addition, the EncroChat handset will routinely scan for Wi-Fi access points in the vicinity of the handset. The implant will instruct the EncroChat handset to provide a list of those Wi-Fi access points (such as a Wi-Fi router) in the vicinity of the device. This command from the implant will result in the JIT receiving the MAC address which is the unique number allocated to each Wi-Fi access point and the SSID which is the human readable name given to that access point.

Duration

The period of exploitation is planned to last for up to 2 months which was orgininally scheduled to take place from 10 March 2020. However, there has been a slight delay in the commencement of this activity but it is now expected to take place imminently. After the 2 month period has concludedthe JIT plans to conduct overt law enforcement activity to cause total disruption to the EncroChat service. This will include the seizure of the French based servers and a large scale media campaign.

It has been acknowledged that the Administrators of the EncroChat service could have a contingency plan in place and be in a position to re-instate their servers in another country. However, the seizure of the servers by the French Gendarmerie will likely cause significant disruption to the service in any event. The media campaign is intended to discredit the brand entirely with the intention that all users will cease using their phones immediately.

The media campaign will publicise that the EncroChat service has been infiltrated by law enforcement and will likely include any successful law enforcement activity that has occurred as a direct result of the exploitation.

It is worth noting that it is not the intention of the JIT to retrieve the implant. This is because the overt action described above is expected to effectively shut down the EncroChat service which will mean that the handsets will no longer be in use. The JIT, rather than the NCA is in control over uploading or removing the implant. Although the implant will remain on devices once the service has been shut down it will no longer be able to transmit any further data to the JIT and therefore the NCA will not be in receipt of any data.

_____

Lynne Owens QPM CBE
Director General NCA

Internal Reference: **VENETIC**

INVESTIGATORY POWERS ACT 2016
Section 115(4)(a)

SCHEDULE OF EQUIPMENT
for a Targeted Equipment Interference Warrant

Warrant Number: **91-TEI-0141-2020**

Schedule Number: **91-TEI-0141-2020-SE-01**

Description(s) of the type of equipment to be interfered with:

EncroChat handset devices within the United Kingdom, estimated to be 9000 (nine thousand).

_____
Lynne Owens QPM CBE
Director General NCA

Internal Reference: **VENETIC**

INVESTIGATORY POWERS ACT 2016
Section 115(3)

SCHEDULE OF SUBJECT MATTER DETAILS
for a Targeted Equipment Interference Warrant

Warrant Number: **91-TEI-0141-2020**

Schedule Number: **91-TEI-0141-2020-SMD-01**

Subject matter details:

Ref.	Type	Subject matter detail
1	Description of Investigation	This investigation relates to the criminal use of technology in the form of the Encrochat service which is provided to the criminal fraternity.
2	Unknown Persons	Users of EncroChat devices within the UK.

_____
Lynne Owens QPM CBE
Director General NCA

Internal Reference: **VENETIC**

INVESTIGATORY POWERS ACT 2016
Section 106(1)

TARGETED EQUIPMENT INTERFERENCE WARRANT INSTRUMENT
issued by the Law Enforcement Chief

Warrant Number: 91-TEI-0141-2020

To be completed after Judicial Commissioner approval:

Issue Date: 26/03/2020
Expiry Date: 25/09/2020

To Wayne J[redacted]

Authorisation

In exercise of the power conferred on me by section 106(1) of the Investigatory Powers Act 2016, I authorise Wayne J[redacted] to secure-

- interference with equipment belonging to, used by or in possession of subject matter(s) described in the schedule of subject matter details for the purpose of obtaining communications, equipment data or other information,
- the obtaining of communications, equipment data or other information by means of that interference, and
- the disclosure, in any manner described in the schedule of conduct, of anything obtained under the warrant.

The conduct the person to whom the warrant is addressed is authorised to take is described in the schedule(s) of conduct. The type of equipment which this warrant authorises interference with is described in the schedule(s) of equipment.

This warrant also authorises:

- any conduct which it is necessary to undertake in order to do what is expressly authorised or required by this warrant, including conduct for securing the obtaining of communications, equipment data or other information, and
- any conduct which is conduct in pursuance of a requirement imposed by or on behalf of Wayne J[redacted] to be provided with assistance in giving effect to the warrant.

Warrant Number: 91-TEI-0141-2020

Law Enforcement Chief decision to issue

Having considered the application made on behalf of the person to whom the warrant is addressed, I consider that the warrant is necessary For the purposes of preventing or detecting serious crime and that the conduct authorised is proportionate to what is sought to be achieved by that conduct. I consider that satisfactory arrangements made for the purposes of sections 129 and 130 of the Act are in force in relation to this warrant.

_____

Date of Signature: 25/03/2020

Lynne Owens QPM CBE
Director General NCA

Internal Reference: **VENETIC**