

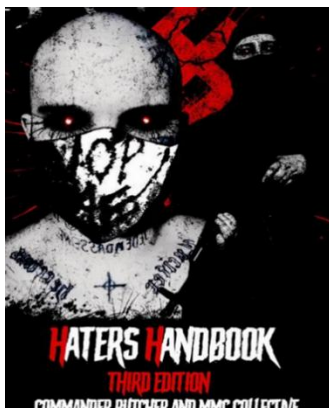


The COM Network – Partnership Briefing Note

The COM Network (Community Online Networks) refers to transnational virtual networks (TVNs) of predominantly teenage offenders who engage in serious online criminal activity.

TVNs : A transnational virtual network is an online group or community made up of individuals from multiple countries who interact and coordinate primarily through digital platforms. These networks are not tied to a physical location and often use encrypted or mainstream apps (like Discord, Roblox, Telegram, or gaming forums) to share information, plan activities, or pursue common goals.

What are Com groups?



Com groups, sometimes referred to as Com networks can be defined as online collectives of individuals who work together or compete on chat platforms to cause harm and commit crimes. They do this to make money, gain notoriety or to promote their ideologies.

These collectives often adopt different self-imposed names and branding. Their focus is generally on one of the following three pillars of criminality, although some individuals are part of multiple groups and commonly offend across the pillars:

1. Sextortion Com groups groom minors, forcing them to produce and share indecent, sexually explicit and/or degrading images, commit extreme self-harm, and suicide. This can also include extortion whereby they will force someone to give money, property, or services through **threats of harm** (physical, reputational, or financial). The threat is usually about violence, damage, or exposure of secrets.

2. Cyber Com groups engage in cybercriminal activities (such as swatting and doxing), often escalating to the targeting of organisations and infrastructure (e.g. network intrusion and ransomware).

3. Offline Com groups promote opportunistic, real-world violence including arson, assault, and murder. They may also share extremist content linked to terrorist organisations.

N.B. Key to this threat is offenders working together as part of an online group to commit criminality across those three pillars. Violence-fixated individuals or those committing this type of criminality in isolation sit outside of this definition.

These networks can be used for legitimate purposes (like global gaming communities) or illicit activities including CSAM (child sexual abuse material), gore, violent pornography, and extremist propaganda. Some networks are linked to cult-like ideologies, requiring acts of violence for membership, and are known for tactics like doxxing and swatting.

Victims are typically children or vulnerable adults, and perpetrators are often males aged 14–17 seeking notoriety and peer validation. The networks are fluid, decentralized, and difficult to track, making cross-border intelligence sharing and digital literacy critical for prevention and response.

Who is at risk?

Primary victims are predominantly children under 18. Offenders specifically target vulnerabilities in people seeking help and advice on forums for:

- mental health disorders
- neurodiversity
- self-harm and suicidal ideation
- body image concerns

- discrimination on the basis of ethnicity, race and/or religion
- sexual orientation exploration
- gender identity exploration
- those who have experienced sexual or physical abuse
- substance misuse
- physical vulnerabilities (elderly, homeless)

The harm caused by these groups can extend beyond the individual directly targeted. Previous cases have identified that victims may be manipulated or coerced into harming family members, often under threat, blackmail or psychological pressure. This can include being forced to physically or sexually abuse siblings or other children, or to injure or kill pets.

As often seen in cases of grooming and coercion, victims of Com group offending may not recognise or identify themselves as a victim. This may present as reluctance to engage with professional support, and in extreme cases, seek to disrupt safeguarding attempts by targeting frontline professionals, including officers through 'doxing' (publishing personal information), 'swatting' (making false emergency calls) or live streaming safeguarding visits.

Examples of harm are below;



Doxxing:

- **Definition:** Doxxing is the act of publicly revealing someone's private information (such as their real name, home address, phone number, or workplace) without their consent, usually with malicious intent.
- **Impact:** It can lead to harassment, stalking, identity theft, and even physical harm. Victims often experience fear and trauma because their personal safety is compromised.

Example of Doxxing

- A person in an online gaming forum gets into an argument. Another user searches for their real identity and posts their full name, home address, and phone number publicly on social media. This exposes the victim to harassment and stalking.

Swatting:

- **Definition:** Swatting is a dangerous prank or attack where someone makes a false emergency report (such as claiming there's a hostage situation) to send armed police to a victim's address.
- **Impact:** This can result in severe emotional distress, property damage, and even injury or death during the police response. It's considered a criminal offense in many jurisdictions.

Example of Swatting

- Someone calls emergency services pretending there's a hostage situation at a streamer's house. Police respond breaking into the home while the streamer is live online. The victim is terrified, and the situation could lead to injury or worse. Doesn't have to be live streamed and can happen for harassment or revenge purposes.

Who are the suspects?

Engagement and the sharing of extreme content in Com groups may [but not always] appeal more to young people who:

- are socially rejected or isolated offline
- are seeking belonging and community
- spend significant amounts of time online
- are often unsupervised online for extended periods
- are seeking approval and notoriety from other group members
- are neurodivergent
- have unstable home environments

How to recognise the warning signs

Possible victim indicators

- Self-harm, such as skin lacerations depicting numbers, symbols, initials, usernames or group names (known as 'cutsigns' or 'fansigns')
- Numbers, letters symbols written in blood, knowns as 'blood signs'
- Reluctance to engage with authorities, fear of consequences associated with disengaging from an online group
- Unwillingness to surrender electronic devices
- Continued engagement with offenders after police intervention
- May livestream police visits or message the group to demonstrate non-compliance
- Unexplained injuries to siblings or pets
- Possession of extremist symbols (e.g. swastikas, occult symbols)

Possible offender indicators

- Promoting an online network or group, or encouraging others to join
- Possession of extreme content on their device, including child sexual abuse material, bestiality, the infliction of injuries or suicide and terrorist material
- Banners, symbols, or extremist flags in home environment

- Showing an interest in violence or extreme themes
- Unexplained injuries to siblings or pets

Possible Cyber Com-specific indicators

- An intense interest in cyber activities
- In possession of advanced software that does not reflect typical use
- An advanced understanding of digital technologies, hardware, and software
- 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)
- A known history of hacking, SIM swapping, swatting, Distributed Denial of Service (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

DCI 1637 Chris Cook – Warwickshire Police

20/11/25