City, Territory and Architecture

RESEARCH ARTICLE

Open Access

Technology and organised crime in the smart city: an ethnographic study of the illicit drug trade

Mark Berry*

Abstract

The term "smart city" has circulated across the developed world affecting urban development programmes and government strategies. Such "future cities" are heralded for their efficient networked technologies embedded within the fabric of urban environments that provide new means of social control for the state. These cities are envisioned as a technological fix for the many problems of modern city life, yet emerging technologies are not flawless and have vulnerabilities that can be manipulated by criminal actors. Even so, there is an interesting silence about the issues of security amongst the advocates of smart cities. Furthermore, there remains limited insight into the impact of the smart cities programme from criminologists, particularly in relation to hitherto prioritised threats of organised crime, notably the illicit drugs markets and associated harms. Those who have addressed the impact of emergent technologies have done so through critiques of governmental programmes, drawing largely upon insights from science and technology studies. A key absence in this, as well as the commercial and governmental literature, is the voice of actors involved in the networks that actually constitute threats to urban security, and how they perceive and use emerging technologies for illicit ends. This paper aims to augment but also challenge this treatment of the impact of emergent technologies, by switching the analytical focus towards the principal actor-networks that constitute these threats, with a particular focus on ICT (mobile technologies and internet drug sales). It uses data from a 5-year ethnography to demonstrate how ICT reconfigures and virtually extends illicit drug markets, whilst providing insights into the workings of drug markets of the future.

Keywords: Organised crime, Smart city, Technology, Drugs, Ethnography

Introduction

Technologically advanced smart cities have begun to emerge across the developed world, but within them, criminals are adapting and taking advantage of the technologies they are founded upon. The illicit drug trade is evolving quickly, with advances in chemistry creating a barrage of new psychoactive substances, whilst ICT provides means in which buyers and sellers can communicate and coordinate their transactions with relative anonymity over vast geographical distances. This evolution has driven by the combination of evolving technologies and the need for protection and concealment from the law. Indeed, the ubiquity of digital surveillance in the smart city has done little to reduce the supply of drugs, but questions remain as to how vendors and actual or potential purchasers communicate with each other within these circumstances. A central argument of this paper is that rather than replacing traditional drug markets, ICT extends them (Lawson 2010; Brey 2017) into virtual domains, creating communication channels and buying platforms that alter power relations between stakeholders. Whilst also retaining elements of market territoriality. Studies of virtual drug markets are growing but largely due to their methodologies, tend to ignore the offline life-worlds of criminal actors who engage in them. By restricting the source of their data and analysis to the internet itself, criminologists provide a limited picture of the impact of emergent technologies in this field. The

*Correspondence: berryma1@cardiff.ac.uk
Cardiff University, Cardiff, UK

virtual does not replace the real (Woolgar 2002). This paper utilises ethnographic fieldwork of manufacturers and distributors of illicit drugs operating in physical as well as virtual domains. It draws upon actor-network theory and assemblage thinking to sketch out the ever-evolving nature of organised crime within the sociotechnical system of the smart city.

Data-driven urbanism and the "smart city": governmentalities and programmes

To further substantiate these arguments, it is first important to place the impact of emergent technologies on the illicit drug trade in the broader context of the smart city as a commercial construct. The smart city is a fuzzy concept that has various definitions. Broadly speaking it relates to the construction of new relationships between technology and society (Söderström et al. 2014) but can be differentiated along two lines (Kitchin 2014):

1. The smart city is composed of pervasive digital technologies embedded in the fabric of the urban environment. These technologies, as Greenfield (2010) puts it, are "everyware" (sic), they penetrate and collect unprecedented amounts of real-time information on all levels of the infrastructure of cities as well as the lives of the citizens within them. These range from utility services such as traffic control management and surveillance systems to personal computers and other mobile technologies. The subsequent "big data" is gathered in an attempt to render the city knowable so that it may be governed (Edwards 2017). The technologies alone, however, are not enough to make the city "smart", they must;
2. Coincide with the development of the knowledge economy potentiating the innovative and entrepreneurial capacities of its citizens and government. These learning, or knowledge, cities are "actively involved in building a skilled information economy workforce" (Nam and Pardo 2011, p 285) and are designed to facilitate the nurturing of knowledge (Edvinsson 2006). The smart city then, is one which employs advanced technology to monitor and coordinate its infrastructure, while providing inhabitants with the knowledge and (smart) tools, to improve their lives and increase their creative and economic capacities. At least that is how it is envisioned by its proponents.

On its surface, the smart city presents itself as a utopian dream; a technologically empowered panacea to many of the problems of modern city life. Yet, if we gaze beneath the glossy veneer and unpick its etiological roots, a different picture begins to emerge. The smart city is not a social scientific concept grounded in real concrete relations and connections. It is a commercial construct designed to sell a particular vision of capital accumulation and the necessity of digital technologies to achieve this. Big tech companies employ the smart city as a narrative device to sell their products and services (Söderström et al. 2014), which explains why it has so many incarnations (see Cocchia, 2014, for a review). Its spectacle is intended to capture the imagination of prospective clients who buy into the claims of these IT companies. Such assertions are often unrealistic and can bring with them a whole host of problems. Emerging technologies can have negative side effects that cannot always be predetermined, and even if they are tech companies may not be concerned as long as their products sell. Once established, governments may become reliant on these technologies thereby putting IT companies in extreme positions of power. It would be wise to adopt a healthy scepticism toward the smart city, considering where the concept originates from and the interests it privileges. It does nonetheless have real-world consequences, and it is for this reason that criminologists should be concerned. New technologies can create vulnerabilities that may be exploited by criminal actors.

Insofar as criminologists and sociologists of deviance and social control have addressed the impact of emergent technologies it has been through critiques of governmental programmes, with a particular emphasis on securitisation and digital surveillance (Haggerty and Ericson 2000; Lyon 2014; Schuilenburg 2015; Amoore and Raley 2017). These studies have employed concepts taken from science and technology studies (STS) and actor-network theory (ANT) to avoid the social determinism and methodological individualism of well-trodden criminological theories, such as routine activities and rational choice. The strength of ANT lies in its ability to account for the agency of material objects, which is particularly fitting in a digitally entrenched society in which technologies are literally gaining a life of their own (Ritzer 2015). ANT dissolves the ontological divisions between humans and non-humans and places them within a network of associations in which power is relational rather than inherent in the "actants" (human/nonhuman actors) themselves (Latour 2005). The network is an assemblage of diverse, heterogeneous elements which is arranged and fitted together (Livesey 2010, p 18). Within these networks, struggles occur to displace actants from competing networks by enrolling and mobilising them forward (Callon 1986).

A further facet of ANT is the attention to the dynamism of the networks in which actors are enrolled. Controllers and organisers of crime adapt and alter their practices whilst gearing up on new hardware to outmanoeuvre and derail their rivals. It is this mutability that drives the technological uptake within security services and the criminal networks they seek to control (Dorn 2003; Ekblom 2017). The technological arms race is well acknowledged by criminologists yet is presented in the traditional sense of people using tools, a passivity that ignores the very active nature of the technologies themselves. To move past this socially determinist and somewhat outdated position, the research outlined in this paper builds upon assemblage thinking by placing technology, criminals and crime controllers along the same ontological plane. The resulting assemblage is a mesh of human, technological, and institutional parts, which exert both dissonance and concordance in their relationship to each other. The arms race is an emergent property of this dialectic. As Hilgartner asserts:

> *"Another advantage of the system/network perspective is that it provides the basis for dynamic accounts of sociotechnical evolution... Changes in network structure occur as system components are added, deleted, connected in new ways, as they are reconstructed, recombined, and refined-all for the purpose of changing the power of the system and the distribution of power within it." (Hilgartner 1992, p 45).*

The conceptual toolkit of ANT is well suited to a study of the illicit drug markets given the increasing adoption of smart technologies by actors in these markets. Illicit drug markets are socio-technical systems, in that they are both socially and technically determined. Even so, there is little, if any recognition of the utility of ANT by those who specialise in the field of organised crime. Nonetheless, the uptake of ANT into the wider field of criminology is growing. Haggerty and Ericson (2000) were among the first to draw upon these concepts by examining the spread of digital surveillance in western society. The "surveillant assemblage" as they call it, synthesises a wide variety of surveillant systems which work by generating virtual data doubles of human actors to be later targeted with interventions. In a later piece, Schuilenburg (2015) reasoned that surveillance is but a part of the securitization agenda, which he describes as, the spread of techniques mobilised by a hybrid system of state and non-state actors, with the intention of making the future certain and secure.

Indeed, the smart city is bound up in fine-grained monitoring and the predictive modelling of the actions and movements of its "citizens". It is not the case that it is an "individual", as in a single person, that is "targeted" through various techniques and technologies in the Foucauldian sense (Foucault 1977, 2009). Rather, that what a citizen "is" is the product of algorithmic neural network modelling and aggregation from which new indices of normality, deviance, and risk arise. These are then reapplied or "folded back" on to, and into, the everyday lives of people. The "normal" way to talk and walk, for example, is being built through digital modelling (Amoore and Raley 2017). These algorithmic calculations and statistical representations feed into policing techniques on the ground (Sanders and Sheptycki 2017). Following the positivist logic of evidence led policy, data is assumed to have value neutrality. Yet, techniques such as predictive policing target the usual suspects in poverty-stricken areas creating a self-confirming algorithmic bias (Hannah-Moffat 2018). Nonetheless, the drive towards the uptake of these systems is relentless, see Barbuta (2017) for recommendations.

Whilst critiques of governmental programmes are not unwarranted, a significant absence in this literature is the voice of criminal actors that generate and constitute threats to urban security. The weakness of much criminological research is its one-sidedness and partiality (Young 1986). As with many others in this field, their work is missing the voice of the underdog, which requires more empirical labour than most are willing, or able, to pursue (Becker 1967). The arguments laid out do not do enough to recognise that the technologies of the securitisation agenda can be (but not always are) outmanoeuvred and even adopted by the criminal networks they seek to control (Edwards 2016). In this respect, they begin to fall into a "techno-centric rhetoric and narrative where urban and societal problems are rendered docile and amenable subjects to technology" (Wang 2017, p 378). Indeed, questions remain as to how criminals organise their activities within these conditions of heavy digital surveillance. This paper aims to remedy this absence and further build upon these contributions, by switching the analytical focus towards the criminal actor networks who present such threats, namely those who distribute illicit drugs.

The study

The paper draws upon data from a 5-year ethnography on the manufacture and supply of illicit drugs (ongoing). Interviews and semi-covert observations were conducted with twenty-six criminal actors, many of which were criminally active at the point of study and unknown to the authorities. The participants ranged from local retail dealers to international wholesale traffickers. The majority of the participants operated wholly offline, but there were some who operated online. Two participants ran websites selling drugs whereas another distributed through online forums. To complement the fieldwork, interviews were conducted with official actors from the criminal justice system, the private sector and the third sector, bringing the total number of interviews to 37.

Data was also collected from the websites of the online distributors. Anonymity was ensured in all cases.

The digital extension of organised crime

The following section begins with a brief introduction of the impact of ICT on the illicit drug market over time. It draws upon the experience of criminal actors working with emergent technologies to demonstrate how they manage the associated risks of their activities whilst responding to the demand for their products.

Organised crime is a market-based activity in which buyers and sellers interact to purchase and distribute illicit goods and services. Illicit drug markets have been variously characterised as being open, semi-open, or closed. In open markets, distributors usually operate from a fixed location, such as a street corner, and sell openly to most people wishing to buy their goods. In closed markets, distributors will only sell to trusted individuals who have been previously vetted. Semi-open markets fall somewhere between the two and relate to spaces such as nightclubs, bars or cryptomarkets. Before the emergence of ICT, transactions were made face to face through spoken communication. In this respect, it was important for drug dealers to be in an area where customers knew they would be. This mode of working was significantly risky as being in a fixed location made dealers easy targets for the police. With the advent of the mobile phone, distributors could be more mobile and arrange transactions in advance leading to a more closed networked economy (May and Hough 2004; Wainwright 2016).

As a conduit for communication, the mobile phone is an obligatory passage point (Callon 1986) which restructured the drug market and shifted it into a less visible and less risky form. As Callon explains, “technologies transform the spatial and temporal settings in which collectives exist and act” (Callon 2004, p 5). Yet, whilst technologies can enable and enhance human capacities, they can disable and diminish others (McLuhan and Fiore 1967; McLuhan and McLuhan 1992). ICT leaves digital traces which may be accessible to the police thus frustrating attempts for dealers to remain concealed. Police penetrate criminal sociotechnical networks by enrolling elements of the assemblage and drawing information from them. As digital technologies take a more central position in the illicit drug trade, then it is these technologies and their “trace data” that become as, if not more, important sources of intelligence than their human counterparts. In this sense, the police have delegated tasks (Latour 1994) that were traditionally assigned to human informants to the technologies within these networks. To counteract these efforts, distributors must protect and stabilise the network or risk prosecution.

According to Hilgartner, risk is composed of sociotechnical networks that link objects within them to harm. It is the relationship between elements within the network that lead to the construction of risk. Through such relationships, risks can be embedded in people, materials, technology or tasks. These “risk objects” must be contained or displaced from the network to avoid harms associated with the linkage (Hilgartner 1992). The following account is taken from an interview with Max, who has an extensive history distributing illicit drugs at the retail level. The discussion relates to issues in using mobile phones to coordinate drug sales:

> *Max: When I started back up again I was more clued up about surveillance, buying a sim card isn’t enough if you’re stupid enough to put your sim card from your burner in your contract phone the IMEI number would match up with it, so just being aware of the trail how a phone number can lead back to you. If you carry your contract phone around with you as well as your burner, they can trace it back to the cell sites, and they can show that both phones took exactly the same path, and it’s very hard to dispute you aren’t the same person. I always had two phones one phone for selling drugs and contacting my mates and another for contacting family and paying bills things like that. I had a clean phone for that stuff. I was always very careful about how I used the burner.*

“Burners” are temporary mobile phones which have sim cards registered with false names and addresses making it difficult for police to link to a particular person (Salinas-Edwards 2013). Drug dealers frequently swap their burners to evade wire taps and the geo-location trails that can establish their involvement in crime and support successful criminal prosecutions. The international mobile equipment identity (IMEI) numbers that Max refers to are unique codes that are assigned to all cellular mobile devices to identify them. These codes allow signal towers to recognise devices in the service network and establish their geographical location. This information can help the police track criminals and prove their whereabouts in court (Bennett 2012). If distributors make the mistake of putting a sim card that is registered in their name in a phone they were using to sell drugs, the police can tie the sim to that particular device. Nonetheless, the monitoring of cellular devices can actually benefit criminals if they use them intelligently. A heroin dealer called Teeth, for example, created digital alibis by leaving his registered phone turned on at his home address whilst he went out about his business in the city. By using these methods, drug dealers are essentially blocking and subverting the process in which criminogenic information is digitised and monitored. Berry (Forthcoming) observes a similar phenomenon in his study of the electronic monitoring of offenders.

The police are not the only threats to distributors of illicit goods, however. The absence of formal regulation from the state creates a hostile environment which leaves vendors open to attack from other criminals on the street. Competitors may seek to gain control over access to goods and services making business difficult to establish. Technologies can become targeted by other criminals who wish to dominate territories in which drugs are sold. The following example is taken from a distributor called Rocco describing his experiences retailing heroin and crack cocaine:

> *Rocco: At the time we had it like, one area, literally lock down me and my mate, and then our other two mates had the other side on sort of like lock down as well, so if anything happened we'd go sort it. Literally there was a group of like ten-twelve of us all done little bit different bits and pieces but if something happened to one of our mates or whatever, you'd all be there and get it sorted so no one would fuck about. But I can remember one time the phone was going quiet and I was like "what the fuck how can it be that quiet" and he was like "oh yeah this kiddy" like's basically saying "fuck you" on about me, "he's gonna be taking over".*
>
> *Mark: Your patch?*
>
> *Rocco: Yeah, that sort of side so, I said "oh right we will see about that". I tried stopping him in the car and he sprinted off and carried on doing his thing but we knew where he was doing it to. So I went round with a couple of mates went through the door with a fire extinguisher, I had a door brace, went in with the fire extinguisher, he's come running down the stairs just by the door in case anyone come. As he's come running down, smashed him on the head with the fire extinguisher and knocked him out. With that the two mates who I was with grabbed what he had there and a bit of cash and the most important thing I wanted was his phone.*
>
> *Mark: Yeah?*
>
> *Rocco: Cos obviously that's their line so they would have to set up and go round again.*

Distributors require significant social and material resources to control a drug market in an area at a given time. As Rocco explains, he was connected to 10–12 criminal associates who could be mobilised when needed. This critical mass, worked together to govern the local market to ensure their positions were upheld. By taking the dealers drugs and money he was able to recoup some of his losses, the physical violence was a further punishment and is one that sends out a message to deter others. By taking his phone, however, Rocco gained control over the network which would enable him to redirect the custom base within that geographical area. By controlling the network, he was able to control the territory. As Graham (1998) asserts, "every social and economic activity is necessarily geographical" (Graham 1998, p 175). It was the combination of actions that led to the maximum disruption of his operations.

Coordinating drug sales via ICT is only one half of the process, however. Drugs need to be delivered to the customer and this can be risky if done in public. It is also important to consider how drug dealers mitigate the risks of visual surveillance in the city from police officers and technologies such as CCTV. As Sacks notes in an early piece, "the police are occupational specialists on inferring the probability of criminality from the appearances persons present in public places" (Sacks 1972, p 282). This process has now been delegated to the algorithmic systems of the smart cities surveillance technologies which detect "abnormalities" in the behaviour of people. In the following example, Max discusses the techniques he used to conceal his movements in the city:

> *Max: When meeting people either they jump in my car or I'd go into their house. I would always sell in a discrete place away from CCTV and somewhere no-one's listening. If someone jumps in a car and they drive off it doesn't look dodgy, but if they get in and get straight out again it looks dodgy as fuck. The same thing if people meet and they suddenly part ways like going into a house.*

To remain "invisible" from surveillance organised criminals can operate under the cover of activity that replicates the activities of something or someone else. Drug dealers carry out their movements in ways that blend into the flows of city life. In this sense, there is a reflexive relation of "training" (Goffman 1956; Foucault 1977) between the surveillant and the surveilled, between the human and the algorithm. This reflexive responsibilisation of risk is an integral characteristic of "reflexive modernisation" (Beck 1994; Lyng 2016) that has been transposed within the digital frontiers of the smart cities surveillance systems. As Amoore and Raley argue, "human and non-human beings are constantly attuned to novel events and features in their data environment, becoming perennially creatively alert" (Amoore and Raley 2017, p 3).

Virtual markets

As drug markets move online, they become reconfigured once more. The most significant change is that suppliers and customers do not meet face to face (in most cases). Transactions are made online using digital currencies, and the drugs are sent in the post (Hillebrand et al. 2010). This means that controlling and building a local custom base becomes less important for suppliers as drugs can be delivered to people across large geographical distances, from a single fixed location. Cryptomarkets anonymise stakeholder activity through the TOR browser which bounces digital communications through various relays across the world. Online drug markets are generally less violent as distributors identities can be concealed (Aldridge and Décary-Hétu 2014).

It is not always necessary to use the darknet to distribute drugs anonymously online, however. Various techniques can be employed to anonymise the identity of distributors whilst allowing them to operate websites openly on the clear net that can be accessed by anybody. Charley, for example, works for a small illicit company that distributes steroids in this manner. Pharma-Labs distribute their products internationally and take around a million pounds in sales per year:

> *Mark: Do you think there's more risk going online, does that create more risk or do you think it's less risky for getting knicked?*
>
> *Charley: Well the more branches you got of the tree I guess… The websites, all the IP addresses they are all like covert like the silk road… They have the servers in other countries so they can't be traced… You know the people who run the website the people whose name it's in is somebody that's nothing to do with us, they get paid they get a percentage, so that person gets a percentage off the sales and because obviously they are taking the risk. You know it's the same as what you'd do if you gave someone a cut off a crop of weed that you grow in their house…*
>
> *Mark: So with your mates or whatever you notice any violence or any disputes with any other people?*
>
> *Charley: Uh no, I mean there's people I know, on social media, you know sort of slagging the products off, because they are selling other products there's a lot of forums, people go on and slate certain things.*
>
> *Mark: So is it like a rating system or?*
>
> *Charley: Well there's certain labels, pay people to do social media to go on forums yeah, I know people who get paid a thousand pound a month.*
>
> *Mark: To like slag people off and stuff?*
>
> *Charley: Yeah to slag off all the other products and rate theirs, yeah don't take this that's fucking shit, I made some really good gains with this one blah blah, and get a thousand pound a month what they do is they get people who are known in the industry to do it, like good bodybuilders you know, I'll give you a grand a month just go on this website and tell them our product is mint. They do that with you know you put David Beckham on a Pepsi advert it's the same principle.*

Steroids carry softer legal penalties for distribution and can be acquired for personal use in the UK making sales difficult to prosecute against. Operating on the clear net widens the potential scope of sales as more people can access the website. Measures were, however, put in place to protect the identity of the core members of the group by hiring a technical specialist who runs the website on their behalf. Even if it was possible to get through the digital layering process employed by the specialist and identify who was running the site, the core members of the group would remain protected. Unless, of course, their facilitator chose to give up their information (Dorn et al. 1998).

The anonymity of the internet creates new problems for distributors as it allows others to compete in the virtual space without fear of violent reprisals. In this environment, distributors compete for customers by providing a superior service (at least as their customers see it) and building their brand (Aspers 2011; Aldridge and Décary-Hétu 2014). Websites on the clear net are different from cryptomarkets as they do not usually have the same ranking systems in place. Instead, suppliers rely on written feedback on user forums to build positive reputations. Those with greater resources can employ well known respected actors in their field to promote their goods. In this respect, the illicit market begins to resemble the licit one; the major difference is that these sites are illegal and cannot go to the courts for dispute adjudication. This creates further issues if customers do not pay for their goods or competitors copy and counterfeit their brand.

A common scam which customers can employ to get free products is a credit card chargeback. Once the goods arrive the customer contacts their credit card company and states that they have not received an item they paid for; it is then down to the company to prove otherwise. Illicit enterprises may encounter additional risks from refuting this claim as they are forced into contact with legitimate actors who may question their line of business. Furthermore, if the customer is not in the local area, tracking them down in person may not be easily achieved. Even if it were, online distributors have other options available to them. Customers give up some form of personal information to buy the drugs and have them sent in the post. Distributors can use this data and post it to online forums to name and shame the transgressor. The following example is taken from a "scammers list" on Pharma-labs forum:

> Bryan Renolds Scammer from Brighton
>
> *Package was sent 06/03/18 but could not be delivered as no one was at address, royal mail left collection card. This scammer immediately issues a charge back from his credit card and has the cheek to slag us off online saying his products were not sent.*
>
> *Bryan could have emailed us for the tracking number instead he is BANNED and is indexed online as a steroid scammer. Well done Bryan…*
>
> *Bryan Renolds*
> *13 Grenfell Street*
> *Woodingdean*
> *Brighton*
> *BN2 8TL*
> *bryanrenolds@emailme.com*
> *https://www.facepageuser.com/bryanrenolds84*

> *Image by Gujjar (2016) (all data has been anonymised following ethical protocol)*

In the example above, it is possible that the collection card went missing leading the customer to assume it had not been sent. If that was the case, he could have avoided being listed if he had contacted Pharma-labs for the tracking details of the parcel. A more likely explanation is that he received the collection card and issued the chargeback with the plan of picking up the goods without having paid for them. With his details listed online, anyone who searched for him would have been able to find where he lived, what he looked like, and that he was a user of steroids. This could be devastating if a vigilante took it upon himself to take action against him, it could also deter prospective employers who undertake background searches on potential employees. Here we can see that the anonymity of the internet changes the power relationship between buyers and sellers, largely in favour of the latter group. Having personal details placed online is a powerful deterrent that identifies transgressors in their very homes. Technologies create folds between time and space that redistribute presence and absence (Callon 2004). Whilst Charley's team was not physically present in Bryan's local territory, they had, nonetheless, been able to penetrate these boundaries through this virtual form of panoptic surveillance (Bentham 1798).

Distribution

Online distributors typically use postal services as this enables them to get goods to customers at a distance without having to meet them in person. In virtual markets, transactions are carried out online, but the drugs and the customers exist in the physical world. Getting products to their destination can create problems for vendors as they are forced to use the physical infrastructure of the city and interact with members of the public. The following example demonstrates some issues relating to using postal services to distribute illegal goods:

> *Mark: How's business?*
>
> *Charley: Things are hot at the minute there's a month long internal investigation going on at royal mail, they are looking for drugs so we can't send anything out. It's cost me a fortune.*
>
> *Mark: How did your mates (bosses) find out about this?*
>
> *Charley: Another online distributor told them and gave them the heads up they know people in royal mail so passed on the information. Well, they actually bought an entire post office to stop people asking questions.*
>
> *Mark: Wow.*
>
> *Charley: Obviously it's a big risk if I post stuff with this is all happening so I don't know what we're gonna to do about it.*
>
> *Mark: So have you put it up on you website that you are closed for the moment?*
>
> *Charley: I don't know what's going on with that, the guy in China who runs the website doesn't like to close it because, if he does that, he won't be making any money and he'll lose out. I can't use Royal Mail*

> *and using a different courier is too risky, I'll have to wait it out. (Looks distressed).*

Distributing drugs by post creates risks as postal workers may ask questions if people are sending suspicious packages or are using their service on a regular basis. To resolve this, they can be paid off and corrupted. Indeed, there have been a number of cases of drug-related corruption in Royal Mail over the years (Independant 2015). Charley informed me that he used a small local post office and paid them additional money to stop them from notifying the authorities. The example of the online distributor who bought an entire post office branch demonstrates the lengths that suppliers will go to protect themselves and the amount of money that this type of business can generate. Criminal agents mobilise actants into allegiances, extending their relational networks, to achieve their aims (Callon 1986). As the business grows, it becomes more integrated with the legitimate economy as it becomes more reliant on its services (Von Lampe 2015). Most significantly this example demonstrates that the local dimension of organised crime is as important as ever. Virtual platforms may extend the geographical boundaries of illicit markets but the actors within them still operate in a local manner. Making allegiances with local service providers is no less important than the virtual markets themselves.

Manufacture

There is a growing trend for domestically produced drugs in the UK. Advances in technology shrink supply chains by making it possible to localise the production process. Domestic production reduces the costs of distribution and the risks of being caught, as drugs are manufactured much closer to their consumers. Indeed, technology provides both the knowledge and tools to produce illicit goods. The internet is a vast repository where people can find information on almost anything. Anyone looking to grow cannabis, for example, can find everything they need online to successfully cultivate the drug (Wax 2002). This also applies to other drugs as is demonstrated in the example below, Sam is a bodybuilder who frequented bodybuilding forums on a regular basis:

> *Sam: I became a member, an active member, a very active member in fact. After a while, after sort of a few thousand posts, I sort of built up trust with the members there even though I had never met them. I was approached by the owner of the forum and he asked me to do some administrative duties for him, moderating the forum. Uh and I got promoted, when I was promoted I got access to a secret area of the forum. The secret area of the forum was where all the suppliers would discuss business. I got put in touch with a source from China who, had a range of steroid products for sale. It was the raw testosterone powders which would need to be synthesised into the final product. On the website there was complete guides and tutorials on how to make it yourself, so it's safe, sterile, pure… you need a few precursors, grape seed oil, benzyl alcohol, benzyl benzoate… I used the anabolic steroids on myself that I had made, I injected them and I had good results.*

Trust is an essential requirement in the illicit drug market (as it is in most markets for that matter). There is little to stop actors from passing on information to the police, or the police posing as criminals themselves. This is not to mention the difficulties distributors have in protecting themselves from robbery or ensuring debts are repaid. In such a high-risk environment stakeholders must build levels of trust to ensure that co-offenders are reputable (Von Lampe and Johansen 2004). Trust facilitates social ordering by "providing the cognitive and moral expectational maps for actors and systems as they continuously interact" (Barber 1983, p 19). Ultimately, trust reduces social complexity in actor-networks and increases their stability (Tong 2016). What is interesting about Sam's case is that he was able to build trust with members of the forum without having met them in person. Sam informed me that he had purchased steroids from other members who sent them to his home, he also invested many hours talking on the forum about his personal life and training protocol. In this respect, he was building a digital representation of his life that influenced the other members. Having invested his time there, the owner approached Sam directly and asked him for his help. This demonstrates that trust on internet forums follows much of the same social conditions as it does offline when people interact face to face. Connected co-presence (Pellegrino 2011) can be enough to establish criminal cooperation in virtual environments.

Having gained the trust of the owner, Sam was invited into a private area of the forum where he gained the contact details of individuals who sold high-quality precursors at a relatively low price. This sensitive information was kept secret from other members of the forum who were not trusted enough to be given clearance. It may also have been used to stop competitors from gaining access to their suppliers in order to maintain a comparative advantage. The secret area can be described as a spatial mechanism for controlling access to certain aspects of the distribution network as market territories are re-established online, "Rather than simply substituting or revolutionizing the city… the evidence suggests that new technologies actually diffuse into the older urban fabric offering potential for doing old things in new ways" (Graham 1998, p 173). With the correct access, the forum provided all the information that Sam required to manufacture anabolic steroids for himself. He had complete control over the production process which enabled him to ensure the drugs were not adulterated and were correctly dosed.

If illicit drugs become easier to produce for personal use this could benefit society by reducing the number of criminal actors in the supply chain; it would also mean that drugs would be safer for consumers reducing the risk of adulteration and drug-related deaths from overdose. Such a scenario could become a reality with advances in technology such as 3D printers (Schubert et al. 2014). Scientists have also found ways to synthesise opium from yeast (Galanie et al. 2015), which could 1 day replace the international trafficking chains that are common today. Local manufacturers would need to access other precursors, however, which could pose problems if they are tightly regulated. "Economics does not begin with the allocation of scarce resources, but rather with their localisation" (Callon 1990, p 152). If illicit drugs do become readily available at low costs, it may lead to higher levels of problematic drug use.

Conclusion

The purpose of this article as expressed in the title, is to examine the relationship between technology and organised crime within the smart city. The paper began by defining the smart city as a commercial construct that is presented by its advocates in positive terms. Yet, what is missing from this discussion is the fact that emergent technologies can enable and enhance criminal activity, creating vulnerabilities in the city that have not been recognised. Furthermore, as criminological research in this area is limited and preoccupied with governmentality and political rationalities, it has missed the voice of the true object of crime, the criminals themselves. The study aimed to remedy this absence, by examining the accounts of criminal actors operating in arguably one of the most significant security challenges to the smart city: the illicit drug trade. It questioned how buyers and sellers of illicit goods coordinate transactions within conditions of ubiquitous digital surveillance.

Having examined these accounts, the paper demonstrated how security problems have evolved with emergent technology rather than being made obsolete. Organised criminals are learning to subvert the smart cities surveillance systems and use these data sources for their own ends. Moreover, as technologies take a more central position in criminal actor networks, they too can become targeted by predators who wish to gain control of the networks they occupy. This process has reshaped the structure of the illicit drug trade, amplifying its associated harms in some cases and diminishing them in others. There exists a continuum between the analogue and the digital in which traditional forms of organised crime are enhanced by emergent technologies but also reconfigured through their application. Rather than replacing the physical territories of the terrestrial city, ICT extends them with the effect of re-orientating the geographical movements of human actors as they interact with and within them. In the UK, Media attention has recently focused on a spate of knife attacks that were carried out in London between rival gangs. It is said that these attacks took place after arguments broke out on social media (Telegraph 2018). ICT enables criminal actors to communicate in new ways which can compound disputes as rivals seek to gain dominance over both virtual and physical territories (as well as the technologies within them).

The internet has created a virtual space in which illicit goods can be bought and sold but this development is far from over. Virtual reality (VR) technologies further transform our relationship with time and space and are becoming more affordable. Questions remain as to how buyers and sellers of illicit goods will respond to and interact within these new virtual environments. It is possible that dedicated marketplaces will emerge in the virtual like those currently seen on the darknet. Alternatively, suppliers may seek out virtual environments where potential customers are likely to visit such as in virtual nightclubs. There are already cases of people consuming drugs in virtual reality (Techradar 2016) which may have serious consequences if they overdose in an isolated location. People may be connected in the virtual but absent in the real. Nonetheless, organised criminals who make use of these virtual environments will still have to use the cities' infrastructure and forge links with local actors, which is important to recognise.

The paper introduced the idea of illicit drug markets as sociotechnical systems, in that they are both socially and technically determined. A closer inspection is required then, of not only the effects of technology but also the institutional effects of policy and policing. Policy differentially affects forms of organised crime, as is evident in the more open nature of the anabolic steroid trade. By legalising or decriminalising certain substances, the arms race may begin to slow as criminal opportunities are removed. The government can regulate illicit drug markets before they spiral further out of control, especially as technologies such as 3D printers which can manufacture drugs and weapons become readily available. Ultimately, efforts to resolve these issues must span across both virtual and physical dimensions to be effective.

The paper contributes to the growing embryonic of research on digital disruptive technologies, which are present in the broader "STS turn in criminology". In doing so, it demonstrated how territorial space can no longer be conceptualised solely in terms of the physical built environment. Criminologists must consider the interdependencies between physical territory and digital ether to understand how it is that illicit markets now function. The conceptual toolkit of ANT is particularly useful in examining this relationship considering its stance on technological agency. Technology both shapes and is shaped by human action in ways that cannot always be predetermined. Simple technological fixes are not likely to resolve the vulnerabilities of the smart city considering this fact. Criminal entrepreneurs will continue to innovate in response to technological change. The paper strongly argues for greater use traditional ethnographic methodologies to bolster research in this field. Methodological innovations in online social research cannot replace conventional offline methods but can complement them. The paper is a step in this direction but has only touched upon the crest of these technological developments. It is hoped that such work will be taken up in the next wave of science, crime and technology studies (SCTS), as far more research in this field is required.

Authors' contributions

MB carried out the research and drafted the manuscript. The author has read and approved the final manuscript.

Competing interests

The author declares that there are no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 1 March 2018 Accepted: 30 May 2018
Published online: 29 October 2018

References

Aldridge J, Décary-Hétu D (2014) Not an 'Ebay for Drugs': the Cryptomarket 'Silk Road' as a paradigm shifting criminal innovation. Available at SSRN 2436643

Amoore L, Raley R (2017) Securing with algorithms: knowledge, decision, sovereignty. Secur Dialogue 48(1):3–10

Aspers P (2011) Markets. Polity

Barber B (1983) The logic and limits of trust. Rutgers University Press, New Brunswick

Barbuta A (2017) Big data and policing: an assessment of law enforcement requirements, expectations and priorities. https://rusi.org/sites/default/files/201709_rusi_big_data_and_policing_babuta_web.pdf

Beck U et al (1994) Reflexive modernization: politics, tradition and aesthetics in the modern social order. Stanford University Press, Stanford

Becker HS (1967) Whose side are we on? Soc Probl 14:239–247

Bennett D (2012) The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations. Inf Secur J 21(3):159–168

Bentham J (1798) Proposal for a new and less expensive mode of employing and reforming convicts. London

Berry C (Forthcoming) The life of the tag: An actor network theory ethnography of electronically monitored punishment. Bristol: Bristol University

Brey P (2017) Theorizing technology and its role in crime and law enforcement. In: The Routledge handbook of technology, crime and justice. Routledge, pp 43–60

Callon M (1986) Some elements of a sociology of translation: domestication of the scallops and the fishermen of St. Brieuc Bay. Power Action Belief 32:196–223

Callon M (1990) Techno-economic networks and irreversibility. Sociol Rev 38(S1):132–161

Callon M (2004) The role of hybrid communities and socio-technical arrangements in the participatory design. J Center Inf Stud 5(3):3–10

Cocchia A (2014) Smart and digital city: a systematic literature review. Springer, Smart city, pp 13–43

Dorn N (2003) Proteiform criminalities. In: Transnational organised crime: perspectives on global security. p 227

Dorn N et al (1998) Drugs importation and the bifurcation of risk. Br J Criminol 38(4):537–560

Edvinsson L (2006) Aspects on the city as a knowledge tool. J Knowl Manag 10(5):6–13

Edwards A (2016) Multi-centred governance and circuits of power in liberal modes of security. Global Crime, New York, pp 1–24

Edwards A (2017) Big data, predictive machines and security. Crime and Justice, The Routledge Handbook of Technology, p 451

Ekblom P (2017) Technology, opportunity, crime and crime prevention: current and evolutionary perspectives. In: Crime prevention in the 21st century. Berlin: Springer, pp 319–343

Foucault M (1977) Discipline and punish: the birth of the prison. Random House, New York

Foucault M (2009) Security, territory, population: lectures at the Collège de France 1977–1978. Macmillan, New York

Galanie S et al (2015) Complete biosynthesis of opioids in yeast. Science 349(6252):1095–1100

Goffman E (1956) The presentation of everyday life. University of Edinburgh, Edinburgh

Graham S (1998) The end of geography or the explosion of place? Conceptualizing space, place and information technology. Prog Hum Geogr 22(2):165–185

Greenfield A (2010) Everyware: The dawning age of ubiquitous computing. New Riders, New York

Gujjar N (2016) How to blur face in Adobe Photoshop easy and fast. https://i.ytimg.com/vi/u4XIrYPD6r8/maxresdefault.jpg

Haggerty KD, Ericson RV (2000) The surveillant assemblage. Br J Sociol 51(4):605–622

Hannah-Moffat K (2018) Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates. Theor Criminol. https://doi.org/10.1177/1362480618763582

Hilgartner S (1992) The social construction of risk objects: or, how to pry open networks of risk. Org Uncertain Risk 259:39–53

Hillebrand J et al (2010) Legal highs on the Internet. Subst Use Misuse 45(3):330–340

Independant (2015) Criminal gangs infiltrated postal delivery services to intercept drugs, say officials. https://www.independent.co.uk/news/uk/crime/criminal-gangs-infiltrated-postal-delivery-services-to-intercept-drugs-say-officials-10488954.html

Kitchin R (2014) The real-time city? Big data and smart urbanism. GeoJournal 79(1):1–14

Latour B (1994) On technical mediation. Common Knowl 3(2):29–64

Latour B (2005) Reassembling the social-an introduction to actor-network-theory. Oxford University Press, Oxford

Lawson C (2010) Technology and the extension of human capabilities. J Theor Soc Behav 40(2):207–223

Livesey G (2010) Assemblage. The deleuze dictionary, Columbia, pp 18–19

Lyng S (2016) Goffman, action, and risk society: aesthetic reflexivity in late modernity. UNLV Gaming Res Rev J 20(1):61

Lyon D (2014) Surveillance, snowden, and big data: capacities, consequences, critique. Big Data Soc 1(2):2053951714541861

May T, Hough M (2004) Drug markets and distribution systems. Addict Res Theor 12(6):549–563

McLuhan M, Fiore Q (1967) The medium is the message, vol 123. Times Book Review, New York, pp 126–128

McLuhan M, McLuhan E (1992) Laws of media: the new science. University of Toronto Press, Toronto

Nam T, Pardo TA, eds (2011) Conceptualizing smart city with dimensions of technology, people, and institutions. In: Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times. ACM

Pellegrino G (2011) The politics of proximity: mobility and immobility in practice. Ashgate Publishing Ltd, Farnham

Ritzer G (2015) Automating prosumption: the decline of the prosumer and the rise of the prosuming machines. J Consum Cult 15(3):407–424

Sacks H (1972) Notes on police assessment of moral character. Studies in social interaction, New York, pp 280–293

Salinas-Edwards M (2013) Men at work. Manchester University, Manchester

Sanders CB, Sheptycki J (2017) Policing, crime and 'big data'; towards a critique of the moral economy of stochastic governance. Crime Law Soc Change 68:1–15

Schubert C et al (2014) Innovations in 3D printing: a 3D overview from optics to organs. Br J Ophthalmol 98(2):159–161

Schuilenburg M (2015) The securitization of society: crime, risk, and social order. NYU Press, New York

Söderström O et al (2014) Smart cities as corporate storytelling. City 18(3):307–320

Techradar (2016) What it's like to take drugs in virtual reality. https://www.techradar.com/news/wearables/what-it-s-like-to-take-drugs-with-virtual-reality-1318460

Telegraph (2018) Cressida Dick: social media fuels murder and knife crime among children. https://www.telegraph.co.uk/news/2018/03/31/cressida-dick-social-media-fuels-murder-knife-crime-among-children/

Tong J (2016) Do you trust your car? http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8894338&fileOId=8894339

Von Lampe K (2015) Big business: scale of operation, organizational size, and the level of integration into the legal economy as key parameters for understanding the development of illegal enterprises. Trends Organized Crime 18(4):289–310

Von Lampe K, Johansen PO (2004) Organized crime and trust: on the conceptualization and empirical relevance of trust in the context of criminal networks. Global Crime 6(2):159–184

Wainwright T (2016) Narconomics: how to run a drug cartel; What big business taught the drug lords. Public Affairs, New York

Wang D (2017) Foucault and the smart city. Design J 20(sup1):S4378–S4386

Wax PM (2002) Just a click away: recreational drug web sites on the internet. Pediatrics 109(6):e96–e96

Woolgar S (2002) Virtual society?: technology, cyberbole, reality. Oxford University Press on Demand, Oxford

Young J (1986) The failure of criminology: the need for a radical realism. Confronting Crime. Sage, London, pp 9–30