The Potential for Serious Spaceships to Make a Serious Difference

Robert Fleet
Australian National University
robert.fleet@anu.edu.au

Terhi Nurmikko-Fuller
Australian National University
terhi.nurmikko-fuller@anu.edu.au

ABSTRACT

Identifying, investigating, and potentially disrupting organised criminal networks is difficult. Data gathered by law enforcement and regulatory authorities are often inconsistent, incomplete, and inaccurate. Computational criminology attempts to address these limitations by modelling the behaviour of virtual "humans" in virtual places. However, virtual humans are rule-based and can never fully replicate actual human behaviour. This study takes a new approach by utilising the benefits of the observable and controllable environment of virtual worlds but examining real people and real behaviour. To do this, it explores real people's behaviour in a virtual environment similar to the circumstances found in organised criminal networks. Massively Multiplayer Online (MMO) video games with player-driven markets present real humans with similar circumstances in controlled and observable virtual environments.

Market conditions within MMO games and illicit markets are both characterised by trust, reputation and, when all else fails, violence. Overall, MMO games are a novel data source to identify, investigate, and provide prevention strategies to the problem of organised criminal networks. Using social network analysis of real-world players from data broadcast by EVE Online (an MMO); spatial, temporal, and behavioural patterns of both offenders and victims are examined. The data broadcast from the game is consistent, complete, and accurate and provides a much larger sample size than obtainable in real-world environments.

The data set consists of a seven-year period containing approximately 7M-9M events. It captures the activities of 600,000 individuals and 2,500 groups. This paper proposes that video games can approximate the circumstances found in the real world and human agents can and do act in the most rational way to maximise success in those circumstances. Overall, MMO games offer a powerful social science data generator that offers insights into real-world social problems (such as organised criminal networks) that are typically difficult to examine.

CCS CONCEPTS

• **Networks → Online social networks**; • **Applied computing → Law**; **Sociology**;

KEYWORDS

Online Behaviour, Massively Multiplayer Online Games, Social Network Analysis, Surveillance, Victimisation, Computational Criminology

1 INTRODUCTION

Information about the actions of illicit market groups can be difficult to accurately observe and record [9, 10, 42, 45, 46]. Yet these activities are of interest to law enforcement agencies (who seek prohibition), regulatory agencies (who seek both tax revenue, and links between legitimate and illicit market activities) and criminal justice systems (who are required to make/enforce policy to deal with illicit markets) [3, 4, 20]. By necessity, illicit market groups are covert in their operations and resistant to infiltration [35]. Even when individuals and groups allow researchers to observe and record their actions and decisions, the data must be approached with some caution as to its accuracy and reliability [43].

The lack of accurate observation leaves a gap in the knowledge about the activities and social structures of covert illicit market groups. This paper argues that interested researchers must look for novel ways of improving the observation of individual and group behaviour in conditions that allow markets to form that are characterised by reputation, trust, and violence. In order to address this lack of "observability", this paper argues that novel data sources should be investigated. A novel extant data source that addresses the present limitations are player-driven markets found in Massively Multiplayer Online games (MMOs). These are virtual markets that can be observed that hold similarities to physical world illicit markets in that groups operate to control a market position and make profit while utilising violence as a tool to resolve disputes, protect market positions and enforce financial obligations.

More recent attempts to define organised crime beyond an ethnic commonality or a particular criminal activity have highlighted a common profit-motivated thread amongst what are identified as organised criminal groups. There has been some consensus that organised crime is often based on profit-motivated criminal enterprise [1, 39, 44]. The process of committing ongoing crime is itself identified as the inherent danger of criminal organisations and while loosely associated turf-focused groups do exist, there has been a distinct shift in group activities towards being involved in illicit markets [16, 18]. Therefore there is some ongoing interest amongst interested regulatory and criminal justice organisations

in monitoring and disrupting ongoing criminal enterprise. Especially in light of the suspected links of organised crime to terrorist activities through financial support [32, 34].

Critics argue that the analogy between legitimate and illicit enterprises can only be extended so far and that comparisons tend to overlook some key differences [16, 17, 35, 37, 38]. However there are still some significant characteristics that allow legitimate and illicit enterprises to be compared and contrasted [16, 17]. Each characteristic is centred on a key business need or decision that legitimate and illicit enterprises face in conducting business. The objective of each decision is similar for each enterprise group but the factors that weigh into the decision making process are specific to the enterprise's chosen market [40, 41]. The understanding that the process of organised crime is based on on-going yet fluid collaborative relationships between individuals and groups suggests that an appropriate approach to investigating organised criminal groups is to adopt a network model [17]. Further given the consensus that there is an aspect of criminal enterprise to the majority of the activities of criminal groups, an economic model is also applicable to any investigation [17]. The use of these two models will allow the paper to focus predominantly on self-organising networks of collaborating individuals whom are interested in operating and protecting a for-profit enterprise across the three distinct market types (legitimate, illicit, and virtual).

2 RELATED WORK

Virtual worlds can provide insight into physical world phenomena [5]. Previous research has established the benefits and usefulness of using Massively Multiplayer Online Role-Playing Games (MMORPGs) as a reliable and valid source to study physical world social phenomena, including criminal activities. Whilst epidemiology (the study and analysis of the distribution and determinants of conditions within a population) has been used as a basis for crime research, especially repeat victimisation and hotspot analysis [7], social network analysis has been applied to co-offending and repeat victimisation studies [10]. Economic theory has, in turn, been used to understand and reinforce rational choice and decision-making in property crimes [38].

2.1 Epidemiology

Epidemiologists have utilised MMORPG to study the outbreak of diseases. For example, in 2005 an unforeseen error in the computer code controlling the game world of a popular MMO, World of Warcraft, introduced an outbreak of a disease-like bug into the game [31]. The outbreak was the unintended consequence of a new type of computer-controlled behaviour escaping the strict confines of the area in which it was supposed to operate. The disease (known as a *debuff* in-game) was intended to be limited to a particular area (it was attached to a certain computer controlled enemy); within that area it would be annoying but not fatal to those infected (a moderate continuous drain on player health) and able to spread between other players in the same immediate area. By use of a certain action in the game (a teleport spell) the disease was ported to populous areas outside of the containment area. Due to the disease being intended to infect more powerful higher level players (more powerful translates to higher health numbers,

greater resistances to debuffs and higher health recovery rates) once released into the common areas, where players of all levels congregated, it proved to be fatal to players of lower levels. Also due to this contagious nature it spread rapidly in areas of high population concentrations. It took a number of concentrated efforts by the company that runs the game to eliminate this problem. This outbreak provided epidemiologists and social scientists a wealth of information on both disease behaviour and public behaviour in response to wide-scale infectious outbreaks [31]. They found that virtual disease displayed similar traits to physical world disease. This example illustrates the experimental value of virtual worlds.

2.2 Complex networks

Virtual worlds have been useful in studying the ways in which networks form between individuals and entities. Complex networks have been observed in a number of different scientific fields including computing, biology, economics and social networks [6]. In a cross-comparison between the different field type networks there have been a number of features that have been found to be similar between them. Similar features include average shortest-path length; high clustering coefficients and scale-free connectivity are almost universal in complex networks across the differing fields. The features have also been observed in social networks formed in virtual game worlds [21].

The difficulties of studying covert behaviour have been made easier with the use of virtual game worlds. Virtual game worlds have been used to study dark networks (clandestine networks of criminal individuals or entities that are used to channel information, funds and goods between each other). Due to their clandestine nature the networks that exist in the physical world are hard to locate and characterise in full. Law enforcement and intelligence agencies are interested in characterising these networks as a number of criminal and terrorist organisations rely on these dark networks for the gathering of funds and the distribution of information and material. Similar networks exist in virtual game worlds that seek to exploit the virtual game worlds for physical world profits [26].

Gold farming, power levelling, and account/equipment sales for real money are all activities that are prohibited in almost all virtual game worlds, as they have a detrimental effect on the economy and fairness of the game worlds that they exploit for profit [14]. As such, the people who engage in these activities form dark networks, which are similar to physical world dark networks. The motivation to form dark networks in order to conceal the activity from game administrators (and at the same time maximise effectiveness) mirror the same reasons dark networks form in the physical world [33]. The ability to identify and visualise the network topology of in-game dark networks allows for researchers to better characterise the hidden networks in the physical world which would otherwise be problematic.

The usefulness of using virtual worlds has also been demonstrated in studying dynamics of a network. Complex networks are not fixed, with relationships forming and breaking over time. The change in relationships between network entities changes the shape and flow of information and resources across the network [22]. These changes can be hard to capture in the physical world, especially for highly mobile social networks. The virtual world's ability

to record and playback activities allows for these hard-to-visualise changes to be tracked and observed. This ability also allows for the investigation of network attack tolerance and network adaption [2]. Attack tolerance and network adaption are related concepts about the changes networks undergo when network entities are deliberately removed. This has applications in the studies of drug trafficking organisations and other organised crime groups [46].

2.3 Economics

Another area where virtual game world have shown extensive promise is economics studies. Virtual economies have been observed to emulate physical world and theoretical economies accurately [11]. The economies observed in virtual game worlds are often player-driven, free market economies where players directly influence the supply and demand of goods within them. Due to the similarities between the game economies and physical world economies the rational decision making processes and economic strategies found in the game world are useful in characterising and predicting physical world economic behaviour [30].

Economics plays a significant part in the way players approach MMORPGs [47]. Game economies provide suitable ways of measuring player success and self-efficacy in the absence of more traditional physical world measures [27]. Surplus in-game currency is used to obtain goods that will visually display the player's status and power to other individuals. The need to acquire certain goods that indicate elite status or special powers over other players can be a driving factor in gaming addiction and other problematic game related behaviours [24].

Game economies are also linked to cybercrime activity with virtual game worlds. The ability to illegally convert or sell in-game currency for physical world currency has spawned a number of behaviours that while officially banned by the game developers still continues. Syndicates of individuals will play the game in a deliberate fashion to exploit the game design to extract the largest amount of in-game currency for the least effort in a timely fashion (gold farming) [28]. The in-game currency that is farmed is later sold outside of the game for physical world money. Other illegal player syndicates will exploit the game design to obtain rare or unique in-game items that can be later traded outside of the game (for example, via eBay) for physical world currency [23]. These real money trading activities provides motivation for criminal exploitation of the game and an alternative, though strictly illegal, pathway for legal players to exploit for their own in game benefit [29].

In summary, virtual worlds have provided researchers with a reliable and valid source. Virtual worlds have been utilised in a broad range of research areas including criminal activities. Virtual worlds display similar features to physical world activities, providing accurate representations of the physical world to allow players to make similar decisions in the game as they would in the physical world. The benefits of virtual worlds (especially MMORPG) include capturing a large data samples, in a timely fashion, and are even able to identify covert behaviour.

3 METHODOLOGY

Our analysis focuses on data collected from EVE Online, a MMORPG set in a persistent futuristic science fiction setting. The game is a

subscription-based service meaning that the players must pay a monthly fee to access the game [12]. The aim of the game is to accumulate in-game wealth and power. Player also gains reputation that extends from within the game to the physical world through meta-gaming channels. While the game itself has objectives for the player to accomplish there is little in the way of narrative engagement thus allowing players enough freedom to insert their own narrative and play objectives. In this case the most effective way of achieving high levels of wealth, power and reputation is to group up with other players [12, 13].

The computer system controlling EVE Online generates a report in real time every time a player-controlled ship is destroyed. The report (referred to as *killmails*) is sent to the victim and the aggressor who laid the final blow. Killmails can be thought of as being analogous to the homicide/crime reports gathered in the physical world by law enforcement agencies. The computer system controlling EVE online also broadcasts them to third parties with an API.

The broadcast data contain a range of information relating to the circumstances of the ship loss, including the involved parties, their group affiliations, time and location as well as financial losses. These reports form the basis for the analyses used in this research, as they contain information that is not always apparent from physical world homicide reports (for example, a definitive list of all parties involved in the event). This data can be analysed in ways similar to the ways information from the physical world can be. Furthermore, reports generated in close temporal and spatial proximity to each other might be considered part of a larger conflict event.

Killmails were gathered from a third party which records all killmails broadcast by the game via the API. It is proposed that the data set being used includes the activities of all players engaged in violence over a period of 7 years (2007-2014). The data set contains the records of approximately 500,000 individual players and encompasses approximately 9,800,000 individual events.

The data gathered was examined using Social Network Analysis (SNA). SNA allows the generation of descriptive statistics in regards to the size and characteristics of in-game co-operating groups, whilst at the same time allowing for the investigation of conflict between individuals and groups and provide descriptive statistics on the amount of victimisation and violence occurring. The temporal and spatial distributions of the events will be examined in future using a Geographic Information System (GIS).

The data subset used in the preliminary investigation outlined in this paper was drawn from the entire data set between the time stamps 2007/12/05T23:26:00 and 2007/12/06T09:01:00 and contains 920 nodes and 3457 edges. The network graphs and visualisations (Figures 1 – 4) were produced in Gephi (0.9.2).

4 EVE ONLINE

EVE is notable for a number of features that differentiate it from other games in the genre [25]. These features make it more suitable for research than some other games within the genre. These features more accurately mirror the physical world in the degrees of freedom given to the player to act as they might in the physical world. Firstly, all of the players are hosted on a single server cluster meaning that any player accessing the game occupies the same

virtual space as every other player. As this is feature is computationally difficult to achieve for very large numbers of players many other games split the players up into separate yet identical virtual worlds hosted on separate servers [12]. EVE Online has approximately 350,000 subscribers with an average concurrent user figure of approximately 21,000 players. The record for peak concurrent users is 65,303 players online at one time [12].

Secondly, the game employs a laisse-faire free market economy that is solely driven by the players. This means that the in game economy is reliant on player intervention and actions to operate. Players must obtain raw materials, manufacture goods and sell these goods on the open market to make money [13]. This means that the players must be engaged with the virtual world to progress in the game, as the one of the purposes of the game is to accumulate wealth in order to more effectively accumulate wealth. In the absence of a formal score keeping mechanism, wealth is a useful measure of overall power in the game [25].

Finally of note is the way in which the game deals with player development. Within EVE players have the capacity to train any skill that they feel best suits the requirements of the way they approach playing the game. The learning of skills provides a number of benefits to the player by being able to utilise more advanced ships, modules and weapons as well as making the use of these items and other facilities more effective [25]. EVE uses a time-based model of skill development rather than skill acquisition being based on repeated in-game actions as in many other games. Skills are learnt over time on a passive basis as players receive a set number of skill points per hour in real time. Skills continue to develop in real time even if the player is not actively playing the game. Simple skills may take minutes to learn while skills that are more complex can take months to learn [13]. To illustrate, in order to fly one of the most powerful military vessels in the game it requires knowledge of over 20 different skills and a total training time of 194d 6h 24m 16s. This is the minimum amount of time required to simply pilot the vessel, as further skills would be required to most effectively use the ship in battle [13].

4.1 Environmental Characteristics

The EVE environment is composed of a contiguous interconnected network of systems that are grouped into loose constellations [12]. Systems can be thought of as being analogous to street corners, city blocks or census mesh blocks and therefore form one of the basic geographic units of analysis in the research. Constellations can be thought to be analogous to neighbourhoods, jurisdictions or other geographic divisions within urban areas and therefore form another basic geographic unit of analysis in the research. A constellation is a close grouping of systems that contain more links to one another than to other systems. Constellations are typically separated from each other by a small number of systems that serve as bridges between the adjacent constellations. These bridging systems provide natural bottlenecks and barriers to travel, as the space between systems and constellations is impassable [13].

Systems and constellations form the main activity sites for players to access resources and to interact with other players. The systems provide valuable resources to players similar to locations for the provision of illicit services and goods in the physical world.

Players need to act collectively in self-organising groups to effectively claim and defend areas from other groups [13]. Systems that can be claimed by player-controlled groups are the likely sites of conflict between competing player-controlled groups. Player groups identify with the occupied space as their home areas and will invest time and effort improving and solidifying their territories. All these are activities that can be observed in the physical world [25].

The virtual game space is divided into two distinct areas; Computer Controlled Space and Player Controlled Space. Computer controlled space because of its rigidly controlled nature, high traffic volumes and central location can be thought of as being analogous to the CBD of a large city [12]. Within computer-controlled space, formal behavioural control of violent activity is provided by a computer generated police response in the form of an in-game police force (CONCORD) [25]. CONCORD will respond to inter-player violence within computer controlled spaced based on a rating given to each system. As the systems in computer-controlled space get farther away from the central systems the rating given to each system decreases from 1.0 to 0.1. CONCORD response times become increasingly longer as the rating falls [13]. This reflects a measure of policing effectiveness in the physical world with inner suburbs being better patrolled and more likely to draw a timely response while outer suburbs and rural locations are less likely to have immediate responses.

Player controlled space consists of the systems and constellations surrounding computer controlled space. These systems can be thought of as being analogous to drug street corners, territories and organised criminal groups set spaces. The systems in this space are not controlled by the computer and are therefore free to be claimed and defended by player formed groups [12]. Player groups can further improve controlled systems to make them more profitable to occupy which means that there is also an incentive to continue to hold and defend these systems [13].

It takes time to travel within and between systems; while travelling the player is also exposed to risks from other players and computer controlled enemies [13]. This introduces a type of friction similar in the physical world to the distances willing to be travelled by players. Meaning that players are more likely to travel shorter distances than longer distances due to the time and effort it takes to travel longer distances as well as the increased risk. Without this friction, a player could quickly and with little effort jump across the long distances between the systems that would not be possible in the physical world.

4.2 Individual Player Characteristics

Individual players are one of the primary units of analysis in this research. In the game world player characteristics are derived from the skills those players choose to train. As noted before skills take physical world time to develop; with higher level and advanced skills taking much longer to train than lower level basic skills. Skills and skill training can therefore be thought of as representing experiential knowledge in the physical world [25]. In the physical world individuals receive training and gain experience in their chosen activities that make them more effective at doing that activity in the future. In the game the skill system achieves the same effect.

The player's combined skill set reflects the type of game play style that the player chooses. Aggressive players will train skills that will aid in combat whereas acquisitive players will train skills that aid in manufacture and sales. Skills also determine the types of space vessels that a player is able to operate and the equipment that can be fitted to the vessel. Higher skill levels allow for better vessels to be used, better equipment to be fitted and more effective operations of both [25].

Vessels form the primary tool for interfacing between the game world and other players in the game. Vessels are the player's physical presence in the game that when combined with a skill set represent the player's capacity to effectively perform an activity in the game [12]. This is similar to the physical world where experiential knowledge and physical ability add together to make performing activities more effective.

For other players the vessel that is being flown by an individual represents that individual's strength and level of threat posed by that player. The vessel also represents the potential reward that might come from victimising the player [13]. This parallels the types of information used by offenders in the physical world to make assessments of the risks and rewards associated with offending.

Players also have security ratings that reflect their activities in the game. Negative ratings indicate aggressive and violent acts while positive ratings indicate friendly acts towards computer-controlled players and groups [12]. This is another source of information that players can use to assess the threat posed by other players in the game. Strong negative ratings indicate that a player may have participated in violence before and is therefore more adept at using violence [13]. Security ratings are similar to physical world criminal records held by law enforcement agencies.

4.3 Player Group Characteristics

Players are able to organise themselves into groups known as corporations (sub-groups). Each corporation has a unique name and identifier in game. Corporations have a hierarchy of membership roles that can be assigned to individual players or groups of players. Corporations have the capacity to pool resources and funds in common locations for all members to access [12]. Players will group together to more effectively achieve in-game activities (Maniac, 2004). These types of characteristics are commonly found in similar types of groups in the physical world. However given the virtual world's lack of legal recourse to resolve disputes between corporations often corporations will be involved in violence as a means of dispute resolution. This makes corporations more like physical world criminal organisations.

Corporations by themselves are unable to claim territory in player-controlled space. Corporations must team-up with other corporations to form alliances (groups). Alliances are able to claim sovereignty over systems in player-controlled space [12]. Claiming sovereignty means that claimed system belongs to the alliance and allows the owner to exploit the resources present. The alliance may also invest in the system to improve the resources present [13]. Claimed systems must be defended, as they are open to attack by other groups who wish to claim sovereignty [25]. This is parallel to the physical world where smaller groups of offenders group
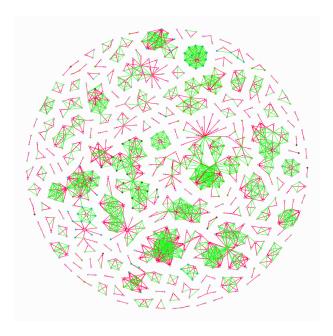

Figure 1: Complete Network Diagram for EVE Online 2007/12/05T23:26-2007/12/06T09:01 (Fruchterman Reingold)

together to form coalitions to more effectively occupy and defend valuable territory and resources from outside interference.

5 ANALYSIS

The initial exploratory analysis of the data set focuses on producing network descriptive statistics and visualisation for the observation of patterns. Figure 1, complete network, displays the social network graph for all nodes within the sample data set. In this instance, the nodes are coloured by the top 7 player groups (alliance) by node count. Edges are displayed in green for co-offending (non-directed edges) and red for victimisation (directed edges) with arrows indicating the relationship from offender to victim. Figure 2, large connected component, shows the largest connected component from within the the network graph shown in Figure 1. The connected component shows the structure, relationships and violent victimisations of a group with the in game Alliance name of "Triumvirate". The nodes which are associated with the group are shown in green.

Simple metrics such as degree distribution (a measure of the distribution of edges per node) demonstrate the overall shape and nature of the network. Figure 3, co-offending, shows that the distribution of co-offending links in the network graph. It can be seen that while there is variability in the distribution of these links it does conform to a scale-free distribution that we would expect to see in a non-random collaboration network [8]. There are a number of things that can be inferred from this distribution. There is a large number of unconnected nodes which indicates that the majority of offending that takes place is simple one-on-one opportunistic assaults rather than coordinated attacks. While much lower in number multiple offender attacks with less than 15 co-offenders still make up the remaining majority of attacks. This may demonstrate
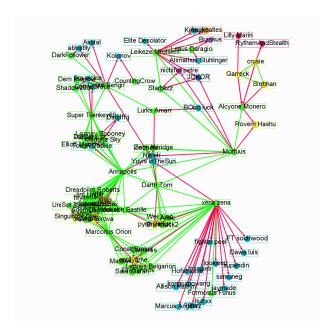
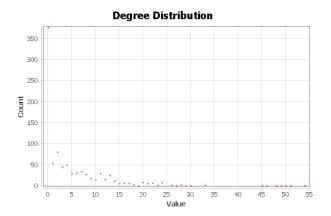**Figure 2: Large Connected Component - Triumvirate (in green)**

Figure 3: Co-offending Degree Distribution - all nodes

a level of organisation to the offending but further analysis is likely to uncover that these groups are ad-hoc in nature and only come together to achieve a specific goal or take advantage of a transient opportunity before disbanding. It is also observed that there are a small number of highly connected nodes. These nodes act to connect groups across space and time. These nodes are referred to as Brokers and are of significant interest to law enforcement and regulatory agencies due to their position in criminal networks. Removal of individuals in brokerage positions is likely to cause widespread disruption to the network [36].

Figure 4, Victimisation, also shows a scale-free distribution. In this case the distribution is closer to a power law distribution. This is close to the ideal distribution that would be observed in the physical
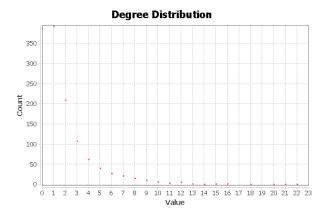

Figure 4: Victimisation Degree Distribution - all nodes

world for vistimisation rates. There are a large number of individuals who are victimised once and not again while there is only a small number of individuals who experience multi-victimisation [19]. Further observations can be made about the network structure if a single large connected component is isolated from the larger network graph. Figure 2 provides a number of examples in regards to how social network graphs can be used to uncover important information about the activities of a group over time and space. Within the graph an individual (label: Xena Zena) has a high number of out-degree edges. It is likely that this individual is taking advantage of a criminal opportunity where there are a number of vulnerable targets and a lack of disincentives to commit the violence. While this highly violent behaviour would likely cause this individual to be brought to the notice of law enforcement quickly it can be observed that this individual is not highly connected to the core group. The arrest of this individual while important will have little affect on disrupting the overall network. It can also be observed that the highly violent individual is not heavily involved in the conflict that can be observed between the main group (green nodes) and the rival group (yellow nodes).

As mentioned previously it can be observed that there are a small number of highly connected individuals that serve as brokers between clusters of the main group. It can be observed that the individual (label: Annapolis) is connected to the main group and as well as being placed between three larger sub-groupings as well as other brokers. Further investigation shows that this particular individual connects the main group and sub-groups across multiple locations and times. The removal of this individual from the network would cause significant disruption to the main group's activity and would therefore be of most interest to law enforcement and regulatory agencies. In contrast to the highly violent individual the broker does not participate in many violent encounters so may not be readily identifiable depending on how the violent incidents are investigated and/or observed by law enforcement. Further there is no direct link between this individual and the highly violent individual meaning that while the highly visible and dangerous individual will likely come to the attention of law enforcement they are unlikely to be able to expose the key brokering individual.

The final feature of note is revenge. Towards the top right of the graph a pair of green nodes (label: Mortuus and Alcyone Monero) have attacked a rival yellow node (label: Rovern Hashu). Subsequently, one of the green nodes (label: Alcyone Monero) is attacked by three rival yellow nodes (label: Siobhan, Garreck, cruise). This demonstrates that there is a current conflict occurring between these two groups. Further investigation in the future would be needed to uncover the dynamics and scale of this conflict which is not contained within the current sample. It is also noticeable that the person victimised does not retaliate directly but is avenged by other members of the group. Additionally, the victim of the revenge is isolated from the group and therefore more vulnerable. While proximity to the original event is likely to play a part in why the revenge act was targeted at the player it also highlights the vulnerability of members of the group who are not tightly bound to the core active members of the group. This is similar to the physical world where the rivalry and retaliatory violence is more likely to be waged between rank-and-file members than higher ranking members of a group [15].

6 CONCLUSIONS

Existing research has proved the applicability and suitability of data collected from virtual worlds to shed light on research questions and to provide insights into physical world phenomena in the context of epidemiology, complex networks, and economics. In this paper we have argued that data collected from virtual environments, specifically MMORPGs such as EVE Online and World of Warcraft, can be effectively used to model and thus increase our understanding of criminal behaviour and dark networks.

Our case study example, which applied SNA techniques to a sample data set capturing almost 400 individual events engaged in by some 920 individuals over an nine and a half hour period illustrate that the patterns which are emerging tend to match those patterns that can be observed in general crime statistics and from within the descriptive literature surrounding crime science and computational criminology.

Thus, virtual environments can be seen to have a proven legitimacy as an information source regarding human behaviour, and ought to play an increasingly significant role in future research and modelling endeavours, providing rich and diverse data to researchers across several disciplinary boundaries.

7 ACKNOWLEDGEMENTS

REFERENCES

[1] Sabrina Adamoli, Andrea Di Nicola, Ernesto U Savona, and Paola Zoffi. 1998. *Organised crime around the world.* Heuni Helsinki.
[2] Reka Albert, Hawoong Jeong, and Albert-Laszlo Barabasi. 2000. Error and attack tolerance of complex networks. *Nature* 406, 6794 (2000), 378–382. http://dx.doi.org/10.1038/35019019
[3] Peter Andreas. 2004. Illicit international political economy: the clandestine side of globalization. *Review of International Political Economy* 11, 3 (2004), 641–652.
[4] Pino Arlacchi. 1998. Some observations on illegal markets. *The new European criminology: Crime and social order in Europe* (1998), 203–215.
[5] William Sims Bainbridge. 2007. The scientific research potential of virtual worlds. *science* 317, 5837 (2007), 472–476.

[6] Stephen P. Borgatti, Ajay Mehra, Daniel J. Brass, and Giuseppe Labianca. 2009. Network Analysis in the Social Sciences. *Science* 323, 5916 (2009), 892–895. https://doi.org/10.1126/science.1165821
[7] Paul J Brantingham and Patricia L Brantingham. 1993. Environment, routine and situation: Toward a pattern theory of crime. *Advances in criminological theory* 5 (1993), 259–294.
[8] DA Bright, C Greenhill, and N Levenkova. 2010. Attack of the nodes: Scale-free criminal networks and vulnerability to targeted law enforcement interventions. In *2nd Illicit Networks Workshop, Wollongong, Australia.*
[9] David A Bright and Jordan J Delaney. 2013. Evolution of a drug trafficking network: Mapping changes in network structure and function across time. *Global Crime* 14, 2-3 (2013), 238–260.
[10] David A Bright, Caitlin E Hughes, and Jenny Chalmers. 2012. Illuminating dark networks: a social network analysis of an Australian drug trafficking syndicate. *Crime, Law and Social Change* 57, 2 (2012), 151–176.
[11] Edward Castronova, Dmitri Williams, Cuihua Shen, Rabindra Ratan, Li Xiong, Yun Huang, and Brian Keegan. 2009. As real as real? Macroeconomic behavior in a large-scale virtual world. *New Media & Society* 11, 5 (2009), 685–707.
[12] CCP. 2019. EVE Online. (2019). https://www.eveonline.com/
[13] CCP. 2019. EVElopedia. (2019). https://www.evelopedia.org/Main_Page
[14] Kim-Kwang Raymond Choo and Russell G Smith. 2008. Criminal exploitation of online systems by organised crime groups. *Asian journal of criminology* 3, 1 (2008), 37–59.
[15] Scott H Decker. 1996. Collective and normative features of gang violence. *Justice Quarterly* 13, 2 (1996), 243–264.
[16] Frederick Desroches. 2007. Research on upper level drug trafficking: a review. *Journal of Drug Issues* 37, 4 (2007), 827–844.
[17] Frederick John Desroches. 2005. *The crime that pays: Drug trafficking and organized crime in Canada.* Canadian Scholars' Press.
[18] Adam Edwards and Pete Gill. 2002. Crime as enterprise?–The case of"transnational organised crime". *Crime, Law and Social Change* 37, 3 (2002), 203–223.
[19] Graham Farrell. 1992. Multiple victimisation: its extent and significance. *International Review of Victimology* 2, 2 (1992), 85–102.
[20] H Richard Friman and Peter Andreas. 1999. *The illicit global economy and state power.* Rowman & Littlefield.
[21] Andrzej Grabowski and Natalia Kruszewska. 2007. Experimental study of the structure of a social network and human dynamics in a virtual society. *International Journal of Modern Physics C* 18, 10 (2007), 1527–1535.
[22] A Grabowski, N Kruszewska, and RA Kosiński. 2008. Dynamic phenomena and human activity in an artificial society. *Physical Review E* 78, 6 (2008), 066110.
[23] Yue Guo and Stuart Barnes. 2007. Why people buy virtual items in virtual worlds with real money. *ACM SIGMIS Database* 38, 4 (2007), 69–76.
[24] Maria D Haagsma, Marcel E Pieterse, Oscar Peters, and Daniel J King. 2013. How Gaming May Become a Problem: A Qualitative Analysis of the Role of Gaming Related Experiences and Cognitions in the Development of Problematic Game Behavior. *International Journal of Mental Health and Addiction* (2013), 1–12.
[25] hideodate. 2019. EVE University. (2019). https://www.eveuniversity.org/
[26] Brian Keegan, Muhammad Aurangzeb Ahmed, Dmitri Williams, Jaideep Srivastava, and Noshir Contractor. 2010. Dark gold: Statistical properties of clandestine networks in massively multiplayer online games. In *Social Computing (SocialCom), 2010 IEEE Second International Conference on.* IEEE, 201–208.
[27] Julia Kneer, Sabine Glock, Sara Beskes, and Gary Bente. 2012. Are digital games perceived as fun or danger? Supporting and suppressing different game-related concepts. *Cyberpsychology, Behavior, and Social Networking* 15, 11 (2012), 604–609.
[28] Yungchang Ku, Ying-Chieh Chen, Kuo-Ching Wu, and Chaochang Chiu. 2007. *An empirical analysis of online gaming crime characteristics from 2002 to 2004.* Springer, 34–45.
[29] Vili Lehdonvirta. 2005. Real-money trade of virtual assets: ten different user perceptions. *Proceedings of Digital Arts and Culture (DAC 2005), IT University of Copenhagen, Denmark* (2005), 52–58.
[30] Vili Lehdonvirta. 2009. Virtual item sales as a revenue model: identifying attributes that drive purchase decisions. *Electronic Commerce Research* 9, 1-2 (2009), 97–113.
[31] Eric T Lofgren and Nina H Fefferman. 2007. The untapped potential of virtual game worlds to shed light on real world epidemics. *The Lancet infectious diseases* 7, 9 (2007), 625–629.
[32] Tamara Makarenko. 2004. The crime-terror continuum: tracing the interplay between transnational organised crime and terrorism. *Global crime* 6, 1 (2004), 129–145.
[33] A. Malm and G. Bichler. 2011. Networks of Collaborating Criminals: Assessing the Structural Vulnerability of Drug Markets. *Journal of Research in Crime and Delinquency* 48, 2 (2011), 271–297. https://doi.org/Doi10.1177/0022427810391535
[34] Donato Masciandaro. 2017. *Global financial crime: terrorism, money laundering and offshore centres.* Taylor & Francis.
[35] Carlo Morselli, Cynthia Giguère, and Katia Petit. 2007. The efficiency/security trade-off in criminal networks. *Social Networks* 29, 1 (2007), 143–153.

[36] C. Morselli and J. Roy. 2008. Brokerage qualifications in ringing operations. *Criminology* 46, 1 (2008), 71–98. <GotoISI>://000254485300003

[37] Howard Rachlin. 2004. The behavioral economics of violence. *Annals of the New York Academy of Sciences* 1036, 1 (2004), 325–335.

[38] Peter Reuter. 1983. *Disorganized crime: The economics of the visible hand.* MIT press Cambridge, MA.

[39] Mark Shaw. 2014. Typologies of Transnational Organized Crime Groups. *Centre for International Crime Prevention, UNODC, accessed February* 12 (2014).

[40] Herbert A Simon. 1979. Rational decision making in business organizations. *The American economic review* 69, 4 (1979), 493–513.

[41] Herbert A Simon. 1982. Models of bounded rationality: Behavioral economics and business organizations. *Jg., Cambridge (MA)* (1982).

[42] Malcolm K Sparrow. 1991. The application of network analysis to criminal intelligence: An assessment of the prospects. *Social networks* 13, 3 (1991), 251–274.

[43] Petrus C Van Duyne and Maarten Van Dijck. 2007. *Assessing organised crime: the sad state of an impossible art.* Springer, 101–124.

[44] Alan Wright. 2013. *Organised crime.* Routledge.

[45] Jennifer Xu and Hsinchun Chen. 2005. Criminal network analysis and visualization. *Commun. ACM* 48, 6 (2005), 100–107.

[46] Jennifer Xu and Hsinchun Chen. 2008. The topology of dark networks. *Commun. ACM* 51, 10 (2008), 58–65. https://doi.org/10.1145/1400181.1400198

[47] Nick Yee. 2006. Motivations for play in online games. *CyberPsychology & Behavior* 9, 6 (2006), 772–775.