Tobias Jones Consulting Limited (TJC)

Case Study 3: Fraud strategy and futures for Home Office's Innovation & Research InSight unit (IRIS)

What was the challenge?

1. Z/Yen (via the Home Office's Accelerated Capability Environment's Futures & Insights Service) was invited to produce a **foresight report** outlining various scenarios against which HMG's emerging Fraud Strategy could be tested. The challenge was to present accounts of types of future fraud, informed by themes and scenarios for how fraud might evolve over the course of the next ten years. The purpose of the report was to:

   a. inform the future vision or high-level strategy, to ensure that priorities and objectives are rooted in better understanding of potential risks;

   b. identify challenges and opportunities that could arise in the future, and stress-test how well the assumptions which underpin a given plan or policy may stand up to a range of external conditions;

   c. assess the potential strengths and weaknesses of different strategic objectives or policy options; and

   d. 'future-proof' planned investments or other decisions that are under consideration to ensure that potential risks and unintended consequences are identified and considered as part of overall risk management.

How did we approach it?

2. Our work explored both how future technological developments could be exploited by fraudsters or make an individual vulnerable to exploitation, as well as novel ways to tackle fraud. The emphasis was on the experience and vulnerability of individuals from large-scale, high-volume, automated fraud, where technology can make a difference, with an 80/20 weighting between how individuals are victimised and fraud against businesses.

3. The methodology included **open-source desk research** and **stakeholder interviews**. This component covered a whole variety of literature and stakeholders including, but not limited to, law enforcement (e.g. City of London Police as the national lead force for fraud); victims groups (e.g. Victim Support, Citizens Advice); consumer groups (e.g. Which?; National Trading Standards); civil society and charities (e.g. Age UK); and professional groups. From this, we identified a set of trends. **Foresight techniques including Dator's future scenarios** were also used. The trends were generated using **societal, technical, economic, and political analysis**, and assigned scores on their impact and likelihood. **Compelling and challenging (yet well-informed and plausible) scenarios** for how fraud modalities will develop under varying technological and social conditions over the 10-year period were created against the backdrop of a **'three horizons' framework**. This was tested against the trends, against Dator's scenario classifications, and **against Adams' risk/reward typologies**. Examples of the variables in play included the maturity and commoditisation of AI techniques for creating and detecting fraudulent or deep faked materials and personas at scale, and the extent to which governments and/or technology platforms collaborate internationally to mitigate fraud. The trends and scenarios were sent for consultation to the ACE Futures and Insights Faculty community and to experts in two highly respected think tanks and amended according to their feedback. **Five 'future narratives' were compiled** and contrasted with the scenarios.

4. A **viable systems approach** was used to **model two systems**; the criminal system and the anti-fraud authority system. An observe–orient–decide–act (OODA) loop was applied to identify explorations for tackling fraud over the next ten years. These explorations, along

with the scenarios, were used to set out a handful of 'challenge' themes as suggestions to guide the anti-fraud agenda over the next decade.

5. The assumptions, trends, scenarios, future narratives, models, and challenges underlying and developed through the research were **tested at a webinar**, which was attended by 51 representatives from academia, the public sector, the ICT Industry, the financial services sector, and fraud prevention specialists. Feedback from the webinar was incorporated into the report.

What was the outcome or impact of the work?

6. The final **foresight report** delivered by Z/Yen and submitted to Home Office IRIS significantly informed the HMG's 10 year Fraud Strategy. It was shared internally with relevant officials and comments made. Following a final edit the finished report was sent to the No.10 Policy Team.

7. A version of the report[1], with HMG prior approval, was distributed through the Z/Yen website and via a regular newsletter to Z/Yen's extensive private mailing list. Within the first week it was downloaded 600 times.

[1] https://www.longfinance.net/media/documents/The_Future_Of_UK_Fraud_-_Challenging_High-Volume_Automated_Fraud_2022.06.16_v4.6.pdf