2018 3(1) 7-13 Submission: 2018/05/10, Peer review: 2018/05/20, Accepted: 2018/05/25, Published: 2018/06/30

International journal of protection, security & investigation

Publication state: Japan
ISSN: 2423-8368

Publisher: J-INSTITUTE
Website: http://www.j-institute.jp

Corresponding author
E-mail: sback008@fiu.edu

Peer reviewer
E-mail: editor@j-institute.jp

http://dx.doi.org/10.22471/protective.2018.3.1.07

Spatial and Temporal Patterns of Cyberattacks: Effective CYBERCRIME Prevention Strategies around the Globe

Back Sin-chul[1*]

Florida International University, Miami, United States

LaPrade Jennifer[2]

University of Texas, Dallas, United States

Sadhika Soor[3]

Florida International University, Miami, United States

Abstract

The issue of cyberattacks has become very pervasive and increasingly dangerous in the digital age. Many industrialized nations are highly dependent upon computer systems and other technologically supported infrastructures. An attack on such infrastructures may very likely compromise a nation's security and economic vitality. However, to date there has not been a multinational cooperation system as an effective cyberattack prevention strategy.

While the policing of high crime areas, known as hotspots, has garnered much attention among scholars and law enforcement officials, the spatial identification of hotspots in cybercrime has been limited. Routine activity theory has often been applied to explain crimes in the physical space, and consistent with this framework, a new theory has been put forth to explain crimes in cyberspace: cyber-routine activities theory. This theory contends that an unguarded virtual network must be present in addition to a potential offender and potential target in order for a cybercrime to occur. Further, unlike the spatial and temporal convergence of the physical world, the virtual world is not bound by the same spatial and temporal orderings. Due to the dynamic nature of cyberspace, a cyberattack may be committed against a target in different real-world time zones, while also allowing the attacker to escape.

The current study seeks to address gaps in the literature concerning spatial and temporal patterns of cyberattack origins and victimizations. The purpose of this study is to identify spatial and temporal patterns of cyberattack hotspots, which can help law enforcement establish an effective cybercrime prevention strategy for international communities. In terms of methodology, Geospatial Information System(GIS) technique is employed to investigate the patterns of cyberattacks and victimizations. Data was derived from the Norse website from February 15-16, 2017, which feeds a livestream of cyberattacks worldwide. The data includes cyberattack origins, types, targets, times, IP addresses, locations, and ports.

This study focuses on answering the following four research questions: Which nations are the top seven countries by count: cyberattack origins? Which nations are the top seven countries by count: cyberattack victimizations? Do the spatial hotspots for cyberattack origins differ from the spatial hotspots for cyberattack victimizations? Does a temporal pattern of cyberattacks in the daytime differ from a temporal pattern of cyberattacks in the nighttime? Thus, the findings of the current study indicate (1)the spatial hotspots of the cyber attackers and victims, and (2)the difference between temporal patterns of cyberattacks in the daytime and nighttime. Finally, policy implications and limitations of the current study are discussed.

[Keywords] ***Protection Security, Cyberattack Hotspots, Cybercrime Preventions, GIS Technique, Spatial-Temporal Patterns***

1. Introduction

Cyberattacks have been a controversial issue for modern society in recent years[1]. A cyberattack is defined as any action to alter, disrupt, deceive, degrade, or destroy a computer systems or networks for a political or national security

purpose[2]. Most industrialized nations heavily rely on the internet and technologically supported infrastructures. Consequently, if cyber perpetrators attack these critical infrastructures, national security and economic vitality could be threatened[3]. Others have argued that the use of technology by cyber perpetrators is in its infancy, but it is difficult to deny the existing and considerable risks of cyberattacks. In doing so, major cyberattack incidents have caused substantial impacts on critical infrastructures.

People are still the central actors for committing cyberattacks or cybercrimes, even though cyberattacks are actively executed by using cutting-edge technologies in the virtual environment. Research on cyberattacks has increased over the last decade. These existing studies normally focus on illustrating the law and policy of cyberattacks or the technical prevention systems of cyberattacks(e.g., cyberattack detection and firewall systems). Only a few studies assess the characteristics of cyberattacks and victimizations. Accordingly, the criminology field needs to conduct further research concerning the characteristics of cyber attackers and victims, specifically spatial and temporal characteristics for cyberattacks. As a result, the identification of spatial and temporal characteristics could be a key answer to understanding the phenomenon of cyberattacks. Thus, the purpose of this study is to examine spatial and temporal patterns of cyberattacks and victimizations through the implementation of Geographic Information System(GIS), which can assist law enforcement in establishing an effective cybercrime prevention strategy for the international communities.

2. Literature Review

2.1. Theoretical framework

From the perspective of routine activity theory[4], crime in the terrestrial world may occur when three elements(motivated offender, suitable target, and absence of capable guardian) converge in a certain space and time. According to routine activity theory, if any one of these elements are missing, then crime is less likely to occur. This theory has had an impact on crime prevention policy. For example, one way to increase the capable guardianship of an area and thereby prevent crime, according to the theory, is through the use of situational crime prevention measures, such as added lighting, CCTV cameras and increased police officers in high crime places[5][6]. However, how does routine activity theory apply to the cyber world where there is not necessarily a physical time and space convergence in order for a crime to occur?

Using the basis of routine activity theory, Choi[7] created an integrated theory, cyber-routine activities theory, to explain crimes in cyberspace since such crimes do not require the physical convergence of time and space between the victim and offender. Cyber-routine activity theory states that three elements must be present in order for a crime to occur: a potential offender, a potential target, and an unguarded virtual network. Choi especially stresses the need for a specialized form of digital guardianship to decrease the incidence of many types of cybercrime. He further argues that this guardianship must be present 24/7 because of the temporal instability of most cybercrime, unlike many types of street crime. In addition, Choi touches on the temporal aspects of cybercrime, but does not address the spatial aspects of cybercrime.

The spatial aspects of street crime have received considerable attention from criminologists and law enforcement officials in recent years. Many studies have shown that street crime is not randomly distributed in place, but generally occurs in clusters across a given area. In fact, studies consistently show that approximately 50 percent of crime calls to police are generated by a mere 3 to 5 percent of places in a city[8][9][10]. These findings have led to the identification of these “hotspots” of crime across a city, and have narrowed law enforcement efforts into those micro locations through increasing the guardianship, known as hotspot policing. Because of this heavy crime concentration, hotspot policing has generally shown to be effective in reducing crime in a given area[11][12]. While a large body of research has been conducted on hotspots of physical crime, studies on the spatial identification of hotspots of cybercrime have been limited. The current

study will address this gap.

Yar[13] argued that the condition of spatial and temporal convergence in the virtual world may differ from the condition of spatial and temporal convergence in the terrestrial world. He asserted that there is the collapse of spatial and temporal orderings between the motivated offender and suitable target. In other words, the spatial and temporal structures of cyberspace allow perpetrators to commit cyberattacks against suitable targets living in different real-world time zones(24/7) without border controls. Space transition theory[14] posits that individuals behave differently when they move from the physical space to the cyber space, due in part to the dynamic nature of cyber space. Specifically, a tenet of space transition theory associated with the current study is that there is the dynamic spatial-temporal nature of cyberspace, which can provide cybercriminals with the chance to escape. In short, based on routine activity theory, traditional crime occurs when three elements converge in a certain space and time; however, based on Choi's cyber-routine activities theory, Yar's argument, and Jaishankar's space transition theory, criminals commit cyberattacks against suitable targets without spatial and temporal orderings between offender and victim.

2.2. Present study

In addressing these gaps in the literature, the following four research questions related to determinants of spatial and temporal patterns of cyberattacks and victimizations are guided in the present study:

1. Which nations are the top seven countries by count: cyberattack origins?
2. Which nations are the top seven countries by count: cyberattack victimizations?
3. Do the spatial hotspots for cyberattack origins differ from the spatial hotspots for cyberattack victimizations?
4. Does a temporal pattern of cyberattacks in the daytime differ from a temporal pattern of cyberattacks in the nighttime?

Based on Choi, Yar, and Jaishankar, the following hypotheses are proposed for the present study.

1. There is no spatial ordering between the motivated offender and suitable target, due to the dynamic spatial-temporal nature of cyberspace.

2. There is no temporal ordering between the motivated offender and suitable target, due to the dynamic spatial-temporal nature of cyberspace.

3. Methodology

Data was collected from the Norse website, which is dedicated to providing live cyberattack intelligence that uncovers hidden breaches and tracks cyber threats emerging around the world[15]. The live cyberattacks were recorded using Ocam, a video recording tool from 00:04 on February 15, 2017 to 00:10 on February 16, 2017. The recorded data included cyberattack origins, types, targets, times, IP addresses, locations, and ports. As a next step, the researchers coded the information – cyberattack origins, IP addresses, victimizations, and times of occurrences using an Excel worksheet. The data were comprised of an Excel worksheet with 1733 cyberattack incidents worldwide. "Geocode by awesome table," a Google spreadsheets add-on, was employed to geocode longitudes and latitudes for location information of the cyberattack origins and victimizations.

The researchers used the world shapefile and the coded data set for cyberattacks. Within ArcGIS, the points were plotted using the GCS North American 1983 coordinate system. This coded data set was utilized for displaying xy data and then two files were made. These two files were joined into the world shapefile for the layer's features. After the data was joined by spatial location, it compressed the xy points into a count per country, the layer properties were opened and graduated colors were applied to create the color coded choropleth map included.

In addition, the "kernel density raster" method was utilized. The researchers created a kernel density map, which demonstrates the

hotspots for cyberattack origins and victimizations via the use of Arc Tool Box. Natural breaks with 4 classes were selected to help readers have a better understanding of the data distribution. The red color was selected to indicate the hotspots for cyberattack origins and the blue color was selected to indicate the hotspots for victimizations. Also, to clearly demonstrate the hotspots for cyberattack origins and victimizations, the researchers selected 20% transparency for the red color and 40% transparency for the purple color.

In order to create <Figure 1>, <Figure 2>, < Figure 5>, and <Figure 6>, the "select by attributes" method was employed. The researcher has respectively exported data from the files of all cyberattack origins and all victimizations. Accordingly, times of occurrences during the daytime were selected from 10:08 to 13:02 and times of occurrences during the nighttime were selected from 23:01 to 02:07. The time was limited to collect a broad range of cyberattack incidents, so the researchers utilized the simple random sampling technique to collect a certain number of samples(1733 cases).

Figure 1. Top 7 countries by count: cyberattack origins(February 15, 2017).

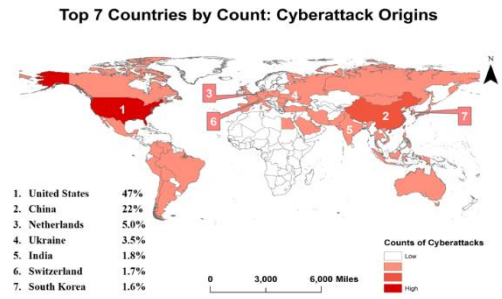
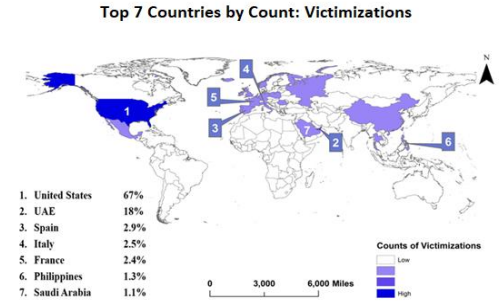


Figure 2. Top 7 countries by count: victimizations(February 15, 2017).



4. Results

The current study examined the spatial and temporal patterns of cyberattack origins and victimizations. By implementing GIS techniques, four maps were created – <Figure 1>, <Figure 2>, <Figure 5>, and <Figure 6>. <Figure 1> reveals that most cyberattacks occurred in these seven nations: United States 47%), China(22%), Netherlands(5.0%), Ukraine(3.5%), India(1.8%), Switzerland(1.7%), and South Korea(1.6%). <Figure 2> indicates that most cyberattack victimizations occurred in these seven nations: United States(67%), United Arab Emirates(18%), Spain(2.9%), Italy(2.5%), France(2.4%), Philippines(1.3%), and Saudi Arabia(1.1%).

<Figure 5> demonstrates that there are spatial concentrations for both cyberattack origins and victimizations. Interestingly, the hotspots for cyberattack origins are slightly different from the hotspots for cyberattack victimizations around the globe. For example, the hotspots for cyberattack origins are formulated on the west coast of the United States(California and Washington), western and eastern Europe(Netherlands, Switzerland, and Ukraine), and northeast Asia(China and South Korea), whereas the hotspots for cyberattack victimizations are intensively formulated on the northeast and west coast of the United States, western Europe(Spain, Italy, and France), and middle east Asia(United Arab Emirates and Saudi Arabia). According to attribute tables for both daytime and nighttime cyberattacks, 783 incidents occurred in daytime and 950 incidents occurred in nighttime. In a related sense, <Figure 6> suggests that there is no difference of temporal pattern between daytime and nighttime. In fact, temporal factors may not substantially impact the occurrence of cyberattacks.

Figure 3. Top 10 countries by count: cyberattack origins.

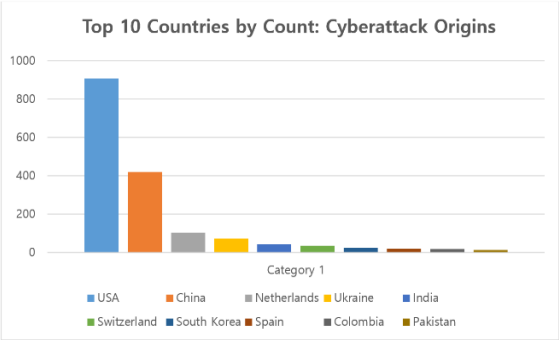


Figure 4. Top 10 countries by count: victimizations.

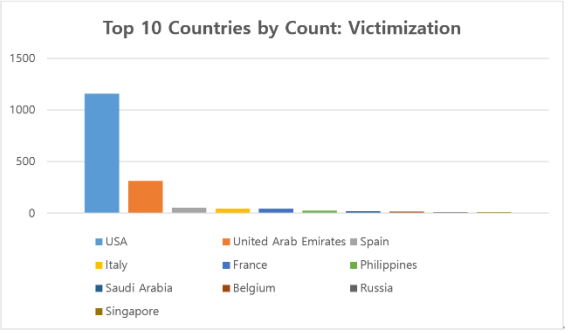


Figure 5. Hotspots: Cyberattack origins vs. victimizations(February 15, 2017).

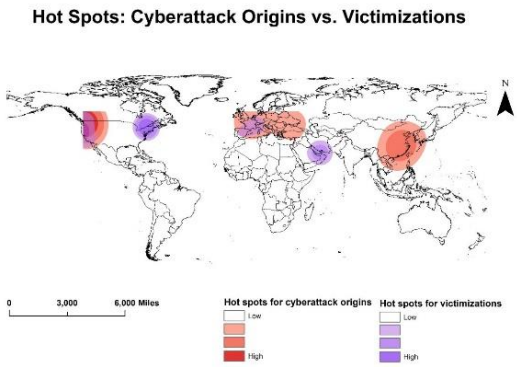
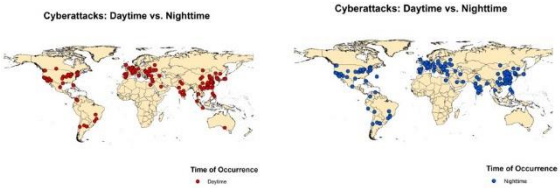


Figure 6. Cyberattack: Daytime vs. nighttime(February 15, 2017).



5. Discussion

The findings of the current study reveal that there are spatial concentrations for both cyberattack origins and victimizations, creating hotspots for cybercrime across the globe. Most cyberattacks and victimizations occurred in industrialized countries of the world. For example, nine out of 14 nations from the top seven countries for cyberattack origins and victimizations are members of G20, which is a forum for international co-operation that brings together the governments and central bank governors from 20 major economies in the world[16]. In other words, most active cyberattackers and victims live in industrialized or developed countries in the world. Also, the findings suggest that the hotspots for cyberattack origins differ from the hotspots for cyberattack victimizations. Consistent with the statements of Choi, Yar, and Jaishankar, the researchers found support for a principle element of cyberspace—that there is no spatial ordering between motivated offender and suitable target. At the same time, the findings of this study demonstrate that there is no difference of temporal pattern between daytime and nighttime. This means that the temporal factors may not substantially impact the occurrence of cyberattacks. Therefore, both hypotheses of this study were supported. As a consequence, the present study confirmed that the spatial and temporal structures of cyberspace allow perpetrators to freely commit cyberattacks against suitable targets who live in different real-world time zones(24/7) without border controls.

These findings have policy implications to reduce the occurrence of cyberattacks. According to cyber-routine activity theory, capable guardianship must be increased to reduce cyberattacks. However, because cyberattacks can be carried out globally without regards to borders, a fragmented approach with various countries taking diverse and independent actions is less likely to have an impact. Instead, the results suggest a multi-national cooperation system for the global community as an effective cyberattack prevention strategy. Due to the spatial and temporal structures of cyberspace displayed in this study, cyberattacks tend to be implemented at the transnational level on a 24/7 basis. Therefore,

global collaborative work may be an essential step to effectively combat cyberattacks[17][18]. Some steps to make progress could include an international agreement on the multifaceted problem, such as a global definition of cyberattack and cybercrime, as well as unified data collection, prevention strategies, and prosecution efforts.

Spatially, just as in hotspot policing, efforts can also be focused on "hotspots" of cybercrime. This may be efficient where there exist increased offenders as well as enhanced prevention efforts in the areas where victimization is more likely to occur. Furthermore, temporally, results of this study suggest that this monitoring must be around the clock, since no temporal association was found.

As a limitation, our analyses were only based on cross-sectional data gathered at one point in time. Consequently, the present study was limited to demonstrate the broad scope of patterns and trends regarding the spatial and temporal patterns of cyberattacks and victimizations. As another limitation, due to the size of world shapefile, it was unable to clip hotspots map in <Figure 5>. Future research should use longitudinal data to support more in-depth studies pertaining to cyberattacks.

6. Conclusion

The present study used GIS techniques to identify spatial and temporal patterns of cyberattack hotspots around the globe. Based on the work of Choi, Yar, and Jaishankar, two hypotheses were empirically examined. The first hypothesis was that there is no spatial ordering between the motivated offender and suitable target, due to the dynamic spatial-temporal nature of cyberspace. The second hypothesis was that there is no temporal ordering between the motivated offender and suitable target, due to the dynamic spatial-temporal nature of cyberspace. Using data from the Norse website detailing international cyberattacks occurring on February 15-16, 2017, the results of this study provided support for both hypotheses.

The study also identified the global hotspots of cyberattack origins, which included the west coast of the United States(California and Washington), western and eastern Europe(Netherlands, Switzerland, and Ukraine), and northeast Asia(China and South Korea). Furthermore, the results identified that the hotspots for cyberattack victimization were somewhat different and included the northeast and west coast of the United States, western Europe(Spain, Italy, and France), and middle east Asia(United Arab Emirates and Saudi Arabia).

As technology continues to advance, the risk of cyberattacks is also likely increase. Due to the unique spatial and temporal structures of cyberspace, traditional crime prevention measures are unlikely to be effective. Therefore, a 24/7 global effort across time and space will be necessary to reduce cyberattacks.

7. References

7.1. Journal articles

[1] Holt TJ & Kilger M & Chiang L & Yang CS. Exploring the Correlates of Individual Willingness to Engage in Ideologically Motivated Cyberattacks. *Deviant Behavior*, *38*(3), 356-373 (2017).

[2] Hathaway O & Crootof R & Levitz P & Nix H & Nowlan A & Perdue W & Spiegel J. The Law of Cyber-attack. *California Law Review*, 100(4), 817-885 (2012).

[3] Ten CW & Manimaran G & Liu CC. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. *IEEE Transactions on Systems Man and Cybernetics-Part A: Systems and Humans*, *40*(4), 853-865 (2010).

[4] Cohen LE & Felson M. Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44, 588-608 (1979).

[5] Clarke RV. Situational Crime Prevention. *Crime and Justice*, 19, 91-150 (1995).

[7] Choi K. Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, 2(1), 308-333 (2008).

[8] Sherman L & Gartin P & Buerger M. Hot

Spots of Predatory Crime: Routine Activities and the Criminology of Place. *Criminology*, 27(1), 27-56 (1989).
[9] Summers L & Johnson SD. Does the Configuration of the Street Network Influence Where Outdoor Serious Violence takes Place? Using Space Syntax to Test Crime Pattern Theory. *Journal of Quantitative Criminology*, *33*(2), 397-420 (2017).
[10] Weisburd D & Telep CW. Hot Spots Policing: What We Know and What We Need to Know. *Journal of Contemporary Criminal Justice*, 30(2), 200-220 (2014).
[11] Sherman LW & David W. General Deterrent Effects of Police Patrol in Crime Hot Spots: A Randomized Controlled Trial. *Justice Quarterly*, 12(4), 625-648 (1995).
[12] Braga AA & Andrew VP & David MH. The Effects of Hot Spots Policing on Crime: An Updated Systematic Review and Meta-analysis. *Justice Quarterly*, 31(4), 633-663 (2014).
[13] Yar M. The Novelty of Cybercrime an Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427 (2005).

7.2. Books

[6] Eck J & Guerette R. Own the Place own the Crime-prevention How Evidence about Place-based Crime Shifts the Burden of Prevention. The Future of Criminology. New York Oxford University Press (2012).
[14] Jaishankar K. Space Transition Theory of Cyber Crimes. Crimes of the Internet 283-301 (2008).
[17] Choi KS. Cyber Criminology and Digital Investigation (2015).
[18] Holt TJ & Burruss GW & Bossler A. Policing Cybercrime and Cyberterror (2015).

7.3. Additional references

[15] http://www.norse-corp.com (2018).
[16] http://www.oecd.org (2018).

Lead Author
Back Sin-chul / Florida International University Researcher
B.S. Northeastern University
M.S. Bridgewater State University
Ph.D. Florida International University

Research field
- Capable Guardianship and Crisis of Identity Theft in the United States: Expanding Cyber-routine Activities Theory, International Journal of Crisis & Safety, 2(1) (2017).
- The Effect of Terrorism Risk Perception and Agency's Interaction on Police Homeland Security Preparedness, International Journal of Police & Policing, 2(1) (2017).

Major career
- 2007~2008. Korean National Assembly, Legislative Aide.
- 2011~2012. Massachusetts State House, Legislative Aide.
- 2017~Present. Florida International University, Teaching Assistant.

Co-Author
LaPrade Jennifer / University of Texas Researcher
B.A. University of Texas at Dallas
M.A. University of Texas at Dallas
Ph.D. University of Texas

Research field
- The Effect of Terrorism Risk Perception and Agency's Interaction on Police Homeland Security Preparedness, International Journal of Police and Policing, 2(1) (2017).

Major career
- 2013~present. The University of Texas at Dallas, Teaching Assistant.
- 2015~present. Brookhaven College, Adjunct Professor of Government.

Co-Author
Sadhika Soor / Florida International University Researcher
B.A. University of Ottawa
M.S. Florida International University

Research field
- Juvenile Hackers: A Test of Self-control and Social Bonding Theories, Paper Presented at Academy of Criminal Justice Sciences(ACJS), New Orleans, LA (2018).

Major career
- 2017~2018. Everglades Correctional Institution, Internship.
- 2018~present. Florida International University, Research Assistant.