Sic Transit Gloria Mundi Virtuali? Promise and Peril in the Computational Social Science of Clandestine Organizing

Brian Keegan
School of Communication
Northwestern University
Evanston, IL 60201 USA
bkeegan@northwestern.edu

Muhammad Aurangzeb Ahmed
Dept. of Computer Science and Engineering
University of Minnesota
Minneapolis, MN 55455 USA
mahmad@cs.umn.edu

Dmitri Williams
Annenberg School of Communication
University of Southern California
Los Angeles, CA 90089
dmitri.williams@usc.edu

Jaideep Srivastava
Dept. of Computer Science & Eng.
University of Minnesota
Minneapolis, MN 55455 USA
srivasta@cs.umn.edu

Noshir Contractor
School of Communication
Northwestern University
Evanston, IL 60201 USA
nosh@northwestern.edu

ABSTRACT
Massively multiplayer online games (MMOGs) maintain archival databases of all player actions and attributes including activity by accounts engaged in illicit behavior. If individuals in online worlds operate under similar social and psychological motivations and constraints as the offline world, online behavioral data could inform theories about offline behavior. We examine high risk trading relationships in a MMOG to illuminate the structures online clandestine organizations employ to balance security with efficiency and compare this to an offline drug trafficking network. This data offers the possibility of performing social research on a scale that would be unethical or impracticable to do in the offline world. However, analyzing and generalizing from clandestine behavior in online settings raises complex epistemological and methodological questions about the validity of such mappings and what methods and metrics are appropriate in these contexts. We conclude by discussing how computational social science can be applied to online and offline criminological concerns and highlight the "dual use" implications of these technologies.

Categories and Subject Descriptors
K.4.1 [**Computers and Society**]: Public policy issues – *abuse and crime involving computers, ethics, privacy, regulation, use/abuse of power*

General Terms
Management, Security, Human Factors, Legal Aspects.

Keywords
Gold farming, clandestine organization, social network analysis, massively multiplayer online game, drug trafficking, risk

1. INTRODUCTION
At papal coronations between 1352 and 1963 the master of ceremonies would ignite a bundle of flax and proclaim the Latin phrase "sic transit gloria mundi" or "thus passes the glory of the world." The significance of this part of the ceremony was to remind both the leader and the audience of the impermanence of life and its earthly distinctions.

In this paper, we argue that despite the exciting implications of virtual worlds, research in social computing and web science should also take a critical eye towards the ways in which popular socio-technical systems like massively multiplayer online games (MMOGs) are still embedded in latent biological, social, psychological, and cultural forces. Like the papal ceremony's existential reminder, scholars should also be reminded that socio-technical systems do not emancipate us from these constraints. However, one should not heed this "passing of the glory of virtual worlds" solely as the cry of pessimists, but also as an opportunity to illuminate the structures and dynamics of social ills that had hitherto been intractable or impossible to rigorously analyze. These opportunities for analysis, in turn, raise complex ethical questions which merit serious consideration.

Many popular accounts of MMOGs paint these virtual worlds as idyllic realms that will "change the way people work and businesses compete" [1], a prototype of the future of Western culture [2], and the precursor to an exodus to a new social, political, and economic order [3]. The "golden age" of MMOGs which exculpated virtual worlds from the sins of the real world by virtue of their novelty and autonomy has long since passed if it ever existed at all. Virtual worlds are becoming centers of significant social, economic, and political activity which only further embeds them in offline cultural mores and social structures [4].

Trafficking virtual items for "real", offline currency offers just one example of how virtual worlds, rather than being wholly apart from, unencumbered by, or capable of addressing the shortcomings of offline concerns, are highly permeable to illicit behavior. In light of the permeability of the digital barrier to offline social and economic pressures, it is unclear whether distinctions between the "offline" and "online" are warranted in the first place [5]. The need to regulate this behavior in turn raises complex questions about how administrators should best monitor illicit behavior, what rights individuals have within these worlds, and who gets to adjudicate these claims. In light of the increasing role that social, mobile, and other mediated communication and information technologies play in our ostensibly "offline" lives, these contemporary questions echo concerns of communities and polities from time immemorial.

On the other hand, the superabundance of digital trace behavioral data and the potential similarity of online behaviors to offline analogues might provide new insights into general social and organizational processes. This blurring of the distinctions between the online and offline offers profound opportunities to analyze, model, and understand complex social, cultural, economic, and political processes which occur in both. The richness of online data may provide a lab bench on which to observe social dynamics and test theories which had been hitherto impracticable or impossible to study before and may even generalize to offline behavior. But these systems must be designed to comply with the regulations of offline jurisdictions and precedents. In addition, the mediated nature of these interactions implies that administrators can increasingly detect, monitor, and eliminate disobedience, dissent, and deviance with immaculate data. The increasingly mediated nature of "offline" life as well as the possibility of mapping from "online" to "offline" contexts suggests that what individuals, organizations, and governments are capable of doing with these data raises complex issues with which the emerging fields of social computing, computational social science, and web science will need to grapple.

To ground our argument that illicit behavior in online worlds exhibits structural patterns observed in the offline world, we use digital trace data about trade between players in the MMOG *EverQuest II* to understand the organizational structure of one particular kind of virtual item trafficking known as "gold farming". We characterize the structural patterns of four types of trade patterns in an online game and we use statistical network analysis methods called p*/exponential random graph models (p*/ERGMs) to compare the structures of these online networks to the structures observed in an offline drug trafficking network. Despite the fact that this data includes users engaged in gold farming and the undetected affiliates who support them, it also includes a number of typical players. We outline the barriers to mapping online game behavior to offline criminal behavior and discuss the implications of congruence in spite of them. We conclude by reviewing the tensions between the assumptions inherent to our network analysis methods, their implications for validity, and prevailing ethical and legal norms about how authorities should operate to identify and remove deviant agents.

2. BACKGROUND

2.1 Gold Farming in MMOGs

Massively-multiplayer online games like *World of Warcraft*, *EverQuest II*, and *EVE Online* are role playing games in which thousands of players interact in persistent virtual environments. Users play the game alone or in groups with other players to accumulate experience as well as virtual items and wealth that allow them to improve their power and confront more challenging opponents. Although the digital nature of these virtual goods and in-game currencies means they could be created in any quantity, the demands of effective game design as well as economic logic requires these items to scarce in order to be valuable. Players invest substantial amounts of time and effort to procure these virtual currencies and items. As a result, in-game economies not only exhibit macro-economic characteristics similar to those observed in offline "real" economies [6], they also possess illicit markets for acquiring goods and skills [7].

"Gold farming" and "real money trading" refer to practices that involve exchanging in-game virtual items for offline currency via transactions outside of the game architecture. The name stems for a variety of repetitive routines ("farming") which are employed to accumulate virtual wealth ("gold") which is sold to other players who lack the time or desire to accumulate their own capital. Gold buyers use this virtual currency to purchase more powerful game items, accelerating them through tedious stages of the game or by-passing the onerous steps needed to acquire these items. The third-party firms which provide these services employ tens of thousands of low-skilled workers in China and Vietnam to play these games so to harvest digital resources for resale to predominately wealthy Western players [8].

Gold farming is constructed by the player community and game designers as an illicit activity for a variety of reasons. Farmers upset the equilibrium of the in-game economy by inflating prices for goods and services for the majority of players who earn their own currency. Gold farmers' repetitive activities often lead them to monopolize control over productive regions in the game thereby excluding other players who need to play through them. The ability to buy one's way into the upper echelons of the game likewise seriously undermines the meritocratic "magic circle" of the game [9].

The major reason game administrators crack down on gold farming is because condoning the practice raises complicated legal questions about virtual items being property. Users of these games agree to End-User License Agreements (EULAs) which are unanimous across games in asserting that currency, items, and services within the game remain the property of the game developer [4]. If this were not the case, game developers would need to negotiate complex legal questions over whether the accumulation of in-game property are subject to income or capital gains taxes; the loss of a valuable item to an in-game rogue is a criminal offense akin to robbery; or users are subject to labor regulations for shift lengths or occupational safety [10]. These questions are not trivial for the gold farming industry which is estimated to employ over 100,000 workers and generates revenues in excess of $3 billion annually [8]. Rapid changes and intense competition within the market, the need to evade both game administrators online and law enforcement offline, popular perceptions of gold farming as a frivolous novelty, significant language and cultural barriers, and geographic distance have largely insulated gold farming from systematic participant observation [11].

2.2 Clandestine Network Analysis

Gold farming operations within MMOGs operate under many of the same constraints as offline clandestine and criminal organizations. Gold farmers must balance efficiency with security and operational flexibility with resilience against attack [12, 13]. Despite popular portrayals of clandestine networks as hierarchical and centrally-organized operations, the aforementioned constraints require participants to assume network organizational forms. Networks are better suited to clandestine organizations' demands for flexible teams [14], division of labor, and mediation of functional relationships (like communication and resource exchange) through latent trust ties [15, 16].

Analyzing clandestine networks is complicated by the necessarily difficult task of collecting data about their relationships and attributes. This paucity of data is a function of first, the difficulty of collecting the data; second, the unwillingness of other actors to share this data; and third, problems of collecting the appropriate type of data [17]. By definition, clandestine networks seek to avoid detection by recruiting members with demonstrated trustworthiness and willingness to keep secrets as well as structuring themselves to operate autonomously and without centralized oversight [18, 19]. To the extent that law enforcement, intelligence, or national security agencies are able to collect data about members' communication, exchange, and affiliations to build out networks of their interactions, these institutions do not make this data publicly available because of the obvious risks that criminal elements will adapt their behavior in response to the findings of this surveillance [20].

Even if data on clandestine networks were collected and made available for analysis, these data are of dubious validity owing to issues of actor and relational boundary specification as well as temporal censoring and lack of individual attribute data.

- The boundaries of membership in a clandestine organization are very fuzzy and the relationships and behavior of legitimate actors such as defense attorneys, accountants, and family members can make them operationally important. Removing these peripheral actors from the analysis or failing to monitor their relationships undermines the reliability and validity of subsequent analyses about how these organizations operate and are structured.
- Clandestine organizations rely on a variety of relationships such as trust, family ties, and previous affiliations as well as more functional relationships such as communication and resource exchange. Analyses which fail to account for these multi-dimensional relationships are likewise prone to being biased in any conclusions about the importance of particular individuals or structures of groups [16].
- Data collection on clandestine organizations presumes that no interactions of value occur before or after surveillance begins. Ceasing data collection too early or beginning it too late may obscure by prior and subsequent interactions and affiliations and thus omit crucial trusted members or processes governing how the network evolved [21, 22].
- The network is not only structured by endogenous tendencies to assume particular structural configurations, but also by exogenous factors such as actors' intrinsic abilities, motivations, and preferences [23]. Data on clandestine networks which fails to capture actors' genders, age, backgrounds, or psychological states may improperly ascribe particular network features to structural position alone rather than analyzing how actors' attributes influence network structure [24]. Analyses need to consider the recursive processes by which clandestine actors structure and are structured by their networks.

Because gold farming practices are mediated through information infrastructures logging every user's activity, these digital trace data logs can potentially provide an immaculate record of all activity within the game, including acts like gold farming transactions. The glut of data allows researchers to ask questions which would have been impracticable or impossible to answer using traditional data collection techniques but it also requires melding theories and methods from information and computer science, statistics, and the social sciences [25]. Our prior research has employed machine learning approaches to develop models for the automatic detection of gold farmers based on activity patterns [26] and using frequent pattern mining techniques on latent trust relationships to detect unidentified gold farmers [27].

Assuming that members of these clandestine organizations operate with similar motivations and under similar constraints as offline clandestine organizations, these findings can potentially be mapped from an online setting to inform theories and findings about offline behavior [28]. Drug trafficking operations, in particular, provide a model form of offline clandestine organization against which we can compare clandestine networks. Both classes of organizations have similar entrepreneurial and profit-motivated business models to engage in arbitrage of illicit goods and, face substantial challenges for structuring the organizations to optimize and adapt the distribution of their goods, and have significant risks and costs if their organizations are detected by authorities [29]. Our previous findings suggest that gold farming networks and at least one offline drug trafficking network exhibit similar topologies which support their resilience despite breakup attempts by enforcement agents [30].

3. DATA AND MODELING APPROACH

3.1 Data

Anonymized database dumps were collected from Sony Online Entertainment's (SOE) MMOG *EverQuest II* (EQ2). These data include both observed and self-reported attribute data about characters and accounts in the game as well as longitudinal data cataloging character-to-character interactions such as trade exchanges of currency or items. Users are clustered onto distinct servers which operate in parallel but exhibit slightly different rule sets depending on players' preferences for hardcore player-versus-player (PvP) action, immersive role-playing (RP), or the standard player-versus-environment rule set (PvE). For all servers, the trade records include 44.3 million observations of player-to-player trade (4.97 million observations), player-to-merchant trade (32.3 million observations), and trade via an in-game auction house (6.95 million observations). The data spans January through September 2006, approximately two years after the game was launched.

We examined a one-week sample of the 9.8 million transactions on the Guk PvE server. The list of transactions is interpreted as a directed network edgelist whereby the initiator of the transaction is the sender of a link and the target is a receiver of the link. Despite this directed nature of a transaction, within individual transactions currency or items can be reciprocally exchanged by the sender and target of the exchange. This provides several possible permutations of relationship types between actors. We separate these relations into distinct networks described below.

- *Donation* (send money, receive nothing) – Currency is transferred from the sender to receiver, but nothing is reciprocated during that transaction. In the context of gold farming, this is the operant exchange which captures farmers "delivering" the gold to their customers or moving it between accounts. Because this is an unusual signal, it is an obvious heuristic for game administrators. In light of this risk, we expect it to be used sparingly and among trusted confidantes. The resulting network has 1,519 players and 1,318 edges.

- *Gift* (send items, receive nothing) – Items are transferred from the sender to receiver, but nothing is reciprocated during that transaction. In a gold farming context, this is a suspect signal for farmers delivering high-value items to

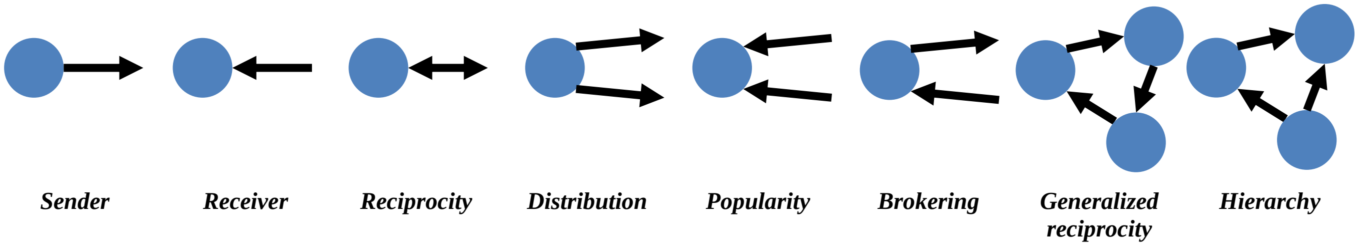

Figure 1: Visualizations of model structural parameters.

customers. The resulting network has 5,461 players and 9,239 edges.

- *Market* (send money, receive items) – Items are transferred and currency is reciprocated in kind during the same transaction. This is a legitimate exchange pattern which we expect occurs no more or less frequently among gold farmers than among typical players. The resulting network has 1,022 players and 768 edges.
- *Barter* (send items, receive items) – Items are transferred and other items are reciprocated during the same transaction. Like market exchange, this is also a legitimate exchange pattern which we expect occurs no more or less frequently among gold farmers than among typical players. The resulting network has 1,138 players and 1,323 edges.

Other permutations such as currency exchanged for currency or items exchanged for currency and items can be deduced, but these transactions are not observed in the data. The validity and implications of these and other modeling assumptions are discussed in greater depth in Section 5.

As an offline analogue, we used data collected by Morselli, et al. [17, 19] about a drug trafficking organization disrupted by Canadian law enforcement officers. Following [22], the data is collected from evidence submitted by prosecutors gathered from wiretaps and observations about communication and exchange relationships among members of the "CAVIAR" ring. The size of this network, limitations of data collected by surveillance, lack of attributes, and the types of substantive interactions among agents are all significantly different in the CAVIAR network as compared to the EQ2 gold farming network, this is nevertheless the most contemporary, largest, and complex drug trafficking network data which has been validated and made publicly available. We discuss the implications for validity by using this data as a comparison for gold farming in Section 5.

3.2 Modeling approach

We adopt a network perspective to model the interactions among individual characters within the game. Techniques for measuring local and global properties of networks such as centrality, clustering, density, shortest paths, diameter, and subgroup membership serve valuable roles for describing the properties of nodes, subgroups, and the entire networks. However, attempts to develop statistical models of networks using traditional methods such as linear or logistic regression are often fundamentally flawed because network data violates assumptions about the independence of ties in a network. Statisticians have developed a class of methods called p*/exponential random graph models (p*/ERGMs) which explicitly incorporate dependence assumptions to allow inferential statistical models for network analysis [31].

p*/ERGMs allow us to specify the observed network structure as the outcome variable which can be predicted by independent variables about both the structure and attributes of the nodes in this network. These statistical models are thus superficially similar to a logistic regression for the likelihood that a tie exists between nodes as a function of other variables. Unlike logistic regression models however, p*/ERGMs do not assume that the observation of a network tie is independent from the presence or absence other adjacent or other network ties. As such, this approach allows us to model the network as a complex system with stochastic outcomes but also retains the logic of a regression model by allowing us to specify local-level parameters which correspond to theoretically relevant structures and processes [32]. More importantly for our purposes of analyzing networks in offline and online contexts, p*/ERGMs allow us to compare parsimonious models of complex network structures [33].

The edgelists for each type of the four classes of transactions identified in section 3.1 were exported from an Oracle database. The `ergm` and `statnet` packages in the R statistical computing environment were used for p*/ERGM analysis [34, 35]. Parameters were added sequentially and the full models were observed have the best model fit as measured by Akaike information criteria and maximum-likelihood estimate likelihoods (see Table 1).

3.3 Hypotheses

Our goal in this analysis is to assess whether any of the four types of trade exchange networks in EverQuest II exhibit structural tendencies similar to those observed in the CAVIAR drug trafficking network. We expect that the structural signatures for high-risk transaction types in the MMOG (donations and gifting) will be more similar to the drug-trafficking network than the low-

	Parameters	Barter	Market	Donation	Gift	CAVIAR
Model 1	Sender + Receiver + Distribution + Popularity	-6658.9 13323	-6278.0 12526	-11129.5 22267	-81928.6 163865	-990.8 1989
Model 2	Model 1 + Brokering + Reciprocity	-816.5 1645	-6188.1 12388	-9278.2 18568	-62132.4 124277	-714.2 1441
Model 3	Model 2 + Generalized reciprocity + Hierarchy	-799.8 1615.6	-6178.4 12373	-8798.8 17614	-59382.7 118781	-677.0 1371

Table 1: Model fit with MLE likelihood on top, Akaike information criterion on bottom. The complete model (Model 3) is the best fitting model for all five networks.

		Barter			Market			Donation			Gifting			CAVIAR		
		Est.	SE	P	Est.	SE	P	Est.	SE	P	Est.	SE	P	Est.	SE	P
	Receiver	-7.357	2.52E-01	***	-7.075	4.89E-02	***	-6.786	4.57E-02	***	-8.811	1.83E-02	***	-5.559	1.35E-01	***
	Sender	0.853	1.20E-01	***	-0.039	4.89E-02		-0.122	4.57E-02	**	-0.040	1.83E-02	*	-0.002	3.80E-04	***
H1	*Reciprocity*	12.681	1.09E-01	***	3.524	3.93E-01	***	6.408	6.32E-01	***	7.195	6.06E-02	***	4.163	1.31E-03	***
H2	*Popularity*	0.913	1.41E-01	***	0.126	4.58E-02	**	0.090	4.57E-02	*	0.135	3.77E-04	***	0.044	2.86E-02	
H3	*Distributor*	-0.324	1.72E-01	.	0.181	4.01E-02	***	-0.461	6.91E-02	***	0.074	1.30E-02	***	0.099	2.07E-05	***
H4	*Brokering*	-2.159	2.88E-02	***	-0.314	4.76E-02	***	-0.480	4.46E-02	***	-0.035	2.12E-03	***	-0.012	4.40E-05	***
H5	*G. R.*	2.699	1.07E+01		2.843	1.12E+00	*	0.147	8.56E-01		-0.642	2.07E-02	***	-0.533	6.98E-05	***
H6	*Hierarchy*	-0.094	9.43E-02		1.228	6.84E-01	.	3.004	2.71E-01	***	1.359	1.25E-02	***	0.434	4.77E-05	***

Table 2: Parameter estimates, standard errors, and significance (* < 0.001 < ** < 0.01 < * < 0.05) for Model 3**

risk transaction types (market and barter). Despite the variety of attribute data about characters in *EverQuest II* which could be used in a model, corresponding attributes are not present in the CAVIAR data. We discuss this analytic shortcoming in more detail in Section 5. Instead we develop a multi-theoretical, multi-level model including only structural parameters of the network [36]. Although, space constraints do not allow us to unpack the theoretical rationales for each of these parameters, we posit the following hypotheses as being of theoretical interest and associate them with specific structural configurations. These parameters are visualized in Figure 1.

- H1 – *Reciprocity* – High risk transactions will rely on strong trust ties [15, 16]. There will be a tendency for nodes to reciprocate links in the network.
- H2 – *Popularity* – High risk transactions will concentrate risk in specific individuals responsible for receiving goods and currency from many other accounts [18]. There will be a tendency for nodes to be popular in the network.
- H3 – *Distribution* – High risk transactions will concentrate risk in specific individuals responsible for sending goods and currency to many other accounts [18]. There will be a tendency for nodes to be distributors in the network.
- H4 – *Brokering* – High risk transactions will avoid employing brokers who could compromise the trade [12, 13]. There will be a tendency to avoid brokering in the network.
- H5 – *Generalized reciprocity* – High-risk transactions emphasize operational efficiency, not social well-being [13]. There will be a tendency to avoid generalize reciprocity and cyclicality in the network.
- H6 – *Hierarchy* – High-risk transactions reflect latent hierarchical power relationships [12, 16]. There will be a tendency to have transitive hierarchies in the network.

4. RESULTS

The parameter estimates, standard errors, and significance levels for the model in each of the five networks are reported in Table 2. We interpret these findings and describe the similarities and differences between the models of the networks below.

The strong negative receiver estimate across all five models demonstrates that, absent other effects, the probability of a random trade relationship being initiated is between 0.34% for the CAVIAR network and 0.015% for the gifting network. The analogous sender parameter is also observed to be significantly negative across all the networks save the market relationships. As "intercept terms", these estimates suggest that characters in the game do not randomly trade with other players just as drug traffickers do not randomly interact with others.

In all five relationships reciprocity occurs substantially more often than would be expected by chance alone. Although this strong tendency to reciprocate relationships supports Hypothesis 1, reciprocity is also a general feature of many kinds of social and organizational networks. Thus, strong reciprocity in of itself is not a distinguishing feature of either a drug trafficking or online transaction network.

All four of the MMOG networks exhibited a significant tendency for nodes to accumulate links pointing to them, or popularity. However, a similar significant effect was not observed for the CAVIAR network. Hypothesis 2 is thus supported for the MMOG networks but not for the drug trafficking networks.

The similarities across trade types break down for nodes having many outbound ties, or distribution. The CAVIAR network exhibits a significant tendency for this structural process which is also found in the gifting and market exchange relationships. However, the bartering and donation networks in the MMOG both exhibit significant and relatively strong tendencies to avoid forming distribution structures. This provides mixed evidence for Hypothesis 3; distributing was favored and avoided for networks in both the high-risk (gifting and donations) and low-risk (bartering and market) transaction types although it was supported in the offline context.

There was uniform evidence across all five networks that brokering structures occur significantly less often than chance. This comports with contemporary theories about the risks and benefits of brokers to both themselves and the groups they broker – the position confers power, but is also easy to undercut. While these findings support Hypothesis 4, they do not allow us to distinguish the structure of high-risk transactions from low-risk transactions because all models avoid this structural feature.

The cyclic parameter we used to test generalized reciprocity was generally absent for the gifting and CAVIAR networks while it was overrepresented in the other three MMOG networks. The absence of generalized reciprocity in the gifting network is especially surprising because it suggests that this behavior is not "gifting" at all, but serves a less social and more instrumental alternative purpose in allocating items among characters. This parameter supports our Hypothesis 5 that high-risk transactions will avoid generalized reciprocity and focus on less redundant and more operational relationships.

Finally, the transitive parameter we used to test hierarchy occurred significantly more often than would be expected for all of the networks except barter. This supported our Hypothesis 5. Like reciprocity, transitivity is an innately strong endogenous force for structuring social and organizational networks. As such, the observation of transitivity as a hierarchical tendency of networks is likely a necessary but not sufficient condition for understanding high-risk and clandestine network structure.

To assess the similarity of the networks, we take the vector of parameter estimates for each of networks and use a cosine similarity function to compare the MMOG networks to the CAVIAR network. The similarity between the CAVIAR network and bartering network is 0.874, market 0.894, donations 0.956, and gifting 0.997. In contrast, the gifting network has a cosine similarity of 0.890 with the bartering network and 0.898 with the market exchange network but a similarity of 0.976 with the donation network. The substantive and quantitative similarities between the structures of the high risk transaction networks – particularly the gifting network – in the MMOG and the structures of the drug trafficking network suggests both high-risk networks are structured by similar processes despite operating in very different contexts.

5. DISCUSSION

High risk transactions such as the unreciprocated exchange of items or currency exhibit structural patterns that are both distinct from low risk transactions while also being similar to the structures observed in an offline drug trafficking ring. More compellingly, these high risk networks exhibit many of the hypothesized structural features hypothesized and observed to occur in a clandestine network while lacking the features which might plausibly excuse the structure. For example, a "true" gift exchange network would likely exhibit a very strong tendency towards generalized reciprocity as individuals exchange goods without expectation of immediate or dyadic reciprocation. The observed "gifting" network has a very strong tendency toward reciprocation, high centralization of activity, and avoids generalized reciprocity all of which suggest it is likely not gifting at all, but a more instrumental exchange. These findings reinforce our previous research which demonstrated similarities between the topology and resilience of online clandestine organizations and the structures an offline drug trafficking ring [30].

By leveraging large-scale digital trace data repositories in MMOGs, it is potentially feasible to develop a computational social science of criminology or clandestine organizational behavior. These findings provide an opportunity to illuminate the structures of clandestine behavior that had hitherto been intractable or impossible to rigorously analyze. As socio-technical systems, MMOGs raise complex issues about virtual sociality, economic activity, and legal rights which social computing, computational social science, and web science will need to grapple with in the years ahead.

To return to our case, engaging in high risk transactions is not in of itself actionable evidence of being affiliated with illicit behavior. Gold farmers and their undetected affiliates made up only a fraction of the total nodes in the network and their observed structural configurations were not entirely orthogonal to lower risk transaction types. A variety of other models or analyses could be run which attempt to ascertain the extent to which an individual participating in multiple types of transactions, exhibiting behavioral patterns in conjunction with interaction patterns, or exchanging particular types of items could all be run. These introduce additional assumptions into the equation and further abstract the findings from the behavior. In these data rich environments, what principles should guide this optimization? We conclude by discussing the limitations and threats to validity of this study, the ethical, legal, and larger implications of computational social science research in this vein, and directions for future work.

5.1 Validity, Limitations, Future Work

Validity looms large not only when attempting to make claims of generalizability, but also tracing the inferential jumps from observations to constructs to measures. These concerns are further compounded when using statistical models to generate and compare parsimonious descriptions of complex networks. We discuss the limitations of our approach, threats to validity, and directions for future work.

Online worlds have constraints and affordances that are simply impossible to readily map to offline behavior or organizations. Just as offline contexts lack immediate analogues to teleportation, instantaneous healing, or limitless supplies of items, online contexts lack features like the ability to intimidate or coerce the authorities or engage in civil disobedience to undermine unethical laws and rules. Indeed, the behavioral norms in online games can even be orthogonal to offline norms when the former tolerates or incentivizes behavior like killing and robbing other players. Similarly, the consequences of being penalized the by authorities in each context are hugely different: gold farmers only risks the loss of their online account if discovered by administrators while incarceration or violent retribution await members of drug traffickers indicted by prosecutors or discovered by competitors. Despite the profound differences in affordances and consequences of the MMOG and a drug trafficking operation, this is nevertheless the second study to identify striking similarities in the way that these clandestine operations structure themselves. This potentially speaks to latent evolutionary traits which clandestine organizations retain in response to selection pressure.

There are three component tests of validity in virtual worlds: face, concurrent, and predictive [28]. We met the threshold for face validity of testing clandestine organizations because MMOGs like *EverQuest II* have gold farmers and other types of deviant players who are banned by administrators for engaging in deviant activities involving the trafficking of virtual currency or valuable items. By analyzing four different types of trade relationships in the game corresponding with high and low-risk transactions, we also established concurrent validity with the high risk behaviors behaving similarly to each other and relatively distinct from the low-risk transaction. We also established predictive or external validity by demonstrating high-risk transactions assume similar structural patterns as offline drug trafficking behavior. However, because we only sampled a single week of trade data from the game, these findings needs to be replicated across other weeks in the data set to establish reliability.

The digital trace data used for this analysis was the by-product of user activities produced and stored by an information system which was not designed to be a research instrument. Howison, Crowston, and Wiggins [37] review the validity issues which arise when using digital trace data to understand meaningful interaction potentially without direct or complete measures of a relationship. For example, the transmutation of the records of transactions between players and stored on a database potentially raises validity issues about the way in which this data was captured (were there other means to exchange items or currency which were not recorded?), the reliability of the resulting records (would a double-entry accounting of transaction entries ultimately balance?), the type(s) of nodes and links we did or did not capture (is trade mediated by chat or grouping relationship?), misspecification (if characters are embedded within accounts, are trades just within accounts?), activity left out because of temporal boundaries (have they traded before?), and the intensity of these links (are these offline acquaintances?). Despite the ability to model how exogenous attributes such as player gender, user expertise, or character type influence the structure of the network, these parameters were excluded because there were either no corresponding data against which to compare or model or no ready analogues which would make a valid comparison.

Future work should develop p*/ERGM models incorporating node attributes like character class, expertise, and deviant status would provide important insights into the ways in which exogenous processes structure the network above and beyond the endogenous processes we modeled in our analysis. Incorporating the multi-relational nature of the network would allow us to test whether specific dyadic covariates such as communication, friendship, or grouping relations strongly mediate the use of high-risk transactions or the structure of the organization. The cat-and-mouse game of gold farmers and administrators also suggests future analyses should explicitly model the temporal dynamics by which gold farmers' behavioral and interaction patterns co-evolve with attempts by administrators to identify and remove them.

5.2 Ethical and Legal Dimensions

The logic of our analysis was predicated on the theory that individuals' behavioral patterns in online contexts are governed by similar social, cultural, and psychological forces as they encounter and negotiate offline. The fact that the behavior and interactions of these individuals were mediated through computer databases which record records was initially framed as beneficial for data collection and empirical analysis of online behavior to map back to offline behavior. However, if we believe that data about users' online clandestine behavior can be validly and reliably mapped to understand offline clandestine behavior, does that necessarily imply users assumed these illicit interactions would remain private or anonymous? This in turn raises questions of whether users are fully rational about the fact that any and everything they do within an online can be queried and discovered by the administrators. Especially in the context of clandestine organizing in a data-rich environment, do users operate with the assumption they cannot be surveilled or do they interact in spite of this surveillance? Scientists would do well to reflect on the implications of these dramaturgical stages.

This raises fascinating issues at the intersection of information theory and legal due process. Just as network analysts make inferential jumps which threaten validity as we outlined in the previous section, other models and methods developed by statisticians or computer scientists operate on a variety of assumptions all of which are potential threats to validity and reliability. In the context of game administrators or other authorities identifying and acting against individuals engaged in deviant behavior, the use of different methods will necessarily foreground different suspects. What should be these authorities' guiding optimization function: minimizing false positives, minimizing false negatives, maximizing true positives, or maximizing true negatives? Our previous research demonstrated how the introduction of various feature sets to machine learning models employing different decision algorithms classifies the effective guilt or innocence of individuals in a population with very different levels of performance [26]. What standards for the quality of data, stability of outcomes, or complexity of models ultimately guide the decisions on whom to ban?

Moreover, given the superabundance of data in these socio-technical systems, is there a heightened or altered burden of proof for game administrators or other authorities to demonstrate intent, liability, or causation? What recourse to notice, hearing, standing, and representation does an individual have to challenge actions taken against him or herself? Would the adjudication of this process require authorities to disclose proprietary methodological approaches for identifying and detecting problematic behavior as a part of discovery? For MMOGs, these questions are currently moot because of the contractual agreements players agree to when the log in to a game [10]. However, computer-mediated clandestine organizations are not confined to MMOGs and these issues will certainly emerge outside of the safe confines of EULAs as more interactions and behavior become mediated.

The ability to analyze and characterize the behavior of clandestine organizations likewise requires some reflexivity on the part of computational social scientists. Abstract thought experiments from studying online games about the best methods for identifying and "removing" influential nodes from a network take on euphemistic hues when extended to military, intelligence, and law enforcement contexts. In light of this, the computational social science of clandestine activity is inherently a "dual use" technology which can be constructed and used towards beneficial (identifying and detaining criminals and terrorists) or detrimental ends (identifying and detaining political opponents and activists). These distinctions are political frames which can be shifted. Are there boundaries to the technologies and methods computational social scientists should develop lest these be appropriated for regressive, unjust, or destructive ends? Should there be professional guidelines or principles about the ethical conduct for computational social science?

The similarity of network structures associated with high risk transactions to other kinds of high risk transactions in both online and offline contexts have significant implications. Not only are there clandestine organizations present in MMOGs, they appear to operate under similar organizing logics as offline clandestine organizations. If highly mediated online environments nevertheless give way to illicit behavior like trafficking, it may be necessary to break out the flax and ritual to remind ourselves the distinctiveness of new media are likewise temporary and passing.

6. ACKNOWLEDGMENTS

This research was supported by the National Science Foundation via award number IIS-0729505, the Army Research Institute via award number W91WAW-08-C-0106, and the Air Force Research Laboratory by contract number FA8650-10-C-7010. The anonymized data used for this research was provided by Sony Online Entertainment. We thank members of the Virtual Worlds Observatory team for their support and feedback.

7. REFERENCES

[1] Reeves, B. and Read, J. L. *Total engagement: using games and virtual worlds to change the way people work and businesses compete*. Harvard Business School Press, 2009.

[2] Bainbridge, W. S. *The Warcraft civilization: social science in a virtual world*. The MIT Press, 2010.

[3] Castronova, E. *Exodus to the virtual world: How online fun is changing reality*. Palgrave Macmillan, 2007.

[4] Dibbell, J. *Owned!: Intellectual property in the age of dupers, gold farmers, eBayers, and other enemies of the virtual state*. New York University Press, City, 2003.

[5] Lehdonvirta, V. Virtual Worlds Don't Exist: Questioning the Dichotomous Approach in MMO Studies. *Game Studies*, 10, 1 (2010).

[6] Castronova, E., Williams, D., Shen, C., Ratan, R., Xiong, L., Huang, Y. and Keegan, B. As real as real? Macroeconomic behavior in a large-scale virtual world. *New Media & Society*, 11, 5 (2009), 685.

[7] Dibbell, J. *Play Money: Or, How I Quit My Day Job and Made Millions Trading Virtual Loot*. Basic Books, New York, 2006.
[8] Lehdonvirta, V. and Ernkvist, M. *Converting the Virtual Economy into Development Potential: Knowledge Map of the Virtual Economy*. infoDev/The World Bank, Washington, D.C., 2011.
[9] Consalvo, M. *Cheating: Gaining advantage in videogames*. MIT Press, Cambridge, MA, 2007.
[10] Lastowka, F. G. and Hunter, D. *Virtual Crime*. New York University Press, City, 2006.
[11] Heeks, R. *Current Analysis and Future Research Agenda on "Gold Farming": Real World Production in Developing Countries for the Virtual Economies of Online Games*. Institute for Development Policy and Management, University of Mancester., 2008.
[12] Milward, H. and Raab, J. Dark networks as organizational problems: Elements of a theory. *International Public Management Journal*, 9, 3 (2006), 333-360.
[13] Morselli, C., Giguère, C. and Petit, K. The efficiency/security trade-off in criminal networks. *Social Networks*, 29, 1 (2007), 143-153.
[14] Podolny, J. M. and Page, K. L. Network Forms of Organization. *Annual review of sociology*, 24, 1 (1998).
[15] von Lampe, K. and Johansen, P. O. Organized crime and trust: On the conceptualization and empirical relevance of trust in the context of criminal networks. *Global Crime,* 6, 2 (2004), 159-184.
[16] Stohl, C. and Stohl, M. Networks of terror: theoretical assumptions and pragmatic consequences. *Communication Theory,* 17, 2 (2007), 93-124.
[17] Morselli, C. *Inside Criminal Networks*. Springer, 2008.
[18] Baker, W. and Faulkner, R. The social organization of conspiracy: Illegal networks in the heavy electrical equipment industry. *American Sociological Review*, 58, 6 (1993), 837-860.
[19] Morselli, C. and Petit, K. Law-Enforcement Disruption of a Drug Importation Network. *Global Crime*, 8, 2 (2007), 109 - 130.
[20] Kenney, M. *From Pablo to Osama: trafficking and terrorist networks, government bureaucracies, and competitive adaptation*. Pennsylvania State University Press, 2007.
[21] Kossinets, G. Effects of missing data in social networks. *Social Networks*, 28, 3 (2006), 247-268.
[22] Sparrow, M. The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks*, 13, 3 (1991), 251-274.
[23] Contractor, N., Wasserman, S. and Faust, K. Testing Multitheoretical, Multilevel Hypotheses about Organizational Networks. *Academy of Management Review*, 31, 3 (2006), 681-703.
[24] Robins, G. Understanding individual behaviors within covert networks: the interplay of individual qualities, psychological predispositions, and network effects. *Trends in Organized Crime*, 12, 2 (2009), 166-187.
[25] Lazer, D., Pentland, A., Adamic, L., Aral, S., Barabasi, A., Brewer, D., Christakis, N., Contractor, N., Fowler, J. and Gutmann, M. Life in the network: the coming age of computational social science. *Science (New York, NY)*, 323, 5915 (2009), 721-723.
[26] Ahmad, M. A., Keegan, B., Srivastava, J., Williams, D. and Contractor, N. *Mining for Gold Farmers: Automatic Detection of Deviant Players in MMOGs*. City, 2009.
[27] Ahmad, M. A., Keegan, B., Williams, D., Srivastava, J. and Contractor, N. *Trust Amongst Rogues? A Hypergraph Approach for Comparing Clandestine Trust Networks in MMOGs*. AAAI, City, 2011.
[28] Williams, D. The mapping principle and a research framework for virtual worlds. *Communication Theory*, 20(2010), 451-470.
[29] Kenney, M. The architecture of drug trafficking: network forms of organisation in the Colombian cocaine trade. *Global Crime*, 8, 3 (2007), 233-259.
[30] Keegan, B., Ahmed, M., Williams, D., Srivastava, J. and Contractor, N. Dark Gold: Statistical Properties of Clandestine Networks in Massively Multiplayer Online Games. *IEEE Conference on Social Computing*(2010).
[31] Robins, G., Snijders, T., Wang, P., Handcock, M. and Pattison, P. Recent developments in exponential random graph (p*) models for social networks. *Social Networks*, 29, 2 (2007), 192-215.
[32] Robins, G., Pattison, P., Kalish, Y. and Lusher, D. An introduction to exponential random graph (p*) models for social networks. *Social Networks*, 29, 2 (2007), 173-191.
[33] Faust, K. and Skvoretz, J. Comparing networks across space and time, size and species. *Sociological Methodology*, 32(2002), 267-299.
[34] Handcock, M., Hunter, D., Butts, C., Goodreau, S. and Morris, M. statnet: Software tools for the representation, visualization, analysis and simulation of network data. *Journal of Statistical Software*, 24, 1 (2008), 1548.
[35] Hunter, D. R., Handcock, M. S., Butts, C. T., Goodreau, S. M. and Morris, M. ergm: A package to fit, simulate and diagnose exponential-family models for networks. *Journal of Statistical Software*, 24, 3 (2008).
[36] Monge, P. and Contractor, N. *Theories of communication networks*. Oxford University Press, USA, 2003.
[37] Howison, J., Crowston, K. and Wiggins, A. Validity issues in the use of social network analysis with digital trace data. *Journal for the Association of Information Systems*(2011).