NCA
National Crime Agency

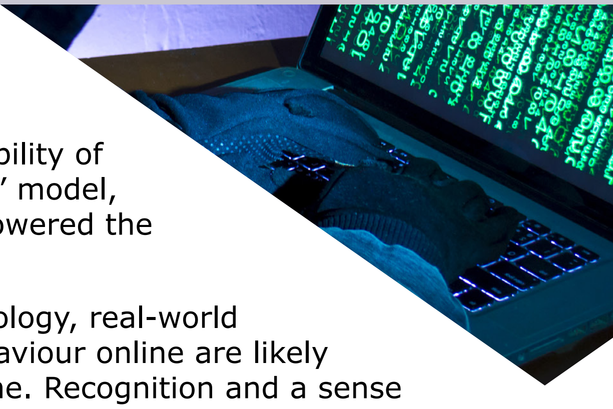
Intelligence Assessment

Youth Pathways into Cyber Crime in the UK

NAC
National Assessments Centre
for Serious and Organised Crime

NAC(22)311

June 2022



Key Judgements

KJ1 (High Confidence): It is almost certain that the availability of DDoS for hire, similar tools offered through the 'as-a-service' model, and step-by-step instructional videos on social media have lowered the barrier of entry into cyber crime.

KJ2 (Moderate Confidence): High IQ, an interest in technology, real-world social isolation, and a higher appetite to engage in risky behaviour online are likely identifiers of those at risk of becoming involved in cyber crime. Recognition and a sense of belonging within social networks are likely to be key motivating factors for progression of cyber offences.

KJ3 (Moderate Confidence): Cyber Prevent activity can deter progression of cyber offending. It is likely children would benefit from Cyber Prevent input before they start playing online games and risk becoming involved in illegal activity. It should contain information about the Computer Misuse Act 1990 and how to develop and apply cyber skills legally. It is worth noting that the vast majority of online gamers do not progress from gaming into cyber crime.

Key Findings

KF1: The major pathways and motivations into cyber crime are broadly the same as those identified in *0325-CYB Pathways into Cybercrime 2017*.

KF2: Females make up about 40% of gamers in the UK, but less than 1% of cyber crime Prevent referrals.

KF3: Frequently, young cyber criminals initially learn how to use cyber crime tools, such as web stressers, via video hosting sites prior to interactions on forums.

KF4: Some offenders using DDoS for hire tools in online gaming do not know their actions are criminal.

KF5: Online gaming provides a common initial exposure and pathway into UK based, low level cyber crime, but can also provide the skills for more complex offending.

KF6: Social networks are an important driver for cyber crime as they provide a learning environment and motivation for offenders.

KF7: Younger cyber criminals perceive cyber crime is not a priority for law enforcement and that low level offences will not attract attention.

Team: Cyber, National Assessments Centre

Introduction

1. This assessment outlines the common initial exposures and pathways for young persons[1] into UK based, low level cyber crime, as well as how this can progress to complex offending. It explores the social and technical pathways into, through and out of the cyber offender lifecycle in the UK. We have analysed law enforcement Cyber Prevent and Pursue activity, as well as reporting from academia and industry partners.

2. The assessment addresses the following questions:

   - What are the motivations and pathways into cyber crime?
   - What changes have occurred since 2017 and why?
   - What are the key intervention points where NCA resources should be targeted?

Summary

3. The major pathways into cyber crime and the factors that motivate young persons are broadly the same as those identified in 2017. Online gaming is highly likely a common exposure and pathway into UK based cyber crime offending. It provides an entry into low level cyber crime but can also provide the skills for more complex offending. Most offenders using Distributed Denial of Service (DDoS) for hire tools in online gaming do not know their actions are criminal.

4. Frequently, cyber criminals initially learn how to use cyber crime tools via video hosting sites, rather than through interactions on forums. It is almost certain that the availability of DDoS for hire, similar tools offered through the 'as-a-service' models, and step-by-step instructional videos on social media have lowered the barrier of entry into cyber crime.

5. High IQ, an interest in technology, real-world social isolation, and a higher appetite to engage in risky behaviour online are likely identifiers of those at risk of committing cyber offences. Social networks are an important driver for cyber crime, as they provide a learning environment and motivation for offenders. Recognition and a sense of belonging within social networks are likely to be key motivating factors for progression of cyber offences.

6. Younger cyber criminals incorrectly perceive that cyber crime is not a priority for law enforcement, and that low level offences will not attract attention. Cyber Prevent activity can deter progression of cyber offending. It is likely children would benefit from Cyber Prevent input before they start playing online games and risk becoming involved in illegal activity. It should contain information about the Computer Misuse Act 1990 and how to develop and apply cyber skills legally. It is worth noting that the vast majority of online gamers do not progress from gaming into cyber crime.

[1] For the purposes of this report 'young persons' refers to people between 10 and 21 years old.

What are the Pathways into Cyber Crime in the UK?

Common Initial Exposures to Cyber Crime

7. It is highly likely a common initial exposure and pathway into low level cyber offences is through online gaming and, to a lesser extent, social media account takeovers. In many instances, the young person was first exposed to cyber crime as a victim or as a friend of a victim.

8. Low level cyber offender's motivations likely stem from online gaming, where DDoS attacks against opponents are common. This is most prevalent with PC gaming, but also occurs in console gaming. Young gamers, including some at primary school age (up to 11), become victim to DDoS/stresser attacks which are used in online gaming to force the user offline during play (a process known as 'booting').[2] The victim consequently explores and experiments with DDoS for hire tools. This results in some using these tools against others, both as a form of revenge and to get an advantage during gaming.

9. Law enforcement reporting suggests it is also likely that social media or gaming account takeovers are a common initial exposure to cyber crime. In a typical scenario, an individual, usually secondary school age (11-18), will have their accounts 'hacked'. This is often by someone in their social network, motivating the individual to identify how it happened. As with gaming, this leads the subject to experiment and take revenge against those who 'hacked' them.

Social Networks

10. It is highly likely that off and online social networks are a driver for cyber crime. Lower level cyber offenders are influenced by gaming social networks to DDoS attack each other and perform other anti-social behaviours, such as account takeovers of social media accounts. Offline social networks also play a part; for example friends with a similar interest and skill set in computing, who encourage each other to commit escalating offences.

11. Networking also develops as offenders progress onto more skilled offending. There are a variety of motivations for this, including curiosity and a drive to learn new skills. However, it is likely that a key motivation for developing skills and engaging in an escalating pattern of offending is the sense of belonging and kudos within these networks. A Social Policy Think Tank identified that individuals who perceive themselves as socially isolated in the real world are more likely to be influenced by online social networks, and this sense of belonging will counteract their real-world social isolation.

Progression into More Complex Cyber Crime

12. Most young people committing low level cyber offences stop after law enforcement contact or by leaving contributing social influences like hacking communities within some forms of gaming. However, a smaller group will develop their skills and progress onto other offending. In relation to DDoS incidents researched for this assessment, eight (12%) of 67 young people went on to commit more serious cyber offences. This progression towards more serious cyber offences occurs through an evolution in skills, curiosity and social networks.

[2] According to Imperva Research Labs 2019 Global DDoS Threat Landscape Report, gaming accounted for about 36% of DDoS activity worldwide in 2019.

13. It is a realistic possibility that the main driver for this progression is an interest in technology and computing. This interest is evident in the types of offending identified. The use of DDoS for hire tools is prevalent in referrals from schools or local policing, but offences requiring a greater skill level, such as network intrusion, were also common. Many of these offenders used network intrusion techniques to bypass school and parental controls or used their school as a target to test their skills. Such skills represent a marked step-up from the DDoS tools used in gaming and require the individual to have an interest in computing and a desire to learn. In order for this interest to become a driver, there must also be the correct environmental factors, such as exposure to cyber crime as a victim or participation in groups committing cyber offences.

14. There is an incorrect perception among younger cyber offenders that the level of crime they are involved in is below the threshold for law enforcement activity. The belief that the internet provides a degree of anonymity, and that they will not be of interest to law enforcement because of their age, adds to this mistaken judgement that they will not be identified or arrested. This is likely to be a major motivating factor in them continuing and progressing with their offending.

15. It is likely gaming is used in other ways as a pathway into more technically advanced cyber crime. Altering or creating extra content for games, or ‘modding’, has long been part of gaming and widely discussed within the gaming community. It is likely that the skills acquired in modding, such as coding, can then be used to create and modify cyber crime tools. Modding is a legal ‘grey area’, mostly concerning copyright. Some games’ publishers deter gamers from creating and using mods, which can include banning players. Other publishers actively encourage modding as it can increase the life span and interest in their games. Many of these companies produce tools to help modding and these kits can provide an introduction to coding skills.

Forums

16. It is likely that for some young people, participation in the gaming sections on forums provides an introduction to hacking forums. These are often contained on the same websites, where offenders can discuss their skills and learn new techniques from other experienced individuals. Gaming forums are likely to be where low level offenders become aware that techniques such as DDoS for hire or credential stuffing[3] can be used against more complex targets.

17. Although English-language hacking forums exist, the most sophisticated, and by definition those linked to the most sophisticated cyber criminal groups, are exclusively Russian-language. It is therefore highly likely that the ability to speak Russian with a degree of fluency creates a barrier of entry for UK cyber criminals.

Other Pathways

18. There are almost certainly other pathways into cyber crime. For example, individuals can be drawn into cyber crime through their job; it is likely these offenders are opportunistic, using access and skills acquired as part of their work. It is unlikely that individuals seek out employment to commit these offences. It is also unlikely that criminal exploitation is a major pathway into cyber crime, however it cannot be ruled out that young people will be exploited by SOC criminals to commit offences.

[3] Credential Stuffing is a cyber attack whereby lists of stolen usernames/email addresses and passwords are used to gain unauthorised access to an account through large-scale automated log-on requests.

What Changes Have Occurred Since 2017 and Why?

19. It is a realistic possibility that the average age of offending and age of initial exposure to cyber crime has fallen since 2017. This reflects law enforcement consensus and there are a handful of reports of children as young as ten being reported for intervention activity. It is a realistic possibility that most young UK cyber crime offenders are aged 13-17 at the time of initial offending.

20. This assessed fall in average age of offending correlates with more children becoming involved with online gaming. Using data from 2019, Ofcom, the UK's communications regulator, reported that 59% of 5-15 year olds now play games online, up from 45% in 2015. More specifically, the report found that 66% of 8-11s and 72% of 12-15s are now involved in online gaming. This increase correlates with the greater popularity of games favoured by younger children, such as Fortnite.[4]

21. It is almost certain that the availability and accessibility of cyber crime tools, especially DDoS for hire and Remote Access Trojans (RATs) have lowered the barrier of entry into cyber crime. DDoS tools can still be purchased on the clear web.

22. It is likely individuals learn of the existence of these tools and where to purchase them from discussions on gaming forums, rather than cyber crime specific ones. This again links to a lack of knowledge of the law. Subjects do not necessarily know that these tools and actions are criminal, but rather see them as part of gaming and something widely spoken about on gaming forums. These tools are advertised as legal penetration testing tools, further legitimising this offending.

23. It is likely that how young people interact with social media is a factor in this learning. The presence of cyber crime tools and instructional videos on these platforms suits how young people already consume media. This links to their gaming activities; streaming is now a large part of the gaming community, with gaming and use of social media now merged.

What are the Key Intervention Points Where NCA Resources Should be Targeted?

Identifiers of Potential Involvement in Cyber Crime

24. Certain factors such as high IQ, an interest in technology, and real-world social isolation are likely identifiers of those at risk of becoming involved in cyber crime. Academic and industry research suggests that although most individuals committing cyber crime demonstrated high IQ, this did not necessarily correlate with good academic performance. The subjects showed an interest in, and aptitude for, technology and usually an interest in gaming. They identified as experiencing social difficulties in the real world.

25. An individual's character is also likely to be a major factor in determining if they will go on to commit cyber offences following initial exposure. Academic research indicates that those with a higher appetite for engaging in risky behaviour are likely to be driven to identify the methods used in DDoS or account takeovers, and engage in this activity.

[4] Fortnite is rated 12, however it is known to regularly be played by children as young as eight.

26. Females are estimated to make up 40% of gamers in the UK, but based on analysis of Cyber Prevent cases, they make up less than 1% of cyber crime referrals. The reasons for this are unclear, and further research is required to identify what encourages male gamers to become involved in cyber crime. Anecdotally, many gaming forums are regarded as a toxic environment for females, which may deter many from engaging in these social networks and as a result not engage in discussions around cyber crime tools.

27. About 17% of subjects referred for Cyber Prevent or Pursue activity between 2017 and 2020, either had a diagnosis for Autistic Spectrum Disorder (ASD) or self-referred as having autistic-like traits. This rate is far higher than ASD diagnosis in the general population (1-2%), but does not provide a conclusive link between those with ASD and cyber crime. Academic research has suggested that this link may be due to a greater level of digital skills. Autistic individuals are more likely to be drawn to computing as it suits their logical thinking style, evidenced by higher levels of ASD in employees and students involved in computer science and related disciplines.

28. It is a realistic possibility that the educational and healthcare support available for young people with an ASD diagnosis prevents many of them from becoming involved in cyber crime. This is supported by academic research which suggests an ASD diagnosis is not a contributing factor in committing cyber crime. However, when an ASD diagnosis is absent, autistic-like traits and an interest in computing are a driver for involvement in cyber crime.

Evaluation of Prevent Activity

29. Cyber Prevent activity linked to investigations is unlikely to be the best way to identify skilled cyber offenders. Analysis was conducted on a sample of 188 individuals reported to the National Cyber Crime Unit (NCCU) for Cyber Prevent activity between 2017 and 2020. Almost all those identified by the NCCU were for low level, low skilled activity, such as DDoS for hire and purchasing web stresser tools. Those reported by schools and local policing were likely to be for more skilled offences such as network intrusion or hacking a peer’s social media account.

30. Before intervention activity, law enforcement has little if any interaction with the subjects. This may explain why referrals from other sources appear better at identifying skilled cyber offenders. In most cases, characteristics such as a high IQ and higher appetite for risk will be more apparent to teachers, parents and others in direct contact with the young person.

31. Cyber Prevent activity is widely seen by law enforcement to work. Most subjects referred for interventions engage well and less than 5% of individuals (9 of 188) have been identified committing further offences. The perceived anonymity provided online is not present in other areas of crime; it is likely that this acts as a deterrent for offenders to become involved in offline criminal activity. Evaluation of data for those who ceased their criminality both before and after law enforcement activity, and those who continue in spite of it, may develop our understanding of the most effective Cyber Prevent activity.

32. Early intervention for criminals committing low level cyber offences and who have autistic traits is likely to have a significant effect. Concepts like Immersive Labs[5] and the Cyber Prevent intervention workshops are likely to provide the impetus to influence these individuals to use their skills in legitimate industry.

33. It is a realistic possibility that the age of initial exposure to cyber crime has fallen and Cyber Prevent activity needs to be targeted at a younger audience. Current education packages target Key Stage 3;[6] it is a realistic possibility that those at risk of becoming involved in

[5] Immersive Labs is an on-demand cyber skills platform. Prevent activity has included licences to this website, so the individual can test their skills in a safe manner.

[6] Ages 11 to 14.

cyber crime will have already had initial exposure by this time. A package aimed at Key Stage 2[7] children is being developed and it is likely this will limit their risk of being drawn into offending.

34. It is likely packages aimed at younger children that equate online offences to real-world equivalents would be easier for younger people to understand. For example, an education package about staying safe online could compare network intrusion to burglary.

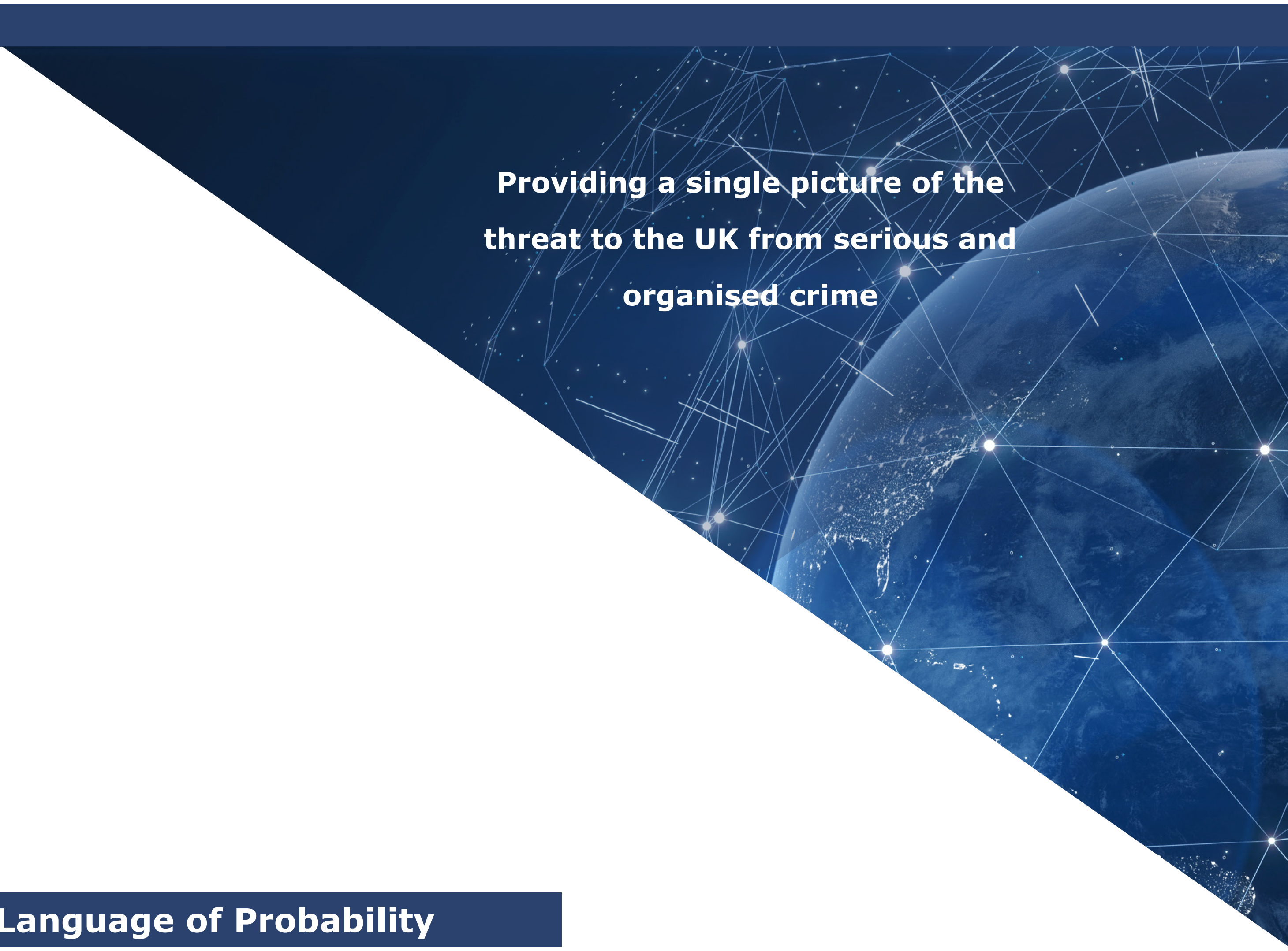
35. There can be a lack of knowledge in the gaming community that DDoS is illegal. As a result, it is almost certain a minority of subjects using DDoS for hire tools to conduct 'booting' do not know that they are committing a crime. Better education about offences within the Computer Misuse Act (CMA) is likely to have a positive diversionary effect on those tempted to commit cyber offences.

36. Initiatives such as Immersive Labs and the CyberLand Challenge are likely to be effective at preventing some individuals from engaging in cyber crime. These initiatives provide a safe way for individuals to test their skills and learn about the CMA. After the Winter CyberLand Challenge in December 2020, of those that responded, the vast majority indicated they had a better understanding of CMA after the event.

37. While some criminals incorrectly perceive that low level cyber crime is not a priority for law enforcement, recent takedowns of services and malware have demonstrated that these actions are illegal and have impacted on some users. Similar information campaigns and law enforcement operational activity would likely provide a similar deterrent effect for other low level cyber offenders.

38. Many young people who are interested in cyber activities are unaware that their skills can be used constructively in IT security and ethical hacking. Including ethical hacking as a career in the education packages and wider Cyber Prevent messaging is likely to have a strong deterrent effect.

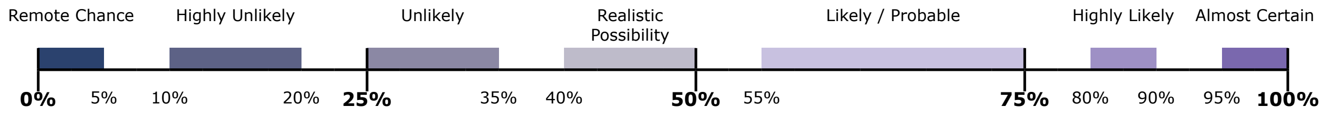
[7] Ages 7 to 11.



Providing a single picture of the threat to the UK from serious and organised crime

Language of Probability

Throughout this paper, language of probability is used, which is defined by the Professional Head of Intelligence Assessment (PHIA) ‘Probability Yardstick’. The probability ranges for such terms are as follows:



Confidence Levels

Confidence levels are attributed to Key Judgements to convey the quality of the evidence used to reach those judgements, and are described as follows:

High Confidence	Good quality and/or corroborated from a range of different sources, or situations where it is possible to make a clear judgement.
Moderate Confidence	Open to various interpretations, or credible and plausible but lacks corroboration.
Low Confidence	Scant or very fragmented, and/or based on sources of suspect reliability.

www.nationalcrimeagency.gov.uk