Safer and Stronger Communities Board

29 September 2023

Future Crime Horizon Scan

Purpose of Report

For decision.

Summary

This report reviews some of the key qualitative and quantitative trends in crime that councils' community safety teams are likely to see in the next 5-10 years as a result of developments in artificial intelligence (AI). It also sets out some case studies on how local authorities are already responding to these changes. Finally, it proposes, subject to the direction of members a work programme to support the local government sector to manage these trends.

LGA Plan Theme: **Championing climate change and local environments**

Recommendation(s)

That the Board:

(a) Note the potential for AI to shape and change the way crime is committed, and the impact this could have on councils' community safety work; and

(b) Agree to the proposed work programme set out at paragraph 33, and provide a steer in relation to the points set out in paragraphs 34 and 35.

Contact details

Contact officer: Joseph Sloyan

Position: Graduate Trainee

Phone no: 020 7664 3291

Email: joseph.sloyan@local.gov.uk

Future Crime Horizon Scan

Background

1. Changes in technology over the last thirty years have seen the emergence of new types of crime. Board members will be familiar with the rapid rise in cybercrime created by the digitalisation of many areas of life. Technological developments in for example nanotechnology, robotics and cybernetics are likely to create further crime opportunities.

2. The relationship between technological innovation and crime seems to follow a three phase pattern with; development without much consideration of the impact on crime; the exploitation of the new technology by criminals; and then a response by government and bodies involved in tackling crime. It is therefore not a question of whether technological developments will be exploited by criminals, but a case of when that happens and how.

3. The latest data from the Crime Survey of England and Wales which is conducted by the Office of National Statistics and covers the period until the end of March 2023 listed fraud as the largest crime type with 3.5 million incidents or offences. This was relatively stable compared to the period immediately before Covid-19, but over 2 million of these offences related to bank and credit account fraud, though advanced fee fraud is increasing.

4. Given the impact technological developments will have on crime, the Board may wish to consider whether it examines the impact of a range of different technological developments on crime in its work programme. This paper though considers the impact of the development and prevalence of artificial intelligence (AI). Please see the Appendix for relevant definitions and key terminology related to AI.

5. This report provides members with an overview of what academic and other research suggests will be the emergent trends in crime as a result of AI in the next 5-10 years. It is organised by qualitative factors - how crime might change as a practice; and quantitative factors - how certain crimes may increase.

6. These trends are not mutually exclusive and often closely related, but it is important to draw a distinction between, for example, utilising AI as an accessory to an otherwise common crime, such as theft, and crimes which legal and regulatory systems do not currently have a clear approach to, such as political audio-visual impersonation.

7. Then it provides case studies of how local authorities and other public sector bodies are managing these trends and what lessons can be drawn from them.

Qualitative changes: how might crime change?

8. As members will likely appreciate, the use of artificial intelligence (AI) to commit crime could represent a substantial qualitative shift in how certain crimes will look in the near future. In reviewing the relevant academic and third sector literature, the following emerged as the primary, and most salient ways in which AI is likely to shape how crime looks in the future, based on likelihood of prevalence and difficulty in prevention:

9. **Audio-visual impersonation:** the use of artificial intelligence to accurately impersonate another person on video and or audio for the purposes of committing a crime. This could be used in a wide range of ways from for example defrauding the vulnerable to partner abuse. This is understood as a qualitative change because it could be deployed to conduct a large range of crimes including for example blackmail, theft, and undermining community cohesion.

10. Developments in deep learning (see the Appendix for a definition) have meant that audio-visual impersonation can be highly sophisticated and can be proliferated through a large number of difficult to regulate domains, such as social media. There is currently research into algorithmically detecting audio-visual impersonation (sometimes referred to as deep fakes), but these are not currently highly sophisticated or widely available.

11. This is of particular concern to local authorities since they are often the interface for vulnerable residents to access services which may be of interest to criminals – such as the provision of benefits. Trusted figures from local authorities may therefore be the target of audio-visual impersonation in the commission of theft or extortion.

12. **A distinct but related trend is the use of large language models to improve the efficacy of phishing** – an already common process whereby a party aims to collect secure information, such as bank details, through installing malware while impersonating a trusted party. A local authority is a likely target of this impersonation as they communicate not only with vulnerable residents, but also the wider community for example around the collection of council tax, and the provision of wide-ranging services.

13. As members are likely to be aware, the majority of phishing scams are currently unsophisticated, and rely on indiscriminately circulating crude messages which capitalise in simple human error, particularly by the elderly and vulnerable.

14. The increased sophistication of language models and natural language processing means that this is likely to change. Criminals could utilise these capabilities to produce messages which are both highly targeted and extremely difficult to distinguish from legitimate communications.

15. This is of particular concern due to the difficulty of defeating such systems. Phishing scammers are able to experiment with the efficacy of various messages at virtually no cost, and large language models – such as ChatGPT – are already highly sophisticated and can replicate messages that are indistinguishable from legitimate parties. Further, phishing relies on human error, which means it is likely to increase in use as these scams become more sophisticated.

16. **Terrorism:** the use of artificial intelligence for the purposes of making more effective the delivery of a terror attack, or the radicalisation and co-ordination of terrorists.

17. The relevant horizon-scans have raised particular concern about the possibility of driverless vehicles being utilised as weapons. This would serve to proliferate vehicular terrorism by reducing the need for driver recruitment, enabling lone actor attacks, and potentially co-ordinating a large number of vehicles at once.

18. As drones become more technologically sophisticated, there is a high possibility that these are used for terroristic purposes- such as the deployment of explosives without the need for an operator in close proximity. It is also currently being evaluated by actors such as the United States military, who are considering how AI can be used to improve drone targeting systems and minimise the need for human input.

19. These developments do, however, have substantial implications for legislation of importance to local authorities- such as Martyn's Law or the 'Protect Duty'. Once this legislation is introduced councils will need to have a strong working understanding of these emergent risks in order to ensure they are complying with their obligations under this duty.

20. The Board has received presentations in the past from the National Protective Security Authority (NPSA), which is the technical government body chiefly concerned with physical and protective security. Members may wish to consider whether they would benefit from a further presentation from the NPSA about how local authorities can best prepare for these expected changes in how terror attacks are conducted.

21. In addition to the material risk posed by the use of AI systems to conduct terror attacks, the rise in audio-visual impersonation may also serve to increase radicalisation through both creating deceptive and incendiary content, as well as targeting it more effectively.

22. The LGA's Special Interest Group on Countering Extremism (SIGCE) has been considering how artificial intelligence is currently being utilised for the purposes of spreading misinformation and encouraging radicalisation, and has been looking at conducting a practitioner roundtable on this topic. It would be helpful to have members' views on what this roundtable might cover, and what further work in this area should be undertaken going forward.

23. These qualitative changes to crime brought on by the increased sophistication of artificial intelligence is by no means exhaustive, and Board members may wish to raise other changes that could arise from the use of AI in carrying out criminal activity.

Quantitative changes: how might the prevalence of certain crimes change?

24. The 2022 Interpol Global Crime Trend Report summarises perceptions of crime types across Europe that currently post a substantial threat and are likely to increase in the near future, primarily through digitalisation:

    24.1. **Organised crime:** the use of legitimate business technologies, and potentially local authorities, as a vehicle for organised crime.

        24.1.1. The LGA already has research and resources dedicated to understanding and combatting the risk of organised crime to local authorities. See, for example, Local Authority Serious and Organised Crime Checklist and the Counter Fraud Hub.

    24.2. **Illicit trafficking:** the use of digital and online recruitment for targeting victims, and information distribution.

24.2.1. This is expected to increase in both conventional forms, such as the production and distribution of illicit drugs, as well as new emerging forms of human trafficking, particularly relating to the proliferation of certain forms of pornography such as OnlyFans. High profile cases such as that of Andrew Tate have illustrated how such digital platforms can be utilised to facilitate complex forms of human trafficking.

24.3. **Financial Crime and Corruption:** the use of online and digital tools to perpetrate financial crime more effectively.

24.3.1. A range of these crimes would fall under a conventional understanding of financial crime: such as AI-assisted identity fraud, or the increased vulnerability of financial systems which operate within a single application.

24.3.2. However, a distinct trend within financial crime is criminal responses to the introduction of new regulations and national policy objectives (such as those with an environmental objective) for example, the creation of fraudulent carbon capture/offset technologies.

24.4. **Cybercrimes:** the growth in prevalence and sophistication of conventional online scams and ransomware.

24.5. **Terrorism:** similarly to those outlined in the previous section, with particular attention to the use of the internet for the purposes of radicalisation.

Case Studies

25. As well as offering greater opportunities for criminals, AI offers local authorities opportunities to address widespread criminal activity in their areas, such as tackling fly-tipping. For example:

25.1. Birmingham City Council has deployed cameras in fly-tipping that are capable of automatically detecting incidences of fly-tipping and reporting this to the Council. These were funded by a £45,000 grant from central government to combat fly-tipping. Importantly, these were supplemented by more conventional ward engagements such as posters and written communications.

25.2. Westminster City Council is trialling a similar system which will also report registration plates.

25.3. Utilising AI in surveillance and predictive policing more broadly is one of the key active trends in AI, particularly for cities and local authorities.

25.4. Such systems are technically simple and inexpensive and remove the need for operators to manually observe potentially hours of recorded footage of reported fly-tipping.

25.5. Unlike other uses of AI, these systems are also not significantly legally or ethically problematic, since the data that it is learning from and analysing is environmental data, which carries far less legal or ethical implications than personal data.

25.6. These case studies therefore reported a high degree of success, with little technical or ethical difficulties.

26. Use of AI systems and algorithms to assist decision-making on benefit claims and welfare issues.

    26.1. The lack of legal and ethical difficulties associated with AI-assisted fly-tipping detection contrasts clearly with attempts by some local authorities to improve their decision-making capabilities and capacity in assessing welfare claimants.

    26.2. These attempts were ultimately scrapped following a number of serious concerns which included: simple inaccuracies, demographic biases, and a lack of transparency and 'explainability'.

    26.3. The problematic nature of this case study primarily originates in the substantial legal and ethical considerations that arise from the use of personal data in contrast to environmental data.

27. These case studies on uses of AI within a broad community safety context illustrates the legal, technical, and ethical issues associated with AI which local authorities need to address, as well as the need for councils to have a clear understanding of where AI might have utility and where it might not.

Key considerations for local authorities

28. These trends highlight a number of key considerations that councils should be making to ensure that they are adequately prepared for the identified trends.

Being prepared for risks

29. A number of these trends capitalise on information and technology for which there is not a high degree of literacy and awareness in the general public. Similarly, many of these trends – for example the use of driverless vehicles for terrorism – have not yet materialised. This positions local authorities at an intersection where the most productive response will be to ensure that they themselves highly literate in these technologies and therefore aware of their risks, in order to both educate residents and respond to threats as they emerge.

30. Going forward it will be important for councils to be able to access to the technical expertise to prepare for new types of crime and new ways in which existing crime may be committed, and support residents to minimise their likelihood of being victims of crime.

Ethical considerations

31. In order to respond to crimes committed with the assistance of AI, and also to use AI to strengthen their own community safety response local authorities need a clear understanding of the ethical issues associated the use and abuse of AI.

Data protection

32. As members are aware from previous NPSA briefings local authorities are controllers of substantial amounts of often personal and sensitive data and could be targeted through AI systems. The LGA's cyber, digital and technology programme assists councils in improving the secure use of digital technology.

Proposal

33. In order to place councils in a better position to respond to the impact of AI on crime over the next five years, it is proposed a programme of work is developed for the Board covering:

    33.1. Raising awareness among councils of the potential criminal use of AI in the near future for example through webinars, Leadership essential course and collaboration with the LGA's cyber, digital and technology programme.

    33.2. Undertake further research on how councils and community safety partners might use AI to address crime and community safety issues.

    33.3. Sharing emerging practice in councils and from other sectors, including in addressing the ethical and legal issues related to combatting crime facilitated by AI, and also in the use of

34. It would also be helpful to have a steer from members on what could be covered at the planned SIGCE practitioners' roundtable on the use of AI for the purposes of spreading misinformation and radicalisation.

35. Members views are also sought on whether the Board should explore other emerging technological developments which could be used to carry out crime.

Implications for Wales

36. There are no specific implications for Welsh councils but we will engage with colleagues at the WLGA to see if the work proposed in this paper would assist Welsh local authorities.

Financial Implications

37. There are no financial implications from the Board arising from the proposed actions.

Equalities implications

38. Any research that Officers conduct regarding the use of artificial intelligence in community safety teams must ensure that they are paying adequate attention to the known equalities implications of such systems- for example, the ability of these systems to learn prejudices and biases.

Next steps

39. Subject to members' agreement officers will develop the programme of work set out at paragraph 33.