2013 5th International Conference on Cyber Conflict
K. Podins, J. Stinissen, M. Maybaum (Eds.)
2013 © NATO CCD COE Publications, Tallinn

Illicit Network Structures in Cyberspace

Kaarel Kalm
Department of Security and Crime Science
University College London
kaarel.kalm.12@ucl.ac.uk

Abstract: Different types of covert illicit networks in cyberspace hold the potential to become actors in cyber conflicts. Current literature on structures of covert networks in cyberspace is often constrained by the lack of quantitative data and researchers mostly focus on networks operating outside the cyberspace. The purpose of this paper is to review the current state of research into illicit networks in cyberspace and to apply the terminology and concepts of Social Network Analysis on criminal organisations operating online. Social Network Analysis is a quantitative data analysis method, which can identify hierarchies, subgroups, individuals and their relative importance in covert illicit networks, by using data from multiple sources (academic research, law enforcement, black market trading, semantic web analysis etc.). Here I explore how Social Network Analysis offers methods to discover hidden structures of covert networks in cyberspace.

Keywords: *cybercrime, covert networks, illicit networks, social network analysis*

1. INTRODUCTION

Covert networks operating in cyberspace are involved in organized crime, espionage, terrorism, trafficking and a list of other illicit or destructive activities with a high impact on society. Current literature on structures of covert networks is often constrained by the lack of quantitative data and researchers mostly focus on illicit networks operating outside the cyberspace [1], [2]. Along with the advances of technology, the nature and activity of covert networks in cyberspace have changed. A sophisticated underground economy has emerged, along with ideology driven "dark webs", and state sponsored cybercrime groups. Covert networks are stateless, fluid and adaptable and function as the main facilitators of trafficking, proliferation and terrorism [3]. They present an asymmetric threat to nation states and have emerged as one of the main concerns of international political agenda [4]. A research commissioned by BAE Systems in 2012 found that 80 per cent of cybercrime can be attributed to organised groups including hybrid criminal groups which combine online and offline offending [5].

The need to have in-depth knowledge of covert networks will become increasingly acute as such networks develop towards holding a very high threat potential. As this trend is unlikely to reverse, the practical aspects of network identification are of importance to policy makers and law enforcement. Ability to describe and map the properties of such networks is a basis for developing effective prevention, detection and disruption mechanisms. Obtaining information about covert networks is made difficult by their very nature and purpose. However, covert networks have to constantly manage the trade-off between security and efficacy. To successfully function, information must be exchanged inside the network, and if necessary, between network members and outsiders. Through exchange of information, networks become exposed for detection and analysis [6].

This research looks at the problems of covert networks and the general threats they present in the context of cyber conflicts. I shall describe the typology of covert networks in cyberspace and then describe how Social Network Analysis (SNA) can identify hierarchies, subgroups, individuals and their relative importance in such networks. I shall review existing data about covert networks from multiple sources and suggest generic structures of four different type of networks. With each type of network, relevant background is given and data is examined in the social network context. This is followed by a short list of recommendations on how policy makers and law enforcement can counter the threat that arises from specific types of covert networks and what tactics might be useful for detection and disruption. Discussion of limitations of social network analysis methods follows along with some suggestions for further research. The questions of data availability and the cooperation between law enforcement and academia are also briefly addressed.

In this paper, covert and illicit networks refer to organised groups of individuals that are involved in criminal activities taking partly or entirely place in cyberspace. This includes activities associated with crimes for profit, terrorism, espionage, destruction and disruption of property, antisocial behaviour etc. As the definitions of cyber conflict and cybercrime are still very much up for debate [7], [8], I do not aim to make a distinction between them in this paper. Rather, I presuppose that any cyber conflict consists of criminal acts that are enabled by technology. As different criminal acts require different organisational structures, covert networks in cyberspace can take several forms.

There are at least four distinct types of covert illicit networks operating in cyberspace—traditional criminal organisations, cybercriminal organisations, ideologically motivated organisations, and state sponsored organisations [9], [10]. Those four types of networks have both unique and common properties. Unique properties derive primary from motivational and ideological factors. Traditional criminal networks and cybercriminals are mostly profit oriented and therefore more engaged with outside actors. Ideological and government sponsored groups are more closed but also more interconnected. Overlapping properties arise from the need to operate in secrecy, victimisation and structural resilience. They also use similar tactics and technology. The theory of crime-terror nexus also asserts that methods invented and successfully applied by one type of criminal organisation are likely to be appropriated by another type of organisation, regardless of underlying ideology [11]. As such, all four types of covert networks are considered to hold the potential of becoming participants in a cyber conflict and are therefore included in this analysis.

2. SOCIAL NETWORK ANALYSIS

Social network analysis (SNA) is defined as study of structural aspects of networks. Social network theory argues that "Any action of actors is not isolated but correlated. The relationship ties among them are transmission channels of information and resources and network relation structure decides their action opportunities and results" [12]. A social network is represented by nodes (actors) and links (relationships) between those nodes. In the context of this study, those nodes are either people or technical facilitator (e.g. websites, microblogs, forums etc.). SNA is not a precise analysis technique but incorporates a set of mathematical, graphical and theoretical tools to measure the location of network nodes and to identify relationships between them [13].

There has been a considerable increase of interest in networks analysis theories in the past decade. A lot of research on social networks has been done in biology,

geography, economics, information science and sociology [14]. SNA has also been successfully applied to security studies, although the lack of quantitative data has forced researchers to mostly focus on illicit networks operating outside the cyberspace. Social network analysis can be used to establish key members and structural weaknesses of criminal organisations [15], [16], evaluate relative influence and connectedness of a particular actor in a networks [1] and to identify hubs and bridges in illicit networks to study effective disruption tactics [17].

Based on their characteristics, networks can be classified as random, small-world or scale-free. *Random networks* have a small number of nodes and a small number of links between them. *Small-world networks* have a larger number of nodes and a small number of links between them. Unlike random networks, small-world networks often contain clustering of nodes. *Scale-free networks* have similar properties to small-world networks, with an important addition of power-law degree distribution. Power-law degree distribution implies that while most nodes still have a small number of connections, a very small number of nodes are highly connected [18]. In addition to general topological properties, SNA enables researchers to measure several descriptive metrics inside the networks. In relation to nodes—centrality, betweenness, clustering, and eigenvector values describe the relative influence and connectedness of a particular actor in the network. Note that connectedness and influence are separate descriptives as the most connected node might not be the most influential and vice versa.

Node *centrality* measures the location of a node in relation to the centre of the network. The more central a node is, the smaller is the number of links connecting it to other nodes. In human networks, a person with the highest degree of centrality can reach all other people in the network through smallest number of connections. This person is likely in a leadership position, binding the network (or a part of it) together. If network nodes represent technical facilitators, content severity is an additional indicator of influence. From law enforcement perspective, monitoring nodes with high centrality can provide information and removing them can break larger networks into smaller cells.

Betweenness of a node measures the number of shortest connections between two other nodes passing through that particular node. A person with a high measure of betweenness functions as a bridge for communications and should be a prime target for monitoring by law enforcement.

Eigenvector values identify highly connected nodes that are connected to other highly connected nodes. This is also known as the “rich club” effect or the “rich-get-richer” phenomenon [17], [19], where high degree connected nodes tend to become even more interconnected resulting in subgroup clustering. In human networks this

implies that important people are and will become connected to other important people. From law enforcement perspective, it would be meaningful to target such individuals simultaneously. This subgroup holds most information and removing just single individuals from it is less likely to disrupt the rest of the network.

Clustering or transitivity measures the likelihood that if a link exists between nodes A and B, and nodes A and C, it also exists between modes B and C. Link structures are basic indicators of clustering, as for example, described above by the "rich club" effect. In networks with low overall centrality, clustering may still occur in forms of small subgroups connected by central authority. Such groups may not hold information on the larger network, but they also have capabilities to act independently from it.

As both general topological properties and node descriptive metrics influence measures available for disruption, covert network analysis should follow three logical steps: (a) identify covert network type; (b) analyse network characteristics; and (c) evaluate key nodes in the network.

3. COVERT NETWORKS IN CYBERSPACE

As described above, networks can be differentiated between random, small-world and scale-free networks. Covert networks operating in cyberspace follow either financial or ideological motivations, making the existence of a random type of illicit network very unlikely. Yet researchers can use random networks as comparisons models. Most basic random networks are characterised by low average path lengths and low clustering measures [20]. In human networks this would mean that all members are closely connected, while no hierarchical structures and subgroups exist. Such networks are very robust and node removal would have little effect on their overall performance [21]. Concurrently, their overall performance would also be very low, resulting from absence of leadership and coordination. Disruption of covert networks can take a form of targeted attacks against key individuals, simultaneous attacks against a subgroup, progressive attacks or random removal of network members. While random networks might be robust against most forms of attack, small-world and scale-free networks have properties that make some attacks more effective than other. In scale-free networks, a small number of members are highly connected, making the networks robust against random removal of members but vulnerable to targeted attacks. In small-world networks, a larger number of members are well connected to each other, duplicating connections. Therefore such networks are more vulnerable to random attacks (compared to scale-free networks) but targeted attacks may not be sufficient to disable information flow inside the network. Following, I shall explore the network structures of four types of covert networks from the practical viewpoint of detection and disruption.

A. TRADITIONAL CRIMINAL ORGANISATIONS

Organised crime is mostly market-driven, even if the consumer need is created by the organisations themselves. This means that they provide services driven by financial rationality. Interconnected global economy and the spread of Internet has created opportunities and incentives for organised criminal groups to exploit competitive advantages cyberspace can offer. Key drivers of international economy like financial deregulation, technological development, interconnectedness of infrastructure and global labour markets have enabled a surge in trade of drugs, arms, illegal goods, people, and money [22]. A report from UK Serious and Organised Crime Agency suggests that advances in technology are increasingly exploited by members of organised crime groups. The internet provides criminals with tools to commit traditional crimes in a more sophisticated way along with opportunities for new types of crime [23].

Technology-enabled crimes carried out by traditional criminal organisations include network intrusions, identity frauds, online scams, malware distribution etc. Technology connects a geographically very distant demand and supply sides of the illicit market previously outside the sphere of interest of traditional organised crime. Several crime organisations have also established a strong online presence for propaganda and recruitment purposes, to issue threats and monitor the media [24].

Several empirical studies have used social network analysis on police arrest-data and court-data to identify criminal networks [1], [25]. There is also a significant amount of open source data available to enable social network analysis by non-law enforcement organisations [24], [26]. The main findings from those studies indicate that similar social network characteristics describe both offline and online traditional criminal groups. Such networks have small average path lengths and high clustering or transitivity metrics. Therefore they can be classified as small-world networks. This means that the covert network consists of a group of well-connected members who can reach each other easily. Connections with other networks are low as is expected from groups competing for resources. Traditional criminal networks demonstrate also and overall low link density, implying that network members interact mostly inside the network and with a certain set of other members [17]. This can be explained with the traditional structure of organised crime groups, where individual members are tasked with specific assignments and do not operate outside those limits.

The question of power-law distribution in traditional criminal networks can be dependent on their historical structure. Where the crime network operates in strict top-down hierarchical manner, scale-free properties can be not as apparent as

the power dynamics inside the network are more stable. Whereas in horizontally organised networks, the power-law distribution can be more apparent, along with the "rich club" effect [9].

B. CYBERCRIMINAL ORGANISATIONS

Cybercriminal organisations form and operate online and are engaged in technology-enabled crime. As such crimes require specific knowledge and experience, both individual members and the overall networks structure differs from traditional criminal organisations operating in cyberspace. Cybercriminal networks are characterised by technically capable members, anonymous (in relation to real identities) interaction, and opportunistic financial motivations [10].

Cybercriminal networks face a task of leveraging security with the need to interact with outside members willing to pay for their services. In comparison with other types of covert networks, they are most directly involved in what might be described as black market dynamics. Members often take part in direct price negotiations and sales, are influenced by competitors' offerings and customers' demands. As the online black market is increasing, such dynamics can lead to a fully functional marketplace with high utility and low participation risks [19]. Reports suggest disappearance of independent and small-group hackers and appearance of hierarchical cybercrime networks with role-based memberships [27], [28].

Research data about cybercriminal networks suggest that unlike traditional criminal organisations in cyberspace, cybercriminal networks are not scale free. This indicates that while network members form ties based on preference, they also form a substantial number of random links. As cybercriminals have to participate in market activities, there is a need to find orders for services and customers for products. Random link formation can be attributed to members seeking buyers for their services or looking for business opportunities through cooperation. Networks engaged in online black markets are also highly clustered with evidence of hierarchical structures in the networks [19]. This is a result of participating in market activity, where certain positions are established – administrator, escrow, seller, buyer, etc. The need to establish trust in the network requires some members to reveal their transactions to build-up trust and acquire more customers. As more active and more contributing members are likely to have an exponential increase of links to other members, a clustering formation appears [29]. As the overall network is not scale-free, it is more robust against targeted attacks as well as random removal of members. The network can also easily incorporate new members to replace those that are removed. However, gradual appearance of some very well connected members can provide sufficient grounds for targeted attacks that are likely to disrupt the networks but unlikely to disable it.

C. IDEOLOGICALLY MOTIVATED ORGANISATIONS

Ideologically and politically motivated organisations are increasingly taking to cyberspace. This follows a similar trend as observed for traditional criminal organisations. Same technological factors are facilitating this move, but in addition to that, an increasing nexus between ideologically motivated and financially motivated criminal organisations is becoming apparent [11]. As ideologically motivated organisations in cyberspace require increasingly more funding and are unlikely to establish any legitimate base for financial income, it is likely that they will also get increasingly more involved in online illicit economy. In addition to financing, such groups are using internet as a platform for communication and publicity. As their motivation for action is ideological, they actively seek widespread publicity and are largely indiscriminate in their use of force or violence. The internet serves as an effective facilitator of ideological propaganda and recruitment.

Findings from academic studies indicate that ideologically and politically motivated networks in cyberspace are described by very high subgroup clustering with long path lengths compared to traditional and cybercriminal networks. They are scale-free networks with evidence of the 'rich club' effect, where influential members are well interconnected. The power-law distribution is also evident in ideological networks [17] and is also supported by data from web forums analysis', where a small number of members are the most prolific communicators, followed with a sharp decay in number of postings by other members. [28]. High subgroup clustering can result from the overall trend of ideological networks becoming more fluid and horizontal in their structure as well as from recruitment practises, where new members are indoctrinated by a certain subgroup [4]. Members are characterised by a small number of in- and outwards connections, meaning that a member's knowledge about the larger network is limited. The member also has low impact on other members and the network has multiple leadership figures on different levels [12].

Multiple leadership positions make the network as a whole more resilient but the smaller subgroups vulnerable to targeted attacks. This represents a calculated risk on increasing secrecy while reducing operational capability. According to Drozdova and Samoilov [30] "In environments dominated by hostile opponents and where there is significant resource imbalance and incomplete information, the choice of fault-intolerant network organizations structure for clandestine mission networks helps protect the broader organization by minimizing its internal connectivity and allowing all parties plausible deniability of their relations".

D. STATE SPONSORED ORGANISATIONS

State sponsored cybercriminal organisations impose highest threats in the context of cyber conflict as they lack many properties that expose other type of covert networks. They are not directly financially motivated, opportunistic nor ideologically constrained. As state sponsored cybercrime mostly involves espionage and technical operations, a substantial amount of resources is required. While the direct cost of software development and deployment may not be that high in comparison to possible gains from all forms of cybercrime, technology development and operational secrecy requirements impose substantial demands on state sponsors [31]. State sponsored cybercrime also carries a high risk of conflict escalation through retaliation and confrontation, possibly leading to a direct cyber conflict or –war [32].

Alleged state sponsored cyber attacks are a common theme in media with regular reports claiming Russian hackers attacking USA, USA and Israeli hackers attacking Iran, Iranian hackers attacking China, Chinese hackers attacking USA and India, etc. The Director General of the UK Security Service [33] has called the extent of cybercrime "astonishing – with industrial-scale processes involving many thousands of people lying behind both state sponsored cyber espionage and organised cybercrime." There are also well-published incidents of cyber attacks against Estonia, Georgia and Azerbaijan. Yet the data on state sponsored cybercriminal organisations is sparse and academic access and analysis of it is almost non-existent.

Lack of empirical data on state sponsored cybercriminal groups can be explained by several factors. First of all, relevant data could be unavailable for academic research as organisations collecting it are unwilling to share it. Existing data could also be inconclusive, making the academic analysis meaningless and further discouraging its sharing. Secondly, relevant data might actually refer to regular cybercriminal groups that act on behalf of the state when necessary. Several hypotheses have been proposed by researchers on how state structures incorporate cybercriminals and "patriotic hackers" [7], [32], [34]. Based on those hypotheses, some state sponsored cybercriminal networks should display similar properties to regular cybercriminal networks – small-world and non scale-free metrics. While cybercriminal networks have to balance exposure risks with a need to interact with customers, state sponsored groups have no need to establish trust with possible buyers. This should reduce the number of random links and clustering in the network. A special case should be made for state structures are directly participating in cybercriminal activities. While empirical data on them is again non-existent, an argument could be made that their networks will reflect the bureaucratic structures of the state and secrecy oriented structures of traditional covert government organisations. This

would imply hierarchical structures, small size of the network and short average link paths with few very well connected members.

4. IMPLICATIONS AND DISCUSSIONS

Existing data on covert networks in cyberspace allows division of such networks into four groups—traditional criminal organisations, cybercriminal organisations, ideologically motivated organisations, and state sponsored organisations. As different criminal motivations require different organisational structures, covert networks in cyberspace take several forms. Traditional criminal networks are likely to have small-world and scale-free properties. They are resilient to random removal of members but vulnerable to targeted attacks. Cybercriminal networks are small-world and not scale-free. There are preferential links between members, but also a substantial amount of random links. This results from the need to engage with possible clients and establish trust on the market. Both random and targeted removal of members has limited effects as the network can easily incorporate new members. Ideological networks are small-world and scale-free with high sub clustering coefficients. Members have few connections and little influence in the network. High number of subgroups indicates a need for targeted attacks but the overall network is relatively robust to them. Empirical data on state sponsored groups is too scarce to draw meaningful conclusions. If a state has outsourced its cybercriminal activities, similar network properties should be apparent as in regular cybercriminal networks. If state structures are directly participating in cybercriminal activities, hierarchical bureaucratic structures should be expected.

In studying covert networks, this paper has largely ignored the social psychological aspects of networks formation. Arguably, some psychological factors are incorporated into members' link formation and clustering preferences but it would be unwise to assume, that all network dynamics can be described by link paths, clustering coefficients and leadership hierarchies. The human component of covert networks should not be ignored but rather attempts should be made to incorporate that into the analysis. There have been advances in studies of cybercriminal profiling that could be included into future research of covert networks in cyberspace. Focusing on social networks has also disregarded what is popularly known as 'lone wolf' offending. Lone actors are capable of inflicting serious damage in the cyberspace and should also be regarded as possible participants or initiators of cyber conflicts. As 'lone wolf' criminals by definition do not form co-offending groups, social network analysis cannot provide much insight into their activities. At the same time, the very nature of the internet is likely forcing 'lone wolf' offenders into participating in some kinds of social networks to acquire know-how and resources for attacking. Whether indications of 'lone wolf' offending can be found from analysing social networks is another topic for future research.

The question of data availability is a major factor in covert networks research. Sufficient data might be available to law enforcement but the lack of resources and need for operational secrecy hinder their analysis and distribution. This is not a criticism addressed at organisations investigating and countering covert networks but a recognition that law enforcement is always lacking resources and has to triage to prioritise their actions. A solution would be a deeper cooperation between law enforcement and academia. Understandably there are a lot of obstacles that would have to be overcome but the existing studies assert that actionable data and insight can be gleaned from such research. As covert networks in the cyberspace are increasingly developing towards holding very high treat potential, development of effective counter-measures requires active research of such networks, their structure and dynamics.

REFERENCES

[1] M. Tayebi, U. Glässer, and P. Brantingham, "Organized Crime Detection in Co-offending Networks," in IEEE- 9th International Conference Proceedings, 2011.

[2] M. Coscia and V. Rios, "How and where do criminals operate? Using Google to track Mexican drug trafficking organizations," Center for International Development at Harvard, Oct. 2012.

[3] R. Dietz, "Illicit Networks: Targeting the Nexus Between Terrorists, Proliferators, and Narcotraffickers," Naval Postgraduate School, Dec. 2010.

[4] M. Eilstrup-Sangiovanni and C. Jones, "Assessing the Dangers of Illicit Networks," International Security, vol. 32, no. 1, pp. 7–44, 2008.

[5] BAE Systems, "Organised crime in the digital age," 2012. Available at: www.baesystemsdetica.com/news/organised-crime-in-the-digital-age/

[6] R. Lindelauf, P. Borm, and H. Hamers, "The influence of secrecy on the communication structure of covert networks," Social Networks, vol. 31, no. 2, pp. 126–137, May 2009.

[7] J. Carr, Inside Cyber Warfare: Mapping the Cyber Underworld (Google eBook). O'Reilly Media, Inc., 2011, p. 314.

[8] R. A. Clarke and R. Knake, Cyber War: The Next Threat to National Security and What to Do About It (Google eBook). HarperCollins, 1082, p. 320.

[9] K.-K. R. Choo and R. G. Smith, "Criminal Exploitation of Online Systems by Organised Crime Groups," Asian Journal of Criminology, vol. 3, no. 1, pp. 37–59, Nov. 2007.

[10] K.-K. R. Choo, "Organised crime groups in cyberspace: a typology," Trends in Organized Crime, vol. 11, no. 3, pp. 270–295, Jul. 2008.

[11] [T. Makarenko, "The Crime-Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism," Global Crime, vol. 6, no. 1, pp. 129–145, Feb. 2004.

[12] S. Duo-Yong and G. Shu-Quan, “Study on covert networks of terrorists based on interactive relationship hypothesis,” 2011 IEEE International Conference on Intelligence and Security Informatics, pp. 26–30, 2011.

[13] A. Reid, M. Tayebi, and R. Frank, “Will the Defendants Please Rise? A Social Network Analysis of Accused Individuals in the Criminal Court System,” Simon Fraser University, pp. 1–24.

[14] S. P. Borgatti, A. Mehra, D. J. Brass, and G. Labianca, “Network analysis in the social sciences.,” Science, vol. 323, no. 5916, pp. 892–5, Feb. 2009.

[15] M. Sparrow, “The application of network analysis to criminal intelligence: An assessment of the prospects,” Social Networks, vol. 13, no. 3, pp. 251–274, Sep. 1991.

[16] M. Sparrow, “Mapping Networks of of Terrorist Terrorist Cells,” Connections, vol. 24, no. 3, pp. 43–52, 2002.

[17] J. Xu and H. Chen, “The topology of dark networks,” Communications of the ACM, vol. 51, no. 10, p. 58, Oct. 2008.

[18] R. Albert, H. Jeong, and A. Barabasi, “Error and attack tolerance of complex networks,” Nature, vol. 406, no. 6794, pp. 378–82, Jul. 2000.

[19] M. Yip, N. Shadbolt, and C. Webber, “Structural analysis of online criminal social networks,” 2012 IEEE International Conference on Intelligence and Security Informatics, pp. 60–65, Jun. 2012.

[20] D. J. Watts and S. H. Strogatz, “Collective dynamics of ‘small-world’ networks.,” Nature, vol. 393, no. 6684, pp. 440–2, Jun. 1998.

[21] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, “Attack vulnerability of complex networks.,” Physical review. E, Statistical, nonlinear, and soft matter physics, vol. 65, no. 5 Pt 2, p. 056109, May 2002.

[22] M. Naím, “The Fourth Annual Grotius Lecture : Five Wars of Globalization,” American University International Law Review, vol. 18, no. 1, pp. 1–18, 2002.

[23] UK Home Office, “Extending our reach: a comprehensive approach to tackling serious organised crime,” 2009. Available at: www.official-documents.gov.uk/document/cm76/7665/7665.asp

[24] M. Coscia and V. Rios, “How and where do criminals operate? Using Google to track Mexican drug trafficking organizations,” Center for International Development at Harvard, no. 57. p. 23, 2012.

[25] U. Glässer and M. Tayebi, “Estimating Possible Criminal Organizations from Co-offending Data,” Public Safety Canada, 2012.

[26] T. J. Holt and E. Lampke, “Exploring stolen data markets online: products and market forces,” Criminal Justice Studies, vol. 23, no. 1, pp. 33–50, Mar. 2010.

[27] Y. Ben-Itzhak, “Organised cybercrime and payment cards,” Card Technology Today, vol. 21, no. 2, pp. 10–11, Feb. 2009.

[28] C. Lu and W. Jen, “Cybercrime & cybercriminals: An overview of the Taiwan experience,” Journal of Computers, vol. 1, no. 6, pp. 11–18, Sep. 2006.

[29] V. Benjamin and H. Chen, “Securing cyberspace: Identifying key actors in hacker communities,” 2012 IEEE International Conference on Intelligence and Security Informatics, pp. 24–29, Jun. 2012.

[30] K. Drozdova and M. Samoilov, “Predictive analysis of concealed social network activities based on communication technology choices: early-warning detection of attack signals from terrorist organizations,” Computational and Mathematical Organization Theory, vol. 16, no. 1, pp. 61–88, Aug. 2009.

[31] J. B. Sheldon, “Strategic State of the Art : Attackers and Targets in Cyberspace,” Journal of Military and Strategic Studies, vol. 14, no. 2, pp. 1–19, 2012.

[32] H. Lin, “Escalation Dynamics and Conflict Termination in Cyberspace,” Strategic Studies Quarterly, vol. 6, no. 3, pp. 46–70, 2012.

[33] J. Evans, “The Olympics and Beyond,” in Lord Mayor’s Annual Defence and Security Lecture, 2012. Available at: https://www.mi5.gov.uk/home /about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-olympics-and-beyond.html

[34] N. Kshetri, “Pattern of global cyber war and crime: A conceptual framework,” Journal of International Management, vol. 11, no. 4, pp. 541–562, Dec. 2005.