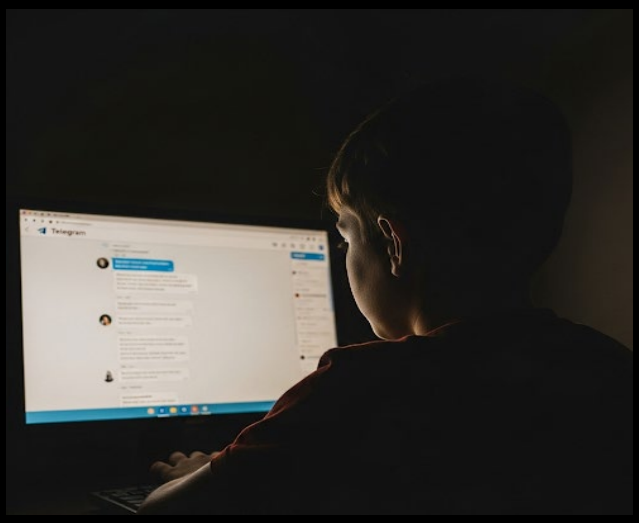
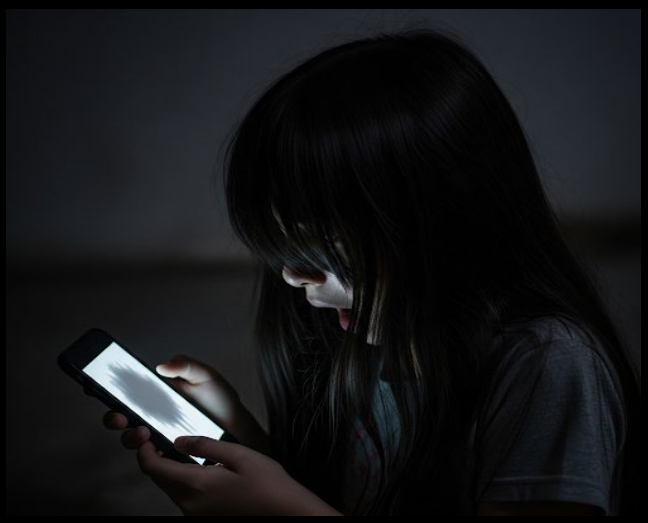
COUNTER TERRORISM POLICING

NCA National Crime Agency

NPCC National Police Chiefs' Council





Com Networks:

Alert for Safeguarding Children Partnerships

Warning – this alert contains material which some may find upsetting

This alert has been designed to inform, raise awareness and assist safeguarding partnerships and practitioners in recognising, and responding to, the emerging threat of Com Networks.

All agencies are likely to come across potential indicators of harm. Awareness raising amongst education and health colleagues as well as responding agencies is key to preventing com network activity and early identification

What are Com Networks?

Community 'Com' Networks are online groups involved in child sexual abuse, cybercrime and offline violence.

These networks are dynamic and often overlap across the threats, although not every case will involve all three. The majority of those involved (victims and perpetrators) are predominantly but not always children under the age of 18.

Members of the Com Network engage with deviant beliefs, behaviours, and offending. Offenders engage in all forms of extreme behaviour, and seek kudos by performing the most severe acts of degrading sexual and physical violence and engendering the greatest fear in their victims.

Com Networks are active on virtually all social media and online gaming platforms but primarily operate on Discord and Telegram which are popular communication platforms.

Definition

Com Networks can be defined as:

Transnational Virtual Networks (TVN) of criminal actors which engage in a variety of illegal acts or coerce others to do so in furtherance of their own personal gain, development of their infamy, or in furtherance of their ideologies.

The networks can broadly be broken down into three identifiable subgroups

- **Sub-Group 1:** A group operating online primarily involved in extorting minors to commit digital and real-world sex crimes, criminal acts against the person, property & animals; and the promotion of self-harm and suicide: (Sextortion Com)

- **Sub-Group 2:** A group acting online who hold extremist mind-set who promote a violent Nihilistic worldview encourages damage to property, harm to individuals & potentially acts of terrorism. (Offline Com)

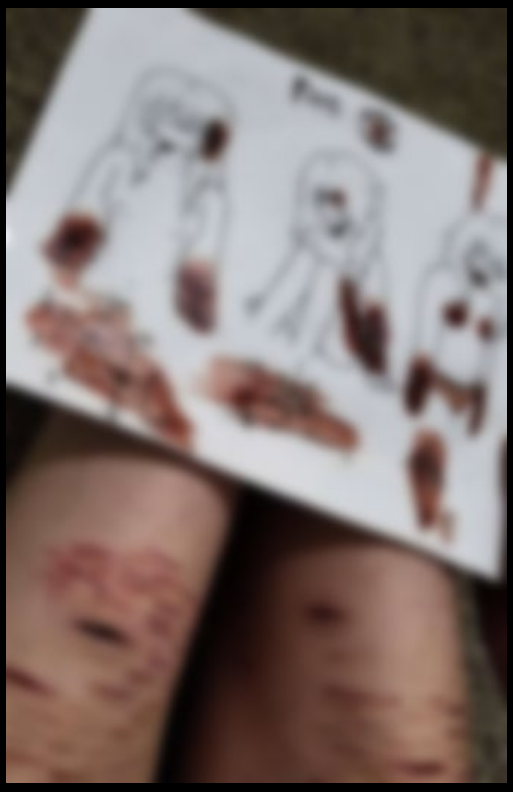
- **Sub-Group 3:** A group who have a common purpose to conduct criminal activities that maliciously use digital technologies that target commerce/ infrastructure by means of Network Intrusions/ Ransomware etc. (Cyber Com)

What Do These Networks Look Like?

Members of Com Networks engage in three types of harmful behaviour.

The first behaviour is the grooming and extortion of young people (often, but not exclusively females) into sharing indecent or degrading images of themselves. These images are then used to further manipulate and coerce. Coerced acts may include self-harm, cutting symbols and initials into their bodies (knowns as cutsigns and fansigns), suicide attempts, the ingestion of toxic/harmful materials, or burning themselves. Victims are coerced into recording or livestreaming these acts, which are then shared within the networks to increase the status and notoriety of the perpetrator.

The victim may not appreciate the seriousness of their involvement with the perpetrator and unable to focus on their own needs and this may impact on their physical and mental health and relationship with their families. The injuries sustained have resulted in hospitalisation, serious injury, and death.



The second type of harmful behaviour that members of Com Networks engage in is sim swapping doxing, swatting and the deployment of ransomware, malware, and specialist malicious tools for cybercrime purposes, their aim is to have the most severe impact on companies and infrastructures.

Young people at risk of committing these very serious crimes may not recognise how a conviction can impact their freedom and future life and career chances

The third type of behaviour is in-person violence. This occurs offline and maybe opportunistic as opposed to targeted. Such violence includes graffiti, arson, serious sexual and physical assault, and murder.

Violence may be targeted towards those perceived to be weak or inferior, however violence can also be indiscriminate.

Who is targeted by Com Groups?

Offenders seek out vulnerable and susceptible victims (children and adults) to groom, manipulate and exploit, individuals may be particularly vulnerable to such targeting if they use online forums providing help and advice for:

- Mental health disorders
- Neurodiversity
- Body image disorders
- Self-harm and suicide
- Sexual orientation and gender identity
- Sexual and/or physical abuse
- Substance misuse

Or due to other bias such as misogyny or ideology

- Ethnicity and race
- Religious orientation
- Physical – the elderly and homeless

Behaviours and indicators of concern

The below are potential behaviours or indicators that a young person maybe involved in an exploitive and /or an abusive relationship with a Com Group and may apply to both victims and offenders.

Offender and victim dynamics are complex and not always clearly defined with some victims coerced or forced into perpetrating abuse. Professionals should assess each referral on a case-by-case basis.

In isolation these behaviours / indicators may be insignificant or unrelated to Com Group offending, grooming or victimisation.

- Self-harm (of note, cutting numbers/letters /symbols, or to the breasts/genitalia) known as cut signs or fan signs)
- Numbers, letters symbols written in blood on walls knowns as 'blood signs'
- Interest, possession or promotion of extreme themes or materials
- Disengaging from education
- Obsession with new online friends
- Unexplained injuries or death of pets
- Unexplained injuries to siblings
- 'Doxing' *(the malicious sharing of private or identifiable information)* and/or '**Swatting**' *(abuse of the 999 system to trigger an armed police response to a location)*
- Unexplained money or gifts
- The use of encrypted or fringe communications platforms (Discord and Telegram)

The following indicators pertain to cyber com

- Individual has an intense interest in cyber activities
- Individual is in possession of advanced software that does not reflect typical use (i.e. TAILS)
- Individual has an advanced understanding of digital technologies, hardware, and software
- Individual has skills in specialised and varied software, programming, and network configuration (i.e. knowledge of how to use Kali-Linux and/or ability to write in code)
- Individual has a known history of hacking, SIM swapping, swatting, DDOS, online fraud (use of compromised credit cards)
- Unexplained wealth – where individual is in possession of items whose value is disproportionately high to family or individual income
- Interest and advanced understanding of cryptocurrency

Perpetrator characteristics

Perpetrators seek acceptance, kudos and notoriety. They are predominantly, but not always, males between the ages of 14-17. They may or may not outwardly display extreme behaviours and beliefs. They share extreme material which may include:

- Child sexual abuse
- Violence and gore
- Animal abuse, torture and bestiality
- Extreme/violent pornography

- Misogynistic and ‘incel’ beliefs
- Extremist and terrorist materials
- Mass casualty events (e.g. school shootings and genocides)
- Racist and occultist materials
- Hacking tools and exploits

The wellbeing of staff is always a priority.

Professionals should be aware that due to this threat and during their interactions with a child or young person, they may experience behaviour, disclosures or material that is distressing and outside of the ‘norm’. Any wellbeing concerns that you have about yourself, or colleagues should be discussed with your line manager or through your organisation’s supervision and wellbeing processes.

Professionals should be aware that offenders have targeted a small number of front-line practitioners and police officers involved in investigations through ‘doxing’ and ‘swatting’.

Professionals should exercise personal safety and security during any interaction and on social media - if you would like further information regarding operational security, please visit:

National Cyber Security Centre - www.NCSC.gov.uk

Referrals

The National Crime Agency (NCA), National Police Chiefs' Council (NPCC) and Counter Terrorism Policing (CTP) are working together to disrupt and degrade the Com Networks.

Despite increased awareness of the Com Network within law enforcement and safeguarding partnerships, the activity remains widely underreported.

Safeguarding

All concerns regarding the safeguarding of a child or young person should be referred in line with local procedures.

Com network crime should be assessed as potential child criminal exploitation. It is likely that the online nature of these crimes will involve multiple perpetrators and victims across a geographical span. Where necessary, safeguarding partnerships should identify a lead coordinating region.

Capturing the following information is key to assisting in identifying offenders and safeguarding victims:

- The online platform being used

- The subjects (victims and suspects) online usernames

- Any group name mentioned (these can be single words such as CVLT, terms such as Harmnation or a series of numbers like 764 114

Local Police Online Child Sexual Abuse and Exploitation teams (OCSAE), Police Online Investigation Teams (POLIT), Child Protection Teams and Cyber Crime Units are investigating these offences

Police: Please ensure intelligence regarding Com Network activity is referred to your local intelligence unit and that it uses the term 'Com Network' as well as describing the concerning behaviours identified. Police forces can task wider ROCU resourcing to assist in these investigations. Seek advice in having these cases MoRiLE scored and enquire as to who is your force 'Com Network' local point of contact for assistance.

COUNTER TERRORISM POLICING

NCA

National Crime Agency

NPCC

National Police Chiefs' Council