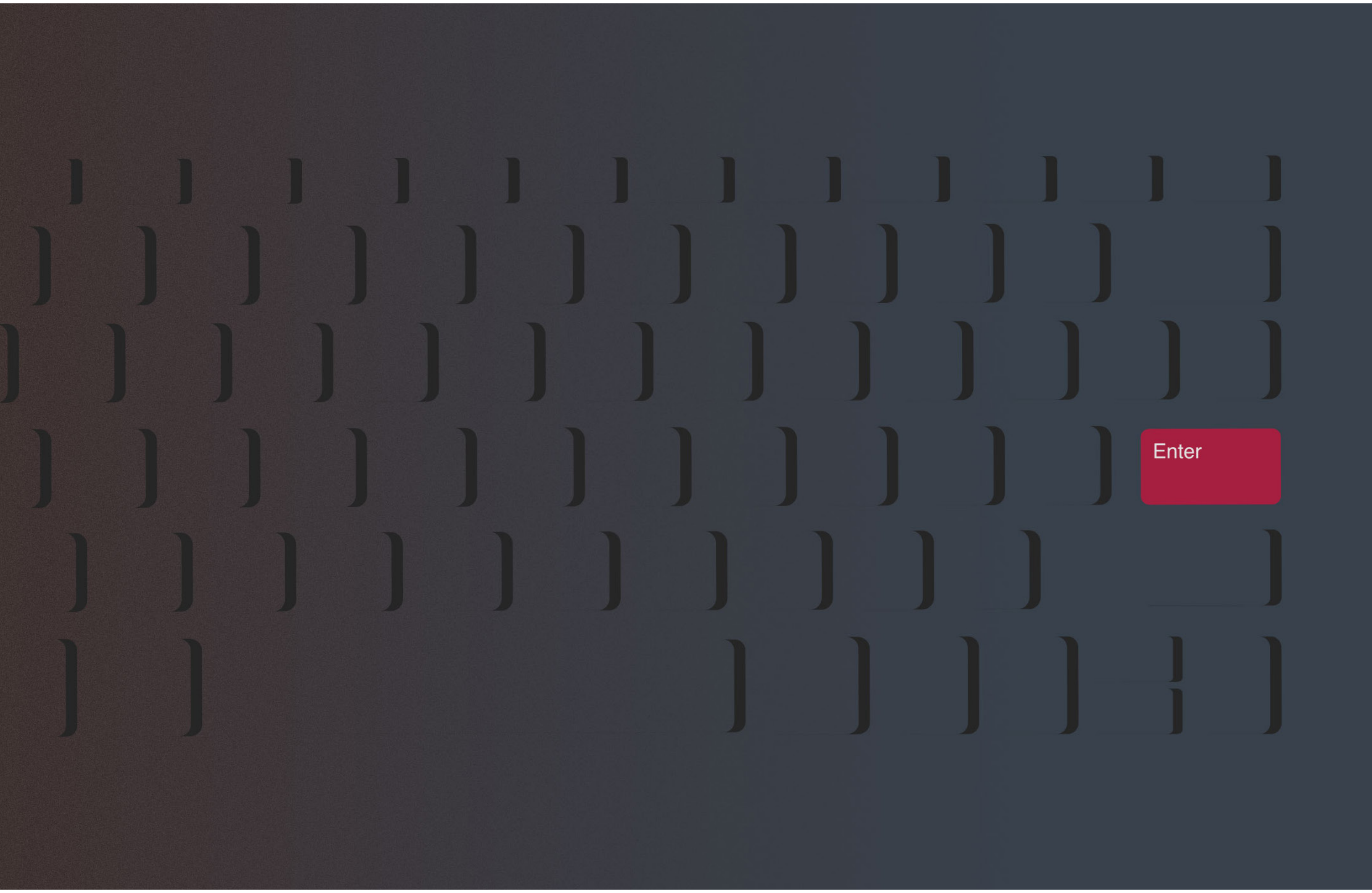
INSURANCE FUTURES

Policing and crime in a networked world

By Ian Kearns of The Oracle Partnership

JANUARY 2020



As more people go online, more systems are networked and the Internet of Things (IoT) expands, the context in which crime occurs and the police attempt to deal with it will change markedly. Some technological developments, coupled to the way criminals innovate around them, may tip the balance in favour of those interested in breaking the law. Others, if police forces, public policy-makers, consumers and citizens can learn to adapt and adopt them quickly, may point to improved crime prevention and increased law enforcement effectiveness. There are competing narratives.

Two things do seem relatively certain. The first is that, as the networked world expands, the opportunities for cyber-criminals, spies, terrorists and foreign governments to exploit it will expand with it. The second is that the outcome of the battle between networked crime and networked policing will have significant implications for crime rates and for those tasked with underwriting the risks associated with crime.

A digital ‘crime harvest’?

One possible scenario that could evolve between now and 2035 involves a catastrophic loss of law enforcement effectiveness, leading to a huge digital crime harvest.

The paths to this scenario include continued growth in cyber-crime activity, a police failure to acquire the skills and specialist capabilities needed to fight crime in the digital age, a loss of public trust and confidence in the surveillance and analysis systems that might help the police fight crime more effectively, and technological breakthroughs that might undermine the ability to encrypt information and communications.

There are signs that each of these elements could fall into place.

It is predicted that cyber-crime will cost companies around the world $6 trillion by 2021, a rise from $3 trillion in 2015.[1] Cyber criminals are thought to be acquiring annual revenues in excess of $1.5 trillion, a large proportion of which is being re-invested in activities like cyber-criminal software development, drug production and human trafficking as part of a self-sustaining criminal ‘platform economy’.[2]

A number of factors are driving this growth.

The explosion in the number of connected devices is increasing the available cyber-attack surface. Since many Internet of Things devices are not secure, they are being attacked at scale to acquire personal information and to launch denial of service attacks on larger corporate entities. Online marketplaces have developed, allowing criminals with only very basic technical knowledge to buy off-the-shelf software, like advanced phishing kits, that enable them to conduct cyber-crime quickly and easily. Money laundering and illicit criminal transactions are being increasingly conducted on crypto-currency platforms like Monero, Zcash and Ethereum. Cyber-criminals are also becoming increasingly adept at using artificial intelligence tools to conduct automated criminal operations at scale, to by-pass cyber-security arrangements or to generate content that appears legitimate but is actually being used to pass through cyber-security filters.[3]

There is also growing evidence of cyber-espionage being conducted by organised and state-backed groups. To name just a few examples, the Russian state is thought to sponsor many groups, each supported by a different part of the state intelligence apparatus, and each developing its own Advanced Persistent Threat (APT) malware.[4] There are reports of state-backed Chinese APT's being used to try to steal health sector intellectual property from the United States[5] and of North Korean malware being used to target ATM's to steal user card details in India.[6]

In acknowledgement of another growing dimension of the threat, the UN Secretary General, Antonio Guterres, has warned of the 'new frontier' of cyber-terrorism, involving the use of the dark web and social media outlets to spread propaganda and coordinate attacks.

In the context of this onslaught, law enforcement agencies around the world face huge challenges and are struggling to cope. Many lack sufficient numbers of officers and agents trained in fields such as digital forensics. As the number of devices and sources of data that may be relevant to criminal investigations explodes, police forces are also being overwhelmed by the sheer scale of the data analysis task. Many more crimes today are carried out across national and international jurisdictional boundaries too, as criminals use the global nature of the internet to extend their reach. This often leaves national law enforcement agencies powerless or at the mercy of a patchwork of international cooperation agreements and treaties in terms of their ability to investigate crime.

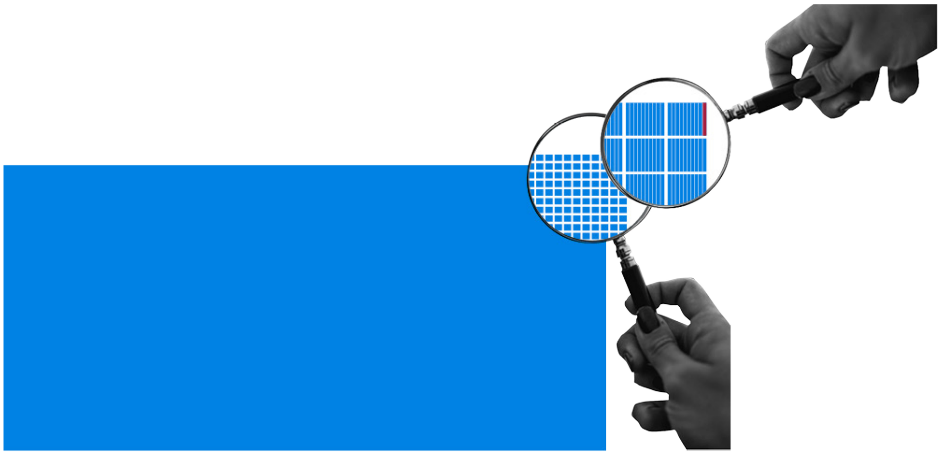
Attempts by policing organisations to seize the crime fighting or crime investigating potential of new technologies are also running into trouble. The global controversy surrounding police use of facial recognition technologies is but one example. Several US cities have banned the use of the technology over privacy and surveillance state concerns. Some point to China's use of surveillance technology and the backlash it has provoked in Hong Kong, as a sign of what is to come.

Elsewhere, police use of artificial intelligence tools to help sift through vast amounts of data, predict hotspots of crime and assess whether those arrested are likely to re-offend—and therefore need to be given custodial sentences—are highly controversial. This is partly because such systems have been demonstrated to exhibit bias. They can lead to some crimes being investigated and not others. They can lead to the over-policing of some communities and neighbourhoods and the under-policing of others. Machine learning algorithms used, once trained on a body of data, can operate like a black-boxes that cannot be reverse engineered to understand precisely why some predictions and judgements have been arrived at by the algorithm, and not others. For that reason, they cannot be 'cross-examined' in court by a suspect's legal team.

The significance of all this is that it is not a given that citizens around the world are going to trust their law enforcement agencies to use these new technologies responsibly. It is also possible that the attempts to use them, if not handled with great sensitivity, may destroy the public trust, legitimacy and confidence that some police services already enjoy.

In the background to all of this, a great technological battle is under way with regard to encryption. There are concerns that breakthroughs in quantum computing may overwhelm current encryption standards, rendering all electronic networks hackable and destroying confidence in virtual networks while undermining the foundation stone of the networked society in its entirety. What is secret and secure today—from commercially sensitive contract details, personal health data and intellectual property databases to systems that manage essential infrastructure—may become insecure and accessible tomorrow. This may drive a sudden retrenchment from virtual to physical worlds, with massively destabilising consequences.

In September 2019, reports began to circulate to that effect. A Google research paper was temporarily published and then removed, which claimed the company had achieved quantum 'supremacy' through the building of a quantum computer that took only three minutes and 20 seconds to perform a calculation that the most powerful existing computer would have taken around 10,000 years to perform.[7] The implication was that brute force attacks could in future 'break' encryption codes by trying every possible numerical permutation in a very short space of time.



The result of all of these developments and challenges, seen collectively, could be a major increase in crime, a catastrophic loss of public confidence in the police's ability to maintain law and order, and huge public concern over the security and safety of a wide range of digital systems and services, leading to a refusal to adopt and rely on them.

A digital policing breakthrough?

At the other extreme, it is possible to see the outlines of a far more upbeat scenario as we move toward 2035.

In this more positive scenario, new technologies deliver such huge advances in both crime prevention and detection that criminals are deterred and crime rates fall dramatically. Law enforcement leaders and politicians succeed in overcoming privacy concerns with regard to systems of surveillance. Public confidence in the use of facial recognition and other surveillance and monitoring tools like Automatic Number Plate Recognition (ANPR) systems grows as awareness of their benefits increases. As a result, the mass deployment of sensors and cameras in public places, transport systems, homes and places of work, rolls out and becomes largely trusted and socially acceptable.

The public also become more comfortable with law enforcement use of artificial intelligence tools to enable predictive policing. These tools combine historical data on crime patterns with real-time data sources to give the police a fine-grained understanding of where crime can be expected to occur and when. Deployments of officers then take place to prevent crime before it happens.

Alongside this, the machine 'reading' of vast amounts of digital data in the criminal investigation process becomes publicly accepted as the only way to prevent the police being overwhelmed. The Internet of Things effectively becomes the digital crime scene. When a crime does occur, investigators and their algorithms can access the mass of data from widely deployed sensor and surveillance systems to piece together what happened. Crime detection rates soar to such an extent that criminals are deterred, given the high chance they will be caught.

In this more positive scenario blockchain technologies are used across a wide front as crime prevention tools, almost eliminating the potential for crimes such as fraud and money laundering. The same systems, coupled with widespread use of smart contracts, are also being used to restore and maintain public confidence in systems of evidence disclosure and the wider criminal justice system.

New post-quantum cryptographic standards emerge, capable of withstanding brute force attacks powered even by quantum computers. Confidence in the secrecy and security of networked systems is preserved.

There are some signs that the building blocks for this scenario are falling into place. Some surveys suggest the public is willing to support large-scale deployment of surveillance technology, at least in some countries. A recent Pew Research Centre survey found, for example, that 56% of Americans do trust law enforcements agencies to use facial recognition technology responsibly, despite the controversy around the issue and the bans that have been introduced in some U.S. cities.[8]

Predictive policing trials are emerging in many jurisdictions and getting results. Cities like Chicago and Vancouver have seen reductions in crime where technology and different approaches to policing have been combined to good effect.[9]

Data from the IoT is being used to stop crime and build cases against suspected criminals once crime has occurred. In one example, sensors on fences and vehicles, coupled to alerts sent over wi-fi, form part of a Reserve Area Network (RAN) in a wildlife park battling against poaching in South Africa.[10] The sensors detect and track the entrance and location of guns entering the park so rangers can intervene before poaching takes place. In another example, data from IoT devices like Fitbits is being used to undermine alibis and bring criminal charges in murder cases.[11]

Blockchain technologies are also being used to prevent crime and combat fraud. A World Wildlife Fund trial in the Pacific tuna industry has fisherman attaching scannable codes to caught fish. The codes are uploaded to a blockchain ledger so buyers can be sure the source of the fish does not breach agreed treaties and rules with regard to preserving fish stocks.[12] The blockchain start-up Verisart is using the technology to prove the provenance of art works and track their movements through the world's art markets in an attempt to make art fraud far more difficult and to protect the interests of artists.[13]

There are claims too that the battle to protect encryption from quantum computing attack is far from lost. The US National Institute of Standards and Technology (NIST) opened a call for ideas on post-quantum cryptographic algorithms in 2016 and is moving toward selection of what it believes could be a new standard that would be capable of withstanding the age of quantum computing. In August 2019, IBM announced that it had successfully tested a quantum-ready approach to encryption that it now hopes to use in protecting cloud-based data.[14]

Implications for insurance

It is clear that in relation to policing and crime in a networked world, very different extremes are possible. At least two plausible scenarios with regard to the future are in play and a third, in which a game of cat and mouse between innovative criminals and innovative law enforcement organisations battle it out to a draw, is also possible.

Against this backdrop, the insurance industry will need to consider a number of issues and responses.

In all scenarios, the industry will need to invest in its understanding of trends in cyber-crime and in organised and state-backed cyber-espionage and disruption. The same applies to understanding of the cyber-security industry's ability to meet the changing cyber threat. Assessing the real potential of blockchain to prevent crime, and how public sentiment about privacy and the use of surveillance and AI systems can impact the crime landscape, will be important. Both will prove pivotal in the ability of law enforcement and wider society to rise to the networked crime challenge. The outcome of the battle over post-quantum encryption will also be of massive consequence to the risk landscape.

The insurance industry's ability to model the impact of various technology developments and deployments on risk will be crucial to putting a price on it.

Beyond that, however, the industry will face a choice. It can either use that modelling to simply vary the price or availability of cover, or it can attempt to lead in ensuring the right kinds of technologies are deployed in the right ways, in the right places, to achieve a desired reduction in crime risk and a better social outcome overall.

The former course of action may imply more available cover, at lower prices, in more extensively monitored societies and settings that are deemed more secure. It may also imply prohibitively priced or non-existent cover in locations and settings where privacy has won out over surveillance and where concerns over police use of AI have taken root. In this case, as the cyber threat grows, the insurance protection gap and the rate of crime may grow with it.

The latter course of action would see the industry acting to drive up the adoption of the best technology facilitated approaches to fighting crime and reducing risk. This could involve work with regulators, device manufacturers and clients to drive up awareness of cyber threats and to improve security best practices and standards. It could involve developing an understanding of and investing in privacy enhancing technologies to help smooth the path to more surveillance and monitoring systems, without undermining public confidence. It might involve building predictive risk reduction software that can more effectively win public trust, perhaps by better handling the challenge of algorithmic bias against particular communities, or by developing machine learning algorithms that can be reverse engineered and have their predictions and decisions challenged in court.

In this latter approach the industry would see itself as an actor helping to shape the overall outcome, inventing new products and services en route.

[1] https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

[2] https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf

[3] https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/

[4] https://www.zdnet.com/article/russian-state-hackers-rarely-share-code-with-one-another/#ftag=RSSbaffb68

[5] https://ciso.economictimes.indiatimes.com/news/chinese-espionage-growing-in-us-healthcare-experts/71198770

[6] https://www.zdnet.com/article/new-north-korean-malware-targeting-atms-spotted-in-india/#ftag=RSSbaffb68

[7] Google claims to have reached quantum supremacy, available at: https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17 Others have subsequently played down the achievement, arguing traditional computers could complete the task in far less time, though not as quickly as via quantum.

[8] https://www.wired.com/story/poll-americans-trust-police-facial-recognition/

[9] https://www.govtech.com/public-safety/Drones-AI-Bodycams-Is-Technology-Making-Us-Safer.html

[10] https://www.aljazeera.com/ajimpact/battle-wildlife-poachers-increasingly-high-tech-190911144002627.html

[11] Fit-bit data used to charge US man with murder, available at: https://www.bbc.co.uk/news/technology-45745366

[12] https://uk.reuters.com/article/oceans-un-fishing/feature-blockchain-ai-hailed-as-new-tools-to-protect-high-seas-idUKL8N1XB7NU

[13] For a description of what they do, see https://verisart.com/ And for some commentary on how blockchain is being used to help fight crime in the art world, including by Verisart, see: https://techcrunch.com/2015/09/27/using-the-blockchain-to-the-fight-crime-and-save-lives/

[14] New Encryption System Protects Data from Quantum Computers, available at: https://www.scientificamerican.com/article/new-encryption-system-protects-data-from-quantum-computers/

About the author

Ian Kearns has 25 years' experience working in the public, private and NGO sectors, the last 13 of them in leadership positions. He is a former Acting Director of the Institute for Public Policy Research (IPPR), Britain's leading policy think tank, and launched the IPPR All Party Commission on National Security. In 2011, he co-founded the European Leadership Network (ELN), a political, military and diplomatic network of former Prime Ministers, Foreign and Defence Ministers, diplomats and senior military figures across greater Europe. Ian served as the organisation's first Director, establishing ELN as a well-respected feature of the policy landscape on foreign policy and security issues. He serves on the Executive Board of Directors. He has written for The Guardian, The Times, The Independent, Newsweek and The New Statesman and he has been a commentator on the BBC and international media. His recent book, 'Collapse: Europe After the European Union' was published by Biteback in April 2018.

More information on Insurance Futures and The Oracle Partnership can be found at:

oraclepartnership.com/insurance-futures

Milliman

Founded in 1947, we are an independent risk management, benefits and technology firm with offices in major cities around the globe. We serve the full spectrum of business, financial, government, union, education, and nonprofit organizations.

milliman.com