Hackers Topology Matter Geography

Mapping the Dynamics of Repeated System Trespassing Events Networks

Amit Rechavi
The Center for Internet Research
University of Haifa
Haifa,
Israel

Tamar Berenblum
The Institute of Criminology,
The Hebrew University,
Jerusalem

David Maimon
Department of Criminology and Criminal Justice,
University of Maryland

Ido Sivan Sevilla
School of Public Policy & Government, The Hebrew University,
Jerusalem

***Abstract*— this study focuses on the spatial context of hacking to networks of Honey-pots. We investigate the relationship between topological positions and geographic positions of victimized computers and system trespassers. We've deployed research Honeypots on the computer networks of two academic institutions, collected information on successful brute force attacks (BFA) and system trespassing events (sessions), and used Social Network Analysis (SNA) techniques, to depict and understand the correlation between spatial attributes (IP addresses) and hacking networks' topology. We mapped and explored hacking patterns and found that geography might set the behavior of the attackers as well as the topology of hacking networks. The contribution of this study stems from the fact that there are no prior studies of geographical influences on the topology of hacking networks and from the unique usage of SNA to investigate hacking activities. Looking ahead, our study can assist policymakers in forming effective policies in the field of cybercrime.**

Keywords: Hacking, Cybersecurity, Cyberspace Policies, Topology, SNA, Hot-spots

INTRODUCTION

William Gibson (1984) coined the term 'cyberspace,' and defined it as: "*A consensual hallucination experienced daily by billions of legitimate operators, in every nation...A graphic representation of data abstracted from the banks of every computer in the human system…clusters and constellations of data*."

"Cyberspace", in this sense, is a ubiquitous fragile dimension, which has a distinct location, though a non-physical one. Therefore, it is a challenging environment for researchers to study (Graham, 2013). Cyberspace therefore is as a "place" with terms that express this conception: "Worlds, Domains, Sites, and Rooms (Barak and Suler, 2008). It is a place with social control and boundaries (Barzilai-Nahon and Neumann; 2005), and a place in which traffic is concentrated within localities, states, and regions. Moreover, its communication efficiency (Murnion and Healy 1998; Thelwall 2002) is depended on physical locations of data, hardware (routers, fiber optic cables, phone lines, etc.), and on the number of miles the data travels (Dodge and Zook 2009; Goldsmith and Wu 2006). The cultural characteristics that translate into different desires, expectations, online routines and behaviors change the Internet experience correspond to geographical boundaries (Goldsmith and Wu, 2006).

Nonetheless, most of us capture the Internet as a technology that creates virtual worlds disengaged from a physical location. As Johnson and Post (1996) claimed, *'a new boundary, made up of screens and passwords that separate the virtual world from the "real world", emerges*.' This is not solely a metaphor. This boundary defines the Cyberspace: a new world, with new rules, regulations, and laws (such as spamming, phishing, and hacking). In addition, Cyberspace has a number of unique characteristics: non-existence geographical boundaries, vague "privacy", and extensive anonymity. These characteristics make cyberspace a perfect setting for hackers who seek to cross-geographical spaces and exceed identity restrictions.

This study explores hacking in cyberspace. Specifically, it analyzes the influence of geographical locations of victimized and attacking computers on hacking-networks' topology. Though hacking is not a new phenomenon (Furnell, 2002), it evolved in recent years and became more sophisticated and organized (Grabosky, 2014). Hacking, thus, carries enormous consequences on commercial, governmental (Rantala, 2008), and individual computer users (Bossler and Holt, 2009).

The focus of this study is cyber-attacks on computer networks. The data was collected using Honey-pots computers (A Honey-pot is a computer that enables the collection of information on real system trespassing events). We designed and deployed these target computers in the infrastructures of two universities – in Israel and China.

Many complex social and natural systems are made of components and obscured web of connections among them. Identifying these components and links is

ASONAM '15, August 25-28, 2015, Paris, France

ACM ISBN 978-1-4503-3854-7/15/08 $15.00
DOI: http://dx.doi.org/10.1145/2808797.2808873

crucial to the understanding of the network, its structure and functionality. To build the attackers' network with the same technique of Tranos and Nijkamp (2013), we used the *IP addresses* of Honey-pots, *Brute Force Attacks (BFA)* - successful attempts by hackers to guess login passwords to target computers for the first time, and *System Trespassing events (i.e. Sessions)* - successful computer intrusions based on credentials gained during BFAs. Both the attackers and attacked computer systems are nodes in a bi-partite network. We then employed SNA techniques to capture the dynamics of attack-networks' typologies. We analyzed the topological and statistical data collected from these target computers and explored the node-level (attacked and attackers attributes) and the network as a whole (patterns of hacking activities).

In the broad, diverse, and rich spectrum of cyberspace attacks, we focus on one specific type of attacks – system trespassing events of SSH servers. We are not analyzing additional types of attacks such as web server attacks, e-mail phishing frauds, and database attacks (e.g. SQL injections). This is an important disclaimer for the validity of our research. Although we reach conclusions on the behavior of the network of cyber-attacks, our conclusions refer to hackers who only choose to use this type of attacking strategy. Although we focus on a specific attacking strategy, this strategy is a common method for gaining control over servers within organizations and throughout the cloud environment. Thus, understanding how hackers directly take over cyberspace resources and use them as their own, is a promising step forward in today's information security research.

The paper comprises seven sections. Following this introduction, we review the related work regarding topology and the spatiality of the Internet. Then, we present our three hypotheses. Next, the research methodology and the research results are reported respectively. Conclusions regarding potential theoretical contributions and suggested future research are discussed in the last section

REALED WORK

a. The Role of Topology

The way a network shapes its basic topology is a challenging issue in social network research in general (Morgan et al., 1997; Kossinets and Watts, 2006; Braha and Bar-Yam, 2006; Viswanath et al., 2009) and in the research of dynamic social networks in particular (Berger-Wolf and Saia, 2006; Hill and Braha 2010). Without understanding the processes that led the network to its current visible topology, the typology is meaningless (Berger-Wolf and Saia, 2006).

The coming section explores the factors that might shape the network's topology and its relevance to geography.

Network's topology is the sum of many sub-topologies, each one having its own purpose (Cross et al., 2001; Holme et al., 2004). It is a field of interests with many goals affecting its final structure (Lickel et al., 2006). This is the case in our current study, with many different Brute Force Attackers and system trespassing events that contain various mal-intentions.

Several studies investigated the relations between topology and functionality of a network. Since topology evolves (or designed) to carry out efficiently the network's mission, and since the network is influenced by its topology, understanding the topology is essential for understanding network's function.

The structure of a network contributes to a network's dynamics (Watts, 1999) and to its ability to carry and deliver messages or viruses (Watts, 2004). For example, the physical topology of Internet servers is a scale-free power law, and it resembles the topology of the World Wide Web, which embodies the logical (Hub and Authorities) layer of the Internet (Faloutsos et al. 1999). Additionally, the small world topology of financial institutions in Canada serves its banks best (Baum et al., 2003). The decay of friendship probability with geographic distance in 'LiveJournal' helps members to navigate in its social structures (Liben-Nowell et al., 2005). Recently, using Messenger communications to investigate geographical properties of the social network, Leskovec and Horvitz (2014) found that geography provides an important cue in navigating between arbitrary source and target nodes and re-approved Liben-Nowell et al. (2005) conclusions.

Another ubiquitous topological example of interests shaping the network topology is the "Structure Holes". These individuals benefit from serving as intermediaries between non-connected vertices or groups. These groups have conflicting interests in the network and structured holes gained from their special position in the network (Granovetter, 1973; Burt 1995; Kleinberg, 2006).

Following these examples, we choose to investigate several centrality measurements of the attacking computers' networks. These measurements include Degree Centrality, Degree Centrality, Eigenvector Centrality and Hub, and Authority Centrality. We use these parameters to understand the structure of the attacking computers and to identify the main nodes in each network. We also use in-degree and out-degree parameters to correlate network's topology with geographic distance.

b. The spatiality of the Internet

In 2001, Cairncross predicted that distance is dead, and yet, in recent years, several studies investigate the dependency of online social networks (OSN) topology in geography. The states' growing involvement in Internet-regulation presents spatial aspect of the Internet. Goldsmith and Wu suggest (2006) that this involvement is due to a bottom-up demand. The citizens want the state to protect them while they use the Internet and it is not an attempt of the state to preserve its power. Moreover, geography matters even in the digital world for reasons such as: the necessity for social depth, the needed physical proximity for knowledge exchange, and the inherited nature of the OSN (Morgan, 2004). Clusters of friends in OSN are often geographically close in the real world (Scellato et al., 2010) and physical distance has a significant impact on the intensity of the Internet infrastructure (Tranos and Nijkamp, 2013). People establish distant online connections with lesser probability than proximate ones (Lengyel et al., 2014).

It seems that even in Twitter distance considerably constrains ties. Almost 40% of Twitter users connect users within the same regional cluster while ties longer than 5,000 km are underrepresented (Takhteyev et al., 2012). Yet, in one study, geographical distance was found to have smaller deflated power on the frequency of online friendships (Onnela et al., 2011). In our study, we will examine these conflicting claims in an attempt to conclude whether distance plays a role on hacking networks' topologies.

HYPOTHESES

In the previous chapter we quoted few studies explaining why "distance is not dead" for Online Social Networks. Our study follows these studies' footsteps and explores the relation between physical location and topology in the context of hacking networks.

We claim that geography has an influence on the behavior of the attacker and as a result, geography has an influence on the topology of networks. Unlike any other network, in the attack network, one side (the Honey-pots i.e. the target computer) is passive and the only factor determining the topology of the network is the attackers' behavior. Specifically, we hypothesize that:

(1) H1: The geographic location of the Honey-pots (i.e. the target computer) has no effect on attack-networks topology. We expect to find that the fact that Honey-pots are differently located (once in China and once in Israel) has no influence on the network's topology of attacking computers' locations.

*(2) H2: The geographic location of the attacking computer influences its network topology. W*e expect to see a similar attackers' behavior, meaning similar network attributes such as centrality-parameters, once the attacks are originated from the same countries (regardless of the Honey-pots' location).

(3) H3: The geographic position of the attackers correlates with their topological positions in the network. We follow Onnela et al. (2011) and expect the geographical distances (in km) between the IP addresses used by hackers to correlate with the number of interactions between them.

METHODOLOGY

First, we will describe the research methodology and then the research set-up and plan. A description of the units of analysis and their properties is following. This study models the relations between hackers' IP addresses and Honey-pots (HP) as a directed network. A Honey-pot is a "*security resource whose value lies in being probed, attacked or compromised*" (Spitzner 2003).

The Honey-pot (HP) enables the collection of information on real system trespassing events. Consistent with past criminological (Maimon et al., 2014) and technological studies (Salles-Loustau, et al., 2011), we deployed research HPs on the computer networks of Chinese and Israeli academic institutions. 240 public IP addresses were used as HP in the Chinese network and 60 public IP addresses were employed for the deployment of HP on the Israeli network. Both computer networks had Linux Ubuntu 10.04 as their operating system. The Chinese HPs were active for a period of 4 months (August 21, 2012-December 21, 2012) and the Israeli HPs were active for a period of 3-month period (May 23, 2013-August 31, 2013).

In line with prior conceptualizations of password-guessing attempts (Keith et al., 2007; SANS Institute 2007), we operationalize a successful brute force attack as any event in which an unauthorized person or automatic tool successfully guesses the password to the system. Thus, we consider any target computer that was subject to a successful remote password-guessing attempt a victim of a brute force attack. Similarly, we follow prior conceptualizations of system trespassing events (Berthier and Cukier 2009; Maimon et al, 2014), and operationalize a system trespassing event as any incident in which an unauthorized person accesses and logs in to a computer system based on a prior brute force attack.

To infiltrate a HP, system trespassers had to scan the network, identify these computers and break into them through vulnerable entry points. In both networks (Chinese and Israeli) The HPs denied intruders' login attempts until a random predefined threshold (between 150 and 200) was reached and then the

target-computer was "successfully" infiltrated and allowed intruders to initiate a system trespassing event.

Once infiltrating the HP, we allowed system trespassers to employ the target computers for a period of 30 days. At the end of a 30-day period, the HP blocked the system-trespasser's access; we cleaned it and re-deployed it on the network. We use HP to explore who the attackers are, where do they come from, and what patterns of attacks they create in their behavior. We collected information on both successful brute force attacks, and system trespassing events, which are both successful break-in attempts into Honey-pots on these networks.

We are fully aware of hackers' tendency to mask their origins. Thus, an IP address of an attacker in our data is most probably not the real IP of the attacker's computer. Nevertheless and even though the IPs might not indicate the exact location of the hacker, it represents the most available IP address that the hacker can use in order to attack HPs, in either the Chinese or Israeli networks for both first (BFAs) and following (Sessions) attacks.

Throughout the data collection period, 752 Chinese target computers experienced brute force attacks. These attacks originated in 347 unique IP addresses. However, not all system trespassers initiated a system trespassing event against our target computers: only 301 Chinese target computers recorded a first system trespassing event. These incidents initiated from 140 unique IP addresses. In contrast, due to the low number of IP addresses employed at the Israeli site, only 118 Israeli target computers experienced brute force attacks during the data collection period. These attacks originated in 115 unique IP addresses. Similarly, first system trespassing events initiated from 60 unique IP addresses against our 72 Israeli computers.

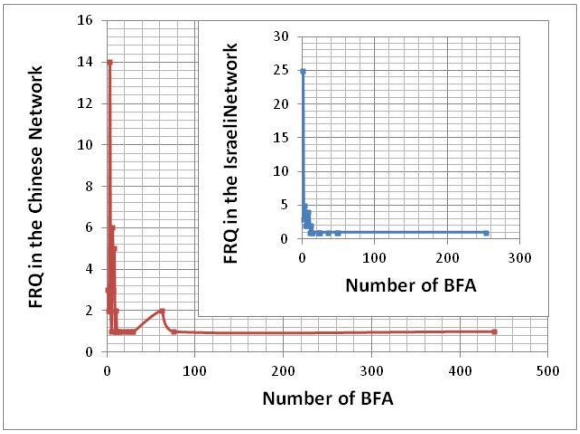
Once we gathered the data, we built the Chinese and the Israeli HP's networks; we deployed SNA techniques to explore their topological parameters and analyzed the results in the country level (in both the attackers and the HPs). In the coming Graphs we present the results. Each time there is s directed link from country A to country B, that link means that a BFA from country A was followed by a Session from country B.

MAIN RESULTS

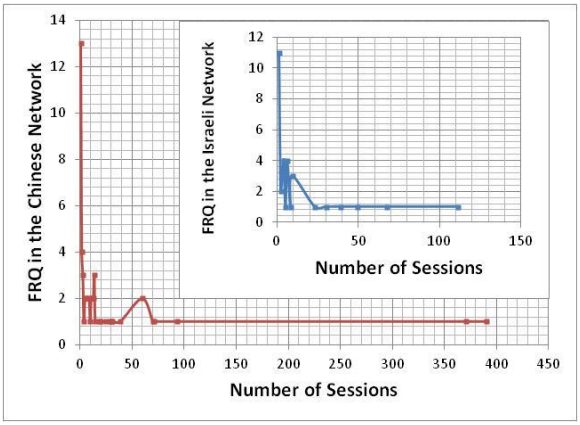
1. The Geographic dimension with relation to the topology

First, we analyzed the structure of the two hacking networks. The honey-pots, located in China and Israel separately are the base for the two networks. Both hacking networks are topologically alike without relation to the geographical location of the honey-pots. Though the honey-pots were located in two different geographic places the topology of the attackers' networks attacking each site is similar.

The following graphs represent the Chinese and Israeli networks. In graph 1 and graph 2 we present the distribution of the attacks (BFA and Sessions) per country in both the Chinese and the Israeli networks.



Graph 1: the distribution of BFA attempts per country in the Chinese and the Israeli networks.



Graph 2: the distribution of Sessions attempts per country in the Chinese and the Israeli networks.

The distribution pattern in China and Israel (graph 1 and graph 2) is almost identical. Many countries are engaged in several attacks and only a few countries are massively attacking the Honey Pots. This might give a hint on the behavior of the hackers in both networks. Next and in order to understand the relation between geography and patterns of hacking activity, we investigated the hacking activity in the country level.

Figures 1 and 2 map the main countries which origin hackers' attacks on Chinese and Israeli Honey-pots networks. Since many countries contribute only few attacks, we filtered the data and figure 1 and figure 2 present the countries that have the highest hacking activity. We only present the countries that their

number of attacks is higher than the *mean value* of attacks in each network (4 in the Israeli network and 5 in the Chinese network). Figure 3 and 4 in the appendix map all the relations between the attacking countries in the Chinese and the Israeli networks.

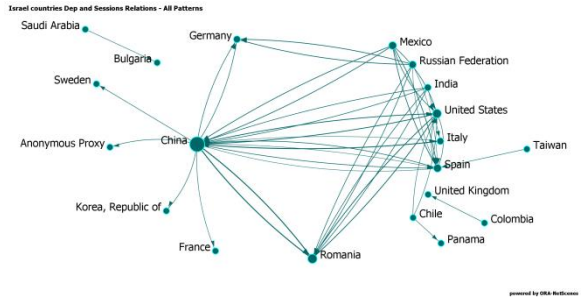


Figure 1: BFA and Sessions relation in Israeli HP's network (links >4)

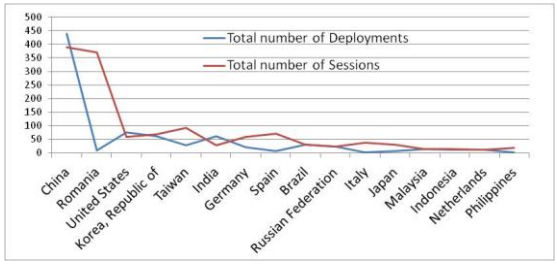
Figure 2: BFA and Sessions relation in Chinese HP's network (links >5)

Figures 1 and 2 make it very clear to notice that once a BFA happens (a node with a pointing arrow) the sessions (a node with an arrow pointing at it) which follow it, originate from all over the globes and not from a nearby country. This phenomenon exists in both Chinese and Israeli networks. Table 1 in the appendix details the list of countries in Chinese and Israeli HP's network. For both Israeli and Chinese Honey-Pots, the frequency of sessions and BFAs is similar, BFAs are originated in three main nodes and sessions are coming from all over the globe. Thus, as predicted in H1, the geographic location of the Honey-pots does not have any effect on the topology of the hacking network.

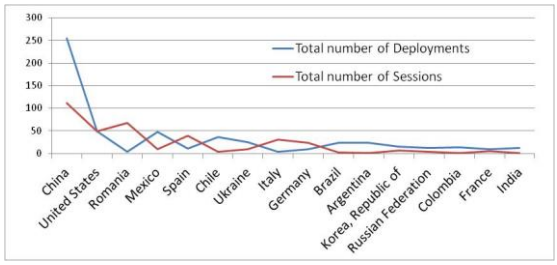
2. Resemblance of nodes and topologies' parameters

First, we explored the main topological identity of the main countries in the Chinese HP network and the Israeli HP network. We used the common network centrality parameters to analyze the main countries in each network and found them almost identical in both Honey-Pots' networks. In graphs 3 and 4 we present the distribution of the attacks (BFA and Sessions) originating from the top 10 countries. In both Chinese and Israeli networks, the "main players", meaning the leading countries with the highest hacking activity level, are similar.

The topological structure of the three leading nodes in figures 1 and 2 (China, Romania and the Unites States) looks quite the same in both networks.



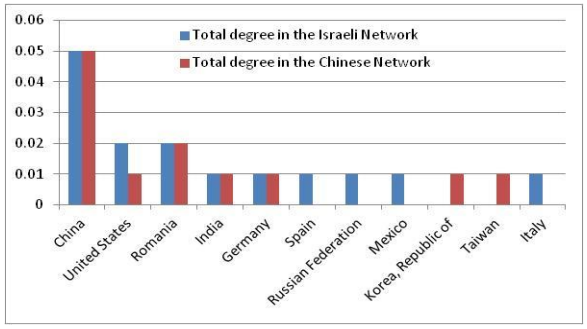
Graph 3: BFA and Sessions relation in Chinese HP's network



Graph 4: BFA and Sessions relation in Israeli HP's network

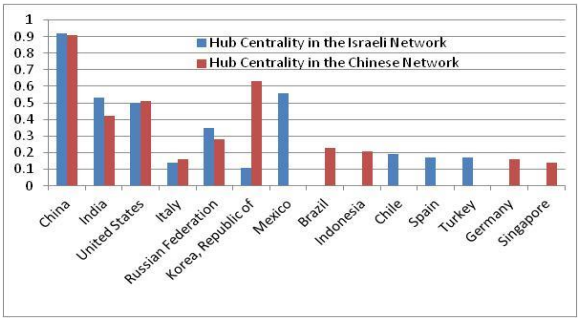
Next, we compared the two hacking networks with regard to five topology measures: Degree centrality, Hub centrality, Authority centrality, Eigenvector centrality and Betweenness centrality. The following graphs present our findings;

In graph 5 we present the "Total Degree Centrality" which calculates the total number of times a country is engaged in hacking activity, either sending HP's data to other countries or getting this data from other countries. The top five most active countries in this parameter are the same in the Chinese and Israeli HP networks.

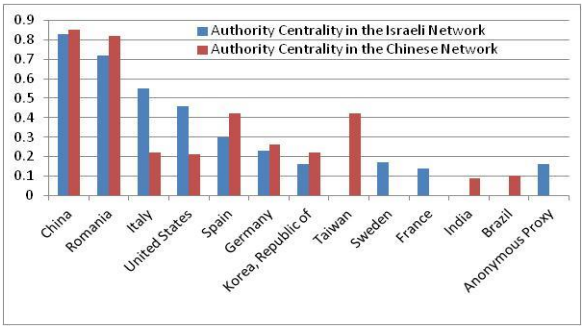


Graph 5: Top Total Degree Centrality in Chinese and Israeli HP Networks

In graph 6 and 7 we present the top "Hub Centrality" and top "Authority Centrality" countries. A country is hub-central to the extent that it sends hacking data (many out-links) to countries that receive a lot of hacking data (many in-links). A country is Authority-central to the extent that it gets a lot of hacking data (many in-links) from countries that have send a lot of data (many out-links). In the Chinese and the Israeli HP Networks, the top Hub and Authority countries are almost identical.

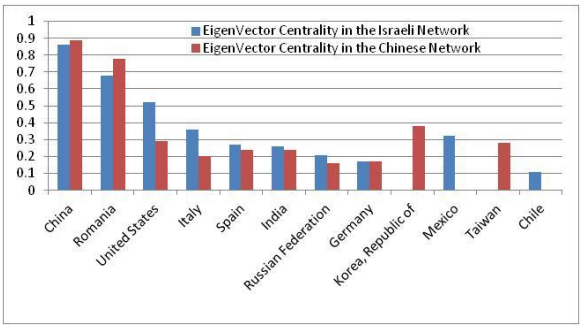


Graph 6: Top Total Hub Centrality in Chinese and Israeli HP Networks



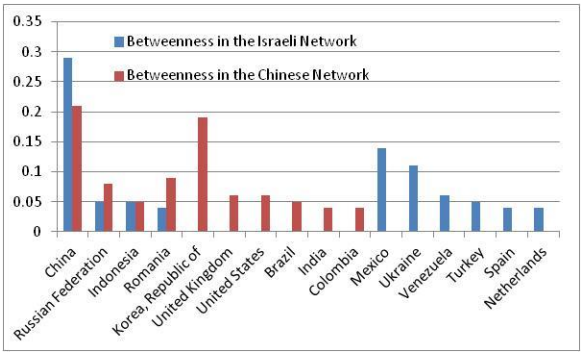
Graph 7: Top Total Authority Centrality in Chinese and Israeli HP Networks

In graph 8 we present the top "Eigenvector Centrality" countries. Eigenvector centrality is a measure of the influence of a country on the hacking network, based on its links to high-scoring countries. It is a high-quality measure for "major players" in the network, since it calculates the links to others that are themselves highly connected to each other. In the Chinese and the Israeli HP Networks, these top Hub nodes are almost identical.



Graph 8: Top Total Eigenvector centrality in both Chinese and Israeli HP Networks

In graph 9 we present the top "Betweenness Centrality" countries. Betweenness centrality is a measure of the influence of a country in the hacking network, based on its influence on the transfer of items through the network. It is a high-quality measure for "major players" in the network, since it calculates the number of the shortest paths from all countries to all other countries that pass through it. In the Chinese and the Israeli HP Networks, these top Hub nodes are almost identical.



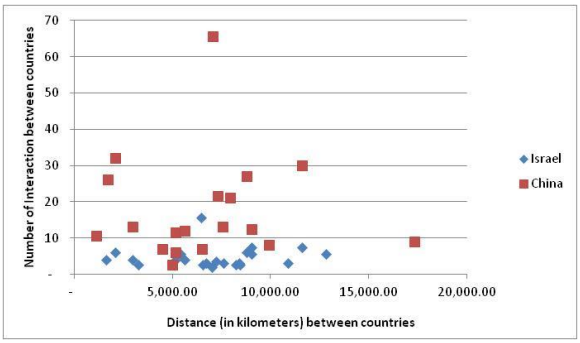
Graph 9: Top Betweenness centrality in both Chinese and Israeli HP Networks

Overall, network analysis of the Chinese and the Israeli HP networks reveals that the node-sets in the two networks are similar (see table 1 in the appendix), the main players in the two networks are almost the same, and their topological measures are alike (see graphs 5-9 above). To conclude this part based on the overall topology and the proximity of the major players in the networks (Rechavi and Rafaeli, 2014), we find that the topologies of the networks, which describe the dynamics between BFA and Sessions, are extremely similar to each other.

3. Physical Centrality and Topological Centrality

In several studies (Scellato et al., 2010; Takhteyev et al., 2012; Tranos and Nijkamp, 2013; Lengyel et al., 2014) the geographical distance had a meaning in people's network. These studies found a correlation between the physical distance between two people in real life and their mutual relations in their social networks.

Though geographical distance has power on topology, geography is not the only parameter that sets the behavior of attackers. We follow Onnela et al. (2011) and in our third hypothesis, we expected that the geographic positions of the attackers (distance between countries) correlate with their topological positions in the network. In graph 10 we present the ratio between geographical distance of the countries and the number of interactions between them.



Graph 10: Chinese HP - Total Number of links and Distance between nodes

As the graph shows, no correlation was found between the geographic distance between nodes and the number of links between them (Total Degree Centrality), in both the Chinese and the Israeli HP network. When we separately explore the "In-degree" and "Out-Degree" of the nodes we found the same results.

Discussion and Conclusions

Analyzing crime in the context of place is not new in criminological research. However, researchers paid little attention to the geography of attackers and victims in cyber sphere. This study attempts to address this gap in the literature and explore the relationship between countries that are involved in hacking activities.

Our findings support the first hypothesis. The HPs computers were "passive victims" and the only information the hackers knew about the HPs was their geographic location – a university campus (in Israel or China). Since the attacks in the Chinese and Israeli campuses looked alike from a network topology perspective, we can deduce that the HPs' location did not affect the behavior of the hackers. Hence, the geographic location of the passive target computer does not have an effect on the attacking dynamics.

Our findings moderately support the second hypothesis. We found that besides similarity in the topology of the two hacking networks, the node-sets in the networks are also similar. Meaning not only topologically speaking the networks look alike but also the nodes, the hacking countries are almost the same in the Chinese and Israeli networks. On one hand the resemblance of the two networks' topologies can explicit a *general attack pattern* and in this case, the location of the attacking has no meaning. On the other, the resemblance of the two networks' topologies can happen because the attacking IPs in both cases come from the same countries. In that case, the topologies can explicit a *specific attack pattern* which is location-dependent. This means that the location of the attacker influences the network's topology, as we suggested in the second hypothesis.

Lastly, with regard to our third hypothesis, we find that there is no correlation between the topological and geographical centrality of nodes within the two networks. The strength of relations between two hacking countries in the network (the number of interactions between two countries) does not correlate with the physical distance between them (number of Km). This finding does not complement other researchers. A possible explanation for that is the special nature of hacking activities. Unlike social network relations, sharing hacking-data is based upon pure interests of both sides. It seems that in this manner "the world is flat" and the hackers share data across the globe without local or spatial characteristics. Digital data (and crime) knows no-border and a clear relation between geographic place and cyber space is still vague.

Our findings are preliminary and refer to specific victims (university network) and to hackers working only in a certain way (SSH protocol). Further study should explore other courses of action of hackers (for example - different protocols of hacking) and other networks (banks, telecommunications companies, etc.).

The fact that our research is based on the last IP address from which the attack was carried out, and not on the actual geographical location of the attacker, is a testament to the challenge faced by law enforcement

agencies in identifying and punishing hackers. Drawing from Hot Spots policing theory (Braga, Papachristos and Hureau, 2012) and the crime concentration rule (Weisburd, Groff, and Yang, 2012), we believe that mapping the 'hot countries' from which the hackers choose to launch their attacks, is critical. We are aware of the fact that a comparison between street segments and the virtual space is not obvious. It requires theoretical development and empirical testing that the network analysis methodology can potentially address.

Overall, the full understanding of hacking activities includes the formation of hacking networks, their evolution, and their functionality. This requires the analysis of the dynamics and structure of hacking networks. The usage of network analysis methodologies is a promising step in this direction; it brings together topology and functionality and investigates them simultaneously. We call for more research in this promising area - the Cyber Criminology Network Analysis (CCNA).

ACKNOWLEDGEMENT

This research was conducted with the support of the Israeli Ministry of Science, Technology and Space (grant number 3-10888) and the college of behavioral and Social Science at the university of Maryland dean's Research award.

REFERENCES

Barak, A., & Suler, J., (2008). Reflections on the Psychology and Social Science of Cyberspace. In: Barak, A., (Ed.). (2008). Psychological aspects of cyberspace: Theory, research, applications. NY: Cambridge University Press. 1-12.

Barzilai-Nahon, K., & Neumann, S. (2005, January). Bounded in cyberspace: An empirical model of self-regulation in virtual communities. In System Sciences, 2005. HICSS'05. Proceedings of the 38th Annual Hawaii International Conference on (pp. 192b-192b). IEEE.

Baum, J. A. C., Shipilov, A. V., & Rowley, T. J., (2003). Where do small worlds come from?. Industrial and Corporate Change, 12(4), 697.

Berger-Wolf, T. Y., and Saia, J., (2006). A framework for analysis of dynamic social networks. Proceedings of the 12th ACM SIGKDD, 523-528.

Berthier, R., & Cukier, M., (2009). An evaluation of connection characteristics for separating network attacks. International Journal of Security and Networks, 4(1), 110-124.

Bossler, A.M., and Holt T.J., (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology 3*, 400–420.

Braga, A., Papachristos, A., & Hureau D., (2012), Hot spots policing effects on crime. Campbell Systematic Reviews 2012:8, 1-97.

Braha, D., & Bar-Yam, Y., (2006). From centrality to temporary fame: Dynamic centrality in complex networks. Complexity, 12(2), 59-63.

Burt, R. S., (1995). Structural holes: The social structure of competition. Cambridge MA: Harvard University Press.

Cairncross, F., (2001). The death of distance: How the communications revolution is changing our lives. Boston MA: Harvard Business Press.

Cross, R., Borgatti, S. P., & Parker, A., (2001). Beyond answers: Dimensions of the advice network. Social Networks, 23(3), 215-235.

Dodge, M., & Zook, M., (2009). Internet Based Measurement. In: Kitchin, R., and Thrift, N., (Eds). The International Encyclopedia of Human Geography. Oxford: Elsevier.

Faloutsos, M., Faloutsos, P., & Faloutsos, C. (1999, August). On power-law relationships of the internet topology. In ACM SIGCOMM computer communication review (Vol. 29, No. 4, pp. 251-262). ACM.

Furnell, S., (2002). Cybercrime: Vandalizing the Information Society. Boston, MA: Addison-Wesley.

Gibson, W., (1984). Neuromancer. London: Harper Collins,

Goldsmith, J., and Wu, T., (2006). Who Controls the Internet? Illusions of A Borderless World. Oxford University Press.

Graham M. (2013). Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities. The Geographical Journal, 179 (2), 177–182.

Grabosky P. (2014). The Evolution of Cybercrime, 2004-2014. RegNet Working Paper 58, Regulatory Institutions Network.

Granovetter, M. S., (1973). The strength of weak ties. American Journal of Sociology, 78(6), 1360.

Hill, S. A., & Braha, D., (2010). Dynamic model of time-dependent complex networks. Physical Review E, 82(4), 046105.

Holme, P., Edling, C. R., & Liljeros, F., (2004). Structure and time evolution of an internet dating community. Social Networks, 26(2), 155-174.

Johnson, D. R., & Post, D., (1996). Law and borders: The rise of law in cyberspace. Stanford Law Review, 1367-1402.

Keith, M., Shao, B., & Steinbart, P. J., (2007). The usability of passphrases for authentication: An empirical field study. International journal of human-computer studies, 65(1), 17-28.

Kleinberg, J. (2006, August). Social networks, incentives, and search. In Proceedings of the 29th annual international ACM SIGIR conference on Research and development in information retrieval (pp. 210-211). ACM.

Kossinets, G., & Watts, D. J. (2006). Empirical analysis of an evolving social network. Science, 311(5757), 88-90.

Lengyel B., Attila V., Ságvári, B. Jakobi Á., & Kertész, J., (2014) Geographies of an online social network". arxiv.org/pdf/1503.07757

Leskovec, J., & Horvitz, E., (2014). Geospatial Structure of a Planetary-Scale Social Network. Computational Social Systems, IEEE Transactions on, 1(3), 156-163.

Liben-Nowell, D., Novak, J., Kumar, R., Raghavan, P., & Tomkins, A., (2005). Geographic routing in social networks. *Proceedings of the National Academy of Sciences of the United States of America*, 102(33), 11623-11628.

Lickel, B., Rutchick, A. M., Hamilton, D. L., & Sherman, S. J., (2006). Intuitive theories of group types and relational principles. Journal of Experimental Social Psychology, 42(1), 28-39.

Maimon, D., Alper, M., Sobesto, B., & Cukier, M., (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, 52(1), 33-59.

Morgan, D. L., Neal, M. B., & Carder, P., (1997). The stability of core and peripheral networks over time* 1. Social Networks, 19(1), 9-25.

Morgan, K., (2004). The exaggerated death of geography: learning, proximity and territorial innovation systems. Journal of economic geography, 4(1), 3-21.

Murnion S. & Healy, R.G., (1998). Modeling Distance Decay Effects in Web Server Information Flows. Geographical Analysis 30: 285-302.

Onnela, J. P., Arbesman, S., González, M. C., Barabási, A. L., & Christakis, N. A. (2011). Geographic constraints on social network groups. PLoS one, 6(4), e16939.

Rantala, R., (2005). Bureau of Justice Statistics Special Report: Cybercrime against Businesses, 2005. Washington, DC: Bureau of Justice Statistics.

Rechavi, A., & Rafaeli, S., (2014). Active players in a network tell the story: Parsimony in modeling huge networks. First Monday, 19(8).

Salles-Loustau, G., Berthier, R., Collange, E., Sobesto, B., & Cukier, M., (2011). Characterizing attackers and attacks: An empirical study. In Dependable Computing (PRDC), 2011 IEEE 17th Pacific Rim International Symposium on IEEE. 174 – 183.

SANS Institute. (2007). SANS Top-20 2007 Security Risks (2007 Annual Update). Available at: http://www.sans.org/ top20/ 2007/

Scellato, S., Mascolo, C., Musolesi, M., & Latora, V., (2010). Distance matters: geo-social metrics for online social networks. In Proceedings of the 3rd conference on Online social networks. 8-8.

Spitzner, L. (2003). The honeynet project: Trapping the hackers. IEEE Security & Privacy, 1(2), 15-23.

Takhteyev, Y., Gruzd, A., & Wellman, B. (2012). Geography of Twitter networks. Social networks, 34(1), 73-81.

Tranos, E., & Nijkamp, P., (2013). The Death of Distance Revisited: Cyber-Place, Physical and

Relational Proximities. Journal of Regional Science, 53(5), 855-873.

Thelwall, M., (2002). Evidence for the Existence of Geographic Trends in University Web Site Interlinking. Journal of Documentation 58: 563-574.

Viswanath, B., Mislove, A., Cha, M., & Gummadi, K. P., (2009). On the evolution of user interaction in facebook. Proceedings of the 2nd ACM Workshop on Online Social Networks, 37-42.

Watts, D. J., (1999). Networks, dynamics, and the small-world phenomenon 1. American Journal of Sociology, 105(2), 493-527.

Watts, D. J., (2004). The "new" science of networks. Annual review of sociology. 30: 243-270.

Weisburd, D. L., Groff, E. R., & Yang, S. M., (2012). The criminology of place: Street segments and our understanding of the crime problem. Oxford University Press.

APPENDIXES

Figure 3: All BFA and Sessions relation in Israeli HP's network

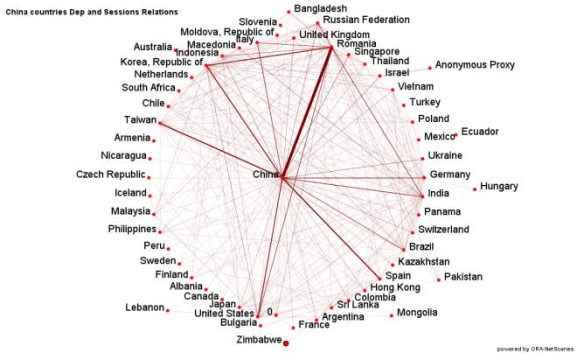


Figure 4: All BFA and Sessions relation in Chinese HP's network

Common countries in the Chinese and Israeli's Networks	Unique Countries in the Chinese Network	Unique Countries in the Israeli Network
Anonymous Proxy, Argentina, Armenia, Australia, Bangladesh, Brazil, Bulgaria, Canada, Chile, China, Colombia, Finland, France, Germany, Hong Kong, India, Indonesia, Italy, Kazakhstan, Korea, Republic of, Mexico, Netherlands, NULL, Panama, Philippines, Romania, Russian Federation, South Africa, Spain, Sweden, Taiwan, Turkey, Ukraine, United Kingdom, United States	Albania, Czech Republic, Ecuador, Hungary, Iceland, Israel, Japan, Lebanon, Macedonia, Malaysia, Moldova, Republic of, Mongolia, Pakistan, Peru, Poland, Singapore, Slovenia, Sri Lanka, Switzerland, Thailand, Vietnam, Zimbabwe	Costa Rica, Dominican Republic, Guatemala, Iran, Morocco, Saudi Arabia, Serbia, Slovakia, Venezuela

Table 1: Detailed list of countries in Chinese and Israeli HP's network