MAY 2025
READOUT

Youth Radicalisation and Harm in Online ("COM") Networks

NABS+ COMMUNITY EVENT

OVERVIEW

We conducted two expert roundtable events to develop an understanding of the phenomenon commonly referred to as, "The COM" (also known as "com groups", "com networks" and "community groups"; e.g., 764, NoLivesMatter, Manic Murder Cult, Order of 9 Angles). We suggest the following multi-agency definition:

The COM are competitive, sadistic, and exploitative transnational online networks in which members achieve status and social capital gains for the perpetration or incitement of violence, degrading acts, self-harm, and/or cybercrime, and the associated generation and sharing of extreme content (including terrorism-related material, and content depicting child sexual abuse, self-harm, and animal cruelty).

Key characteristics

- Members of the networks may engage in multiple criminal offences, and incite or facilitate a variety of harms. These include radicalisation, terrorism (TACT) offences, incitement and perpetration of violence and self-harm, child sexual exploitation and abuse (CSEA), cybercrime, and violence against women and girls (VAWG).
- The most salient and material threats presented by com groups are the incitement of death by suicide, and spontaneous acts of public violence.
- Victims of com groups are usually children. Members of the groups have an approximate age range of 14-17 years old (although there are also adult participants).
- Victims are most frequently young females, in particular (but not exclusively) from vulnerable communities in which the behavioural and social conditions exploited by com groups exist, such as self-harming and/or disordered eating communities.
- Victims are often groomed and can become offenders.
- The generation and sharing of child sexual abuse material (CSAM) is not necessarily borne out of a pedaphillic interest, but often is a means by which individual members can achieve social and cultural capital, status, and notoriety within the group.
- Some com groups encourage cybercrime, such as sabotage of critical infrastructure.

- Com groups are characterised by several distinct ideologies and shared beliefs, often including militant accelerationism, left-hand satanism, and folk nihilism.

Why do individuals engage?

- Engagement may be related to multiple risk factors, such as high internet usage, exposure to extreme content, and feelings of disenfranchisement from society. Engagement could also be related to gendered perceptions of grievances (e.g., 'manosphere' content).

- Individuals appear to be motivated to produce, post, and collect extreme content, both as a means of attaining social capital, notoriety, and status within the group and (in the case of CSAM) as a means of exploiting and extorting individuals.

- Creating extreme content (any content explicitly involving a victim) may provide both a means of coercive control for further extorting the victim (and producing more harmful content), and also a means of earning social and cultural capital within the group.

- There is insufficient data to claim that there is a causal connection between neurodiversity and engagement.

- (S)extortion practices may be motivated by financial gain.

- Engagement with com groups may be facilitated through the affordances of social media, as algorithms recommend increasingly extreme content, and increasingly homogenous social groups. The impact of such algorithms should be understood as the result of a person-environment interaction, whereby person-based factors affect people's active browsing decisions, which will impact in turn on the recommendations made by algorithms.

- Com groups often require participation in the generation and sharing of extreme content as a criterion for group membership. This creates a hierarchy whereby status is based on tenure, notoriety, and engagement in sharing (the most) extreme content.

What are the implications for Practice?

There is limited empirical research directly examing the issue, therefore:

- Be careful how you generalise. Most of the insights are from case studies or research from analogue contexts, which while really important, can cause blind spots.

- Be very aware of false positives. Bias towards certain offender characteristics (e.g., neurodiversity) may cause the analyst or others to not search for or identify others.

- Motivation for involvement is complex, and the child involved may not truly understand why they are carrying out their acts. Thus, interventions should not solely focus on motivational aspects of engagement and disengagement.

- Frequency of posting may not necessarily indicate high motivation. Sometimes infrequent posters may pose a greater threat. Therefore, be careful of prioritising resources based on this behaviour.

- It maybe at times difficult to separate those who are interested in one aspect of the COM group (e.g., cybercrime or CSEA) from those who are more 'generalist'.

Priority Future Research Areas

Academic research should focus on the following priorities:

- Mapping the scope, nature, and ecosystem to identity scale/prevalence
- Understanding motivations for engagement and disengagement
- Identifying pathways of engagement and roles
- Responses and interventions to protect and disrupt

This roundtable was one of three held as part of the NABS+ Community Event, designed to surface key challenges, priorities, and research needs across national security and defence. Insights from these discussions directly shaped the focus of the newly launched NABS+ Commissioning Call.

For more details on the call topics and how to apply, visit: https://crestresearch.ac.uk/nabs/commissioning

RECOMMENDATIONS

- International collaboration between law enforcement agencies, and between academic researchers and law enforcement.
- Academic research on the priority areas outlined above.
- Data sharing and access for researchers to facilitate academic research.
- Consensus on a multi-agency definition to facilitate operational response.
- Strategy to deconflict and clarify operational response.
- Alerts to notify frontline staff, parents, and carers of the risks and threats, including suitable points of contact for concerned staff/carers.
- Development of educational and training material for frontline staff, parents and carers, and law enforcement.
- Development of mechanism for sharing new insights/standard operating procedures across agencies, domestically and internationally.

NABS+ (NetworkPlus for Analytical Behavioural Science in security and defence) is funded by UKRI and administered by the Economic and Social Research Council (ESRC Award ES/Z502716/1). The views expressed by the researchers and team members are their own and should not be taken as representative of views held by those who fund NABS+. For more information, visit: www.crestresearch.ac.uk/nabs