Sveučilište u Rijeci
University of Rijeka
http://www.uniri.hr

Polytechnica: Journal of Technology Education, Volume 4, Number 1 (2020)
Politehnika: Časopis za tehnički odgoj i obrazovanje, Volumen 4, Broj 1 (2020)

Politehnika
Polytechnica
http://www.politehnika.uniri.hr
cte@uniri.hr

DOI: https://doi.org/10.36978/cte.4.1.2

Prethodno priopćenje
Preliminary note
UDK 004.738.5:343.53

A new Systemic Taxonomy of Cyber Criminal activity

Matej Babič
Faculty of Information Studies,
Ljubljanska cesta 31a,
Novo mesto, Slovenia
babicster@gmail.com

Damir Purković
Study of Polytechnics
University of Rijeka
Sveučilišna avenija 4, Rijeka
damir@uniri.hr

Abstract

Cybercrime commonly refers to a broad range of different criminal activities that involve computers and information systems, either as primary tools or as primary targets. Cybercrime Science combines the methodology of Crime Science with the technology of Information Security. The few existing taxonomies of Cybercrime provide only general insights into the benefits of information structures; they are neither complete nor elaborated in a systemic manner to provide a proper framework guided by real system-principles. The main problem with such taxonomies is the inability to dynamically upgrade, which is why there is no timely cybersecurity actions. The current and past approaches were based mainly on the technical nature of cyberattacks and such approaches classified the impact of the activities from a criminological perspective. In this article, we present a systemic taxonomy of Cybercrime, based on definitions of the field items and the related data specifications. We develop a new method for estimating the fractal dimension of networks to explore a new taxonomy of Cybercrime activity. This method can serve to dynamically upgrade taxonomy and thus accelerate the prevention of cybercrime.

Keywords: *cybercrime, taxonomy, cyber-criminal, terrorists, system theory, network, fractals.*

1 Introduction

Network and computer attacks have become pervasive in today's world. Any computer connected to the Internet is under threat from viruses, worms and attacks from hackers. Crime Science has been developed as a reaction to the difficulty of traditional Criminology in effectively preventing and controlling crime. The focus of Crime Science is on the opportunity for crime. Crime Science is the application of the methods of Science to the prevention or detection of disorder, in particular, of crime. Information Security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, in order to provide integrity, confidentiality, and availability. The growth and severity of Cyber-attacks has significantly increased the costs to society. It is estimated that these attacks are costing the global economy billions of dollars each year.

Cybercrime maybe defined as a crime in which computer networks are the target or a substantial tool. Varieties of definitions of Cybercrime are found in literature; they mostly depend on the purpose for which the definition is needed. Thus, Yazdanifard et al. (2011) define cybercrime as any type of intentional criminal scheme that is computer or / and mediated through the Internet. Such a description covers a wide range of cybercrime, without taking into account the dual model of criminal schemes within cyber space (Ibrahim, 2016). Ogwezzy (2012) states that "cybercrime" means crimes committed by the use of a computer as opposed to "computer crime" which refers to acts against the computer and

data or programs contained therein. Although the computer and its content are direct targets in computer crimes, the significance of cybercrime involves the use of computers and / or the Internet to commit crimes (McGuire and Dowling, 2013). The terms 'computer crime' and 'cybercrime' are intertwined; their entities are intertwined and therefore difficult to disentangle (Ibrahim, 2016). The most common targets of cyber-attackers are: entertainment, hacktivism, financial gain, spying and revenge (Singh Brar and Kumar, 2018). According to the literature analyzed the term cybercrime includes all unlawful attacks and threats to attack computers, networks and information stored in them for the purpose of causing financial and non-financial harm to persons, the economy and society. Various definitions exist for the term 'Cyberterrorism', just as different definitions exist for 'terrorism'. Cyber terrorism is the convergence of cybercrime and terrorism, and essentially consists of using computer technology to engage in terrorism (Brenner, 2006). While crimes are most often committed for personal reasons, such as personal gain or desires, terrorism and cyberterrorism are most often "political" (Brenner, 2006), as acts to intimidate or coerce a civilian population and governments policies. To qualify as a Cyber terrorist attack, it should result in violence against persons or property, or, at least, cause fear and terror. Such definition includes attacks against critical infrastructure. In instances of Cyber terrorism, technology (most prominently the internet) is used to achieve the same goals as more traditional weapons—to undermine citizens' faith in government by undermining their ability to maintain and provide the critical infrastructure systems that form the foundation of everyday life for ordinary citizens.

The development of taxonomy is a theoretical study of classification and identification (Bailey, 1994) whose result, in order to differ from the "typology" typical of the social sciences, requires empirical validation during the creation process (Land et al, 2013). Taxonomy development in general is concerned with the classification of knowledge or ideas in order to improve storage and retrieval of information and 'knowledge about knowledge'. At the most simple level, taxonomies can be maintained manually, through human coding and organization of data, whereas, at the more complex end of the spectrum, statistical algorithms, studying word frequency, placement, grouping and pattern analysis can be, alternatively, applied. One of the key difficulties encountered in creating a taxonomy of Cybercrime arises from the challenge of specifying a universal definition of crime, which is a legal concept. In this regard, the main problem is the dynamic alignment of the taxonomy in order to differentiate cyber-criminal activities and thus indirectly act to reduce the damage caused. For the purpose of dynamically adjusting the taxonomy, appropriate theories and methods can be used that can also accelerate the fight against cybercrime.

This paper will examine cybercrime from a variety of perspectives. Firstly, we select existing classifications related to cybercrime and cyberterrorism, including attackers, attack characteristics, objective, practice, effect motivations and other facets of the phenomenon. These classifications lead to the formation of a Cybercrime Taxonomy. This taxonomy combines, and in some case expands upon, the elements defined in these classifications in order to form the basis of a holistic taxonomy of cybercrime and cyberterrorism. The purpose of a classification or taxonomy is to provide a useful and consistent means of classifying Cybercrime. Currently, cyberattacks are often described differently by different organizations, resulting in confusion as to what a particular attack actually is. Taxonomy also allows for previous knowledge to be applied to new cybercrime while, at the same time, providing a structured way to view such crime. Another of the proposed taxonomy's goals is to provide a holistic approach to classifying Cyber crime, so that all parts of the attacks are taken into account, while at the same time preserving the integrity of the taxonomy. We use method graph theory and fractal geometry to explore networks of taxonomies of Cybercrime activity. Finally, we present a linear model of Cybercriminal activity. New taxonomy can be used as a model or basis for the further development and differentiation of new types of cybercrime activities.

2 Existing taxonomies and previous work

Alkaabi et al. (2010) proposed a Type I and Type II classifications of cybercrime, with detailed subclasses. The Type I of cybercrimes "include crimes where the computer, computer network, or electronic device is the target of the criminal activity". Type II crimes "include crimes where the computer, computer network, or electronic device is the tool used to commit or facilitate the crime".

Ghernaouti (2013) proposed a three dimensional categorization of cybercrime, distinguishing cybercrime from cyber conflicts, wars and terrorism. The field of network and computer security has seen a number of taxonomies aimed at classifying security threats, such as computer and network attacks and vulnerabilities.

Newman (2009) refers to cybercrime as behaviour in which computers or networks are a tool,

a target, or a place of criminal activity (Newman, 2009). According to such a definition, cybercrime is focused on human behaviour, and computers or networks are a tool, target, or place of criminal activity. These are basically places where forensic analysis can be performed and evidence of one's behavior is collected.

Howard (1997) posited in his doctoral dissertation that any taxonomy must have a certain set of properties. He created a new taxonomy with reference to types of attackers, tools used, and access of information, designed to elicit why the computer was broken into, what was used in the access, the results of the break-in, and the objectives of the attack. Howard's work was notable because he included attackers, results and objectives as classification categories, expanding threat taxonomies beyond the technical details of an attack to include more intangible factors such as the attacker's motivation for conducting an attack. He presented a taxonomy of computer and network attacks. The approach taken was broad and process-based, taking into account an amalgam of factors.

Lindqvist and Jonsson (1997) enumerated a similar list, changing only two categories. Probably one of the best-known taxonomies is the Defence Advanced Projects Agency (DARPA) 'attack' taxonomy. This taxonomy was developed in 1998 for classifying attacks in order to simplify the process of evaluating IDSs. A comprehensible taxonomy will be capable of being understood by those who are in the security field as well as those with a different type of interest in it.

Amoroso (1994) added a few more properties. For a taxonomy to be complete/exhaustive, it should account for all possible attacks and provide categories accordingly. While it is difficult to provide a taxonomy that is complete or exhaustive, it can be achieved through the successful categorization of actual attacks.

Krsul (1998) and Bishop (1995) have compiled their own respective lists. Krsul quotes numerous encyclopedias to state, "A taxonomy is the theoretical study of classification, including its bases, principles, procedures and rules". Bishop (1995) has made several important contributions to the field of security taxonomies. He agrees with Krsul stating that taxonomies should classify properties of vulnerabilities and not the vulnerability itself. Bishop's approach is interesting, as, instead of a flat or tree-like taxonomy, he uses axes. In our proposed taxonomy, a similar structure is used albeit with different axes variables.

Lough (2001) proposed another taxonomy called VERDICT (Validation Exposure Randomness Deallocation Improper Conditions Taxonomy) which is based upon the characteristics of attacks. Lough's VERDICT criteria of taxonomy is used as the foundation for the recourse model's taxonomy. This method uses a strategy of classification based on the common denominators revealed by Lough's exhaustive search of the literature.

Singh Brar and Kumar (2018) bring a transparent taxonomy of cybercrime as well as cyberattacks based on cybersecurity principles. In doing so, they focus on cybersecurity, not taxonomy itself. However, it is clear that cybersecurity cannot be achieved without a dynamically aligned taxonomy that will identify new and unknown ways of compromising that security.

3 Proposal for a new prototype taxonomy of Cybercriminal activity and method for analysis

In this part of the paper, we present a proposal for a new cybercrime taxonomy, namely the development of a dynamic taxonomy upgrade model that can serve as a basis for computer-aided identification of new forms of cyberattack. Therefore, the main contribution of this proposal is to apply a specific methodology for the analysis and classification of cybercrime activities. In Figs. [3-5] we present our new taxonomy of cybercrime activity. In doing so, we connect other authors taxonomies of cybercrime and implement it is into our own innovative taxonomy. In addition, our taxonomy presents a profile of cybercrime activity. Since the taxonomy of cybercrime is very important, we used different methods for analysis, which are also a template for the future dynamic development of the taxonomy.

Firstly, we use graph theory (Zhang, 2012) to analyse our taxonomy of cybercrime activity. A dendrogram is a network structure, which generates a dendrogram plot of the hierarchical binary cluster tree. A dendrogram consists of many U-shaped lines that connect data points in a hierarchical tree. The height of each U represents the distance between the two data points being connected. A dendrogram may be presented as a graph (Fig. 1). Graph theory is a suitable playground for the exploration of proof techniques in discrete mathematics, and its results have applications in many areas such as computing, social, and natural sciences. Network analysis has been developing and flourishing for several decades. Network analysis is popular in every type of academic social science, applied social science (such as marketing), studies of nonhuman social life, branches of mathematics, computer science, and even physics. A proposal taxonomy of Cybercrime activity is presented as a graph in Fig. 6. In this graph, we analyse topological properties. Each colour in graph

present subsection of taxonomy of Cybercrime activity from dendrogram.

Centrality is a measure of the relative importance of graph vertex according to given criteria. Betweenness measures are a type of centrality measure used often in the analysis of social or citation networks. They tend to evaluate the influence of each vertex on spreading information over the graph. Shortest-path betweenness is a widely used centrality measure defined as a fraction of the shortest paths between pairs of vertices in a graph that pass through a given vertex, i.e.,

$$BC(v)=\sum_{s\neq v\neq t\in V} s\neq t \frac{\sigma_{st(v)}}{\sigma_{st}}.$$

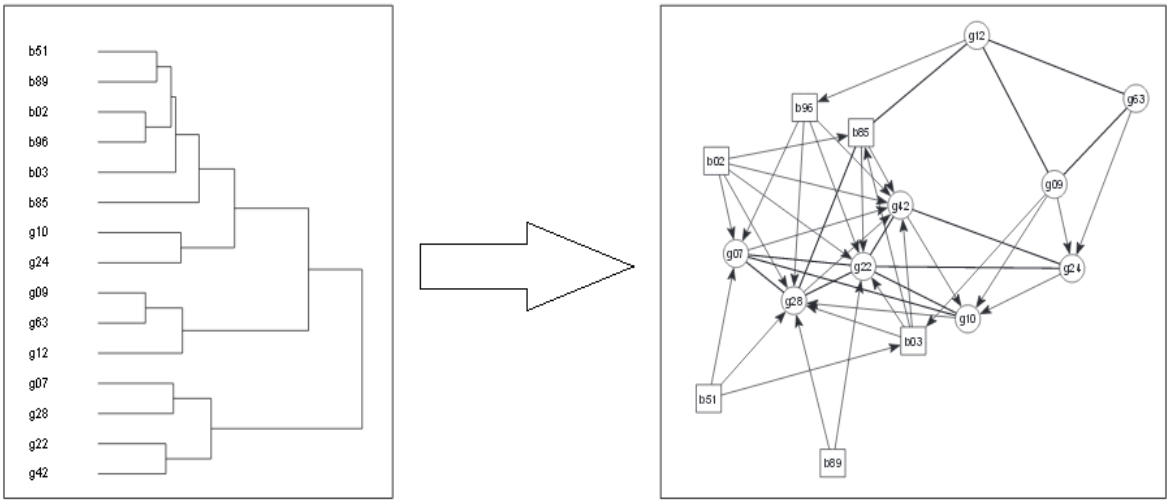

Figure 1. Dendrogram … presented with graph theory

"Network density" describes the portion of the potential connections in a network that are actual connections. A "potential connection" is a connection that could potentially exist between two "nodes"—regardless of whether or not it actually does. The density *D* of a network is defined as a ratio of the number of edges E to the number of possible edges, giving

$$D=\frac{2E}{N\times(N-1)}.$$

Historically first, and conceptually simplest, is degree centrality, which is defined as the number of links incident upon a node (i.e., the number of ties that a node has). The degree can be interpreted in terms of the immediate risk of a node catching whatever is flowing through the network (such as a virus, or some information). In the case of a directed network (where ties have direction), we usually define two separate measures of degree centrality, namely indegree and outdegree. Accordingly, indegree is a count of the number of ties directed to the node and outdegree is the number of ties that the node directs to others. When ties are associated to some positive aspects such as friendship or collaboration, indegree is often interpreted as a form of popularity, and outdegree as gregariousness.

The degree centrality of a vertex v, for a given graph *G:=(V, E)* with *|V|* vertices and *|E|* edges, is defined as

$$C_D(v)=deg(v).$$

The Platt index *F(G)* of a graph *G* is defined as the total sum of degrees of edges in a graph,

$$F(G)=\sum_{i=1}^{M} D(ei),$$

where *D (ei)* denotes degree of the edge *ei*, i.e., number of edges adjacent to ei and *M* denotes the number of edges.

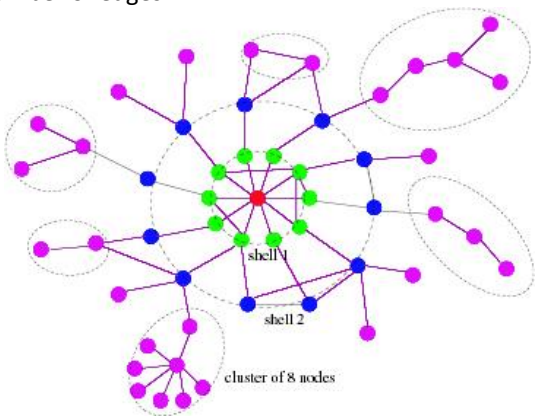

Figure 2. Shell and cluster (component) structure of the boundary of a network

Secondly, we use fractal geometry (Barton, 1995) to analyse the taxonomy of cybercrime activity. The study of complex networks has received a tremendous amount of attention recently, mainly because they are used in several disciplines of science, such as in information technology (World Wide Web, Internet), sociology (social relations), biology (cellular networks) etc. We analyse network taxonomy of Cybercrime activity. The key to fractal geometry is fractal dimension, which determines the complexity of the fractal object. Network taxonomy of Cybercrime activity is very complex. There exist many methods for the determination of complexity, namely box counting, cluster growing method, and fractal scaling in scale-free networks (Feder, 1988). We use the method of fractal properties of network boundaries. We use the concept of the fractal boundary of a complex network (Shao et al., 2013) to describe a set of nodes at a distance larger than the mean distance from a given node in the network. Most work on distances in networks have focused on the average, or typical distance, between vertices. It was found that the number of vertices at a large distance from an arbitrary vertex follows a power law distribution. Consider an *N*-vertex network with some degree distribution *P(k)*. Start from some arbitrary vertex and observe the vertices at distance *l* from this vertex. For *ER* networks and small *l*, the growth with *l* is approximately exponential. The average hop distance between vertices is approximately $\langle l \rangle \sim logN/log\ (\kappa-1)$ when κ is finite. In the following, we study the structure of layers with $l > l$. That is, we study the properties of the vertices at a distance l from an arbitrary vertex, where l is larger than the average distance in the network. We denote the size of clusters as sl and the average diameter of cluster as dl. We calculate the fractal dimension D from the equation $s_l \sim d_l^D$. Fig. 2 represent shell and cluster (component) structure of the boundary of a network. So, we can see how to calculate fractal dimension of network.

4 Results

Hierarchical clustering is one method for finding community structures in a network. The technique arranges the network into a hierarchy of groups according to a specified weight function. The data can then be represented in a tree structure known as a dendrogram. Hierarchical clustering can either be agglomerative or divisive depending on whether one proceeds through the algorithm by adding links to or removing links from the network, respectively. One divisive technique is the Girvan–Newman algorithm. In Fig. [3-5], a taxonomy of Cybercrime activity with dendrograms is presented. Hierarchical cluster analysis of n objects is defined by a stepwise algorithm, which merges two objects at each step, the two that have the least dissimilarity. Dissimilarities between clusters of objects can be defined in several ways; for example, the maximum dissimilarity (complete linkage), minimum dissimilarity (single linkage) or average dissimilarity (average linkage). Either rows or columns of a matrix can be clustered - in each case we choose the appropriate dissimilarity measure that we prefer. The results of a cluster analysis is a binary tree, or dendrogram, with *n –1* nodes. The branches of this tree are cut at a level where there is a lot of 'space' to cut them that is where the jump in levels of two consecutive nodes is large. A permutation test is possible to validate the chosen number of clusters that is to see if there really is a non-random tendency for the objects to group together. Networks of Cybercrime activity have Tree Topologies. Tree Topology integrates the characteristics of Star and Bus Topology. In Bus Topology, work station devices are connected by the common cable called Bus. After understanding these two network configurations, we can understand tree topology better. In Tree Topology, the number of Star networks are connected using Bus. This main cable seems like a main stem of a tree, and other star networks as the branches. It is also called Expanded Star Topology. Ethernet protocol is commonly used in this type of topology. There are some advantages of topologies of Cybercrime activity. They are an extension of Star and bus Topologies; so in networks where these topologies cannot be implemented individually for reasons related to scalability, tree topology is the best alternative. Expansion of the Network is possible and easy. In this regard, we divide the whole network into segments (star networks), which can be easily managed and maintained. Error detection and correction is easy. Each segment is provided with dedicated point-to-point wiring to the central hub. If one segment is damaged, other segments are not affected. However, there are some disadvantages of a topology of Cybercrime activity. Due to its basic structure, tree topology relies heavily on the main bus cable; if such cable breaks, the whole network is crippled. As more and more nodes and segments added, the maintenance becomes difficult. Scalability of the network depends on the type of cable used.

A network of cybercrime activity has 352 vertices and 338 nodes and has tree structure. Table 1 presents a fractal dimension of proposed taxonomy of cybercrime activity (*Taxonomy CC*) and another three existing taxonomy and its topological properties. FD BC present the fractal dimension of the network.

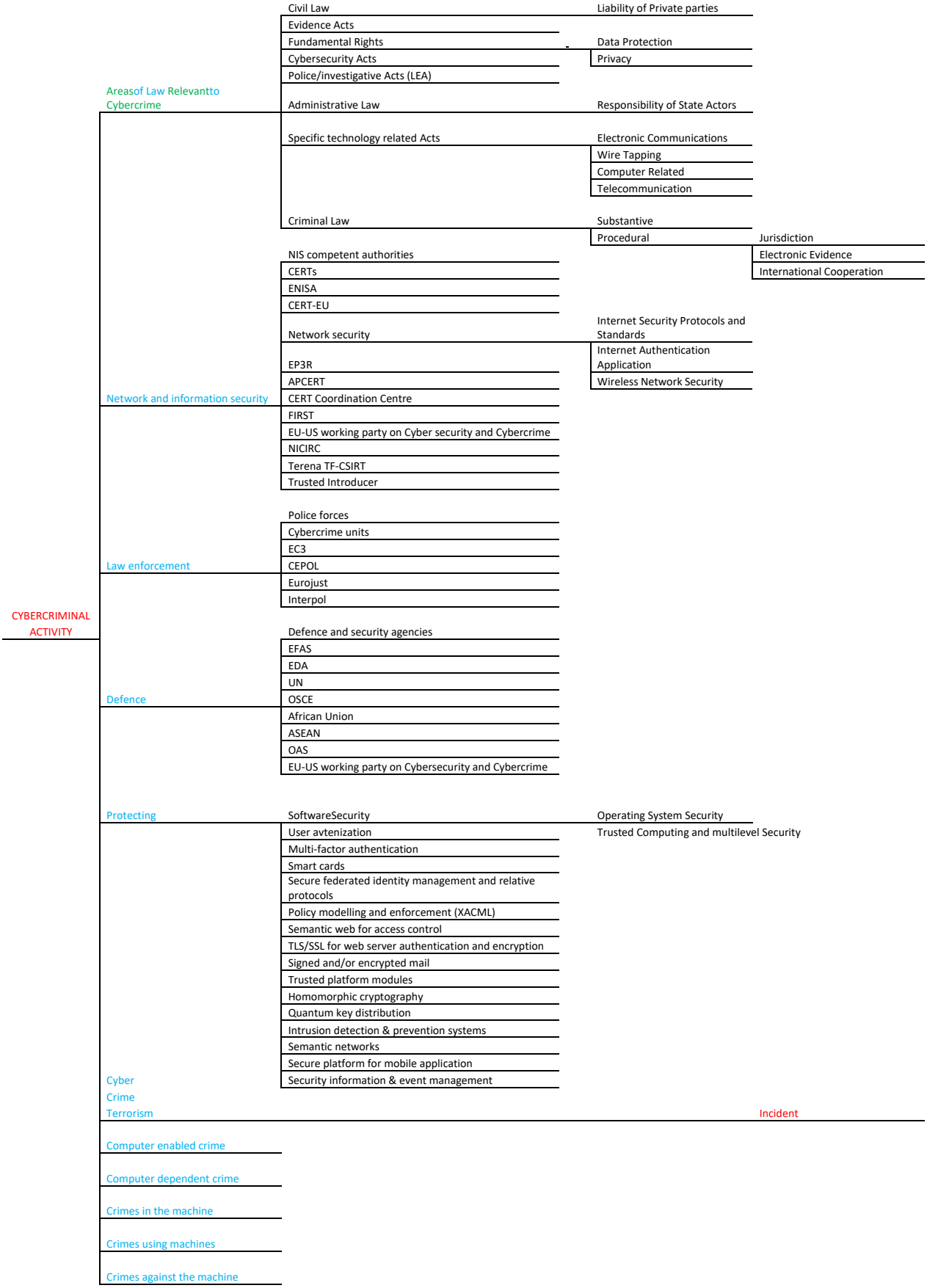

Fig.3: Taxonomy of Cybercrime activity

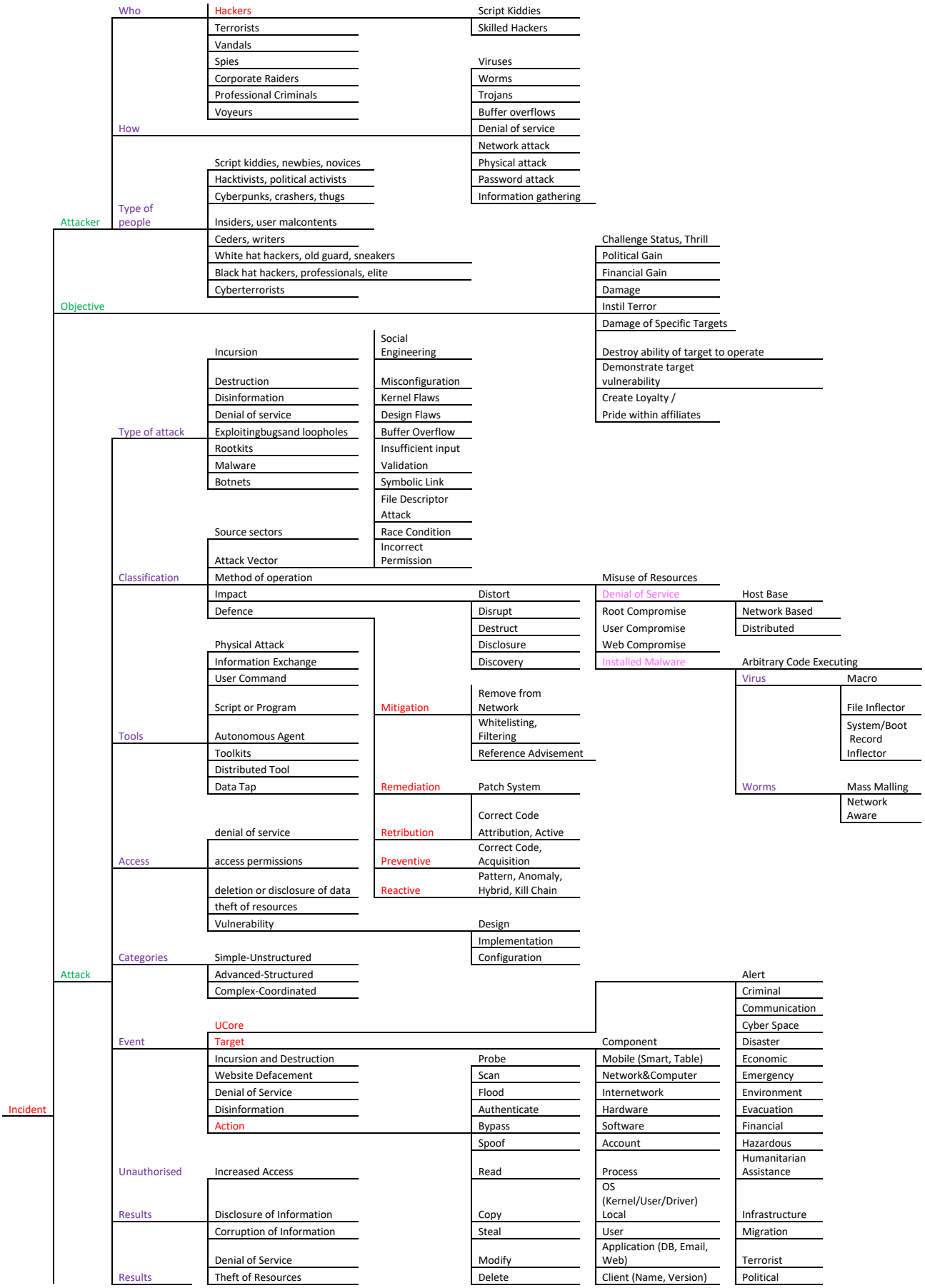

Fig.4: Taxonomy of Cyber Incident

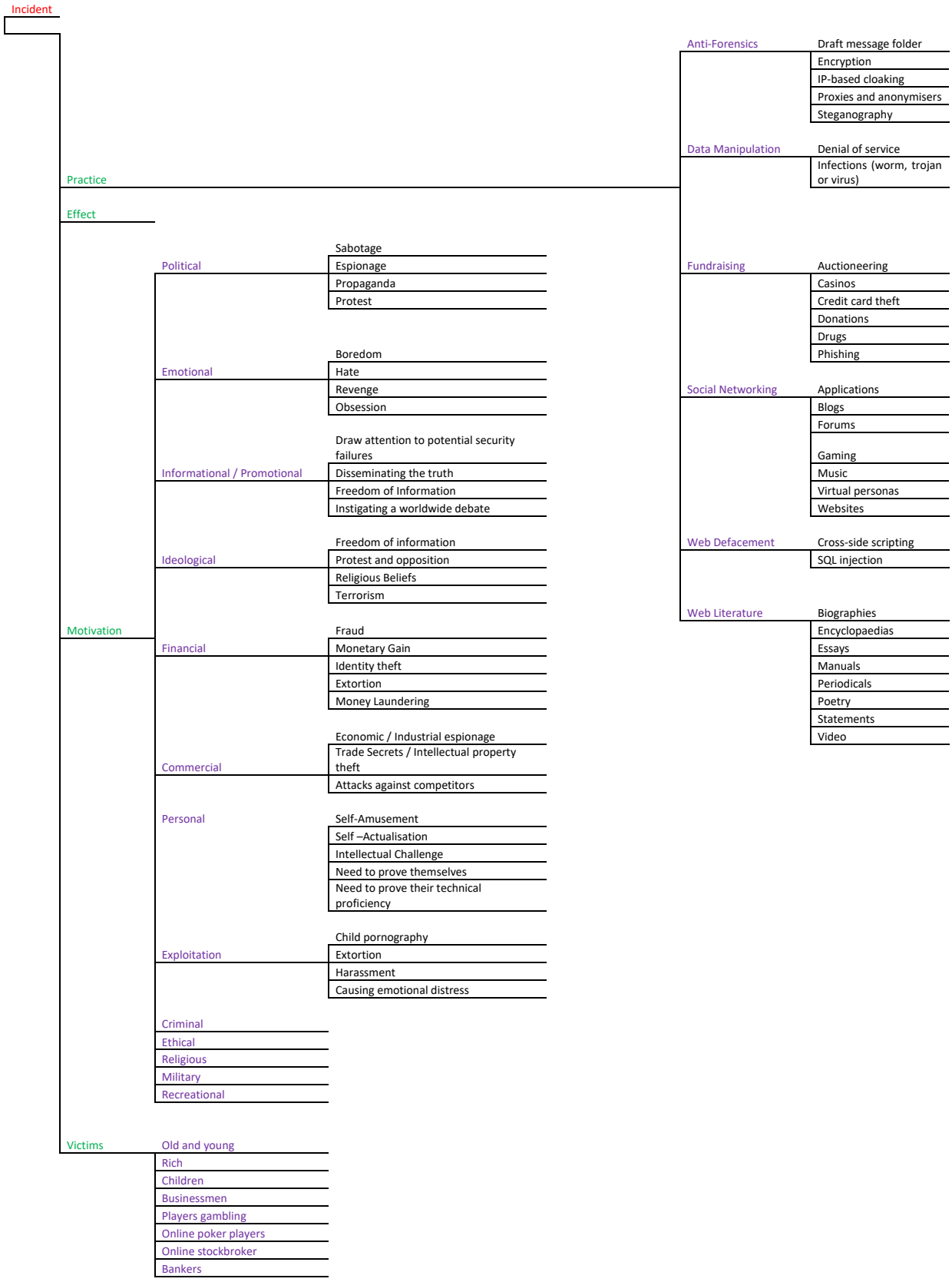

Fig.5: Taxonomy of Cyber Terrorist without Incident

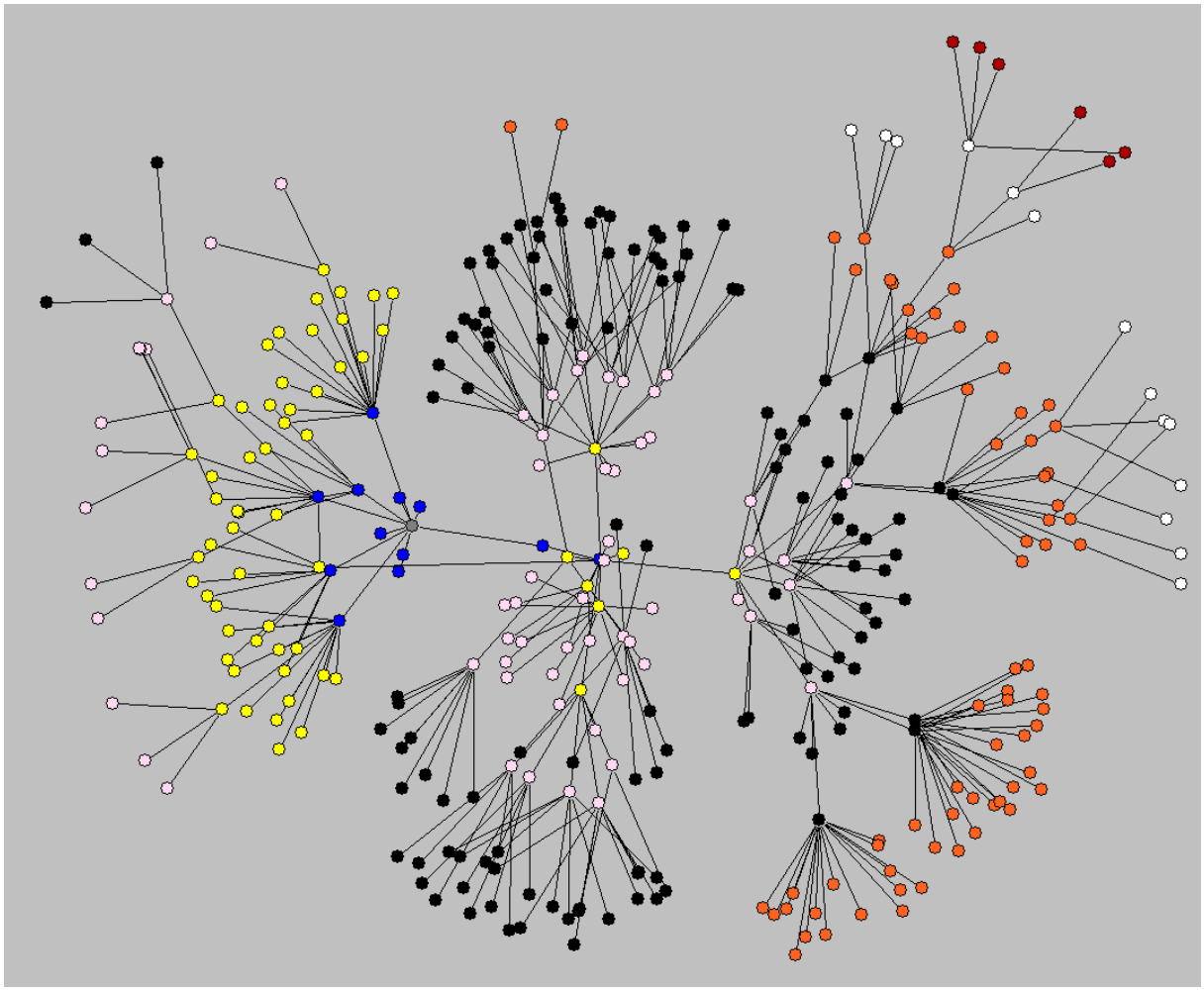

Fig. 6: Taxonomy of Cybercrime activity presented with graph

	FD BC	*T1*	*T2*	*T3*	*T4*	*T5*
Taxonomy CC	3.11	0.673349	0.005970	0.050879	3168	352
Alkaabi et al.	2.58	0.669583	0.050000	0.0	254	41
Ghernaouti	1.58	0.629833	0.083333	0.430830	184	24
Howard	2.32	0.671088	0.043478	0.233333	344	45

Table 1. Properties of proposed Taxonomy of Cybercrime activity and another 3 existing taxonomy

T1 presents topological property Network Betweenness Centralization, T2 presents topological property Density, T3 presents topological property Network Degree Centralization, T4 presents topological property Platt index, and T5 presents the number of nodes. High topological property Network Betweenness Centralization, Network Degree Centralization, and topological property Platt index have a network of taxonomy of Cybercrime (CC). The graph of taxonomy CC has 352 nodes and is bigger than other networks. However, the graph of taxonomy CC has minimal density. In Fig. 3, the Taxonomy of Cybercrime activity is presented with a graph.

5 Discussion

In this paper, we presented a new Systemic Taxonomy of Cyber Criminal activity and its network research. Our taxonomy of Cyber Criminal activity was an extended taxonomy of existing taxonomies of Cybercrime. Firstly, we presented Cyber Criminal activity with a dendrogram. A dendrogram of Cyber Criminal activity was presented with method graph theory. We described Cyber Criminal activity with topological properties of network. Topological property Network Clustering Coefficient was 0.0056818, topological property Network Betweenness Centralization was 0.6733498, topological property Density was 0.0059700,

topological property Network Degree Centralization was 0.0508795 and topological property The Platt index was 3168. The network of Cyber Criminal activity was very complex. We determined the complexity of the network with method fractal geometry. Fractal geometry is very useful in different areas. The fractal dimension FD BC of the network of Cyber Criminal activity was 3.11. Thus, the complexity of the Cyber Criminal activity network was 3.11. We can see that complexity of proposed Taxonomy of Cybercrime activity (*Taxonomy CC*) is more higher as Alkaabi et al., Ghernaouti and Howard taxonomy. Thus, proposed Taxonomy of Cybercrime activity is better. The key of fractal geometry s fractal dimension, which mean complexity ob object. Therefore, we cannot use classical Euclidian geometry to describe complex systems, but we must apply fractals. This methodology can be apply for research deep inside networks of taxonomy.

7 Conclusion and future work

It is true, that the internet has changed our lives, our culture, and our society in countless ways over the past twenty years. It has been observed that, in the last decade, due to a tremendous increase in the number of computer users, Cybercrime has increased anonymously. Cybercrime is a fast-growing area of crime; thus, more and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual. Cybercrime activities are globally diffused, financially-driven acts. Such computer-related fraud is prevalent, and makes up around one third of criminal acts around the world. Cyber-criminal activities are increasing in incidence in a scenario, which has been made worse by the economic crisis. The data provided by security firms on the global impact of Cybercrime are just a raw estimation. They can give a reader just a basic idea of the overall damage caused by illegal activities. In fact, analysing Cybercrime is a very complex task, due to the multitude of entities involved, and their different means and methods. Technology in the Cyber world has posed a challenge to all as there is no trace of Cybercrime and there may be no evidence of it. Many authors have worked on devising an appropriate and suitable taxonomy to classify and evaluate Cybercriminal activity. In this paper, we presented not only the new methods of Cyber-criminal activity, but also the topology of their networks and also their fractal structures. We investigated and analysed some disparate definitions and taxonomies of Cybercrime and developed a refined and extended taxonomy of Cybercrime activities based upon the basic characteristics of the role of the computer and the contextual nature of the criminal activity. Finally, we analysed the topology of the Cybercrime activities network. The main findings can be summarized as follows:

1) We presented a new taxonomy of Cybercrime activity.
2) We used graph theory to describe networks of Cybercrime activity.
3) We calculated the topological properties of networks of Cybercrime activity.
4) Networks of Cybercrime activity are complex.
5) We analysed the complexity of Cybercrime activity networks.
6) Cybercrime activity networks have statistical self-affinity organization.
7) We calculated the fractal dimension of statistical self-affinity organization of Cybercrime activity.

Due to the fact that many of the information technology companies are privately owned, their focus is necessarily on making customers happy as opposed to worrying about transnational crime. We must do our best to keep one step ahead of Cybercrime in order to best protect ourselves. At the very least, we cannot afford to fall too far behind. We will better understand Cybercrime activity and, consequently, be better able to prevent incidents by undertaking extensive and in depth study of Cybercrime activity networks. The study of structural organization, formation and dynamics of the complex fractal network can benefit from studying their geometrical properties and discovering new relationships between geometrical characteristics and network problems of taxonomy.

References

Alkaabi, A., Mohay, G., McCullagh, A., Chantler, A. (2010). Dealing with the problem of cybercrime. *Conference Proceedings of 2nd International ICST Conference on Digital Forensics & Cyber Crime*. Abu Dhabi; 2010.

Amoroso, E. (1994). *Fundamentals of computer security technology*. Englewood Cliffs, New Jersey: P T R Prentice Hall.

Bailey, K.D. (1994). Typologies and Taxonomies: An Introduction to Classification Techniques (Quantitative Applications in the Social Sciences), Sage Publications, Thousand Oaks, the United States of America.

Barton, C. C. (1995). Fractal analysis of scaling and spatial clustering of fractures. In C. C. Barton, and

P. R. La Pointe (Eds.), *Fractals in the earth sciences*. New York: Plenum Press, 1995, pp. 141–178.

Bishop, M. (1995). *A taxonomy of (Unix) system and network vulnerabilities*. Technical Report CSE-9510, Department of Computer Science, University of California at Davis.

Brenner, S. (2006). Cybercrime, cyberterrorism and cyberwarfare. Revue internationale de droit pénal, vol. 77(3), 453-471. doi:10.3917/ridp.773.0453.

Feder, J. (1988). *Fractals.* New York: Plenum.

Ghernaouti, S. (2013). Cyberpower. Crime, Conflict and Security in Cyberspace. EPFL Press.

Howard, J. D. (1997). An Analysis of Security Incidents on the Internet 1989-1995 (Doctoral dissertation, Carnegie Mellon University, Pittsburgh, PA; 1997). Retrieved from www.cert.org/archive/pdf/JHThesis.pdf.

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, 47 (2016), 44-57.

Krsul, I. V. (1998). Software vulnerability analysis. (Doctoral dissertation, Purdue University.

Land, L., Smith, S., & Pang, V. (2013). Building a taxonomy for cybercrimes. In *Pacific Asia Conference on Information Systems, PACIS 2013: proceedings* (pp. 1-11). Atlanta, GA: Association for Information Systems.

Lindqvist, U., Jonsson, E. (1997). How to systematically classify computer security intrusions. *IEEE Security and Privacy* 1997:154 e 63.

Lough, D. L.(2001). A taxonomy of computer attacks with applications to wireless networks. (Doctoral dissertation, Virginia Polytechnic Institute and State University.

McGuire, M., Dowling, S., (2013). Cyber crime: A review of the evidence. available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf (accessed 12.10.2019).

Newman, G. R. (2009). Cybercrime. In M. D. Krohn, A. J. Lizotte, and G. Penly Hall (Eds.), *Handbook on Crime and Deviance, Springer*, Nov 2009, pp. 551-584. (Criminology Cyber crime). Available from: http://www. springer.com/978-1-4419-0244-3. 4, 18.

Ogwezzy, M. C. (2012). Cyber crime and the proliferation of yahoo addicts in Nigeria. *Agora International Journal of Juridical Sciences*, 1, 86-102.

Shao, J., Buldyrev, S. V., Cohen, R., Kitsak, M., Havlin, S., Stanley, H. E. (2008). Fractal boundaries of complex networks. *A letters Journal Exploring the Frontiers of Physics*, 84, 48004. doi:10.1209/0295-5075/84/48004.

Singh Brar, H., Kumar, G. (2018). Cybercrimes: A Proposed Taxonomy and Challenges. *Journal of Computer Networks and Communications*, Vol. 2018, Article ID 1798659, 11 pages, https://doi.org/10.1155/2018/1798659.

Zhang, G. Q. (2013). "A universal assortativity measure for network analysis", APS Journals, (2012) December 28.Tourangeau, R., Conrad, F. G., Couper, M. P. (2013). *The Science of Web Surveys*. New York: Oxford University Press.

Yazdanifard R., Oyegoke T., Seyedi A. P. (2011). Cyber-Crimes: Challenges of the Millennium Age. In: Zheng D. (eds) *Advances in Electrical Engineering and Electrical Machines. Lecture Notes in Electrical Engineering*, vol 134. Springer, Berlin, Heidelberg