Modern International Journal of Pure and Applied Mathematics 2017, 1(2): 30-37
DOI: 10.5923/j.mijpam.20170102.03

Graph Theory for Cybercrime: A Note

M. R. Pinheiro

IICSE University DE

Abstract In this note, we introduce some concepts from Graph Theory in the description of the geometry of cybercriminal groups, and we use the work of Broadhurst et al, a piece from 2014, as a foundation of reasoning. We are also worried about suggesting or even creating, if necessary, mathematical jargon, so that also mathematicians, and those who have similar thinking processes, can connect to Broadhurst et al's work, and create even more ways to deal with cybercrime data. This is a light note, with the sole intent of suggesting ways to go to Broadhurst et al, so that there is even more intersection between their work and ours. What happens with the creation of bridges between Cyber Crime and Mathematics is that we can speak more objectively about things, and, through Mathematics, perhaps optimize the efforts of the computer scientists, or even of the systems analysts, who try to create perfect tools for those who work in such a niche.

Keywords Graph theory, Geometry, Cybercrime, Organized group, Broadhurst, Swarm, Hub

1. Introduction

It seems that not much has been written about the geometry of cybercrime. Kammerdiner (2014) made use of some concepts from Graph Theory to talk about cyberspace security. So did several other authors in Belavkin et al's book (2014). Sarvari et al (2014) did use some concepts from Graph Theory in their work, and they also printed some images:

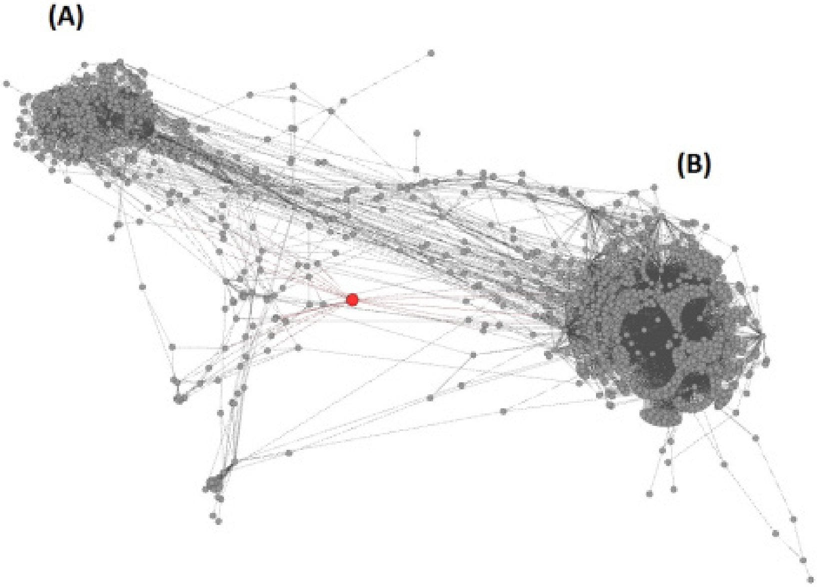


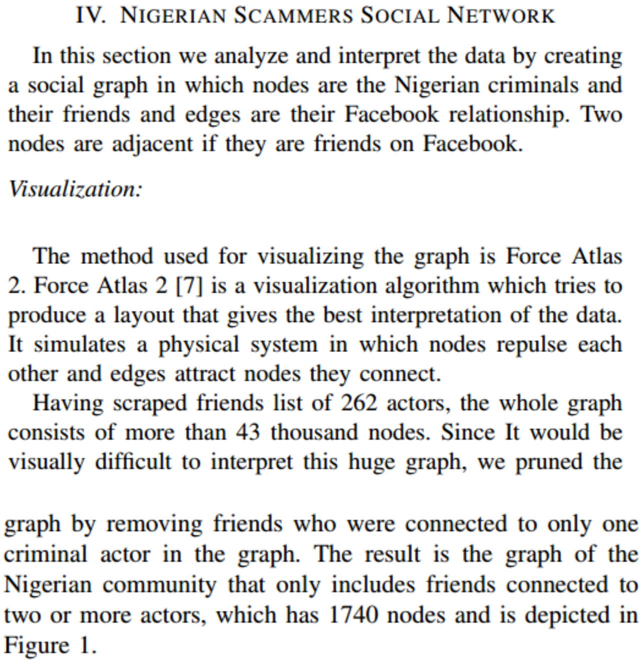
Fig. 1. Graph of Nigerians, discarding the friend nodes connected only to one actor. Two densely connected components of the graph are labeled as A and B

* Corresponding author:
drmarciapinheiro@gmail.com (M. R. Pinheiro)

Published online at http://journal.sapub.org/mijpam

I2 could have produced a very similar graph to the one above: *IBM i2 Analyst's Notebook is a visual analysis tool that helps you turn data into intelligence. The solution provides innovative features such as connected network visualizations, social network analysis, and geospatial or temporal views to help you uncover hidden connections and patterns in data. This insight can help you better identify and disrupt criminal, cyber and fraudulent threats* (IBM, 2017).

This is the explanation for the graph we have just observed (Sarvari et al, 2014):



IV. Nigerian Scammers Social Network

In this section we analyze and interpret the data by creating a social graph in which nodes are the Nigerian criminals and their friends and edges are their Facebook relationship. Two nodes are adjacent if they are friends on Facebook.

Visualization:

The method used for visualizing the graph is Force Atlas 2. Force Atlas 2 [7] is a visualization algorithm which tries to produce a layout that gives the best interpretation of the data. It simulates a physical system in which nodes repulse each other and edges attract nodes they connect.

Having scraped friends list of 262 actors, the whole graph consists of more than 43 thousand nodes. Since It would be visually difficult to interpret this huge graph, we pruned the graph by removing friends who were connected to only one criminal actor in the graph. The result is the graph of the Nigerian community that only includes friends connected to two or more actors, which has 1740 nodes and is depicted in Figure 1.

Force Atlas 2 comes connected to the Gephi Software (Gephi, 2017), and it is a continuous graph layout algorithm for network visualisation (Jacomy et al, 2014). Gelphi (2017) let us know that the software is produced independently, and therefore, in principle, there is no connection between it and IBM or its i2.

Sarvari et al (2014) also present our next graph.

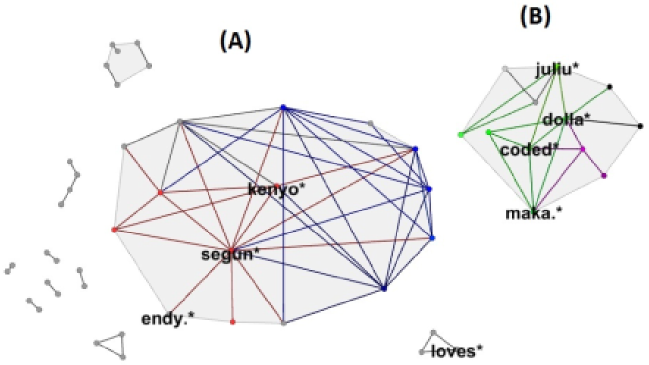
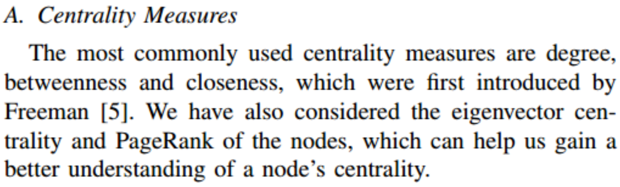


Fig. 2. Graph of connections among Nigerian actors. Actors without any connection to other actors are discarded. Nodes among top-10 actors in centrality measures (introduced in section V and Table II) are labeled by their names. Nodes within the same community (introduced in section VII) are colored the same. Components labeled A and B are subsets of two densely connected components with the same labels in Figure 1.

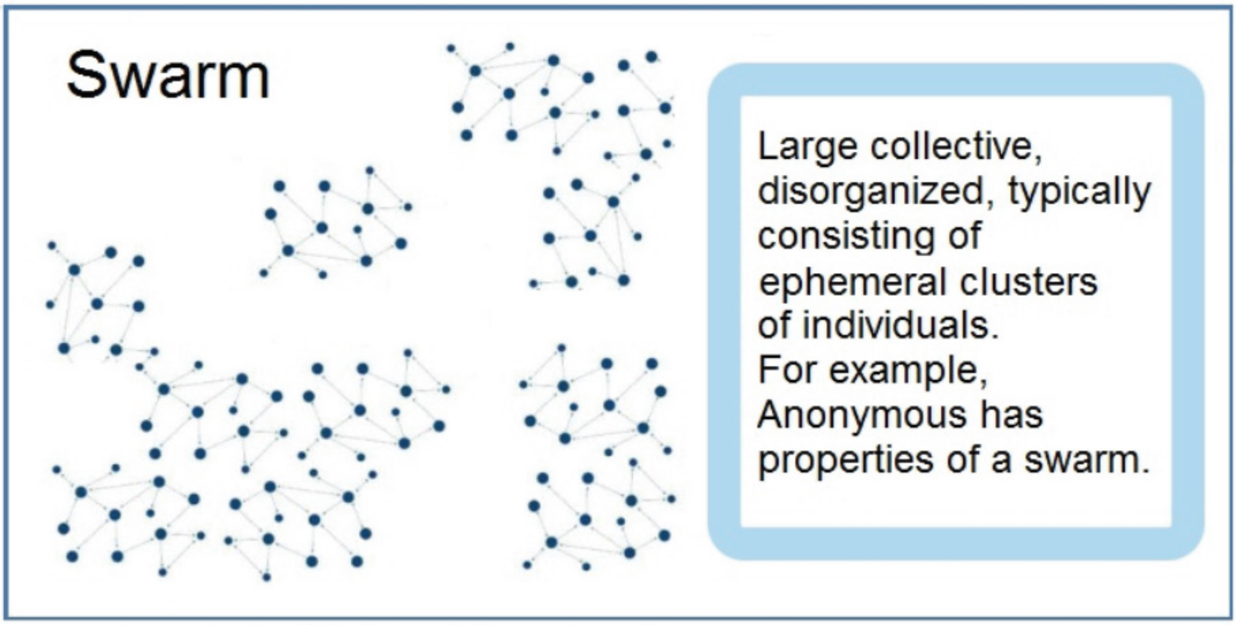


A. Centrality Measures

The most commonly used centrality measures are degree, betweenness and closeness, which were first introduced by Freeman [5]. We have also considered the eigenvector centrality and PageRank of the nodes, which can help us gain a better understanding of a node's centrality.

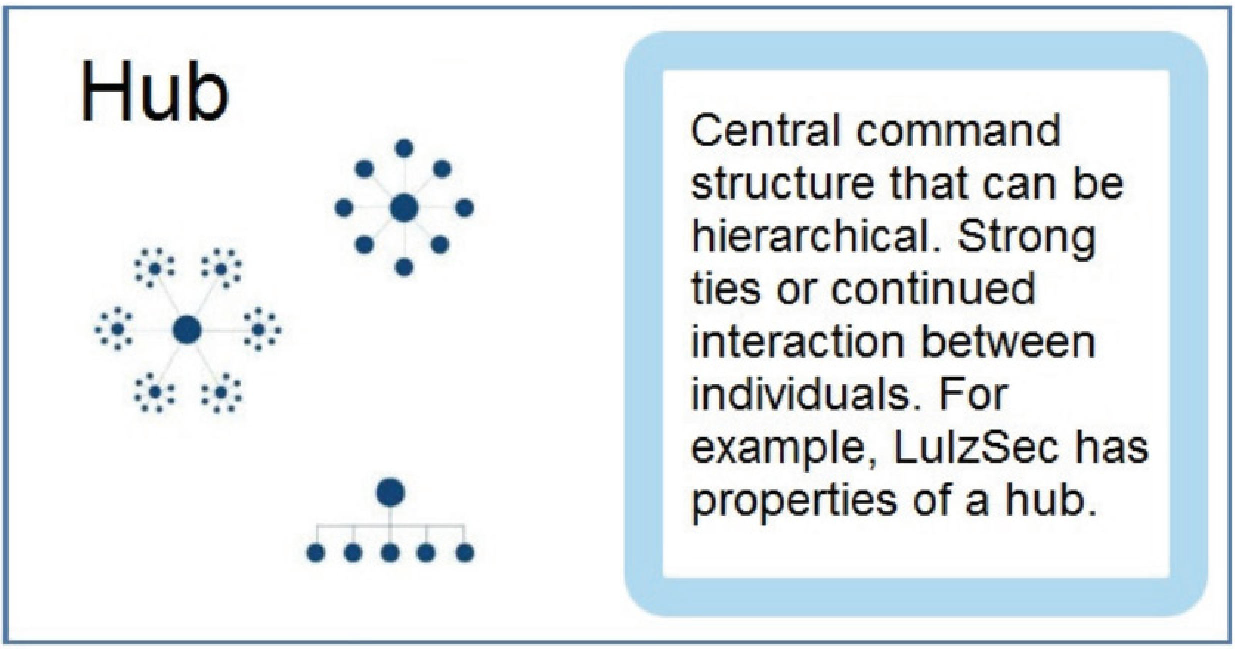
All the concepts mentioned above (centrality measures, degree, betweenness, and closeness) are seen in i2 and degree is part of the basics for Graph Theory (Moura, 2017). I2 has that all in its Social Analysis Tools (IBM, 2017a).

Broadhurst et al (2014) brings pictorial descriptions of the configuration or geometry of the gangs but does not seem to relate those to Graph Theory. See:



Large collective, disorganized, typically consisting of ephemeral clusters of individuals. For example, Anonymous has properties of a swarm.

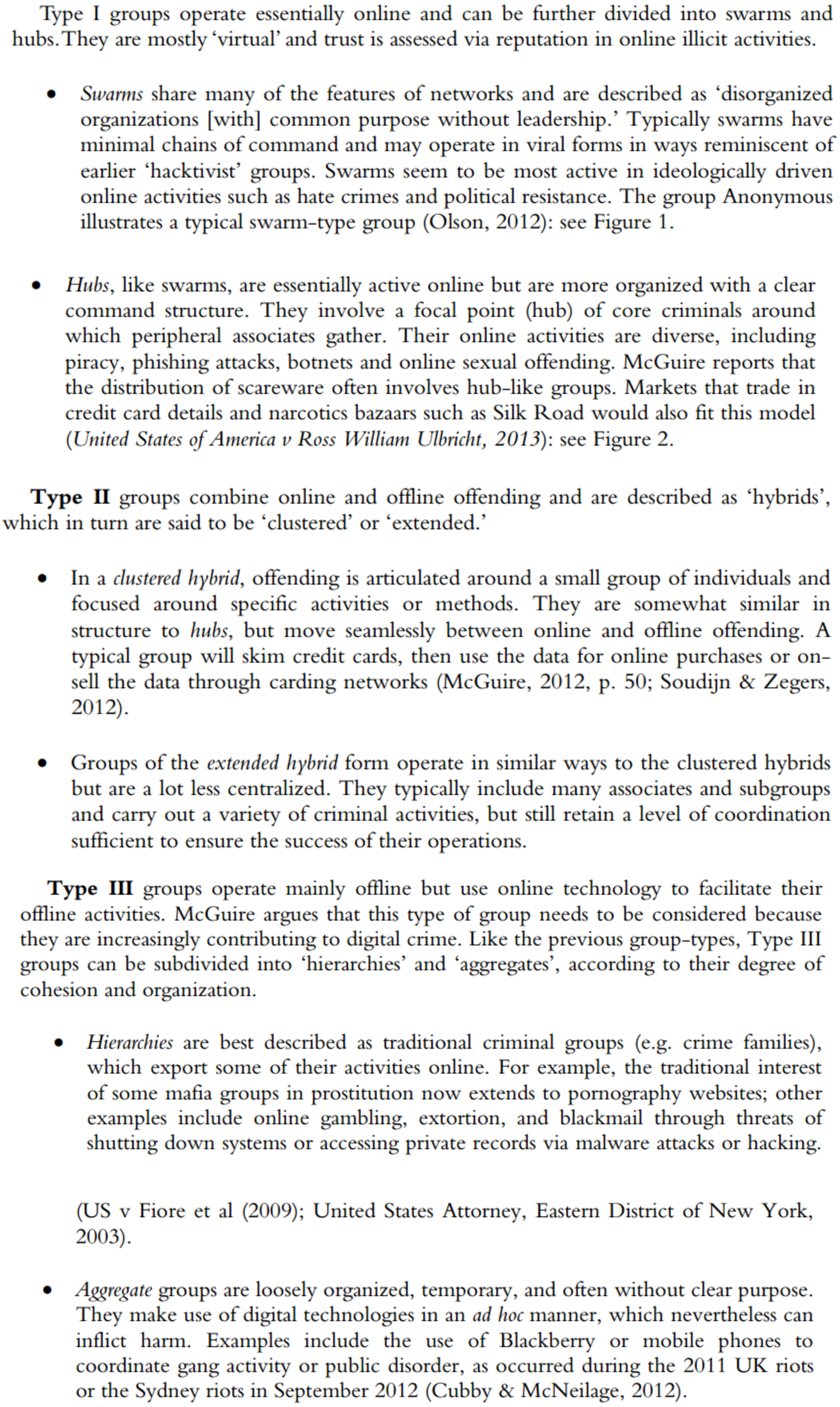
Figure 1: Simplified visual illustration of a swarm.



Central command structure that can be hierarchical. Strong ties or continued interaction between individuals. For example, LulzSec has properties of a hub.

Figure 2: Simplified visual illustration of a hub.

And here the description of the objects provided by Broadhurst et al (2014):



Type I groups operate essentially online and can be further divided into swarms and hubs. They are mostly 'virtual' and trust is assessed via reputation in online illicit activities.

- *Swarms* share many of the features of networks and are described as 'disorganized organizations [with] common purpose without leadership.' Typically swarms have minimal chains of command and may operate in viral forms in ways reminiscent of earlier 'hacktivist' groups. Swarms seem to be most active in ideologically driven online activities such as hate crimes and political resistance. The group Anonymous illustrates a typical swarm-type group (Olson, 2012): see Figure 1.

- *Hubs*, like swarms, are essentially active online but are more organized with a clear command structure. They involve a focal point (hub) of core criminals around which peripheral associates gather. Their online activities are diverse, including piracy, phishing attacks, botnets and online sexual offending. McGuire reports that the distribution of scareware often involves hub-like groups. Markets that trade in credit card details and narcotics bazaars such as Silk Road would also fit this model (*United States of America v Ross William Ulbricht, 2013*): see Figure 2.

Type II groups combine online and offline offending and are described as 'hybrids', which in turn are said to be 'clustered' or 'extended.'

- In a *clustered hybrid*, offending is articulated around a small group of individuals and focused around specific activities or methods. They are somewhat similar in structure to *hubs*, but move seamlessly between online and offline offending. A typical group will skim credit cards, then use the data for online purchases or on-sell the data through carding networks (McGuire, 2012, p. 50; Soudijn & Zegers, 2012).

- Groups of the *extended hybrid* form operate in similar ways to the clustered hybrids but are a lot less centralized. They typically include many associates and subgroups and carry out a variety of criminal activities, but still retain a level of coordination sufficient to ensure the success of their operations.

Type III groups operate mainly offline but use online technology to facilitate their offline activities. McGuire argues that this type of group needs to be considered because they are increasingly contributing to digital crime. Like the previous group-types, Type III groups can be subdivided into 'hierarchies' and 'aggregates', according to their degree of cohesion and organization.

- *Hierarchies* are best described as traditional criminal groups (e.g. crime families), which export some of their activities online. For example, the traditional interest of some mafia groups in prostitution now extends to pornography websites; other examples include online gambling, extortion, and blackmail through threats of shutting down systems or accessing private records via malware attacks or hacking.

(US v Fiore et al (2009); United States Attorney, Eastern District of New York, 2003).

- *Aggregate* groups are loosely organized, temporary, and often without clear purpose. They make use of digital technologies in an *ad hoc* manner, which nevertheless can inflict harm. Examples include the use of Blackberry or mobile phones to coordinate gang activity or public disorder, as occurred during the 2011 UK riots or the Sydney riots in September 2012 (Cubby & McNeilage, 2012).

So, those are the images and descriptions provided by Broadhurst et al (2014), but we do not see, amongst those, much Mathematics. That is why, in this paper, we try to do for Broadhurst et al's work (2014) the same we see done in Sarvari et al's paper (2014): We put as much Graph Theory as possible in place of what seems to be Information Technology lingo so far.

2. Development

A Swarm is a collection of Connected Graphs (Weisstein, 1999): From every node there is a path leading to any other node in each one of the graphs we see inside of the set with title Swarm. Each graph forming a Swarm is a simple graph (Weisstein, 1999a): no loops, no multiple edges, no weights, and no direction. They are all planar graphs (Weisstein, 1999b): no edges crossing over others. If the clustering of the graphs forming the swarm were high, the edges would cross. Each one of them has low clustering instead. Perhaps we need some reassurance in the direction of the graphical illustration representing one swarm and not several, so that we will quote another source before giving our suggestion.

Wall (2017) talks about a swarming model, which would be formations that exist for a limited amount of time to commit a certain type of crime. We then understand that members of a certain gang could specialize in a certain type of crime and come together only when they deem necessary for the commission of a certain offence. Concomitantly, we could have another share of this gang getting together to commit their particular crime, and end up with both results being put together to buy more shares of the company that they are all trying to control. We could also perhaps imagine other gangs doing the same, and, only because of that, the geometric aspect becoming something like what we see in Broadhurst et al's picture (2014). That would be an instantaneous graphical description of what is happening with our gangs of interest.

Kinetically, we could perhaps illustrate those moves through the image of whips hitting somewhere, since we usually see those retracting after the target has been hit: It is a splash, and then end.

Therefore:

A collection of graphs that are planar, connected, and simple is called a Swarm.

Hubs are sets of Starant Graphs (Pinheiro, 2012) because the criminals gather around a command point, a core. The lowest graph presented by Broadhurst et al (2014) makes us have doubts, and it is like that particular graph is not a Starant Graph: The top node will be represented as a core and all the other nodes, those around it, at the exception of the first, third, and last, will be connected to both neighboring nodes (left and right), and will therefore have degree two. The node that is located immediately under the top node has degree three, and is the most connected in Broadhurst's illustration (2014).

In this case, hubs are not yet sets of starant graphs: The nodes that are not the central node have a degree that varies from one to three and the central node does not yet have degree n (Pinheiro, 2012). If the idea of hierarchy, rather than source or core, is essential to explain the system, we can always put the middle node a bit higher in height, so that a bit of geometric manipulation of the graphical display attained in this way should give us optimal results.

We need to understand what Broadhurst et al (2014) meant by the sigmatoid (Pinheiro, 2015) *hub* in the hierarchical situation: From the drawing, we may think that everyone who is on the same line has got the same powers and access to the top node. In this case, the graph is badly built, since we should see a starant, but we are seeing something else. We may also think that to get to any node the top node needs to go through a protocol, which is basically communicating with the node right below it. That node then has to select right or left, and the right path to get to the node the top node intends to communicate with. If the right interpretation is the latter, the top node is less powerful than the node it connects to, so that the node right below it should be the center of all, since the top one is clearly not that who has the greatest connection power (the name is hub). In any hypothesis, there is a mistake with this representation. If only orders circulated in this network, and the top node passed them to the node right below it, we could believe in hierarchy. That would be perhaps a monarchic network, rather than just hierarchic. We then notice that there would be a few spheres of power, since power would be measured according to the distance from the top node. In this case, the node immediately to the left or right of the node that is right below the top node would be a second-in-command node. Basically, the lowest in this network, who would perhaps compare to the diggers from the army (Commonwealth, 2017), would be the nodes that are on the extremes of the segment containing the second-in-command. In this case, there is also a mistake in the graph, since we should have put those in a lower position than the rest: The perfect alignment would have to imply equal powers in geometric display that is intended to be informative, and therefore mathematical. According to Karawan (2008), hubs command connectivity, and are responsible for connecting nodes with fewer connections. We could however interpret hubs in a different way when we say a network is called hub, like if a node is called hub, that is the definition, but if the own formation, the own geometry of the network, is called hub, then we have another definition. If the definition were connector, then we could not imagine that it connects only to one node right below it in a direct way, since just that one would connect to at least three in a direct way, being therefore more powerful, and, according to the definition just given, a better candidate for the label hub. That would again bring inconsistencies if we talk about Mathematics, so that we must think a bit more about this. Eliott (2014) solves the puzzle: *The most common organizational forms are chain networks and hub-and-spoke* ((Kaushik, 2012): Hub and spoke are names taken from a bicycle wheel where the hub is its center and spokes originate from this center and terminate at the circumference) *networks (sometimes also called star or wheel networks)*. Weisstein (1999c) lets it clear that the wheels lack the ability to allow for direct (one-step/edge) connections between one node and a node that is two nodes away from it (*in a wheel graph, the hub has degree n-1, and other nodes have degree 3. Wheel graphs are 3-connected*) on the wheel. Because it is possible that one node connects to the node that is two nodes away from it on the wheel, the best representation for the members of the formation Broadhurst et al (2014) have called hub is the Starant Graph, not the wheel.

We confirm this when reading Broadhurst et al's words (2014): *Strong ties or continued interaction between individuals*.

Having discussed the sigmatoids Swarm and Hub in this paper, we think that Broadhurst et al (2014) should have written Swarms and Hubs in place of Swarm and Hub when they pictorially described the formations they were singling out.

As a consequence, we have that **Hubs** (in Cyber Crime) **is the network configuration that is associated with Starant Graphs in Graph Theory**. **Swarms is a collection of graphs that are planar, connected, and simple.**

Having dealt with Broadhurst et al's Type I groups (2014), we now address those that are classified as Type II (Broadhurst et al, 2014):

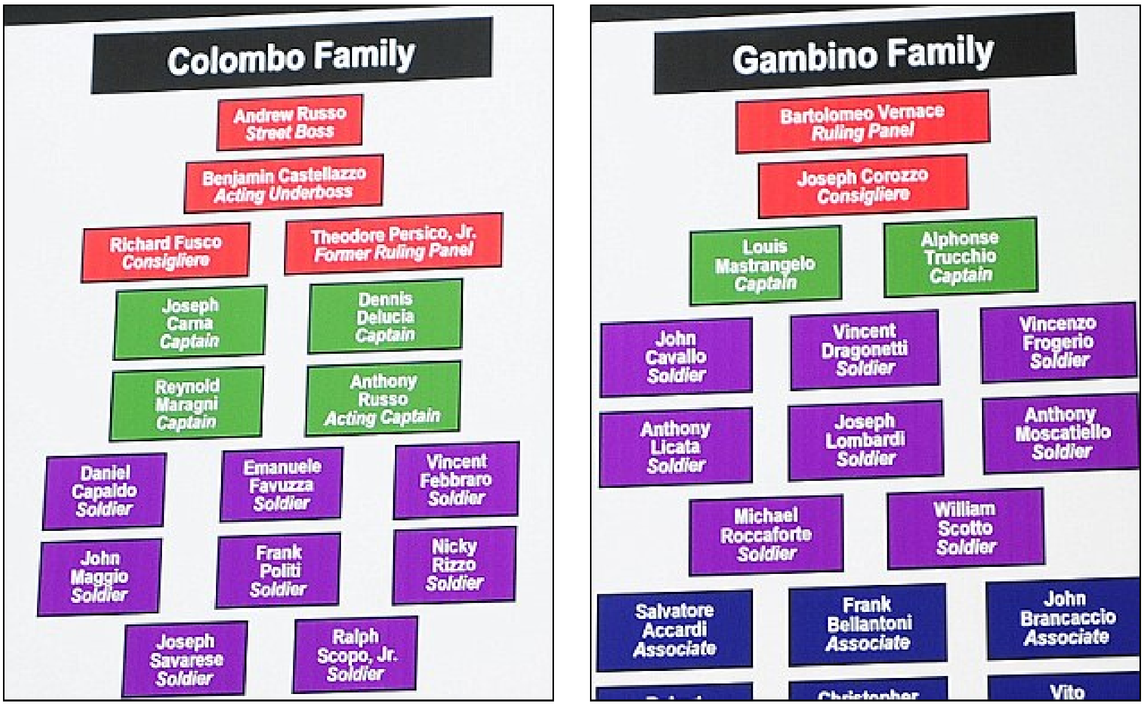
A Clustered Hybrid seems to be a small group that is well connected, so say again a Starant Graph, but what makes it worthy of the note is the fact that it operates in hybrid mode, so off- and on- line.

In this case, we could be calling it Starant Graph of Mixed or Hybrid Operation Mode.

Extended Hybrid groups seem to be Clustered Hybrid groups with a pulverized managerial core, so that we could probably describe them as a set of Starant Graphs where all the central nodes are also end-points.

That is the rewording of Type II. Now let's investigate Type III:

Hierarchies sound a lot like mafia. Daily (2011) brings the following image as a graphical representation of the relationships or communication channels inside of mafia:


Colombo Family
Andrew Russo Street Boss
Benjamin Castellazzo Acting Underboss
Richard Fusco Consigliere
Theodore Persico, Jr. Former Ruling Panel
Joseph Cama Captain
Dennis Delucia Captain
Reynold Maragni Captain
Anthony Russo Acting Captain
Daniel Capaldo Soldier
Emanuele Favuzza Soldier
Vincent Febbraro Soldier
John Maggio Soldier
Frank Politi Soldier
Nicky Rizzo Soldier
Joseph Savarese Soldier
Ralph Scopo, Jr. Soldier
Gambino Family
Bartolomeo Vernace Ruling Panel
Joseph Corozzo Consigliere
Louis Mastrangelo Captain
Alphonse Trucchio Captain
John Cavallo Soldier
Vincent Dragonetti Soldier
Vincenzo Frogerio Soldier
Anthony Licata Soldier
Joseph Lombardi Soldier
Anthony Moscatiello Soldier
Michael Roccaforte Soldier
William Scotto Soldier
Salvatore Accardi Associate
Frank Bellantoni Associate
John Brancaccio Associate
Christopher
Vito

Who's in charge: The colour-coded chart shows the hierarchy of some of the most feared Mafia families in New York - the boss, underboss, captains and soldiers are depicted on different levels of the chart

Here we see the idea of levels of power connected to distance from the top. The more levels to the bottom we go, the more people we see, so that the last level would always be the most populated and therefore the previous level would contain the best candidates to hub in that particular network.

Aggregate groups are perhaps groups without a leader; temporary groups created to commit some offence. In this case, a Circulant Graph could be the ideal representation of an aggregate group. A Circulant not a wheel because we do not want to lose the flexibility involved: Allowing for as many connections as needed between nodes.

3. Conclusions

We here were worried about suggesting or even creating, if necessary, mathematical jargon, so that also mathematicians, and those who have similar thinking processes, can connect to Broadhurst et al's work (2014), and create even more ways to deal with cybercrime data.

Different from a few other authors from Cyber Crime whose work we had access to, Broadhurst et al (2014) bring pictorial descriptions of the configuration or geometry of the gangs, but they do not seem to relate those to Graph Theory.

After discussing the sigmatoids in depth, we decided for the following definition of Swarms and Hubs: A collection of graphs that are planar, connected, and simple is called a Swarms; the network configuration that is associated with Starant Graphs in Cyber Crime is Hubs: Hubs is a collection of Starant Graphs. The same happens to Clustered Hybrids: They would be associated with Starant Graphs in Graph theory. Circulant Graphs are probably the best way to represent aggregate groups.

At least one pictorial description of real-life criminal network of Broadhurst et al (2014) seems not to be so accurate: We probably need a Starant Graph with a central node that appears to be above the other nodes in the pictorial description that we refer to (last one, bottom, hubs) instead of what we currently have.

Some authors have suggested that the hub-and-spoke networks should be better represented by stars or wheels. They are probably wrong, and the best representation is the Starant Graph instead because this graph can become a star, a wheel, and any other network configuration that we seem to see in a hub-and-spoke network.

REFERENCES

Kammerdiner, A. R. (2014). *Statistical Techniques for Assessing Cyberspace Security*. (C. Vogiatzis, J. L. Walteros, & P. M. Pardalos, Eds.). Springer. Retrieved from https://link-springer-com.simsrad.net.ocs.mq.edu.au/chapter/10.1007%2F978-3-319-10046-3_9

Belavkin, R. V., Pham, K., Pachter, M., Pachter, M., Pham, K., Schieber, T. A., … Ravetti, M. G. (2014). *Dynamics of Information Systems*. (C. Vogiatzis, J. L. Walteros, & P. M. Pardalos, Eds.). Springer. Retrieved from https://link-springer-com.simsrad.net.ocs.mq.edu.au/chapter/10.1007%2F978-3-319-10046-3_9

Sarvari, H., Abozinadah, E., Mbaziira, A., & McCoy, D. (2014). Constructing and Analyzing Criminal Networks. *IEEE Security and Privacy Workshops*. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6957290

IBM. (2017). IBM i2 Analyst's Notebook. Retrieved from https://www.ibm.com/us-en/marketplace/analysts-notebook

Gephi.org. (2017). About. Retrieved October 29, 2017, from https://gephi.org/about/

Jacomy, M., Venturin, T., Heymann, S., & Bastian, M. (2014). ForceAtlas2, a Continuous Graph Layout Algorithm for Handy Network Visualization Designed for the Gephi Software. *Plos One*. https://doi.org/10.1371/journal.pone.0098679

Moura, L. (2017). Elements of Graph Theory. University of Ottawa. Retrieved from http://www.site.uottawa.ca/~lucia/courses/2101-17/lecturenotes/08Graphs-CSI2101-2017.pdf

IBM. (2017a). IBM i2 Analyst's Notebook Social Network Analysis *IBM Offering Information* Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZZW03174USEN

Broadhurst, R., Grabosky, P., Broadhurst, M., & Chon, S. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups Engaged in Cyber Crime. *International Journal of Cyber Criminology*, *8*(1), 1–20. Retrieved from http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf

Weisstein, E. W. (1999). Connected Graph. Retrieved August 28, 2016, from http://mathworld.wolfram.com/ConnectedGraph.html

Weisstein, E. W. (1999a). Simple Graph. Retrieved August 28, 2017, from http://mathworld.wolfram.com/SimpleGraph.html

Weisstein, E. W. (1999b). Planar Graph. Retrieved August 28, 2017, from http://mathworld.wolfram.com/PlanarGraph.html

Wall, D. S. (2017). *Crime and Deviance in Cyberspace*. Routledge. Retrieved from https://books.google.com.au/books?id=ZD0rDwAAQBAJ&dq=swarm+cyber+crime+definition&source=gbs_navlinks_s

Pinheiro, M. R. (2012). Starants: A New Model for Human Networks. *Asian Journal of Current Engineering*, *1*, 259–265. Retrieved from http://www.scirp.org/(S(i43dyn45teexjx455qlt3d2q))/reference/ReferencesPapers.aspx?ReferenceID=1690016

Pinheiro, M. R. (2015). Words for Science. *Indian Journal of Applied Research*, *5*(5), 19–22. Retrieved from https://www.worldwidejournals.com/ijar/articles.php?val=NjQ0MQ==&b1=853&k=214

Commonwealth of Australia. (2017). Diggerworks. Retrieved November 1, 2017, from https://www.army.gov.au/our-work/partnerships/diggerworks

Karawan, I. A., McCormack, W., & Reynolds, S. E. (Eds.). (2008). *Values and Violence: Intangible Aspects of Terrorism*. Springer Science & Business Media. Retrieved from https://books.google.com.au/books?id=ol-63orWw68C&dq=hub+hierarch+crime+network&source=gbs_navlinks_s

Elliott, L. (2014). *Criminal Networks and Black Markets in Transnational Environmental Crime*. Retrieved from http://bellschool.anu.edu.au/sites/default/files/publications/attachments/2016-09/elliott_criminal_networks_chapter_2016.pdf

Kaushik, N. (2012). 'Difference Between a Hub, a Spoke, and a Point to Point' *DifferenceBetween.net* Available at: http://www.differencebetween.net/technology/hardware-technology/difference-between-a-hub-a-spoke-and-a-point-to-point/ Accessed 2.11.2017

Weisstein, E. W. (1999c). Wheel Graph. Retrieved October 29, 2017, from http://mathworld.wolfram.com/WheelGraph.html

Daily Mail Reporter. (2011). The Mafia Family Tree: FBI Flowchart Reveals 127 "mobsters" Arrested in Biggest ever Blitz on New York's Crime Empires. Retrieved October 31, 2017, from http://www.dailymail.co.uk/news/article-1348951/127-mobsters-arrested-biggest-blitz-New-Yorks-crime-empires.html