

HART to HART: is there a place for pre-crime?

24/11/2017

The future is now, with algorithms under development to predict the likelihood that individuals will offend. But is this another safety net to catch criminals or a step towards a Minority Report culture where 'the system' itself becomes the danger?



Durham Police force is currently operating the Harm Assessment Risk Tool (HART) which analyses social

factors such as behaviour, gender and residency and then classifies suspects according to how likely an algorithm believes they are likely to re-offend. While supporters of this scheme claim that the justice process will become more efficient and streamlined through use of HART, opponents have raised fears about the degree to which the tool is pre-disposed to 'play it safe' and categorise suspects as higher risk, about potential racial biases, and about the extent to which this is a violation of the right to privacy.

Clearly this is a work-in-progress and all parties have stressed that the ultimate decision still rests with the relevant case officer. However, it serves as a microcosm of the wider argument over the ever-expanding use of 'big data' and technology to make the crucial decisions, and whether this is outpacing human involvement. Just as there is a lobby which claims that artificial intelligence will take your jobs, is there now a chance that artificial intelligence could prevent you getting one in the first place?

The computing revolution saw a genie unleashed from the bottle, the scale of which is still being determined. The full power of algorithms, and the scale of their use in everyday life, is still being explored. The issues are twofold: what data the algorithm knows, and how it goes about using this. The issue is not just confined to law and order either. Similar programs are in use to determine suitability for credit cards, mortgages and job interviews, with some applicants being rejected even before a human ever has knowledge of them.

The biggest worry here is that society will start to move away from the *'human element'* and rely wholly on machines, and this is a very dangerous path to step down. Machines and algorithms may be predicated on logic but on a fundamental level that is all they are; they are unable to make the *leaps* in logic or apply empathy to a situation, which are sometimes required. Machines also, like humans, can make mistakes but can be a lot slower in picking these up.



HART to HART: is there a place for pre-crime?

What is necessary is to find the area between technology being applied to improve systems, and technology (perhaps unwittingly) abusing the system. For instance, one could consider HART a useful tool at a time when budget cuts are stretching the police nationwide, but one could equally see it as a stand against civil liberties if a computer is allowed to decide someone's criminal status. An algorithm ploughing through a thousand mortgage applications may be more efficient than a human, but could not consider the personal circumstances behind each that may merit consideration. The challenge for both the business community, both in the cyber and the layman sides, is to understand where the line exists between use and exploitation. Algorithms need to exist within a framework of problem-solving, not as the end result.

Certainly, one lesson of the HART algorithm is clear. While ultimate decisions should be left to humans, and without straying into the territory of potential 'pre-crime', being 'prepared' through systematic and full-scale intelligence collation is no bad thing. The best and most informed decisions, whether by man or machine, can only be made on a foundation of solid information. Predictive analytics might be a minefield, but having too little information can be just as dangerous.

KCS Group Europe - Strategic Intelligence & Corporate Security

A leading provider of security and intelligence services, we operate discreetly in some of the world's most difficult environments on complex cases of fraud, theft, corruption, or market dynamics. We gather intelligence through the discreet use of human sources to level the playing field and help our clients to identify and deal with any risks, weaknesses and threats which could impact on their business financially or reputationally.

Our key areas of expertise include:

- Corporate Intelligence Services
- New market or sector entry research
- Know your customer screening

In addition, through our specialist team at KCS IS, we also offer a unique service in the areas of Cyber Security and Cyber Risk. This covers penetration testing, vulnerability assessments, intelligence gathering and cyber security audits, providing unparalleled, analysis, contingency planning, and implementation for our clients.

To find out more or to arrange a meeting to discuss your business needs, please... email the team at info@kcsgroup.com or call (00 44) 2072451191