Sprite+

Security, Privacy, Identity, Trust, Engagement, NetworkPlus

UCL

DAWES CENTRE FOR FUTURE CRIME

THE FUTURE OF CYBERCRIME

Results of an Academic Challenge Workshop and Delphi Study

www.sprite.ac.uk

Contents

Executive Summary

Introduction

This report summarises the output of a two-part Delphi study that elicited and then assessed statements about the potential for new technologies and societal changes to influence future cybercrime by 2030. The study was run by SPRITE+ and the Dawes Centre for Future Crime (DCFC) at UCL between December 2023 and April 2024.

Our approach generated a wide and detailed set of opinions on how cybercrime might evolve in the coming years, drawing on the expertise of a heterogeneous group of experts from across disciplines. In general, although these experts did not achieve strong consensus on every risk, there were few topics where there was strong disagreement.

Findings

A. Risks posed by emerging technology

Emerging technology use cases posing the highest risk by 2030

- Deepfake images, audio, video and personalised messages at scale to facilitate frauds
- Deepfake images and text to facilitate cyberbullying and harassment
- GenAI tools that support criminals who offer cybercrime as a service, particularly creation of novel malware
- Cryptocurrencies exploited for money laundering and to facilitate cybercrimes (e.g., ransomware)

Emerging technology use cases posing a medium-high risk by 2030

- The use of AI tools to create and spread mis/disinformation, fuelling mistrust in online content
- GenAI to create child sexual abuse material and material for sextortion campaigns (at scale), to enable impersonation and identity theft, and to facilitate marketplace scams
- Manipulative/malicious chatbots
- Over-reliance on AI support, creating vulnerability to harmful exploitation

Emerging technology use cases posing a comparatively low risk by 2030

- Extended Reality raises privacy and harassment risks
- Online marketplaces, providing easy access to illegal or grey-market goods and services
- Social media sites and online gaming platforms as sites for harm (e.g., grooming, radicalising, harassment, scams, disinformation)
- Cloud labs and other digital biomanufacturing infrastructure provides opportunities for criminals to disrupt, manipulate or steal technology

- Data collected via neurotechnologies (methods/devices to read or modify brain activity) exploited for (say) extortion or impersonation
- Increasing diversity and scope of biometric data collected with new technologies provides opportunities for criminal exploitation
- The use of autonomous vehicles to create physical damage (e.g., deliver bombs)
- The use of 3D printing to create illicit items (e.g., guns, knives, counterfeit goods)
- The use of quantum computing to undermine encryption

B. Potential risks arising from societal changes

Changes that give rise to highest risk by 2030

- Digitisation of infrastructure raises the risk that cybercriminals will hold infrastructure operators to ransom

Changes that give rise to medium risk by 2030

- Widespread adoption of digital services increases electronic transactions, which become more attractive to criminals using AI to scale attacks on digital business systems
- Adoption of voting technology would create opportunities for cybercriminals to damage electoral integrity
- Overconfidence in understanding of technology makes younger citizens vulnerable to cybercrime
- Remote working provides opportunities for criminals to exploit weaker cyber controls at home (compared to an office)

Changes that give rise to comparatively lower risk by 2030

- Services are increasingly delivered / accessed online, creating an ever-greater attack surface, and making it harder for citizens to recognise and mitigate all potential risks
- Increasing automation (of e.g., messaging services) creates opportunities for criminals to overwhelm citizens and public services with harmful and disruptive information
- Reduction in trust in authorities (e.g. government, traditional media) creates new opportunities for misinformation to spread, potentially exploited by hostile foreign states, which could form ideological blocs to spread disinformation
- Widespread adoption of AI tools creates opportunities for those who can influence them (e.g., data, algorithms) to affect how knowledge is generated and shared
- Markets for medications and genetic enhancements will become premium and so subject to extortion attempts
- Future pandemics will be exploited by cybercriminals (e.g., selling fake medicines, fake experts giving fake advice)
- The use of GenAI to code means developers have less understanding of how to spot potential security vulnerabilities

C. Changes to criminal business models, methods, and ecosystems by 2030

Who becomes a criminal may change

- Children and young people may become drawn into cybercrime (as victims and offenders) through the easy availability and accessibility of cybercrime tools and lack of monitoring / guidance from parents/ caregivers
- Easy and apparently unregulated access to new technologies will lower the barriers for some people to become involved in crime (e.g., creating/consuming synthetic abuse imagery, fraud)

How criminal activity is carried out may change

- New technologies allow 'old' crimes to be committed in 'new', lower-risk, and more efficient ways, without the need for sophisticated technical skills
- The establishment of "cybercrime-as-a-service" models will lower barriers to entry to crime
- Some low skilled cybercrime roles will be replaced by GenAI.
- Cybercrime gangs will force vulnerable people to work for them e.g. in perpetuating online scams
- Criminal networks will rely on small, unmoderated encrypted platforms to communicate (rather than established large messaging/networking platforms)
- Automated translation tools will allow criminals to target victims across borders with minimal friction and ease communication within and between global criminal operations

D. Implications and suggestions for cybercrime responders

- Cybercrime response requires a "whole of society" approach
- Responders need to be more creative, take a harm mitigation approach, and pay greater attention to the impact on victims
- Industry needs to take more responsibility for making their products/services secure
- Greater support for small and medium sized businesses is needed
- International relationships will become increasingly important for government and law enforcement
- Public sector responders will lose out to the private sector in the battle for cybersecurity skills, knowledge and experience
- Academics have an important part to play but need to be more "hands on" and nimble
- More could be done to break down barriers between law enforcement, academics, and industry to enable a more effective and faster response to developments in cybercrime.

E. Conclusion

Overall, experts agreed that the highest risks were from increasing adoption of automation and other AI-enabled technologies. These will enable current criminal activities at greater scale, reach, and effectiveness; will create new opportunities for criminal exploitation, in terms of new and broader attack surfaces; and will lead to the growth of new criminal business models, most notably "cybercrime-as-a-service". These developments will be challenging to counter, requiring a whole-of-society response, including more training and education, industry commitment to safety-by-design, and international cooperation in regulation and enforcement.

About the authors

Emma Barrett is Professor of Psychology, Security and Trust at the University of Manchester, and a co-lead for the UKRI-funded SPRITE+ NetworkPlus for Security, Privacy, Identity and Trust. Her research includes understanding and mitigating risk and harm from new and emerging technologies.

Shane Johnson is Professor of Future Crime at University College London. He directs the Dawes Centre for Future Crime at UCL, and co-directs the EPSRC Centre for Doctoral Training in Cybersecurity, and the EPSRC Centre for Doctoral Training in Cyber-Physical Risk.

Dr. Manja Nikolovska is a Research Fellow at the Dawes Centre for Future Crime at UCL. Her research focuses on how technological and social change can affect the future of crime and 'what works' to reduce it

About SPRITE+

SPRITE+ is the UK NetworkPlus for Security, Privacy, Identity, and Trust. SPRITE+ is a platform for building collaborations across the spectrum of issues relating to digital security, privacy, identity, and trust. SPRITE+ is funded by the Engineering and Physical Science Research Council (grant reference EP/W020408/1). Find out more: https://spritehub.org

About Dawes Centre for Future Crime at UCL

Technological and societal change leads inevitably to new types of crime. The Dawes Centre identifies emerging crime threats and works to deliver pre-emptive interventions for the benefit of society. The Dawes Centre is funded by the Dawes Trust and University College London. Find out more: https://www.ucl.ac.uk/future-crime/

List of tables

Introduction

This report presents the results of a two-part academic consultation exercise run by SPRITE+ and the Dawes Centre for Future Crime (DCFC) at UCL between December 2023 and April 2024.

The purpose was to inform a broader UK Home Office review of its approach to cybercrime, which intends to shape investment in and development of UK Government capabilities, powers, and relationships to respond to cybercrime threats as they evolve over the next five years and beyond. The Home Office lead is the Cyber Policy Unit.

This report summarises the output of a workshop and Delphi study that elicited and then assessed statements about the potential for new technologies and societal changes to influence future cybercrime by 2030 and the response to it.

Methods

Part I: Online workshop

We held an online half-day workshop in December 2023, attended by 39 researchers who self-identified as having expertise in relevant areas and who were not working in UK government or law enforcement. The workshop was based on an earlier Home Office workshop on the same topic (attended by government and law enforcement officials and a small number of academics). We invited applications from across the SPRITE+ and DCFC academic networks. The 39 participants included five facilitators, who are also research-active in this area.

The workshop elicited independent expert views through a series of 20-minute breakout sessions on:

A. The harmful exploitation of new and developing technologies
B. Vulnerabilities from societal changes
C. Changes to criminal business models, methods, and ecosystems.
D. Implications and suggestions for cybercrime responders

Participants were randomly allocated to breakout rooms of 5-8 people to consider each topic. The workshops were designed to provide participants with an opportunity to make their own independent contributions but to also create opportunities for interaction. To do this, for the first five minutes of each session, participants wrote their own responses to the breakout session topics, and the remainder of each session was devoted to discussion and elaboration of the responses.

Reponses were captured using Padlet[1] and more than 450 written posts and comments were generated during the online breakout sessions. After the workshop we analysed

[1] https://padlet.com/

these responses to identify and group the themes and issues that emerged. We combined duplicative responses, and removed unclear or irrelevant comments, resulting in a total of 140 statements about the future of cybercrime that were then used in the Delphi study.

Part II: Online Delphi study

The Delphi method is a future scenario forecasting tool used to elicit opinion from experts on a particular topic. Studies usually involve two or more rounds, with the first being used as a "brainstorming" exercise in which experts are asked a set of open questions about the topics of interest. The responses to these questions are then thematically analysed to identify unique themes or forecasted scenarios. In the second round, the group is typically sent a summary of the findings from the first round and asked to indicate which responses they agree with and to what extent they do so. The second round is completed anonymously and serves to identify where consensus or disagreement exists. Where consensus does exist, this can be used to identify priorities for future action.

For our study, round 1 was conducted during the online workshop. Participants from across the SPRITE+ and DCFC networks were then invited to complete round 2 via an anonymous survey which was open for three weeks in March and April. 34 participants (who included people that did and did not attend the workshop) accepted the invitation and completed some or all survey questions.

Procedure

Because of the volume of material, we presented the statements in four blocks corresponding to the themes A-D identified above, and subthemes that emerged during our analysis (Table 1)[2].

Participants could choose to complete one or more blocks. For each block, participants were presented with the statements from Round 1 and asked questions about each, answering on a 1-9 scale (see Table 2). Within each block, the ordering of statements was randomised for each participant.

After completing each subtheme, participants were asked "How would you rate your overall level of expertise and knowledge on the subtopic of [sub theme]? 1=little or no knowledge, 9=expert). Finally, participants had the option to add free text comments at the end of each subtheme, highlighting important issues that were not already covered.

[2] For a full list of all statements in each block, see Appendix 1

Theme	Subthemes
A. Harmful exploitation of new and developing technologies.	Artificial intelligence (AI)
	Extended Reality (XR)
	Biotechnology, neurotechnology, biometrics
	Other new and emerging technology[3]
	Other platforms and applications
B. Vulnerabilities from societal changes	Digitisation and increasing adoption of new technology across society
	Economic, workplace and skills
	Health
	Politics and international relations
C. Changes to criminal business models, methods, and ecosystems.	Criminal profiles (Who might become a criminal and why)
	Modus operandi
	Criminal ecosystems
D. Implications and suggestions for cybercrime responders	Who should respond
	Developing and maintaining knowledge
	Evolving approaches to tackling cybercrime
	International LEA cooperation
	Protecting organisations
	Government policy and regulation
	Civil society's role
	Academic approaches
	Industry's role

Table 1 Summary of themes and sub-themes

[3] Includes: Distributed Ledger Technology, Quantum computing, 3D printing, Autonomous vehicles and Sensors.

Block	Questions
A. Harmful exploitation of new and developing technologies **(47 questions)**	• By 2030, how harmful (e.g., in financial, emotional or other terms) will this threat be? (1=low harm, 9=high harm) • By 2030, how frequently do you expect this threat to occur in any given period of time? (1=low frequency, 9-high frequency) • By 2030, how easy would it be to apply/develop measures to prevent, detect or mitigate the harm or reduce the rewards for perpetrators? (1=difficult to defeat, 9=easy to defeat)
B. Vulnerabilities from societal changes **(18 questions)**	• By 2030, how harmful (e.g. in financial, emotional or other terms) will this threat be? (1= low harm, 9= high harm) • By 2030, how frequently do you expect this threat to occur in any given period of time? (1=low frequency, 9=high frequency). • By 2030, how easy would it be to apply/develop measures to prevent, detect, or mitigate the harm, or reduce the rewards for perpetrators? (1=difficult to defeat, 9=easy to defeat).
C. Changes to criminal business models, methods, and ecosystems **(26 questions)**	• By 2030, how harmful (e.g. in financial, emotional or other terms) will this threat be (1= low harm, 9= high harm) • By 2030, how frequently do you expect this threat to occur in any given period of time? (1=low frequency, 9=high frequency). • By 2030, how easy would it be to apply/develop measures to prevent, detect, or mitigate the harm, or reduce the rewards for perpetrators? (1=difficult to defeat, 9=easy to defeat) • To what extent do you agree with this statement? (1=not at all; 9= Completely agree)
D. Implications and suggestions for cybercrime responders **(39 questions)**	• To what extent do you agree with this statement? (1=not at all; 9= Completely agree)

Table 2 Questions asked in Delphi exercise

Analysis

We exported the results of the Delphi survey to Excel and calculated the average and standard deviation for each response and, where appropriate, used the latter to establish whether there was consensus across participants. Specifically, consensus was considered to have been observed for responses for which the standard deviation of the rating was within 1.5 points (see, Giannarou & Zervas, 2014).

Previous work on crime and futures (e.g. Gomez-Quintero et al., 2024) has estimated the risk associated with future threats. Calculating risk can inform prioritisation as it helps to identify (say) those threats that are both high harm and high likelihood, and to

differentiate these from those that are (say) highly likely but not anticipated to cause much harm. Consequently, for blocks A and B, we calculated a simple estimate of **risk** by taking the product of the Harm and Frequency ratings (Craig, 2018). Given the range of these ratings (1-9), the maximum risk rating possible was 81.

Findings and discussion

How to interpret the tables

In this section we break down the results for both the workshop and the survey, highlighting participants judgements for each theme and subtheme. Note that the ratings provided are relative (they do not represent absolute values). However, quantification is not possible in studies such as this, and the ratings provide a good way of assessing the relative importance of different threats and the extent to which experts agree.

In the tables summarising harm, frequency, defeatability, and risk:

- Higher values indicate greater harm, higher frequency, but less challenging to defeat.
- Statements are ordered by risk score, from highest to lowest.
- Darker shaded cells indicate strong consensus

A. Harmful exploitation of new and developing technologies

Table 3 provides a summary of how subthemes were rated overall. Participants' perceptions of their own expertise varied by subtheme, as did their average ratings of harm, frequency, and defeatability. The threats associated with generative AI (GenAI) were those that were perceived to convey the highest risks by 2030, and these were considered to be the second most difficult to address. Participants expressed the most confidence in their expertise for GenAI, and the least confidence in their expertise for biotechnologies (rated as posing the lowest risk).

	Participants	*Expertise*	*Harm*	*Frequency*	*Risk*	*Defeatability*
AI, including generative AI	*11*	*6.1*	*7.6*	*7.3*	*55.7*	4.1
Extended Reality	*11*	*4.4*	*6.6*	*5.6*	*37.2*	5.0
Other platforms and applications	*10*	*5.7*	*5.8*	*5.8*	*34.2*	4.7
Other new emerging technologies (merged category[4])	*10-12*	*4.6*	*6.2*	*5.0*	*28.9*	4.6
Biotechnology, neurotechnology, biometrics	*10*	*4.1*	*5.8*	*3.7*	*22.2*	3.8

Table 3 Mean ratings for each subtheme (ranked by mean risk)[5].

[4] This category consisted of various emerging technologies including cryptocurrencies (n=11), autonomous vehicles (n=11), 3D printing (n=11), quantum computing (n=10) and sensors (n=12).

[5] Participants = number of participants completing questions on each subtheme. Expertise = mean score for self-reported overall level of expertise and knowledge on this subtopic (where 9=expert).

Artificial intelligence (AI)

In the workshop, concerns about GenAI, including deepfakes, predominated, with a total of 18 threats identified. Table 4 shows the specific threats identified rank ordered by their individual risks. For ease of interpretation, the table is organised into high, medium, lower and low risks. Cells shaded blue are those for which consensus was achieved (i.e., where the standard deviation of the ratings was within 1.5 points). Overall, there was strong consensus that the use of GenAI for fraud and extortion was likely to be widespread and harmful, but participants were also broadly in agreement in their harm and frequency ratings for most harmful applications of GenAI.

ARTIFICIAL INTELLIGENCE	Harm	Frequency	Defeatability	Risk
HIGHER RISK (>60)				
Generative AI will enable the creation of convincing Deepfake images, audio, video and personalised messages at scale to facilitate frauds including romance and phishing scams.	8.1	8.1	2.9	65.9
Generative AI will assist criminals involved in malware-as-a-service, by being used to create new variants, variants of existing malware or to make malware more difficult to detect.	8.0	8.1	4.6	65.4
Generative AI will enable the creation of convincing Deepfake images and audio in real-time to facilitate CEO or similar types of fraud	8.2	7.6	4.1	62.7
Generative AI will facilitate cyberbullying and harassment, including, for example, peers creating deepfaked videos of young people engaging in sexual behaviour.	7.9	7.9	4.1	61.9
Generative AI tools (e.g. LLMs, Dall-E, Stable diffusion, and audio cloning services) are already user-friendly and will enable criminals to offer cybercrime as a service.	7.8	7.7	3.5	60.1
MEDIUM RISK (51-60)				
The use of AI tools to gather and curate more accurate personal details of individuals and organisations will enable more sophisticated disinformation dissemination tools (e.g. via chatbots).	7.9	7.5	3.9	59.4
Generative AI will facilitate the creation of Child Sexual Abuse imagery at scale.	7.8	7.6	4.3	59.3
Generative AI will erode trust in online content (written, audio and video).	7.6	7.6	3.9	58.2
AI videos will be produced by scammers to induce internet users to transfer money to invest in cryptocurrency scams.	7.3	7.8	5.7	57.5
AI-assisted image generation techniques will increase online sextortion; offenders (including sextortion gangs) can use publicly available images of a target to generate convincing sexual blackmail material for financial gain.	7.7	7.4	4.4	57.0
Generative AI and Large language models will be used for online marketplace scams.	7.5	7.5	4.3	56.7

Reliance on, and belief in, the outputs of "helper" tools like ChatGPT (as opposed to other sources of information) will leave people vulnerable to misinformation campaigns and various forms of cybercrime.	7.4	7.5	4.3	55.7
Generative AI will enable the creation of seemingly realistic and increasingly substantive identities - personal or corporate - which can compromise security and background checks.	7.9	6.7	4.6	52.9
The growing use of AI chatbots for social / romantic relationships and support puts individuals at risk of manipulation by the organisations or individuals who programmed the chatbot.	7.1	7.2	3.3	51.1
LOWER RISK (25-50)				
Generative AI will be used to produce fake video to encourage internet users to take violent action or engage with extremist groups.	7.5	6.7	3.3	50.0
Generative AI will exacerbate challenges around anonymity and/or lack of attribution online.	6.9	7.1	3.8	48.7
Generative AI will allow lone actors to create and manage entire networks of authentic-seeming disinformation	7.3	6.6	4.3	48.3
Algorithms in recommender systems will empower influencers (e.g. Andrew Tate) with extreme and hateful views	6.9	6.9	3.7	47.7
Generative AI will be used in e-whoring scams, where images are used to falsely advertise sexual services online.	6.7	5.9	4.3	40.0

Table 4 Potential harmful deployments of AI (average ratings for harm, frequency, defeatability, and risk)

Participants suggested that within the next five years **Gen AI tools** (e.g., Large Language Models, Dall-E, Stable Diffusion, and audio cloning services), which are already user-friendly, would be widely adopted by criminals and others with harmful intent. Participants also identified risks associated with the use of chatbots and other AI-powered technologies.

Participants agreed that AI tools would be used for **a variety of fraudulent purposes**, from automating victim detection and targeting to creating convincing persuasive messages (which could be text, audio, or images). These would be used to facilitate phishing, CEO fraud and romance scams, to promote fraudulent investment schemes, or to masquerade as an authorised user and gain access to sensitive systems and databases.

Other harmful deployments of AI included the use of GenAI to generate convincing sexual images from publicly available images of a victim as part of an **extortion** attempt or to **bully** or **harass** them, and the potential for it to facilitate the creation of child sexual abuse imagery at scale.

Participants also agreed that AI tools will make the creation and dissemination of **mis- and disinformation** easier, and disinformation could potentially be personalised to increase its impact. GenAI could be used to produce fake video which could be used by **extremist groups** to radicalise users or encourage violent action. The use of AI in this way could erode trust in online content (written, audio and video).

Participants also raised ways in which GenAI might **undermine defences against online harms**. For instance, GenAI is likely to exacerbate current challenges around **anonymity** and **attributing responsibility** for harmful actions. Novel modes of content delivery and generation, including extended reality and GenAI, were anticipated to be used to **increase noise** (misleading content, irrelevant content, etc.) to confuse users (which could be private individuals or operators of industrial/ government security apparatus), or to facilitate cyber-attacks.

AI tools were also expected to change criminal business models (see also Theme C). For instance, participants thought that **automated translation tools** would allow criminals to target victims across borders with minimal friction. GenAI has the potential to create new **malware** and new variants of existing malware, making malware more difficult to detect, exploiting new or existing vulnerabilities, or simply operating at larger scale.

None of these potential harmful deployments of AI was considered easy to defeat, although participants varied more on their opinions about defeatability than they did the harms of these threats. Uses of DeepFakes for mass fraud were considered the most challenging to defeat.

Extended Reality (XR)

These technologies include virtual reality, augmented reality, and haptics hardware and platforms, which are beginning to gain traction in education, industry, retail, and leisure sectors. They are sometimes referred to as Metaverse technologies (see, Gómez-Quintero et al., 2024).

As shown in Table 5, participants perceived the most risk of harm would be in social spaces (e.g., VR chat rooms, multiplayer games) where **abuse and harassment**, particularly against children, women, and users from marginalised communities, already occurs. Such spaces are anticipated to be used by criminals to 'groom' **children for sexual abuse and exploitation**, and children exposed to or engaged in age-inappropriate sexualised activity in virtual reality could be exploited by criminals for **blackmail/extortion** and **bullying**, although participants did not reach a consensus on this latter threat.

These technologies gather vast amounts of data about users and bystanders via integrated sensors. There was consensus that this data could be used by hostile actors to infer sensitive information about users and bystanders (e.g., their locations, identity, mental state, emotions, and even in some cases their sexual orientation and personality traits). This could be used for **blackmail** or **fraud** (e.g., impersonation, targeted scams), but despite their being a consensus, the harm perceived was lower than for most of the other threats.

There was also consensus on the risk posed by bad actors hijacking augmented reality glasses to **display hate crime** and other unpleasant material, although the anticipated risk was the lowest for all threats identified in this sub-theme. There was less consensus

on the potential for immersive environments to be used to **spread problematic information** (misinformation, disinformation, hate speech). For instance, it was suggested that 'digital schools' and other immersive learning environments will appear, devoted to spreading conspiracy theories under the guise of truth, however, not everyone agreed about these threats.

The threats associated with XR were not considered to be particularly easy or difficult to defeat, with most rated 5 on the 9-point scale (1=difficult to defeat, 9=easy to defeat).

EXTENDED REALITY (XR)	Harm	Frequency	Defeatability	Risk
LOWER RISK (25-50)				
Abuse and harassment, particularly against children, women, and users from marginalised communities, will be amplified in virtual reality.	7.4	6.8	4.9	50.2
Criminals will 'groom' children using social virtual reality and multiplayer VR gaming for sexual abuse and exploitation.	7.4	6.3	5.0	46.6
Children exposed to or engaged in age-inappropriate sexualised activity material in virtual reality will be exploited by criminals for blackmail/extortion and bullying.	7.3	5.9	4.2	43.4
Novel modes of content delivery and generation, including extended reality and generative AI, will be used to increase visual noise (i.e., misleading content, irrelevant content, etc.) to confuse users (which could be private individuals or operators of industrial/government security apparatus), in order to facilitate cyber-attacks.	6.7	6.1	4.7	41.0
Extremists will find the metaverse to be the perfect space to circulate and legitimise their discourses.	5.8	6.2	5.1	36.0
'Digital schools' and other immersive learning environments will appear, devoted to spreading conspiracy theories under the guise of truth.	5.9	5.8	5.3	34.0
Hostile actors will gain access to data collected by integrated sensors in extended reality headsets (virtual reality, augmented reality), and use this to infer sensitive information about users and bystanders (e.g., their mental state, emotions, and even in some cases their sexual orientation and personality traits) that could be used for blackmail or fraud.	6.5	4.7	5.4	30.2
LOW RISK (<24)				
Individuals or groups will hijack augmented reality glasses to display hate crime and other unpleasant material.	5.7	2.9	5.1	16.6

Table 5 Extended reality technologies (average ratings for harm, frequency, defeatability, and risk)

Other platforms and applications

As shown in Table 6, participants agreed that the easy availability of cybercrime tools (**cybercrime as a service**) will enable offending for those without technical expertise or existing crime connections. Similarly, there was consensus that badly moderated / policed **marketplaces** in the clear or dark web will continue to allow the sale of, or access to, illegal or grey-market goods or services.

The lack of quality control in online marketplaces (even well-known marketplaces like Amazon) was anticipated to contribute to the spread of mis- and **disinformation**, and there was concern that it will be impossible to identify authentic vs inauthentic texts[6]. There was strong consensus that this would be moderately challenging to defeat (average 4.6 on a scale of 1 (easy) to 9 (hard to defeat)).

Participants showed some disagreement over the potential for **online gaming spaces** to create new opportunities for malign actors to find ways of doing harm that will be impossible to moderate/safeguard against. This could include meeting and radicalising others, grooming children for sexual abuse, social engineering for fraud, harassment, and bullying. There was greater consensus that peer-to-peer scamming of users in multiplayer games will escalate, with young people being drawn into cybercrime through the ease of scamming other young users[7].

During the workshop, participants elaborated on the ways in which **social media platforms** would continue to facilitate harm: for disinformation campaigns, fraud operations, and popularising criminal micro-trends (e.g. shoplifting flashmobs), potentially leading to copycat crimes. They noted the potential for more instances of people (particularly children and teenagers), becoming habituated to graphic and violent content online, potentially leading some to act out this violence in real life[8].

The threats associated with these other platforms and applications were not considered to be particularly easy or difficult to defeat, with most rated between 4 and 5 on the 9-point scale (1=difficult to defeat, 9=easy to defeat).

---

[6] One participant stated that "Amazon's top sellers in the 'vaccines' category during the pandemic were all anti-vaxx; at one point almost 400 different editions of the January 6 Report were available on Amazon.com and there was no way to know if any of them contain disinformation or report them if they did".)

[7] E.g., see https://www.ign.com/articles/inside-robloxs-criminal-underworld-where-kids-are-scamming-kids

[8] E.g., "Girl X" (convicted of the murder of a school mate in 2023) "told the jury she began to fantasise about killing people at the age of 14, when she began to take an interest in 'dark materials' such as videos of murder, torture, and serial killers… [and] used an app to search for the materials on the dark web". https://www.bbc.co.uk/news/uk-england-manchester-67660475

OTHER PLATFORMS AND APPLICATIONS	Harm	Frequency	Defeatability	Risk
MEDIUM RISK (51-60)				
It will become even easier to buy cybercrime tools (cybercrime as a service) and buy victims for digital crime, making the tools more accessible for those who don't have technical expertise or existing crime connections.	7.3	7.2	4.2	52.2
LOWER RISK (<25-50)				
Badly moderated / policed marketplaces in the clear or dark web will allow the sale of, or access to, black or grey market goods or products, sale of fraudulent products and money laundering to go unpunished.	6.4	6.1	5.3	39.2
Criminals will hack trusted websites, devices (including AR devices) and public billboards to display malicious QR codes.	6.0	6.0	4.7	35.5
Peer-to-peer scamming of users in multiplayer games will escalate, with young people being drawn into cybercrime through the ease of scamming other young users.	5.9	5.9	4.4	34.8
Online marketplaces will not maintain any quality control, leading to negative outcomes: It will be impossible to identify authentic vs inauthentic books.	5.4	5.8	4.6	31.7
Vast online gaming spaces, offering greater freedom and realism, will create new opportunities for malign actors to find ways of doing harm, that will be impossible to moderate/safeguard against.	5.6	5.2	4.7	29.5
LOW RISK (<24)				
People, particularly children and teenagers, will become habituated to graphic and violent content online and this will lead some to act out this violence in real life.	4.2	4.2	4.9	17.9

Table 6 Online platforms, marketplaces and gaming services (average ratings for harm, frequency, defeatability, and risk)

Biotechnology, neurotechnology, biometrics

Participants identified potential harms associated with the development of **biotechnology**, most notably synthetic biology[9] (see Table 7). There was agreement that a high level of harm would be caused if hostile actors target cloud labs and other digital biomanufacturing infrastructure to disrupt, manipulate or steal biomanufacturing processes (e.g., vaccine development).

Otherwise, the Delphi participants disagreed about the degree of potential harm and the likely frequency for the other threats identified in this topic area, and overall these threats were not considered as high risk as, for example, the threat from GenAI.

[9] E.g., https://www.ucl.ac.uk/future-crime/sites/future_crime/files/synthetic_biology_and_future_crime_final_021221.pdf

Although still in its infancy, the field of **neurotechnology** (methods or devices that are designed to read or modify brain activity) is rapidly developing[10], with medical and non-medical applications (e.g., treatment of neurological disorders, gaming, sports enhancement[11]). Participants noted that if it were possible to 'read' thoughts, this could put people's security credentials at risk or could be used to extract information from people that could be used for blackmail. Workshop participants also speculated that new and existing **behavioural scanning** tools, such as advanced eye tracking and gait detection, and the increasing range of **biometrics** being used in user authentication, could make it easier for criminals to commit impersonation fraud. However, there was a wide range of ratings from the Delphi participants for these technologies, indicating considerable disagreement about their level of risk.

The threats associated with biotechnology were considered to be relatively difficult to defeat, with most rated between 3 and 4 on the 9-point scale (1=difficult to defeat, 9=easy to defeat).

BIOTECHNOLOGY, NEUROTECHNOLOGY, BIOMETRICS	Harm	Frequency	Defeatability	Risk
LOWER RISK (25-50)				
Hostile actors will target cloud labs and other digital biomanufacturing infrastructure to disrupt, manipulate or steal biomanufacturing processes (e.g., vaccine development).	7.3	4.5	3.9	33.0
The increasing range of biometrics being used in user authentication opens up new vectors for identity fraud.	6.3	4.5	4.5	28.2
LOW RISK (<24)				
Neurotechnology (e.g., brain scanning. brain-machine interfaces) that 'reads' thoughts will put people's security credentials at risk.	6.0	3.4	3.5	20.1
Behavioural scanning tools, such as advanced eye tracking and gait detection, will make it easier for criminals to commit fraud.	4.9	3.6	3.2	17.5
Neurotechnology (e.g., brain scanning. brain-machine interfaces) will be used to extract information from people that could be used for blackmail.	4.5	2.7	3.8	12.0

Table 7 Biotechnology, neurotechnology and biometrics (average ratings for harm, frequency, defeatability, and risk)

[10] E.g., UNESCO (2023). The risks and challenges of neurotechnologies for human rights. https://doi.org/10.54678/POGS7778

[11] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1135956/rhc-neurotechnology-regulation.pdf

Other new and emerging technologies

Delphi participants were in strong agreement that the highest threat in the remaining categories of emerging technologies (and the highest risk rating for all emerging technologies) was from the use of cryptocurrencies for criminal purposes such as investment scams, money-laundering, and ransomware payments (Table 8).

There was less consensus across the other technologies in this block, except for 3D printed weapons that would evade current detection methods. Participants agreed that these would be potentially quite harmful (average 6.6).

OTHER NEW AND EMERGING TECHNOLOGIES	Harm	Frequency	Defeatability	Risk
HIGHER RISK (>60)				
CRYPTOCURRENCIES				
Cryptocurrencies (without adequate know your customer (KYC) due diligence and anti-money laundering controls) will be used for money laundering and to facilitate cybercrimes such as ransomware.	8.1	8.5	5.4	68.3
LOWER RISK (25-50)				
AUTONOMOUS VEHICHLES				
All vehicles will be 'always connected' and collect vast amounts of data, creating vulnerabilities and increasing the threat surface.	6.1	6.3	4.4	38.1
Criminals will use autonomous vehicles to carry out attacks, such as delivering bombs via robot taxis.	6.5	3.7	5.3	23.9
3D PRINTING				
3D-printing will allow criminals and terrorists to create weapons from materials that evade current detection methods such as metal detectors.	6.6	5.1	4.0	33.7
3D-printing will facilitate the creation at home of prohibited or monitored items (knifes, guns, explosive parts etc)	6.3	5.2	4.1	32.8
3D-printing will facilitate intellectual property theft through the creation of counterfeit goods.	5.8	5.3	4.1	30.3
LOW RISK (<24)				
QUANTUM COMPUTING				
Quantum Computing will be widely used to undermine existing encryption methods.	5.1	3.0	4.9	15.6
SENSORS				
Thermal imaging cameras will be used by hostile actors to detect keystrokes, thereby compromising sensitive information.	5.5	3.2	4.3	17.8

Table 8 Cryptocurrencies, autonomous vehicles, 3D printing, quantum computing and sensors (average ratings for harm, frequency, defeatability, and risk)

Discussion – threats from emerging technologies

Clearly, participants focused substantially on the threats from GenAI, rating these as conveying the highest risks (with the exception of cryptocurrencies, the threats from GenAI were the only ones to be rated as having "Higher Risks") but also generating the largest number of threats for this technology. The rapid evolution of GenAI may account for this focus, but so too might the level of coverage these technologies have received in the media (science and general news media). It may be that technologies that have received less attention in the media also received less attention during the workshops. This is not to discount the findings of our study but to highlight that experts, just like everyone else, can be subject to biases, including the availability heuristic (people tend to judge the likelihood of an event based on how easily examples come to mind).

It is surprising that some of the technologies, particularly biotechnologies, were not rated as posing a higher future risk than participants' ratings suggested. As levels of self-reported expertise were lower for these technologies than others, participants may not have had sufficient expertise to rate these technologies in the same way that they could others.

B. Vulnerabilities from societal changes

Participants considered how societal changes (at national, regional and global level) over the next five years may create vulnerabilities that cyber criminals can exploit as opportunities, including both gradual changes and acute shocks (e.g., pandemics). Table 9 provides an overall summary of how these were rated in the aggregate. The threats associated with economic, workplace and skills changes were deemed as posing the highest risks over the next five years and were overall considered as moderately difficult to defeat. Threats associated with societal changes among the health sector were perceived to pose the lowest mean risk but were considered the most difficult to defeat. However, participants' perception of their own expertise for this section was low. More detailed results are presented in Tables 10-13.

	Participants	Expertise	Harm	Frequency	Risk	Defeatability
Economic, workplace and skills	8	6.3	6.9	7.0	48.4	5.9
Digitisation and increasing adoption of new technology across society	10	6.2	6.9	6.6	45.6	5.9
Politics and international relations	9	6.3	7.1	6.3	45.1	4.1
Health	9	3.9	6.5	5.7	36.5	4.5

Table 9 Societal changes: mean ratings for each subtheme (ranked by mean risk)

Digitisation and increasing adoption of new technology across society

The most common changes discussed were those associated with the roll out of digital technologies, and most were assessed by Delphi participants as posing medium and lower risk (Table 10).

A consensus view was reached for three of the threats identified. The first, which was also rated as the highest risk, was from the potential for cybercriminals to hold infrastructure operators to ransom, as **digitisation of infrastructure** and the complexity of infrastructure supply chains offer new and increased opportunities for cybercriminals to hold infrastructure operators to ransom.

Second, many of the new technologies described in section A involve **collecting huge amounts of personal data**, which participants suggested could be accessed and exploited by criminals to improve their success in activities such as fraud and hacking.

Third, participants agreed that the widespread adoption of digital services means more people will move money electronically (e.g., banking, property sales) but other technology (e.g. AI) will make it easier to scale **attacks on digital business systems** (email, banking etc).

Participants suggested that increasing digitisation may also **degrade individuals' abilities to protect themselves**, although there was not strong consensus on these risks. For instance, it may become almost impossible to carry out everyday tasks without a smartphone (e.g., park a car, call a taxi, deal with banking issues). Not only does this increase an individual's attack surface, which may continue to grow beyond their control, but it also makes it impossible for people to think through all the security issues every time they use a service. And, as society moves towards remote and digital ways of communication, opportunities to exploit individuals are opened up, especially without sophisticated and reliable methods of verifying content. Participants also thought that it will become easier for third parties to send overwhelming amounts of material to devices (such as phones). This may be used for bullying, to harass public figures or to take important services offline.

DIGITISATION/ INCREASING SOCIETAL ADOPTION OF NEW TECHNOLOGY	Harm	Frequency	Defeatability	Risk
HIGHER RISK (>60)				
Cybercriminals will hold infrastructure operators to ransom	8.5	7.9	5.3	66.9
MEDIUM RISK (51-60)				
Payment interception: Widespread adoption of digital services means more people will move money electronically (e.g., banking, property sales) but the advancement in other tech (e.g. AI) will make it easier to scale attacks on digital business systems (email, banking etc)	7.5	6.8	5.9	50.9
LOWER RISK (25-50)				
New technologies will improve access to potential victims' data, as well analysis of the relevant data in such a way which will improve success rate of criminal activities such as fraud and hacking	7.7	6.4	5.5	49.8
It will no longer be optional to use a smartphone to carry out everyday tasks (e.g., park a car, call a taxi, deal with banking issues), creating opportunities for cybercriminals as people will be unable to think through all the security issues every time they use a service	6.7	7.3	6.0	48.9
The numbers of people receiving phone calls from automated systems will increase massively, with fraudsters automating all their transactions and carrying them out wholesale	6.5	7.1	6.2	46.3
Device bombing: it will become easier to get third parties to send legitimate material to devices (phones etc) and overwhelm the user, and this will be used for bullying, to harass public figures and to take important services offline	6.8	6.2	6.0	42.6
With the evolution of technology, new attack vectors, and the sophistication of adversarial Tactics, Techniques and Procedures, incident responders will be overwhelmed with the volume of information	6.2	5.7	5.5	35.1

Table 10 Potential threats arising from digitisation / increasing societal adoption of new technology (average ratings for harm, frequency, defeatability, and risk).

Politics and international relations

Political shifts in the coming years could create opportunities for harm (Table 11). The most significant risk identified in this section was the threat that cybercriminals will try to **disrupt not only voting intentions but the actual machinery of voting**. A shift toward authoritarian politics (in formerly democratic societies) introduces opportunities for organised criminal groups, corruption, extortion, etc. However, participants did not reach consensus on their opinion about this risk.

Several risks, about which participants reached a consensus view, concerned the potential harms from **mis- and disinformation**, fuelled by large language models and other AI tools that change the way we retrieve and understand information. Potentially, this provides LLMs with a large influence over information and therefore the development and sharing of knowledge, which participants thought could be particularly dangerous in contested and unstable areas (e.g., Israel/ Palestine/ Syria/ Egypt) or used by extremist movements within countries (e.g., QAnon). Participants thought that some nation states may form ideological blocs and work together to spread misinformation, potentially taking advantage of a reduction in trust in authorities (e.g. government, traditional media), which may create new opportunities for misinformation to spread.

Participants reached a consensus that there was a low risk from the mainstreaming of the far right and the **reduction of trust in traditional authorities** which could prompt more individuals to look for information on “alternative” sites of information and to create "digital schools".

POLITICS AND INTERNATIONAL RELATIONS	Harm	Frequency	Defeatability	Risk
MEDIUM RISK (51-60)				
Cybercriminals will try to disrupt not only voting intentions but the actual machinery of voting	7.5	7.0	4.6	52.2
LOWER RISK (25-50)				
Reduction in trust in authorities (e.g. government, traditional media) may create new opportunities for misinformation to spread	7.6	6.6	3.3	50.2
Large language models and other AI tools will change the way we retrieve and understand information, but potentially this provides LLMs with a large influence over information and therefore the development and sharing of knowledge, which will be very dangerous in contested areas (eg Israel/Palestine/Syria/Egypt) or extremist movements within countries (eg QAnon) -	6.9	6.2	3.8	42.8
States will form ideological blocs and work together to spread misinformation	6.7	6.1	4.2	40.8
A shift toward authoritarian politics (in formerly democratic societies) will introduce opportunities for organised criminal groups, corruption, extortion, etc	7.2	5.5	3.3	39.6
LOW RISK (<24)				
The mainstreaming of the far right will prompt more individuals to look for information on "alternative" sites of information, making "digital schools" especially compelling	5.2	4.5	4.2	23.3

Table 11 Potential threats relating to politics and international relations (average ratings for harm, frequency, defeatability, and risk).

Health

Two potential threats in healthcare contexts were judged as representing a lower risk (Table 12). Participants noted that pandemics create new marketplaces for criminals, and opportunities to exploit people and systems for financial gain. Examples highlighted include selling fake medicines, fake experts giving fake medical advice, or inviting contributions to fake research. They also suggested that markets for medications and genetic enhancements will become premium and so subject to extortion attempts. However, participants did not reach a consensus view on these threats.

HEALTH	Harm	Frequency	Defeatability	Risk
LOWER RISK (25-50)				
Markets for medications and genetic enhancements will become premium and so subject to extortion attempts	6.6	5.7	4.7	37.7
Pandemics will offer cybercriminals exploitation possibilities, such as proffering fake medicines, fake experts giving fake advice, inviting contributions to fake research, offering fake medical advice, etc	6.3	5.6	4.2	35.3

Table 12 Potential threats relating to health (average ratings for harm, frequency, defeatability, and risk)

Economic, workplace and skills

Technology (plus the imperative of the Covid-19 pandemic) has made **remote working** / decentralized working environments a common way of working (Table 13). Participants thought that criminals would continue to find ways to exploit the vulnerabilities these environments create (generally weaker cyber controls at home compared to an office). However, this threat was assessed by participants as presenting a lower risk.

Participants noted that people **growing up around technology** (particularly Gen Z and later Millenials) may be overconfident about their understanding of technology, which could make them vulnerable to existing forms of cybercrime (e.g. through social engineering and other scams) and new variants. Participants judged the potential risks raised by people's overconfidence in understanding technology as medium. They assessed the risk posed by poorer understanding of coding vulnerabilities (caused by reliance on LLM code generators) as posing slightly less risk.

ECONOMIC, WORKPLACE AND SKILLS	Harm	Frequency	Defeatability	Risk
MEDIUM RISK (51-60)				
Young people will be overconfident about their understanding of technology, making them vulnerable to existing forms of cybercrime (e.g. through social engineering and other scams) and new variants	7.2	7.5	5.1	54.3
Remote Working/Decentralized Working Environments are here to stay, and criminals will exploit the vulnerabilities these environments create (generally weaker cyber controls at home compared to an office)	6.9	7.4	6.4	50.9
LOWER RISK (25-50)				
If computer science students are using LLMs to learn how to code, making them less savvy in base code, it may create a security flaw – assuming they would transition into security as practitioners	6.5	6.2	6.2	40.1

Table 13 Potential threats arising from economic, workplace and skills changes (average ratings for harm, frequency, defeatability, and risk)

Discussion – vulnerability from societal changes

In general, the threats discussed in this section were related to the fact that as the adoption of technology increases, this will lead to new working methods and potentially a greater attack surface and new opportunities for criminals. Unlike the previous section, with one exception, none of the threats identified in this section were rated as posing a higher risk. The exception scenario concerned cybercriminals holding infrastructure operators to ransom. Participants reached a consensus about the harm that could be caused by this threat (and the level of risk was comparable to the highest harms identified in the previous section) and viewed it to be moderately difficult to address.

In terms of the difficulty of defeating the threats identified, or our ability to mitigate against the potential risks associated with these societal changes, participants ratings varied between 3 and 7. Notably, participants assessed that the most challenging threats to counter were those that would arise from a shift to authoritarianism and a reduction in trust in traditional authorities.

C. Changes to criminal business models, methods, and ecosystems.

Criminal profiles

Participants were asked to consider how changes to criminal business models, methods, and ecosystems may create vulnerabilities exploited by cyber criminals over the next five years. The highest risk (which had a high level of consensus) was judged to come from **children's increasing use of increasingly advanced online technologies**, and the decreasing ability of the adults in their immediate sphere to monitor or fully understand (see Table 14).

Participants discussed how children and young people may increasingly be drawn into cybercrime through the easy availability and accessibility of cybercrime tools, initially through curiosity. Several future changes could **lower the barriers** for some people to become involved in crime (all judged lower risk):

- Lower levels of societal trust might lead some to engage in crimes that could be perceived as "victimless" but against organisations that are seen as ripping ordinary people off (e.g. banks).
- Easy access to new technologies like LLMs, synthetic biology, deepfakes etc. may lead to people thinking that they are not that harmful ("if it was really bad I wouldn't be able to use it").
- In the case of synthetic abuse imagery, people creating/consuming it may think that as it is synthetic it is not doing any harm (whereas in fact it might be normalising abusive behaviour or desensitising people to indecent content).

CRIMINAL PROFILES (WHO MAY BECOME CRIMINAL AND WHY?)	Harm	Frequency	Ease of countering	Risk
HIGHER RISK (>60)				
Children are getting online at younger ages, and the increased pace of technology development means that adults in their immediate sphere are increasingly less able to monitor/ understand their activity.	7.7	8.1	5.4	62.1
LOWER RISK (25-50)				
In the case of synthetic abuse imagery, people creating/consuming it may think that as it is synthetic it is not doing any harm (whereas in fact it might be normalising abusive behaviour).	6.6	7.4	3.3	49.2
The line between 'victims' and 'accessories to crime' will begin to blur as ordinary people are deceived into acting as mules, money laundering fronts, and similar.	6.8	7.0	5.4	47.5
Lower levels in societal trust will reduce the barriers for some people to become involved in crime, particularly in relation to crimes that could be perceived as "victimless" but against organisations that are seen as ripping ordinary people off (e.g. banks).	6.2	6.7	4.7	41.7
Young people will be drawn into cybercrime through the easy availability and accessibility of cybercrime tools, initially through curiosity.	6.4	6.0	5.1	38.3
Easy access to new technologies like LLMs, synthetic biology, deepfakes etc. will lead to people thinking that they are not that harmful ("if it was really bad I wouldn't be able to use it")	5.8	6.1	3.9	35.9

Table 14 Potential trends in who might be drawn into criminality (average ratings for harm, frequency, ease of countering, and risk).

Criminals' modus operandi

For this section, we asked participants to which extent they agree (1=not at all, 9=completely agree) with statements regarding the evolution of criminal's modus operandi. Participants tended to agree that we will see **cybercrime evolution not revolution**: although technology changes, we will see iterations of old patterns, especially when new technologies allow for old crimes to be committed with lower risk and at scale (see Table 15). Participants felt that cyber criminals would adapt their methods and models in line with the opportunity that new technology provides (e.g. deepfakes for impersonation of better researched targets, GenAI for better structured and targeted phishing).

CRIMINALS' MODUS OPERANDI **(n=9, average self-reported expertise = 7.0)**	**Agreement**
Some low skilled cybercrime roles will be replaced by generative AI.	8.0
We will see cybercrime evolution not revolution: although technology changes, we will see iterations on old patterns, especially when new technologies allow for old crimes to be committed at lower risk.	7.6
The recent emergence of cybercrime gangs forcing victims of human trafficking or modern slavery to perpetrate online scams will accelerate.	7.3
With the rise of "cybercrime-as-a-service", criminal models are changing: someone will take care of (a part) of the criminal pipeline for you. This means lower barriers to enter and less knowledgeable malicious actors that can just buy these services (e.g. booting/DDOS, ransomware etc.)	7.2
We will see a growth of malware-as-a-service, making it easier to launch and customize attacks, and opening up opportunities for creating variants of existing malware or infusing malware with additional capabilities to evade detection.	7.1
End-to-end encryption plus the collapse of major platforms means malign actors will move to smaller, less moderated, less surveilled, encrypted platforms to communicate and meet each other (e.g., Telegram, Discord, Signal).	7.0
Conversational user interfaces will mean that deep technological knowledge is no longer required to create or deliver new malign activities.	6.9
There will be increased demand for people with high levels of skill to create bespoke software to achieve goals that cannot be done through the more commonly available software packages and services in the cybercrime ecosystem. This will create a two-tier system in which most cybercriminals have low technological skill, and a small number of experts are the main drivers of new technological developments and in demand for bespoke activities.	6.8
With automation, the costs of entry and carrying out highly sophisticated cybercriminal campaigns will be reduced.	6.7
Poor scientific / digital literacy in public bodies means that criminals will spot or create vulnerabilities in public sector systems before the authorities do.	6.5
Criminals will take advantage of widespread availability of affordable sensors, the accessibility of the metaverse and the simplicity of using AI models.	6.4

Cybercrime will become industrialised, and many cybercriminals will not need to possess any particularly strong technical skills and yet will still cause significant harm with off the shelf tools.	6.4
It will become increasingly possible for one individual to do the work of a 'gang', using automated systems (financial, communications, etc) to take on specialist roles and 'freeing up resource'.	6.4
Lower risk, higher rewards: More sophisticated criminals will migrate away from front line crimes to lower risk options such as providing ransomware as a service.	5.4
Criminal enterprises will use AI to perform horizon scanning to predict law enforcement action and tailor criminal activity to avoid the predicted response.	4.3

Table 15 Average agreement with statements about future criminal modus operandi[12].

As shown in table 15, there were generally high levels of agreement that particular technological developments will mean that many elements of cybercrime will **no longer require complex or sophisticated skills**:

- Some low skilled cybercrime roles will be replaced by GenAI.
- With automation, the costs of entry and carrying out highly sophisticated cybercriminal campaigns will be reduced.
- It will become increasingly possible for one individual to do the work of a 'gang', using automated systems (financial, communications, etc) to take on specialist roles and 'freeing up resource'.
- Conversational user interfaces will mean that deep technological knowledge is no longer required to create or deliver new malign activities.
- Perpetrators of cybercrimes no longer need to know programming to prepare a social engineering attack using an AI model or within a virtual world.
- Cybercrime will become industrialised, and many cybercriminals will not need to possess any particularly strong technical skills and yet will still cause significant harm with off the shelf tools.

With the rise of "**cybercrime-as-a-service**", participants felt that criminal models are and will continue to change. Less knowledgeable malicious actors will increasingly be able to just buy services (e.g., booting/DDOS, ransomware). Participants thought that we will see a growth of **malware-as-a-service**, making it easier to launch and customise attacks, and the opening of opportunities to create variants of existing malware or to infuse malware with additional capabilities to evade their detection by anti-malware technologies. Participants were ambivalent about whether criminals will be tempted to migrate away from front line crimes to lower risk / high reward options such as providing ransomware as a service.

There was also agreement that there be increased **demand for people with high levels of skill** to create bespoke software to achieve goals that cannot be done through the

[12] Rating: 1=not at all, 9=completely agree. Statements in green received strong average agreement (>7) and statements in yellow received medium average agreement. Darker shaded ratings indicate strong consensus.

more commonly available software packages and services in the cybercrime ecosystem. Participants felt that this would create **a two-tier system** in which most cybercriminals have low technological skill, and a small number of experts would be the main drivers of new technological developments, and who are in demand for bespoke activities.

To avoid detection, participants thought that criminal enterprises will continue to exploit End-to-end encryption and felt that the collapse of major platforms would prompt a shift to smaller, less moderated, less surveilled, encrypted platforms where criminals can communicate and meet each other (e.g., Telegram, Discord, Signal).

Participants perceived a moderate risk that criminals will take advantage of the widespread availability of affordable **sensors**, the accessibility of the **metaverse** and the **simplicity of using AI models** to conduct their criminal activities.

Participants reached a consensus that **poor scientific / digital literacy in public bodies** means that criminals will spot or create vulnerabilities in public sector systems before the authorities do, although they only moderately agreed that this would be the case. Nevertheless, it highlights the need for law government to keep ahead in the arms race between criminal actors and law enforcement.

Criminal ecosystems

Participants were also asked to which extent they agree (1=not at all, 9=completely agree) with the statements regarding the evolution of criminal's ecosystems (Table 16). There was medium-strong agreement with several statements about the potential evolution of criminal ecosystems. For instance, that automated translation tools will make communication within **global criminal operations** easier and more effective (and enable criminals to target victims across borders more easily). And that criminals will continue to establish servers in countries with lax enforcement, to facilitate global criminal operations and make them more effective.

They also agreed (albeit less so) that **gaming platforms** have been built or arisen organically without the same degree of moderation or safety by design as other social platforms, but now have massive user bases. And that, given the difficulty of moderating or monitoring video or real-time audio, the use of gaming spaces by criminal or extremist groups for organisation or recruitment will increase.

There was some agreement that **new and/or deeper connections** will be forged between different actors in the cybercrime ecosystem as specialist skillsets become more in demand, and that the traditional notion of the criminal gang will be superseded by sophisticated interdisciplinary criminal teams. However, participants did not reach a consensus view on these two issues and their overall level of agreement was the lowest for these two categories.

CRIMINAL ECOSYSTEMS (n=10, average self-reported expertise = 6.1)	Agreement
Automated translation tools will allow criminals to target victims across borders with minimal friction.	7.9
Given difficulty of moderating or monitoring video or real-time audio, the use of gaming spaces by criminal or extremism groups for organisation or recruitment will increase.	6.9
Automated translation tools will make communication within global criminal operations easier and more effective.	6.8
New and/or deeper connections will be forged between different actors in the cybercrime ecosystem as specialist skillsets become more in demand.	6.5
The traditional notion of the criminal gang will be superseded by sophisticated interdisciplinary criminal teams.	6.1

Table 16 Average agreement with statements about future criminal ecosystems[13].

Discussion

Participants had less to say about criminal ecosystems but felt relatively strongly that existing technologies (e.g. translation tools) and infrastructure (e.g. gaming spaces) would continue to facilitate criminal activities and recruitment.

[13] Rating: 1=not at all, 9=completely agree. The statement in green received strong average agreement (>7) and statements in yellow received medium average agreement. Darker shaded cells indicate strong consensus.

D. Implications and suggestions for cybercrime responders

Discussions about responses were wide-ranging, covering the challenges for and role of law enforcement, government, industry, education and academia, and civil society. The statements generated and rated are presented in Table 17, together with the average level of agreement. Participants showed above average levels of agreement (i.e. for most statements, the average rating was above 7), exhibited strong consensus for most statements, and in every topic area reported high levels of self-reported knowledge and expertise (between 7.3 and 8.1 where high values denote strong expertise).

In particular, participants agreed that in future:

- "whole of society" approaches need to be adopted to respond to cybercrime, engaging communities, schools, industry and others alongside government and law enforcement in raising awareness and developing skills;
- industry needs to take more responsibility for making their products/services secure, and for supporting victims;
- current approaches are unlikely to be adequate as the scale of cybercrime increases. In particular, responders need to be more creative, take a harm mitigation approach, and pay greater attention to the impact on victims;
- greater, more authoritative support for small and medium sized businesses is needed;
- international relationships will become increasingly important for government and law enforcement;
- public sector responders are likely to lose out to the private sector in the battle for cybersecurity skills, knowledge and experience;
- academics have an important part to play but need to be more "hands on" and nimble, and
- more could be done to break down barriers between law enforcement, academics, and industry to enable a more effective and faster response to developments in cybercrime.

Two statements (highlighted in red in Table 17) had low levels of agreement (average agreement <4.0) and there was also strong consensus for these ratings. This suggests that the original statements were outlier opinions that the group collectively disagreed with.

IMPLICATIONS AND SUGGESTIONS FOR CYBERCRIME RESPONDERS (n = 8)	Agreement
WHO SHOULD RESPOND (average self-reported expertise = 7.8)	
There needs to be a greater diversity of responders, with strong disciplinary backgrounds - not just law enforcement, but also computer scientists, social scientists, lawyers, etc. diverse and non-traditional expertise must be engaged eg biotech or other emerging technologies.	8.55
Cybercrime will continue to require a whole of society approach.	7.98
Sometimes there is no responder: banks, for example, will not respond to cybercrimes below a certain monetary value, so if you are an individual or SME they just return your money through insurance. When vulnerabilities in medical devices are exploited, they get withdrawn (maybe insurers end up getting involved here too).	6.68
DEVELOPING AND MAINTAINING KNOWLEDGE (average self-reported expertise = 7.6)	
Police forces will find it difficult to hire qualified staff because they won't be able to afford market salaries for staff with cyber qualifications.	8.52
The police need to be better at reaching out to academics and industry for ad hoc understanding of criminality and tech, including finding a way to bypass many of the internal issues that prevent them from working with both academia and the industry in a more rapid, responsive, and effective way.	8.36
The public sector will need to halt the brain drain out into private sector post-training, often triggered by a lack of support and opportunity in the public sector. Not all retention offers need to be financial.	8.16
There also needs to be better training for front-line policing and mental health services, so they understand what victims are going through, and how to protect or support them.	8.03
One way forward for the police is to make greater use of Degree Apprenticeship/ Graduate Apprenticeship programmes focused on cybercrime.	7.77
Police may be unable to provide staff with time for on-the-job training or qualifications relevant to countering cybercrime (with implications for staff retention).	6.95
Beyond the police, the development pathway for an incident responder may become more unclear as bad actors and 'experts' promise pathways into cyber security with high salaries. Many people will end up turned off the industry, or unskilled for the roles they find, further weakening positions and leading to poor responses.	5.08
EVOLVING APPROACHES TO TACKLING CYBERCRIME (average self-reported expertise = 7.4)	
When dealing with cybercriminals, law enforcement will need to "think outside of the box" when dealing with cybercriminals: arrests are not the only way to stop online crimes.	7.79
Although most criminal activities are not novel, the scale and automation of their execution will pose difficulties in addressing them effectively.	7.71
Combatting cybercrime in future will require more consideration of harm mitigation. Prevention is difficult (and difficult to define in this context), but there will be ways of reducing the impact.	7.46
The response to victims of cybercrime needs to improve. Compared to victims of traditional crime, cybercrime victims are more likely to be seen as responsible for what happened to them and may not immediately realise that they have been victimised. (This creates challenges around the reporting of cybercrime.)	7.37

AI will not replace intelligence gathered by humans.	**6.90**
The police will face huge challenges in combatting crimes in the 'Metaverse'. Compared to other forms of online communication, it can be more difficult to record / evidence interactions that take place in the Metaverse, which could have implications for detection and prosecution.	5.44
Law enforcement should adopt randomised investigations. If they randomly decided whether to investigate a crime (perhaps with a loaded dice to mean that serious ones had a higher chance) then they remove some of the "I will never get caught" feeling and they will (eventually) look at low value high volume crime which is currently overlooked.	3.96
INTERNATIONAL LEA COOPERATION (average self-reported expertise = 7.3)	
Law enforcement must work out how to work cross-border at an investigator-to-investigator level without having to escalate everything up to the top of a pyramid and down again (Borderless crimes need borderless investigations and prosecutions).	7.81
PROTECTING ORGANISATIONS (average self-reported expertise = 7.8	
There is a "market for lemons" in cybersecurity. Organisations cannot determine if their cybersecurity actions have any impact; this allows vendors of supposed security software to sell things which have no impact, allowing them to extract revenue from consumers and businesses with no clear evidence of efficacy.	7.81
To combat cybercrime in future, small and medium sized enterprises need clearer and more consistent advice and support. NGOs such as resilience centres appear to be in 'competition' with small private companies with substantial backing from government, making it difficult to engage with SMEs in any mutually beneficial fashion. Add to this the lack of expertise on response to incidents within authorities such as law enforcement, and the significant financial hurdles to use specialist larger response companies, and small businesses are effective stranded with little support.	7.79
A significant challenge for cybercrime responders in the next 5 years is reaching a common agreement on what measures can protect organisations from harms, and how effective they will be.	6.94
Although startups are encouraged to do the NCSC's "Cyber Essentials", the sorts of security issues that are addressed by implementing Cyber Essentials are not generally the most significant issues for them. A much bigger security issue is where the functionality of the system can be misused.	6.00
GOVERNMENT POLICY AND REGULATION (average self-reported expertise = 7.0)	
Safety by design should be mandatory in new product development, globally.	8.41
When seeking to combat future cybercrime, governments will need to avoid legislative overreach (where governments mandate the presence of technology implementations to avoid harm, but this dissuades multinational organisations from undertaking contracts in that legislative area).	5.84
To combat future cybercrime effectively, governments will need to make better use of existing powers (e.g., Monopoly/anti-trust powers. MLA) not create new powers.	5.71
Governments will need to decide whether what is illegal in physical space should be illegal in cyberspace. If my online avatar assaults yours is that a crime? Should it be? The line becomes blurry with haptic suits in virtual reality etc.	5.34

CIVIL SOCIETY'S ROLE (average self-reported expertise = 7.8)	
Combatting future cybercrime will need greater public awareness, and government, responsible media reporting, and other creative mediums such as films and books can play essential roles in raising awareness. (E.g., using storytelling to depict an accurate portrait of cybercrime and the ways in which it can be mitigated).	8.49
Schools will need to have digital literacy programmes, with staff trained to educate children on privacy, mis/disinformation and the internet. Ready-made curriculum materials could be sent to all schools which they can adapt.	8.36
Society will need to create support channels and raise awareness about them.	8.04
There should be support for community building activities that can help to reduce victimisation by reducing levels of loneliness (lonely people may rely more on online platforms and be more vulnerable to criminals).	7.81
Numerous non-government entities will take a leading role in combating cybercrime, as they are responsible for most innovations that cybercriminals currently exploit to streamline their activities.	7.60
Citizens need to stay up to date with new possible forms of attacks (e.g. to ensure higher bystander engagement, involvement of guardians when their children are using metaverse apps.)	7.59
To deal with cyberbullying at school we should empower head teachers, for instance allowing them to conduct "metadata" enquiries under the Investigatory Powers Act to investigate bullies in their area.	3.99
ACADEMIC APPROACHES (average self-reported expertise = 8.1)	
Law enforcement need to find a way to bypass the internal issues that prevent them from working with both academia and industry in a more rapid, responsive, and effective way.	8.52
Academic cybercrime research can benefit society and funders should put more weight on positive societal impacts when assessing grant applications.	8.12
Academia needs to be less "academic" in its attempt to contribute to the cybercrime discussion, for instance, getting out of the "ivory towers" and "getting their hands dirty".	7.11
Given the rapid pace of technology development, academic cybercrime research needs to be more nimble: faster processes for securing funding (e.g. the current UKRI funding model for supporting academic cybercrime research is not fit for purpose), carrying out research, and conducting peer review."	6.55
Academic cybercrime research could learn from the US model where there is a "revolving door" between academia and government/police.	5.97
ROLE OF INDUSTRY (average self-reported expertise = 7.3)	
More transparency for major platforms is important to mitigate harm, for instance, greater independent scrutiny, academic research, transparency reporting and data provision (within ethical and privacy guidelines).	8.29
Online platforms need to do more to deter criminal usage (e.g., sale of stolen goods on online marketplaces, distribution of disinformation in online bookstores, hate speech on social media, and general reticence of game platforms to engage with law enforcement for fear of alienating their user base). This will mean addressing current financial incentives for companies and the platforms that enable and promote crime.	8.10

Banks should take more responsibility for fraud harm mitigation, for instance, making it easy to reverse fraudulent transactions, developing "bank fraud league tables" so customers can see how well banks deal with fraud.	7.84
Although "security by design" will become more prevalent, the challenge for tech companies will be understanding the threats, in order to implement safety/security/privacy "by design". This in turn argues for more and better threat information sharing between govt and non-government bodies. But concerns about (a) leakage and (b) commercial confidentiality will get in the way.	6.66
To reduce the spread of misinformation/disinformation and contribute to a more trustworthy media landscape, there needs to be increased public funding for media and less reliance on advertising and less reliance on clickbait.	6.50

Table 17 Average agreement with statements about implications for cybercrime responders[14].

Discussion – implications for cybercrime responders

Participants clearly felt that responses to cybercrime will require input across society (including both public and private sector organisations). This will require planning to ensure that public sector organisations, in particular, have the resources and capability necessary – both in terms of their ability to recruit and retain staff, and to respond to problems. Participants suggested ways in which to do this (e.g. making use of degree apprenticeship schemes) but these solutions will require rapid action, given the time it will take to develop sufficient human resources.

The perception was that the types of crime committed would not change but the ways in which they are committed would and that the scale at which they occur would increase. In response, participants felt that it would be necessary to think differently about combatting crime, with harm mitigation and response to victims, as well as international cooperation, being priorities.

There were concerns that while cybersecurity solutions exist, in many cases there is no evidence as to their effectiveness. This clearly needs to change and could be part of a safety by design scheme that enables customers to assess which companies are likely to provide beneficial solutions. Such schemes can help to "push" companies to deliver adequate services, and "pull" consumers to those that do. Such schemes may be particularly beneficial to SMEs who participants agreed need clearer and more consistent advice.

The role that industry should play in addressing problems online was clear. Participants felt that industry need to do more than they do at present but that thought would need to be given to how to incentivise this. Again, push and pull strategies were raised with the use of "bank fraud league tables" suggested as one way of providing the public and others with a way of comparing organisations in terms of how they deal with problems online.

[14] Rating: 1=not at all, 9=completely agree. Statements in green received strong average agreement (>7), statements in yellow received medium average agreement (4 -7), and statements in red received low average agreement (<4).

E. Conclusion

Our approach generated a wide and detailed set of opinions on how cybercrime might evolve in the coming years, drawing on the expertise of a heterogeneous group of experts from across academic disciplines. In general, although these experts did not achieve strong consensus on every risk, there were few topics where there was strong disagreement.

The clear message is that the highest risks are posed by the increasing adoption of automation and other AI-enabled technologies. These will enable current criminal activities at greater scale, reach, and effectiveness; will create new opportunities for criminal exploitation, in terms of new and broader attack surfaces; and will lead to the growth of new criminal business models, most notably "cybercrime-as-a-service". These developments will be challenging to counter, requiring a whole-of-society response, including more training and education, industry commitment to safety-by-design, and international cooperation in regulation and enforcement.

Limitations and future steps

Cybercrime is a general and broad threat landscape, and in this sort of exercise it is not possible to examine specific threats in great detail. Furthermore, although we recruited a broad range of expertise from existing expert networks for this activity, because participants were self-selecting we are likely to have missed some relevant expertise.

Relatedly, participants did not claim expertise in every type of potential threat or development, meaning that in some cases their ratings for harm, frequency, and defeatability / "ease of countering" may be less credible. Defeatability of a particular threat, in particular, is hard to judge without deep expertise in the technologies and behaviours that give rise to that threat, which may explain why defeatability ratings tended to cluster left of centre on the scale (i.e., conservative middle-of-the-road judgements).

Different types of experts may yield different conclusions. The UK Home Office workshop on the future of cybercrime, for instance, drew on expertise from across government departments and law enforcement and security agencies. These participants are likely to have greater insight into countering criminal activity, compared to many academic experts. Novel insights may also be generated in non-academic Delphi studies, drawing on industry experts, and on "pioneer communities" (Hepp, 2024) of cyber-hackers, bio-hackers, and makers (see, e.g., Elgabry et al., 2022).

In terms of execution, while the Delphi approach makes relatively efficient use of experts' time, it is resource-intensive for a research team to run, particularly for data collation and analysis. Future research could build in a prioritisation / consensus judgement process within the initial workshop (e.g., by taking a nominal group approach), which would save time and expedite data collection. Other approaches to prioritising statements about potential futures include the Q-Sort methodology (e.g., Choi & Moon, 2023).

Although consultative exercises such as this are considered to be an effective way of eliciting expert opinion, other approaches may yield different conclusions. For instance, red-teaming, blue-teaming and violet-teaming approaches address the ways in which new technologies might be exploited for harm, how exploitation might be countered, and how these might be informed by and serve societal values, so as to reduce risks and increase societal benefit (Titus and Russell, 2023). Facilitated deliberation using frameworks such as the Three Horizons Model (Curry & Hodgson, 2020) can also result novel expert-informed future scenarios (SPRITE+/RISCS, 2024).

Eliciting and prioritizing potential future threats is valuable but should ideally be accompanied by an assessment of potential signals that would indicate that a particular risk is indeed eventuating, and where and how harm is being caused. This requires sophisticated and ongoing scanning of the threat landscape, ideally by a cross-sector partnership (including government, law enforcement, industry, academia, and civil society groups), and regular revision of future risk predictions.

Finally, the evaluation of the effectiveness of cybersecurity solutions is clearly important. In their review of the literature, Brewer et al. (2019) concluded that "*To date there has been little to no research evaluating the effects of crime prevention initiatives on cybercrime*" (p. 125). This clearly needs to change and thought needs to be given as to how to best evaluate the effectiveness of such interventions, and who should bear the costs of so doing.

REFERENCES

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime prevention: Theory and applications*. Springer Nature.

Choi, S., & Moon, M. J. (2023). Disruptive technologies and future societies: Perspectives and forecasts based on Q-methodology. *Futures*, *145*, 103059. https://doi.org/10.1016/j.futures.2022.103059

Craig, C. (2018). Risk management in a policy environment: The particular challenges associated with extreme risks. *Futures*, *102*, 146-152.

Curry, A., & Hodgson, A. (2020). Seeing in multiple horizons: Connecting futures to vision and strategy. Knowledge Base of Futures Studies, 66-85. https://reevolution.espoch.edu.ec/ wp-content/uploads/2021/11/1.pdf#page=77.

Elgabry, M., Nesbeth, D., & Johnson, S. (2022). The future of biotechnology crime: A parallel Delphi study with non-traditional experts. *Futures*, *141*, 102970. https://doi.org/10.1016/j.futures.2022.102970

Giannarou, L., & Zervas, E. (2014). Using Delphi technique to build consensus in practice. *International Journal of Business Science & Applied Management (IJBSAM)*, *9*(2), 65-82.

Gómez-Quintero, J., Johnson, S. D., Borrion, H., & Lundrigan, S. (2024). A scoping study of crime facilitated by the metaverse. *Futures*, 103338.

Hepp, A. (2024). Curators of digital futures: The life cycle of pioneer communities. *New Media & Society*, 14614448241253766. https://doi.org/10.1177/14614448241253766

SPRITE+/RISCS (2024). When technology and democracy collide: A report on the SPRITE+/RISCS summer camp 2023. https://spritehub.org/wp-content/uploads/2024/05/FUTURES-SUMMER-CAMP-REPORT.pdf

Titus, A. J., & Russell, A. H. (2023). *The Promise and Peril of Artificial Intelligence—Violet Teaming Offers a Balanced Path Forward* (No. arXiv:2308.14253). arXiv. http://arxiv.org/abs/2308.14253

Appendix 1 - Statements

The following statements have been derived from the responses of participants during the 4/12/23 Workshop on the future of cybercrime. We have converted the responses into statements for this Delphi exercise, adding and editing for clarity where necessary, but wherever possible we have kept the language used by participants.

Existing and emerging technologies

Artificial intelligence

1. Generative AI will enable the creation of convincing Deepfake images, audio, video and personalised messages at scale to facilitate frauds including romance and phishing scams.
2. Generative AI will enable the creation of convincing Deepfake images and audio in real-time to facilitate CEO or similar types of fraud.
3. Generative AI tools (e.g. LLMs, Dall-E, Stable diffusion, and audio cloning services) are already user-friendly and will enable criminals to offer cybercrime as a service.
4. Generative AI will facilitate cyberbullying and harassment, including, for example, peers creating deepfaked videos of young people engaging in sexual behaviour.
5. AI-assisted image generation techniques will increase online sextortion; offenders (including sextortion gangs) can use publicly available images of a target to generate convincing sexual blackmail material for financial gain.
6. Generative AI will assist criminals involved in malware-as-a-service, by being used to create new variants, variants of existing malware or to make malware more difficult to detect.
7. Generative AI will facilitate the creation of Child Sexual Abuse imagery at scale.
8. Generative AI will enable the creation of seemingly realistic and increasingly substantive identities - personal or corporate - which can compromise security and background checks.
9. Generative AI and Large language models will be used for online marketplace scams.
10. Generative AI will be used in e-whoring scams, where images are used to falsely advertise sexual services online.
11. Generative AI will erode trust in online content (written, audio and video).
12. Reliance on, and belief in, the outputs of "helper" tools like ChatGPT (as opposed to other sources of information) will leave people vulnerable to misinformation campaigns and various forms of cybercrime.
13. Generative AI will allow lone actors to create and manage entire networks of authentic-seeming disinformation.

14. Generative AI will be used to produce fake video to encourage internet users to take violent action or engage with extremist groups.
15. Generative AI will exacerbate challenges around anonymity and/or lack of attribution online.
16. Algorithms in recommender systems will empower influencers (e.g. Andrew Tate) with extreme and hateful views
17. The growing use of AI chatbots for social and romantic relationships and support means individuals are at risk of manipulation by the organisations or individuals who programmed the chatbot.
18. The use of AI tools to gather and curate more accurate personal details of individuals and organisations will enable more sophisticated disinformation dissemination tools (e.g. via chatbots).

Biotechnology, neurotechnology, and biometric identification

19. Hostile actors will target cloud labs and other digital biomanufacturing infrastructure to disrupt, manipulate or steal biomanufacturing processes (e.g., vaccine development).
20. Neurotechnology (e.g., brain scanning. brain-machine interfaces) that 'reads' thoughts will put people's security credentials at risk.
21. Behavioural scanning tools, such as advanced eye tracking and gait detection, will make it easier for criminals to commit fraud.
22. Neurotechnology (e.g., brain scanning. brain-machine interfaces) will be used to extract information from people that could be used for blackmail.
23. The increasing range of biometrics being used in user authentication opens up new vectors for identity fraud.

Distributed Ledger Technology

24. Cryptocurrencies (without adequate know your customer (KYC) due diligence and anti-money laundering controls) will be used for money laundering and to facilitate cybercrimes such as ransomware.
25. AI videos will be produced by scammers to induce internet users to transfer money to invest in cryptocurrency scams.

Quantum computing

26. Quantum Computing will be widely used to undermine existing encryption methods.

Sensors

27. Thermal imaging cameras will be used by hostile actors to detect keystrokes, thereby compromising sensitive information.

Autonomous vehicles

28. Criminals will use autonomous vehicles to carry out attacks, such as delivering bombs via robot taxis.
29. All vehicles will be 'always connected' and collect vast amounts of data, creating vulnerabilities and increasing the threat surface.

3D Printing

30. 3D-printing will facilitate intellectual property theft through the creation of counterfeit goods
31. 3D-printing will facilitate the creation at home of prohibited or monitored items (knifes, guns, explosive parts etc)
32. 3D-printing will allow criminals and terrorists to create weapons from materials that evade current detection methods such as metal detectors.
33. (Optional question that respondents can skip) Do you have any comments on the risks described in this section? Are there other important risks of crimes or harms that are not covered? [Free text]
34. Extended Reality (including "Metaverse" technologies)
35. Hostile actors will gain access to data collected by integrated sensors in extended reality headsets (virtual reality, augmented reality), and use this to infer sensitive information about users and bystanders (e.g., their mental state, emotions, and even in some cases their sexual orientation and personality traits) that could be used for blackmail or fraud.
36. Abuse and harassment, particularly against children, women, and users from marginalised communities, will be amplified in virtual reality.
37. Children exposed to or engaged in age-inappropriate sexualised activity material in virtual reality will be exploited by criminals for blackmail/extortion and bullying.
38. Individuals or groups will hijack augmented reality glasses to display hate crime and other unpleasant material.
39. Criminals will 'groom' children using social virtual reality and multiplayer VR gaming for sexual abuse and exploitation.
40. Novel modes of content delivery and generation, including extended reality and generative AI, will be used to increase visual noise (i.e., misleading content, irrelevant content, etc.) to confuse users (which could be private individuals or operators of industrial/government security apparatus), in order to facilitate cyber-attacks.
41. 'Digital schools' and other immersive learning environments will appear, devoted to spreading conspiracy theories under the guise of truth.
42. Extremists will find the metaverse to be the perfect space to circulate and legitimise their discourses.

Other platforms and applications

43. Vast online gaming spaces, offering greater freedom and realism, will create new opportunities for malign actors to find ways of doing harm, that will be impossible to moderate/safeguard against.
44. Peer-to-peer scamming of users in multilayer games will escalate, with young people being drawn into cybercrime through the ease of scamming other young users.
45. Badly-moderated / policed marketplaces in the clear or dark web will allow the sale of, or access to, black or gray market goods or products, sale of fraudulent products and money laundering to go unpunished.
46. It will become even easier to buy cybercrime tools (cybercrime as a service) and buy victims for digital crime, making the tools more accessible for those who don't have technical expertise or existing crime connections.
47. Online marketplaces will not maintain any quality control, leading to negative outcomes: It will be impossible to identify authentic vs inauthentic books (e.g., Amazon's top sellers in the 'vaccines' category during the pandemic were all anti-vaxx; almost 400 different editions of the January 6 report on Amazon.com) and no way to a) know if any of them contain disinformation and b) report them if they did.)
48. People, particularly children and teenagers, will become habituated to graphic and violent content online and this will lead some to act out this violence in real life.
49. Criminals will hack trusted websites, devices (including AR devices) and public billboards to display malicious QR codes.

2. Societal changes

Economic, workplace and skills

50. Remote Working/Decentralized Working Environments are here to stay, and criminals will exploit the vulnerabilities these environments create (generally weaker cyber controls at home compared to an office).
51. Young people will be overconfident about their understanding of technology, making them vulnerable to existing forms of cybercrime (e.g. through social engineering and other scams) and new variants.
52. If computer science students are using LLMs to learn how to code, making them less savvy in base code, it may create a security flaw – assuming they would transition into security as practitioners (M)

Health

53. Markets for medications and genetic enhancements will become premium and so subject to extortion attempts.

54. Pandemics will offer cybercriminals exploitation possibilities, such as proffering fake medicines, fake experts giving fake advice, inviting contributions to fake research, offering fake medical advice, etc.

Politics and international relations

55. States will form ideological blocs and work together to spread misinformation.
56. Large language models and other AI tools will change the way we retrieve and understand information, but potentially this provides LLMs with a large influence over information and therefore the development and sharing of knowledge, which will be very dangerous in contested areas (eg Israel/Palestine/Syria/Egypt) or extremist movements within countries (eg QAnon)
57. The mainstreaming of the far right will prompt more individuals to look for information on “alternative” sites of information, making "digital schools" especially compelling.
58. Cybercriminals will try to disrupt not only voting intentions but the actual machinery of voting.
59. Cybercriminals will hold infrastructure operators to ransom.
60. A shift toward authoritarian politics (in formerly democratic societies) will introduce opportunities for organised criminal groups, corruption, extortion, etc.
61. Reduction in trust in authorities (e.g. government, traditional media) may create new opportunities for misinformation to spread.

Digitisation and increasing adoption of new technology across society

62. Device bombing: it will become easier to get third parties to send legitimate material to devices (phones etc) and overwhelm the user, and this will be used for bullying, to harass public figures and to take important services offline.
63. The numbers of people receiving phone calls from automated systems will increase massively, with fraudsters automating all their transactions and carrying them out wholesale.
64. Payment interception: Widespread adoption of digital services means more people will move money electronically (e.g., banking, property sales) but other tech will make it easier to scale attacks on digital business systems (email, banking etc)
65. With the evolution of technology, new attack vectors, and the sophistication of adversarial Tactics, Techniques and Procedures, incident responders will be overwhelmed with the volume of information and the necessity to deal with security incident investigations promptly.
66. As society moves towards remote and digital ways of communication, opportunities to exploit individuals are opened up, especially if the verification of content is not advanced sufficiently.
67. New technologies will improve access to potential victims’ data, as well analysis of the relevant data in such a way which will improve success rate of criminal activities such as fraud and hacking

68. It will no longer be optional to use a smartphone to carry out everyday tasks (e.g., park a car, call a taxi, deal with banking issues), creating opportunities for cybercriminals as people will be unable to think through all the security issues every time they use a service.

3. Criminals

Who might become a criminal and why

69. Young people will be drawn into cybercrime through the easy availability and accessibility of cybercrime tools, initially through curiosity.
70. Children are getting online at younger ages, and the increased pace of technology development means that adults in their immediate sphere are increasingly less able to monitor/ understand their activity.
71. Lower levels in societal trust will reduce the barriers for some people to become involved in crime, particularly in relation to crimes that could be perceived as "victimless" but against organisations that are seen as ripping ordinary people off (e.g. banks).
72. Easy access to new technologies like LLMs, synthetic biology, deepfakes etc. will lead to people thinking that they are not that harmful ("if it was really bad I wouldn't be able to use it")
73. In the case of synthetic abuse imagery, people creating/consuming it may think that as it is synthetic it is not doing any harm (whereas in fact it might be normalising abusive behaviour).
74. The line between 'victims' and 'accessories to crime' will begin to blur as ordinary people are deceived into acting as mules, money laundering fronts, and similar.

Modus operandi

75. Conversational user interfaces will mean that deep technological knowledge is no longer required to create or deliver new malign activities.
76. With automation, the costs of entry and carrying out highly sophisticated cybercriminal campaigns will to be reduced.
77. With the rise of "cybercrime-as-a-service", criminal models are changing: someone will take care of (a part) of the criminal pipeline for you. This means lower barriers to enter and less knowledgeable malicious actors that can just buy these services (e.g. booting/DDOS, ransomware etc.)
78. End-to-end encryption plus the collapse of major platforms means malign actors will move to smaller, less moderated, less surveilled, encrypted platforms to communicate and meet each other (e.g., Telegram, Discord, Signal).
79. We will see cybercrime evolution not revolution: although technology changes, we will see iterations on old patterns, especially when new technologies allow for old crimes to be committed at lower risk.

80. Lower risk, higher rewards: More sophisticated criminals will migrate away from front line crimes to lower risk options such as providing ransomware as a service.
81. Criminal enterprises will use AI to perform horizon scanning to predict law enforcement action and tailor criminal activity to avoid the predicted response.
82. We will see a growth of malware-as-a-service, making it easier to launch and customize attacks, and opening up opportunities for creating variants of existing malware or infusing malware with additional capabilities to evade detection.
83. Cybercrime will become industrialised, and many cybercriminals will not need to possess any particularly strong technical skills and yet will still cause significant harm with off the shelf tools.
84. The recent emergence of cybercrime gangs forcing victims of human trafficking or modern slavery to perpetrate online scams will accelerate.
85. Some low skilled cybercrime roles will be replaced by generative AI.
86. It will become increasingly possible for one individual to do the work of a 'gang', using automated systems (financial, communications, etc) to take on specialist roles and 'freeing up resource'.
87. Criminals will take advantage of widespread availability of affordable sensors, the accessibility of the metaverse and the simplicity of using AI models.
88. There will be increased demand for people with high levels of skill to create bespoke software to achieve goals that cannot be done through the more commonly available software packages and services in the cybercrime ecosystem. This will create a two-tier system in which most cybercriminals have low technological skill, and a small number of experts are the main drivers of new technological developments and in demand for bespoke activities.
89. Poor scientific / digital literacy in public bodies means that criminals will spot or create vulnerabilities in public sector systems before the authorities do.

Criminal ecosystems

90. Automated translation tools will make communication within global criminal operations easier and more effective.
91. New and/or deeper connections will be forged between different actors in the cybercrime ecosystem as specialist skillsets become more in demand.
92. Automated translation tools will allow criminals to target victims across borders with minimal friction.
93. Gaming platforms have been built or arisen organically without the same degree of moderation or safety by design as other social platforms, but now have massive user bases.
94. Given difficulty of moderating or monitoring video or real-time audio, the use of gaming spaces by criminal or extremism groups for organisation or recruitment will increase.
95. The traditional notion of the criminal gang will be superseded by sophisticated interdisciplinary criminal teams.

4. Challenges for cybercrime responders

Who should respond

96. Cybercrime will continue to require a whole of society approach.
97. There needs to be a greater diversity of responders, with strong disciplinary backgrounds - not just law enforcement, but also computer scientists, social scientists, lawyers, etc. diverse and non-traditional expertise must be engaged eg biotech or other emerging technologies.
98. Sometimes there is no responder: banks, for example, will not respond to cybercrimes below a certain monetary value, so if you are an individual or SME they just return your money through insurance. When vulnerabilities in medical devices are exploited, they get withdrawn (maybe insurers end up getting involved here too).

Developing and maintaining knowledge

99. Police forces will find it difficult to hire qualified staff because they won't be able to afford market salaries for staff with cyber qualifications.
100. Police may be unable to provide staff with time for on-the-job training or qualifications relevant to countering cybercrime (with implications for staff retention).
101. One way forward for the police is to make greater use of Degree Apprenticeship/ Graduate Apprenticeship programmes focused on cybercrime.
102. There also needs to be better training for front-line policing and mental health services, so they understand what victims are going through, and how to protect or support them.
103. Beyond the police, the development pathway for an incident responder may become more unclear as bad actors and 'experts' promise pathways into cyber security with high salaries. Many people will end up turned off the industry, or unskilled for the roles they find, further weakening positions and leading to poor responses.
104. The police need to be better at reaching out to academics and industry for ad hoc understanding of criminality and tech, including finding a way to bypass many of the internal issues that prevent them from working with both academia and the industry in a more rapid, responsive, and effective way.
105. The public sector will need to halt the brain drain out into private sector post-training, often triggered by a lack of support and opportunity in the public sector. Not all retention offers need to be financial.
106. Evolving approaches to tackling cybercrime
107. Although most criminal activities are not novel, the scale and automation of their execution will pose difficulties in addressing them effectively.

108. Combatting cybercrime in future will require more consideration of harm mitigation. Prevention is difficult (and difficult to define in this context), but there will be ways of reducing the impact.
109. When dealing with cybercriminals, law enforcement will need to “think outside of the box” when dealing with cybercriminals: arrests are not the only way to stop online crimes.
110. AI will not replace intelligence gathered by humans.
111. The police will face huge challenges in combatting crimes in the ‘Metaverse’. Compared to other forms of online communication, it can be more difficult to record / evidence interactions that take place in the Metaverse, which could have implications for detection and prosecution.
112. Law enforcement should adopt randomised investigations. If they randomly decided whether to investigate a crime (perhaps with a loaded dice to mean that serious ones had a higher chance) then they remove some of the "I will never get caught" feeling and they will (eventually) look at low value high volume crime which is currently overlooked.
113. The response to victims of cybercrime needs to improve. Compared to victims of traditional crime, cybercrime victims are more likely to be seen as responsible for what happened to them and may not immediately realise that they have been victimised. (This creates challenges around the reporting of cybercrime.)

International LEA cooperation

114. Law enforcement must work out how to work cross-border at an investigator-to-investigator level without having to escalate everything up to the top of a pyramid and down again (Borderless crimes need borderless investigations and prosecutions).

Protecting organisations

115. A significant challenge for cybercrime responders in the next 5 years is reaching a common agreement on what measures can protect organisations from harms, and how effective they will be.
116. There is a “market for lemons” in cybersecurity. Organisations cannot determine if their cybersecurity actions have any impact; this allows vendors of supposed security software to sell things which have no impact, allowing them to extract revenue from consumers and businesses with no clear evidence of efficacy.
117. To combat cybercrime in future, small and medium sized enterprises need clearer and more consistent advice and support. NGOs such as resilience centres appear to be in ‘competition’ with small private companies with substantial backing from government, making it difficult to engage with SMEs in any mutually beneficial fashion. Add to this the lack of expertise on response to incidents within authorities such as law enforcement, and the significant financial hurdles to use specialist

larger response companies, and small businesses are effective stranded with little support.

118. Although startups are encouraged to do the NCSC's "Cyber Essentials", the sorts of security issues that are addressed by implementing Cyber Essentials are not generally the most significant issues for them. A much bigger security issue is where the functionality of the system can be misused.

Government policy and regulation

119. Governments will need to recognise the role of foreign policy and international aid. People in other countries suffering loss through climate crisis, war etc. need to have hope for the future or it becomes our problem.
120. To combat future cybercrime effectively, governments will need to make better use of existing powers (e.g., Monopoly/anti-trust powers. MLA) not create new powers.
121. Safety by design should be mandatory in new product development, globally.
122. Governments will need to decide whether what is illegal in physical space should be illegal in cyberspace. If my online avatar assaults yours is that a crime? Should it be? The line becomes blurry with haptic suits in virtual reality etc.
123. When seeking to combat future cybercrime, governments will need to avoid legislative overreach (where governments mandate the presence of technology implementations to avoid harm, but this dissuades multinational organisations from undertaking contracts in that legislative area).

Civil society's role

124. Society will need to create support channels and raise awareness about them.
125. There should be support for community building activities that can help to reduce victimisation by reducing levels of loneliness (lonely people may rely more on online platforms and be more vulnerable to criminals).
126. Numerous non-government entities will take a leading role in combating cybercrime, as they are responsible for most innovations that cybercriminals currently exploit to streamline their activities.
127. Combatting future cybercrime will need greater public awareness, and government, responsible media reporting, and other creative mediums such as films and books can play essential roles in raising awareness. (E.g., using storytelling to depict an accurate portrait of cybercrime and the ways in which it can be mitigated).
128. Citizens need to stay up to date with new possible forms of attacks (e.g. to ensure higher bystander engagement, involvement of guardians when their children are using metaverse apps.)
129. Schools will need to have digital literacy programmes, with staff trained to educate children on privacy, mis/disinformation and the internet. Ready-made curriculum materials could be sent to all schools which they can adapt.

130. To deal with cyberbullying at school we should empower head teachers, for instance allowing them to conduct "metadata" enquiries under the Investigatory Powers Act to investigate bullies in their area.

Academic approaches

131. Given the rapid pace of technology development, academic cybercrime research needs to be more nimble: faster processes for securing funding, carrying out research, conducting peer review. the current UKRI funding model for supporting academic cybercrime research is not fit for purpose given the speed of generational shift.)
132. Academic cybercrime research can benefit society and funders should put more weight on positive societal impacts when assessing grant applications.
133. Academia needs to be less “academic” in its attempt to contribute to the cybercrime discussion, for instance, getting out of the “ivory towers” and “getting their hands dirty”.
134. Law enforcement need to find a way to bypass the internal issues that prevent them from working with both academia and industry in a more rapid, responsive, and effective way.
135. Academic cybercrime research could learn from the US model where there is a “revolving door” between academia and government/police.

Industry’s role

136. Online platforms need to do more to deter criminal usage (e.g., sale of stolen goods on online marketplaces, distribution of disinformation in online bookstores, hate speech on social media, and general reticence of game platforms to engage with law enforcement for fear of alienating their user base). This will mean addressing current financial incentives for companies and the platforms that enable and promote crime.
137. Although "security by design" will become more prevalent, the challenge for tech companies will be understanding the threats, in order to implement safety/security/privacy "by design". This in turn argues for more and better threat information sharing between govt and non-government bodies. But concerns about (a) leakage and (b) commercial confidentiality will get in the way.
138. Banks should take more responsibility for fraud harm mitigation, for instance, making it easy to reverse fraudulent transactions, developing “bank fraud league tables” so customers can see how well banks deal with fraud.
139. More transparency for major platforms is important to mitigate harm, for instance, greater independent scrutiny, academic research, transparency reporting and data provision (within ethical and privacy guidelines).
140. To reduce the spread of misinformation/disinformation and contribute to a more trustworthy media landscape, there needs to be increased public funding for media and less reliance on advertising and less reliance on clickbait.