Researching, anticipating, and preventing future crimes

Professor Shane D Johnson
Dawes Centre for Future Crime at UCL
Online Shopping Fraud in the UK

Project Outputs

Reducing the Crime Harms of the COVID-19 Pandemic
Supported by UKRI Economic and Social Research Council grant ES/V00445X/1

Main page  About  News / blog  People

Three publication series are edited by the project team (asterisk = authored by project team). Contact Nick Tilley at n.tilley@ucl.ac.uk about Special Papers, Graham Farrell at g.farrell@leeds.ac.uk about Stats Bulletins, or the Crime Science journal. Policing Insight reproduces many Special Papers.

Crime Science special collection on COVID-19
1. Queensland property crime variation
2. Six months in: Pandemic crime trends
3. Fear of COVID-19
4. Somehow I always end up alone: COVID-19, social isolation

Jill Dando Institute COVID-19 Special Papers
26. Contactless Card Payment Limits
27. Frauds in the crisis
28. Preventing a Vaccine Crime Wave
29. Covid facemasks as crime facilitators
30. Types of crime

Statistical Bulletin on Crime and COVID-19
14. A Year of COVID-19 and Crime*
15. Second lockdown crime effects less pronounced*
16. Fly-tipping during the pandemic*

Six months in: pandemic crime trends in England and Wales

https://covid19-crime.com
Adapted from Voros. 2003
Some Patterns Repeat

Price ubiquity

Security by Design
PITCHR: Prevention of IoT-enabled Crime using Home Routers

Scoping study of the future crime challenges of the metaverse

Crime enabled by autonomous vehicles

Future crime opportunities arising from Artificial Intelligence (AI)

Securing the Internet of Things (IoT)

Cryptocurrency and Money Laundering
THE BIG DATA BANG

The “Internet of Things” is exploding. It is made up of billions of “smart” devices—from miniscule chips to mammoth machines—that use wireless technology to talk to each other (and to us). Our IoT world is growing at a breathtaking pace, from 2 billion objects in 2006 to a projected 200 billion by 2020. That will be around 26 smart objects for every human being on Earth!
Consumer IoT

Race to market + Security regulation + Cost = ?
Secure by Design

Department for Digital, Culture, Media & Sport

Secure by Design: Improving the cyber security of consumer Internet of Things Report

Press release
New cyber security laws to protect smart devices amid pandemic sales surge

Workshop on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software
Biotechnology

- Traditional biological systems are re-created or modified in novel ways for various application purposes

- CRISPR, DNA testing

- In 2021, £4.5bn was raised by biotech companies in the UK
Synthetic Biology

- Biohacking - Athletes have historically abused steroids and growth hormones (Reardon & Creado, 2014)

- DNA encoded malware (Ney et al., 2017)

- DIY synthetic drugs by 2030 (Bress, 2017)
  - E.coli -> THC
  - Yeast -> LSD

Add gov enquiry stuff and IIoT hack
<table>
<thead>
<tr>
<th>Scoping projects</th>
<th>Longer projects</th>
<th>PhD projects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crime, place and the internet</td>
<td>Cryptocurrency &amp; Fraud</td>
<td>Drug sales on Social Media</td>
</tr>
<tr>
<td>Advanced materials to combat crime</td>
<td>IoT and Crime</td>
<td>Guarding against Adversarial perturbation</td>
</tr>
<tr>
<td>Ageing and online fraud</td>
<td>Refugee flows and instability*</td>
<td>Biocrime</td>
</tr>
<tr>
<td>AI and Crime</td>
<td>Reducing domestic abuse with technology</td>
<td>Refugee flows and instability*</td>
</tr>
<tr>
<td>Metaverse &amp; Crime</td>
<td>Tech and Domestic Abuse</td>
<td>Addressing Online CSE on Social Media</td>
</tr>
<tr>
<td>Autonomous Vehicles &amp; Crime</td>
<td>COVID19 &amp; Crime</td>
<td>Smart Cities: 1) crime prevention 2) Risks</td>
</tr>
<tr>
<td></td>
<td>Detecting counterfeit agro-chemicals</td>
<td></td>
</tr>
</tbody>
</table>
Horizon Scanning Taught Module
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.
AI-enabled future crime
Artificial intelligence (AI) technologies have applications for crime prevention and detection, but they could be employed for criminal purposes in many different ways. This briefing identifies 20 different potential AI-enabled future crimes.

Summary
This study identified 20 applications of AI and related technologies which could be used for crime now or in the future. Future crimes were ranked as either low, medium or high concern in relation to the harms they cause, the criminal profit they achieve, and the financial, temporal or reputational harm caused.

AI-enabled future crimes
- As a target for criminal activity, where AI systems are targeted by criminals – such as attempts to bypass protective AI systems or to make systems fail below expectation.
- As a tool for crime, where the technology in question is used to gain an advantage in criminal activities; such as enabling clients to manipulate others.
- As a means to disrupt, where AI systems are used to disrupt or hinder the operation of other systems.
- As a direct attack, where AI systems are used to directly cause harm.
- As a tool for control, where AI systems are used to control or manipulate others.
- As a means to detection, where AI systems are used to detect or prevent crimes.
- As a means to planning, where AI systems are used to plan or execute crimes.
- As a means to exposition, where AI systems are used to expose or reveal crimes.
- As a means to communication, where AI systems are used to communicate or coordinate crimes.
- As a means to protection, where AI systems are used to protect or defend against crimes.
- As a means to diagnosis, where AI systems are used to diagnose or identify crimes.
- As a means to prevention, where AI systems are used to prevent or stop crimes.
- As a means to intervention, where AI systems are used to intervene or stop crimes.
- As a means to mitigation, where AI systems are used to mitigate or reduce the impact of crimes.
- As a means to detection, where AI systems are used to detect or identify crimes.
- As a means to communication, where AI systems are used to communicate or coordinate crimes.
- As a means to protection, where AI systems are used to protect or defend against crimes.
- As a means to diagnosis, where AI systems are used to diagnose or identify crimes.
- As a means to prevention, where AI systems are used to prevent or stop crimes.
- As a means to intervention, where AI systems are used to intervene or stop crimes.
- As a means to mitigation, where AI systems are used to mitigate or reduce the impact of crimes.
- As a means to detection, where AI systems are used to detect or identify crimes.
- As a means to communication, where AI systems are used to communicate or coordinate crimes.
- As a means to protection, where AI systems are used to protect or defend against crimes.
- As a means to diagnosis, where AI systems are used to diagnose or identify crimes.
- As a means to prevention, where AI systems are used to prevent or stop crimes.
- As a means to intervention, where AI systems are used to intervene or stop crimes.
- As a means to mitigation, where AI systems are used to mitigate or reduce the impact of crimes.
- As a means to detection, where AI systems are used to detect or identify crimes.
- As a means to communication, where AI systems are used to communicate or coordinate crimes.
- As a means to protection, where AI systems are used to protect or defend against crimes.
- As a means to diagnosis, where AI systems are used to diagnose or identify crimes.
- As a means to prevention, where AI systems are used to prevent or stop crimes.
- As a means to intervention, where AI systems are used to intervene or stop crimes.
- As a means to mitigation, where AI systems are used to mitigate or reduce the impact of crimes.
- As a means to detection, where AI systems are used to detect or identify crimes.
- As a means to communication, where AI systems are used to communicate or coordinate crimes.
- As a means to protection, where AI systems are used to protect or defend against crimes.
- As a means to diagnosis, where AI systems are used to diagnose or identify crimes.
- As a means to prevention, where AI systems are used to prevent or stop crimes.
- As a means to intervention, where AI systems are used to intervene or stop crimes.
- As a means to mitigation, where AI systems are used to mitigate or reduce the impact of crimes.
- As a means to detection, where AI systems are used to detect or identify crimes.
- As a means to communication, where AI systems are used to communicate or coordinate crimes.
- As a means to protection, where AI systems are used to protect or defend against crimes.
- As a means to diagnosis, where AI systems are used to diagnose or identify crimes.
- As a means to prevention, where AI systems are used to prevent or stop crimes.
- As a means to intervention, where AI systems are used to intervene or stop crimes.
- As a means to mitigation, where AI systems are used to mitigate or reduce the impact of crimes.
- As a means to detection, where AI systems are used to detect or identify crimes.
- As a means to communication, where AI systems are used to communicate or coordinate crimes.
- As a means to protection, where AI systems are used to protect or defend against crimes.
- As a means to diagnosis, where AI systems are used to diagnose or identify crimes.
- As a means to prevention, where AI systems are used to prevent or stop crimes.
- As a means to intervention, where AI systems are used to intervene or stop crimes.
- As a means to mitigation, where AI systems are used to mitigate or reduce the impact of crimes.
- As a means to detection, where AI systems are used to detect or identify crimes.
- As a means to communication, where AI systems are used to communicate or coordinate crimes.
- As a means to protection, where AI systems are used to protect or defend against crimes.
- As a means to diagnosis, where AI systems are used to diagnose or identify crimes.
- As a means to prevention, where AI systems are used to prevent or stop crimes.
- As a means to intervention, where AI systems are used to intervene or stop crimes.
- As a means to mitigation, where AI systems are used to mitigate or reduce the impact of crimes.
- As a means to detection, where AI systems are used to detect or identify crimes.
- As a means to communication, where AI systems are used to communicate or coordinate crimes.
- As a means to protection, where AI systems are used to protect or defend against crimes.
- As a means to diagnosis, where AI systems are used to diagnose or identify crimes.
- As a means to prevention, where AI systems are used to prevent or stop crimes.
- As a means to intervention, where AI systems are used to intervene or stop crimes.
- As a means to mitigation, where AI systems are used to mitigate or reduce the impact of crimes.
- As a means to detection, where AI systems are used to detect or identify crimes.
- As a means to communication, where AI systems are used to communicate or coordinate crimes.