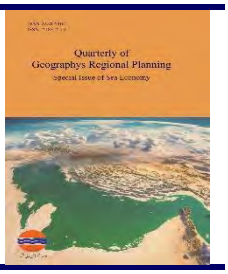
Iranian Association of Geopolitical

Geography(Regional Planning)

Special Issue, Number 2, Winter 2024

ISSN (Print): 2228-6462 - ISSN (Online): 2783-2112

Journal Homepage: https://www.jgeoqeshm.ir/



Research Paper

Evaluation and ranking of indicators in the geographical domain of cyberspace management effective in preventing harmful activities of cyberspace communication from the point of view of university professors

Akram Hafezi*[1]

1. Assistant Professor, Department of Curriculum Planning, Farhangian University, Tehran, Iran

Extended Abstract

ARTICLEINFO

PP: 609-620

Use your device to scan and read the article online

Keywords:
Geographical indicators, management of virtual space, harmful communication activities, cyber space

Abstract

The purpose of the present research was to evaluate and rank the indicators of the geographical domain of virtual space management that are effective in preventing the harmful activities of cyber space communication from the point of view of university professors. In terms of purpose, this research is applied and falls under descriptive-survey research. The statistical population includes all prominent professors in the field of planning and management of Farhangian University of Tehran. First, using the purposeful sampling method, 15 professors who were teaching in Farhangian University of Tehran in the academic year of 2023-2024 were selected as a sample. The research tool includes a researcher-made questionnaire to measure the impact of indicators in the geographical domain of virtual space management. There is a significant difference between the functional indicators of the geographical domain of virtual space management in terms of ranking. According to the results obtained, according to the professors of Farhangian University of Tehran, among the effective factors, in the order of the factor, "the greater dependence of electronics on the cyber network, the transformation of the structure of the cyber military and military forces, the ability to influence the political structures of the country, the management of software production, the centrality of presence "main search engines" have the greatest impact on preventing harmful activities of cyberspace oommunooooooos (p≤. .005)

* **Corresponding author:** Akram Hafezi, **Email:** ak_hafezi@yahoo.com

Citation: Hafezi.A. (2024). **Evaluation and ranking of indicators in the geographical domain of cyberspace management effective in preventing harmful activities of cyberspace communication from the point of view of university professors**. Geography(Regional Planning), Special Issue, Number 2, 609-620.

DOI: 10.22034/JGEOQ.2024.273034.2931

Extended Abstract

Introduction

Today, the methods of communicating with others through the Internet have increased greatly and at a very high speed. In recent years, we have seen the harmful effects of cyber activities, such as cyber harassment, all over the world. Paying attention to the theories of many researchers shows that identifying the effects of virtual space management and preventing the negative effects of virtual space is one of their concerns, and an important part of their theories is also dedicated to explaining the geographic indicators of virtual space control.

Methodology

In terms of purpose, this research is applied and falls under descriptive-survey research.

Results and Discussion

According to the results of the above table, the most average indicators of the geographical domain of virtual space management are effective in preventing the harmful activities of cyber space communication from the point of view of university professors, in order of increasing dependence of electronics on the cyber network 4.6, the ability to access government and individual information 26 4/4, transformation of the structure of cyber military and military forces 3/8; The ability to influence the country's political structures was 3.6, software production management was 3.26, the centrality of the presence of the main search engines was 3.13. The above table is related to the ranking of the importance of each of the functional indicators of the geographical domain of virtual space management on preventing harmful activities of cyber space communication based on the Friedman test. Considering that the chi-square value (28.486) with the degree of freedom (2) is significant at the level of 0.05, it can be said that there is a significant difference between the functional indicators of the geographical domain of virtual space management in terms of ranking. According to the results obtained, according to the professors of Farhangian University of Tehran, among the effective factors, in the order of the factor, "the greater dependence of electronics on the cyber network, the transformation of the structure of the cyber military and military forces, the ability to influence the political structures of the country, the management of software production, the centrality of presence The main search engines have the greatest impact on preventing harmful activities of cyber space communication.

Conclusion

The purpose of the current research was to evaluate and rank the indicators of the geographical domain of virtual space management that are effective in preventing the harmful activities of cyber space communication from the perspective of the professors of Farhangian University of Tehran. The results showed that there is a significant difference between the indicators of the geographical area in terms of ranking. Now the virtual space is known not only as the newest field of war, but also as a vital space for economic, educational and cultural development for all countries. By considering the geographical indicators for the management of cyber space, researchers, policy makers and law enforcement organizations can better understand the cyber dynamics, the factors affecting the prevention of cyber damages and its harmful activities. The effects and regulatory challenges related to cybercrimes can provide targeted interventions and strategies to effectively prevent and reduce cybercriminal activities. Furthermore, understanding the cybercriminal activities and demographics of these groups becomes essential in creating policies and political strategies to address cybercrime and cyberwarfare.

References

1. Abadi, M. A. (2018). Commercial Law, Ganj-e-Danesh, 37th edition.
2. Arrrr ī, H. (8888). Ciii lCccccddrr e [In Persian]. Majd Scientific Cultural Assembly, 2nd edition.
3. Alizadeh, A., & Asadi Ataie, M. (2016). Regulations of Cooperatives: Collection of Laws and Regulations of the Cooperative Sector of the Islamic Republic of Iran, Arman Kherad Publications, 3rd edition. [In Persian]
4. Aminī, ,,, & aa nuuuri, A. ([[[[ ). Justifiability and legitimacy of domestic arbitration awards: A

judicial perspective. Private Law Research Journal, 6(22). [In Persian]
5. Annabi, Alireza, 1401, Geopolitics and cyber space, the third national cyber defense conference, Maragheh, https://civilica.com/doc/1493938[In Persian].
6. Chen, M., Claramunt, C., Çöltekin, A., Liu, X., Peng, P., Robinson, A. C., ... & Lü, G. (2023). Artificial intelligence and visual analytics in geographical space and cyberspace: Research opportunities and challenges. *Earth-Science Reviews*, *241*, 104438.
7. Fuerlinger, G., & Garzik, L. (2022). Silicon Valley Innovation System. *Successful Innovation Systems: A Resource-oriented and Regional Perspective for Policy and Practice*, 225-247.
8. Gao, S., Chen, H., Luo, W., Hu, Y., & Ye, X. (2018). Spatio-temporal-network visualization for exploring human movements and interactions in physical and virtual spaces. *Human Dynamics Research in Smart and Connected Communities*, 67-80.
9. Gundur, R. V., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L. Y.-C., & Mejía, D. D. (2021). Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context. In CrimRxiv. https://doi.org/10.21428/cb6ab371.5f335e6f
10. Hall, T., Sanders, B., Bah, M., King, O., & Wigley, E. (2021). Economic geographies of the illegal: The multiscalar production of cybercrime. Trends in Organized Crime, 24(2), 282–307. https://doi.org/10.1007/s12117-020-09392-w
11. Heydari, Hassan, Milani, Dr. Alireza. (1401). A comparative study of the territorial jurisdiction in dealing with cybercrimes based on Iran's criminal system. Scientific Journal of Law and Modern Studies, 3(4), 1-22. [In Persian].
12. Karimi Pashaki, Sajjad, and Pishgahi Fard, Zahra. (2013). Geographic perspective in the analysis of cyberspace functionality. Geospace, 14(47), 233-256. SID. https://sid.ir/paper/91461/fa[In Persian].
13. Khan, M., Wu, X., Xu, X., & Dou, W. (2017, May). Big data challenges and opportunities in the hype of Industry 4.0. In *2017 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.
14. Lee, R., Wakamiya, S., & Sumiya, K. (2015). Exploring geospatial cognition based on location-based social network sites. *World Wide Web*, *18*, 845-870.
15. Motaghi Dastanai, Afshin, Ahmadi Nouhdani, Siros, and Shafiei, Babak. (1400). Cyberspace is a new platform for exercising social power. Iranian Social Development Studies, 14(1), 271-286. SID. https://sid.ir/paper/1063648/fa [In Persian].
16. Raff, E., & Nicholas, C. (2020). A Survey of Machine Learning Methods and Challenges for Windows Malware Classification (arXiv:2006.09271). arXiv.
17. Roth, C., Mazières, A., & Menezes, T. (2020). Tubes and bubbles topological confinement of YouTube recommendations. *PloS one*, *15*(4), e0231703.
18. Sheldon, J. B. (2014). Geopolitics and cyber power: Why geography still matters. *American Foreign Policy Interests*, *36*(5), 286-293.
19. Wright, D. C. S. (2023). Geographical Aspects of Cybercrime: A Literature Review. Available at SSRN 4521486.

فصلنامه جغرافیا (برنامه ریزی منطقه ای)

دوره ۱۳، شماره ۵۱، پ ۱۴۰۲

شاپا چاپی: ۶۴۶۲- ۲۲۲۸ شاپا الکترونیکی: ۲۱۱۲ -۲۷۸۳

Journal Homepage: https://www.jgeoqeshm.ir/

انجمن ژئوپلیتیک ایران

مقالهٔ پژوهشی

ارزیابی و رتبه‌بندی شاخص‌های حوزهٔ جغرافیایی مدیریت فضای مجازی مؤثر بر جلوگیری از فعالیت‌های زیانبار ارتباطات فضای سایبری از دیدگاه اساتید دانشگاه

اکرم حافظی*– استادیار، گروه برنامه‌ریزی درسی، دانشگاه فرهنگیان، تهران، ایران.

اطلاعات مقاله

شمارهٔ صفحات: ۶۰۹-۶۲۰

از دستگاه خود برای اسکن و خواندن مقاله به صورت آنلاین استفاده کنید.

چکیده

هدف از انجام پژوهش حاضر ارزیابی و رتبه‌بندی شاخص‌های حوزهٔ جغرافیایی مدیریت فضای مجازی مؤثر بر جلوگیری از فعالیت‌های زیانبار ارتباطات فضای سایبری از دیدگاه اساتید دانشگاه بود. این پژوهش از نظر هدف، کاربردی و در زمرهٔ تحقیقات توصیفی – پیمایشی قرار می‌گیرد. جامعهٔ آماری شامل تمامی اساتید مطرح حوزهٔ برنامه‌ریزی و مدیریت دانشگاه فرهنگیان تهران است. ابتدا با استفاده از روش نمونه‌گیری هدفمند تعداد ۱۵ نفر از اساتید به عنوان نمونه‌ای که در سال تحصیلی ۱۴۰۳-۱۴۰۲ در دانشگاه فرهنگیان تهران مشغول به تدریس بودند، انتخاب شدند. ابزار پژوهش شامل پرسشنامهٔ محقق ساختهٔ سنجش تأثیر شاخص‌های حوزهٔ جغرافیایی مدیریت فضای مجازی است. بین شاخص‌های کارکردی حوزهٔ جغرافیایی مدیریت فضای مجازی از نظر رتبه‌بندی اختلاف معناداری وجود دارد. بر اساس نتایج حاصل شده، طبق نظر اساتید دانشگاه فرهنگیان تهران از بین عوامل مؤثر به ترتیب عامل «وابستگی هرچه بیشتر الکترونیک به شبکهٔ سایبر، دگرگونی ساختار قوای نظامی و ارتشی سایبری، قابلیت اثرگذاری بر ساختارهای سیاسی کشور، مدیریت تولید نرم‌افزارها، مرکزیت حضور موتورهای اصلی جستجو» بیشترین تأثیر را بر جلوگیری از فعالیت‌های زیانبار ارتباطات فضای سایبری دارند ($p\leq 0/005$).

واژه‌های کلیدی:

شاخص‌های حوزهٔ جغرافیایی، مدیریت فضای مجازی، فعالیت‌های زیانبار ارتباطات، فضای سایبری.

استناد: حافظی، اکرم. (۱۴۰۳). **ارزیابی و رتبه‌بندی شاخص‌های حوزهٔ جغرافیایی مدیریت فضای مجازی مؤثر بر جلوگیری از فعالیت‌های زیانبار ارتباطات فضای سایبری از دیدگاه اساتید دانشگاه،** فصلنامه جغرافیا (برنامه‌ریزی منطقه‌ای)، ویژه‌نامه، شماره ۲، صص ۶۲۰-۶۰۹

DOI: 10.22034/JGEOQ.2024.273034.2931

* **نویسنده مسئول:** اکرم حافظی، **پست الکترونیکی:** ak_hafezi@yahoo.com

مقدمه

امروزه روش‌های ارتباطی با دیگران از طریق اینترنت، به شدت و با سرعت بسیار زیاد افزایش یافته است .طی سال‌های اخیر شاهد اثرات زیانبار فعالیت‌های سایبری، مانند آزار و اذیت سایبری، در سراسر جهان هستیم. توجه به نظریات بسیاری از محققین نشان می‌دهد که شناسایی اثرات مدیریت فضای مجازی و پیشگیری از اثرات منفی فضای مجازی یکی از دغدغه‌های آنها بوده و جزء مهمی از تئوری‌های آنان نیز به تبیین شاخص‌های جغرافیایی کنترل فضای مجازی اختصاص داشته است.

در سال‌های اخیر، جامعه در سطح جهانی با امنیت فضای مجازی و لزوم توجه بسیار زیاد به این مقوله روبرو شده‌اند، لذا چالش‌های فعالیت‌های زیانبار در فضای مجازی را می‌توان حد نهایت مشکلات کنونی دولت‌های مدرن دانست. اهمیت انتخاب پروژه در این است که با بررسی‌های صورت گرفته مشخص گردید تحقیقات کمّی در رابطه با تأثیر استراتژیک شاخص‌های حوزهٔ جغرافیایی مدیریت فضای مجازی بر جلوگیری از فعالیت‌های زیانبار ارتباطات فضای سایبری، صورت پذیرفته است که نیاز به شناسایی این محیط و آشنایی با نحوهٔ مدیریت آن دیده می‌شود و در این راستا نیازمند به شناسایی مؤلفه‌ها و شاخص‌های مطرح شدهٔ جغرافیایی در سطح کشورهای دنیا می‌باشیم. با توجه به مسائل و مشکلاتی که به دلیل توسعهٔ تکنولوژی و پیشرفت‌های امروزه در جهان و عواقب ناشی از این پیشرفت در دنیای مجازی به وجود آمده لذا لزوم انجام این تحقیق دیده می‌شود که شامل فرضیهٔ زیر می‌باشد: به ترتیب کدام یک از شاخص‌ها و مؤلفه‌های کارکردی حوزهٔ جغرافیایی مدیریت فضای مجازی بر جلوگیری از فعالیت‌های زیانبار ارتباطات فضای سایبری موثر است؟

مبانی نظری

پیشرفت بشر در زمینه‌های مختلف همواره مشکلاتی را نیز دربر داشته است، یکی از این پیشرفت‌ها مربوط به توسعهٔ فناوری اطلاعات و ارتباطات است که از آن جمله می‌توان به ظهور پدیده‌ای به نام اینترنت اشاره کرد، فضای مجازی سبب ارتباط بیشتر اشخاص در سراسر گیتی شده به نحویکه مرزها را درنوردیده و با سرعت زیاد خود باعث تسهیل ارتباطات و انتقال اطلاعات می‌شود. رایانه‌ها ابزار دسترسی به اینترنت در فضای مجازی محسوب شده و با فشردن یک کلید، حجم زیادی از اطلاعات در یک لحظه از یک نقطه به نقطهٔ دیگر قابل ارسال خواهد بود، نقاطی که ممکن است در دو سوی کرهٔ خاکی قرار داشته باشد. لازم به ذکر است که فضای سایبر منحصر به اینترنت نبوده و شامل ماهواره‌های واقع در مدار زمین و ایستگاه‌های زمینی آنها نیز می‌شود لیکن از نظر کاربرد، مهم‌ترین بخش فضای سایبر را اینترنت تشکیل می‌دهد چرا که از نظر تعداد و تنوع کاربران و طیف وسیع ارتباطات و اطلاعات مورد مبادله، اینترنت بیشترین سهم در این فضا دارد (حیدری و میلانی، ۱۴۰۱).

داده‌های جغرافیایی (به عنوان مثال مکان، هویت و معناشناسی) که فضای جغرافیایی و فضای مجازی را به هم متصل می‌کند، فرصت‌هایی را برای درک بهتر رفتارهای انسانی در مقیاس‌های مختلف با وضوح مکانی و زمانی بی‌سابقه ارائه می‌دهد (Lee et al, 2015). از آنجایی که داده‌های فعالیت انسانی در زمان واقعی با فرکانس زمانی بالا تولید می‌شوند، نظارت و تجزیه و تحلیل پویایی‌های مکانی – زمانی برای فعالیت‌های پیچیدهٔ انسانی در یک بافت شهری فعال می‌شود (Roth et al, 2020). با این وجود، شکی نیست که کلان داده چالش‌هایی را در رابطه با ویژگی‌های آن (یعنی ابعاد آن) ایجاد می‌کند (Khan et al, 2017). علاوه بر چالش‌های ابعادی و غیرخطی در مقادیر زیادی از داده‌های تولید شده، علم اطلاعات جغرافیایی و علوم سایبری با هم ممکن است مسیرهای جدیدی را برای پردازش هوشمند فراهم کنند، در حالیکه چالش‌های جدید و پیچیده‌ای را نیز مطرح می‌کنند. استانداردهای داده، اخلاقیات و رویکردهای مدل سازی را می‌توان در پرتو این فضاهای اطلاعاتی جدید مورد بازنگری قرار داد. نحوهٔ ارتباط فضای فیزیکی با فضای مجازی می‌تواند چالش‌های مدل سازی داده‌ها را افزایش دهد. به عنوان مثال، یک دستگاه هوشمند متصل به اینترنت هنگام استفاده از شبکه‌های مختلف می‌تواند بیش از یک آدرس IP داشته باشد که ممکن است بر دقت داده‌ها تأثیر بگذارد. علاوه بر این، با استفاده از محتوای جغرافیایی تولید شده توسط کاربر، جعل موقعیت مکانی می‌تواند مشکلات

کیفیت داده‌ها را زمانی که کاربران این روش‌ها را برای بهبود حفاظت از حریم خصوصی داده‌ها اتخاذ می‌کنند، ایجاد کند (Gao et al, 2018). علاوه بر این، فضای مجازی یک محیط حاصلخیز برای رشد داده‌های منسوخ و بی‌فایده (به عنوان مثال ایمیل‌های ناخواسته و هرزنامه‌های ربات) است، و این پتانسیل وجود دارد که فضای سایبری مملؤ از داده‌های زباله شود (Chi et al, 2013). بنابراین، تجسم و اجرای یک فضای مجازی پایدار و «پاک» ضروری است (Chen et al, 2023).

جرایم سایبری به موضوعی فراگیر و پیچیده در دنیای به هم پیوستهٔ امروزی تبدیل شده است که تهدیدات قابل توجهی برای افراد، مشاغل و دولت‌ها به همراه دارد. هدف این مقاله ارائهٔ یک مرور کلی از جنبه‌های مختلف مربوط به جرایم سایبری، از جمله زمینهٔ تاریخی، ابعاد جمعیتی و جغرافیایی، تأثیرات محیطی و استراتژی‌های پیشگیرانه است. با درک بافت تاریخی، جنبه‌های جمعیتی و جغرافیایی، تأثیرات محیطی و استراتژی‌های پیشگیرانه، سیاست‌گذاران، سازمان‌های مجری قانون و محققان می‌توانند برای مبارزهٔ مؤثر با تهدیدات سایبری همکاری کنند. چنین رویکرد جامعی به ایجاد محیط دیجیتالی امن‌تر و محافظت از افراد، سازمان‌ها و جوامع در برابر اثرات نامطلوب جرایم سایبری کمک می‌کند. علاوه بر این، از طریق تحقیقات و همکاری مداوم، می‌توان راه‌حل‌های نوآورانه را توسعه داد و با چشم‌انداز در حال تحول تهدیدات سایبری سازگار شد و آیندهٔ دیجیتالی امن و انعطاف‌پذیر را تضمین کرد (Wright, 2022). مطالعهٔ چن و همکاران (۲۰۲۳) بر اهمیت درک زمینهٔ جغرافیایی که در آن جرایم سایبری رخ می‌دهد تأکید می‌کند. با در نظر گرفتن چشم‌انداز سیاسی، شرایط اقتصادی و پویایی اجتماعی یک منطقه، محققان می‌توانند ماهیت چند وجهی جرایم سایبری را درک کنند. علاوه بر این، این دیدگاه گسترده‌تر به شناسایی انگیزه‌ها، استراتژی‌ها و تاکتیک‌های مختلف مجرمان سایبری کمک می‌کند و امکان توسعهٔ مداخلات هدفمند و استراتژی‌های پیشگیری را فراهم می‌کند.

مطالعهٔ جرایم سایبری از منظر جغرافیایی شامل کاوش در چندین حوزهٔ کلیدی متقاطع جغرافیای انسانی است. این رویکرد بینش‌های ارزشمندی را در مورد پویایی‌های فضایی، عوامل اجتماعی و تغییرات منطقه‌ای مرتبط با فعالیت‌های مجرمانهٔ سایبری ارائه می‌دهد (Hall, et al, 2021). با بررسی این حوزه‌ها، محققان می‌توانند ماهیت چند وجهی جرایم سایبری را درک کرده و استراتژی‌های مؤثری برای مبارزه با آن ایجاد کنند. مفهوم شکاف دیجیتال در مطالعهٔ جرایم سایبری از منظر جغرافیایی نیز اهمیت دارد. بررسی تفاوت‌ها در دسترسی و استفاده از فناوری‌های دیجیتال در میان مناطق و گروه‌های اجتماعی مختلف، چگونگی دسترسی نابرابر ممکن است به آسیب‌پذیری‌ها و فرصت‌های مجرمانه کمک کند (اسمار و همکاران، ۲۰۲۲). درک تأثیر شکاف‌های دیجیتال به توسعهٔ مداخلات و سیاست‌های هدفمند برای پُر کردن شکاف و کاهش خطرات جرایم سایبری کمک می‌کند (Hall, et al, 2021).

همکاری فرامرزی بین سازمان‌های مجری قانون در رسیدگی به جرایم سایبری فراملی بسیار مهم است (روهونن، ۲۰۲۳). در واقع؛ همکاری بین سازمان‌های مجری قانون کشورهای مختلف برای به اشتراک گذاشتن اطلاعات، هماهنگی تحقیقات، و دستگیری مجرمان سایبری که در فراسوی مرزها فعالیت می‌کنند، ضروری است (Menon & Guan Siew, 2012) .علاوه بر این، درک جنبه‌های ژئوپلیتیکی که بر پویایی جرایم سایبری تأثیر می‌گذارند، به شناسایی تأثیر متقابل بین عوامل سیاسی، اقتصادی و اجتماعی و تأثیر آنها بر فعالیت‌های مجرمانهٔ سایبری کمک می‌کند (لاورگنا، ۲۰۲۰). بررسی ابعاد فراملی جرایم سایبری درک جامعی از گسترهٔ جهانی آن و چالش‌های مرتبط با مبارزه با آن را فراهم می‌کند (پیترز و جردن، ۲۰۱۹).

حوزهٔ جغرافیایی اینترنت

همچنان که شبکهٔ برق یک شهر و یا کشور دارای مولد تولید برق می‌باشد؛ شبکهٔ اینترنت نیز دارای کانون‌هایی جهت راهبری و مدیریت شبکه می‌باشد و تولید فضای مجازی و راهبری جریان اطلاعات در این فضا از نقاط جغرافیایی خاصی در جغرافیای سیاسی جهان انجام می پذیرد که در منطقهٔ «سیلیکونولی» واقع شده است. درهٔ سیلیکون نام رایج منطقه‌ای در ایالت کالیفرنیای آمریکا است. شهرت این منطقه به دلیل قرار داشتن بسیاری از شرکت‌های مطرح انفورماتیک جهان در این منطقه می‌باشد.

درهٔ سیلیکون نقش کلیدی در توسعهٔ فناوری‌های نوآورانه و هموار کردن راه برای روندهای جدید جهانی ایفا می‌کند. این منطقه در حال حاضر رهبر بلامنازع صحنه‌های نوآوری و استارت آپی جهانی است (فورلینگر و گارزیک، ۲۰۲۲).

امروزه انقلاب ارتباطی و اطلاعاتی سبب گردیده که این حوزهٔ جغرافیایی کنترل سرنوشت خود و بسیاری از دیگر کشورها را در فضای مجازی در اختیار داشته باشد. این حوزهٔ جغرافیایی مرکزیت جمع‌آوری، توزیع و پردازش جریان‌های اطلاعاتی و ارتباطی و به طور کلی فرآیند مدیریت بر شبکه را بر عهده دارد و به تبع آن از اهمیت استراتژیک فزاینده‌ای برخودار گردیده است. بنابراین اصطلاح سلطه که به طور سنتی برای اشاره به نفوذ یا اقتدار یک قدرت برتر و مسلط در فضای عینی به کار می‌رود در دورهٔ حاضر در معنای وسیع‌تر حائز شرایط اطلاق به مناطق و نقاط راهبردی و مدیریت شبکهٔ سایبر در سیلیکونولی خواهد بود. بر پایهٔ این خصوصیات و کارکردها این حوزهٔ جغرافیایی توانایی تحت فشار قرار دادن و بازدارندگی طرف‌های رقیب و تحت تأثیر قرار دادن سیاست‌های آنها را دارند (اونز و نی، ۱۹۹۶).

فضای سایبر

فناوری‌های‌نوین، فضایی را به وجود آورده است به نام فضای سایبر. این فضا مجازی نیست بلکه کاملاً واقعی است و انسان همهٔ پدیده‌های فضای واقعی زندگی خود را در این فضا شبیه سازی کرده است. این فضا افراد و بازیگران بین‌المللی را با یکدیگر همراه می‌کند و ساختارهای سیاسی و اقتصادی را با ماهیت سایبری و بدون هیچ فاصلهٔ جغرافیایی در کنار یکدیگر قرار می‌دهد به طوریکه کشورها، سازمان‌های بین‌دولتی و چندملیتی بدون هیچ واسطه و مرز، با یکدیگر تعامل می‌کنند. در واقع به نوعی‌شاهد هژمونی فضای سایبر بر همهٔ ابعاد زندگی بشر هستیم. تجهیزات فنّاورانهٔ پیشرفته که قادر به نمایش فضاهای واقعیت مجازی در فضای سایبری بین‌المللی جهانی هستند به طور گسترده در بازارهای جهانی توزیع شده است. زیرساخت‌های اطلاعاتی بازیگران فردی را در صحنهٔ جهانی بین‌المللی متحد می‌کند. ساختارهای سیاسی، اقتصادی و اجتماعی – فرهنگی بین‌المللی به صورت مجازی وجود دارند. مکانیسم‌های حکمرانی در سیستم، منطقه‌ای و مبتنی بر نظام شبکه‌ای است. سیاست بین‌الملل بیشتر به صورت اجتماعی ساخته می‌شود تا فضای واقعیت عینی. عصر سایبر که گاهی آن را فضای مجازی یاد می‌کنند، در واقعیت اتفاق می‌افتد که بیشتر نشان دهندهٔ قدرت فناورانهٔ کشورهای توسعه یافته است. این تحول جهانی که دوره‌ای در گهواره‌های تمدنی اتفاق می‌افتد این بار وارد عصر اطلاعات و ارتباطات گردید، از آنجایی که هر تغییر، دسته‌بندی تمدنی قدرت اجتماعی جوامع را تحت تأثیر خود قرار می‌دهد این تحول عصر سایبر، قدرت اجتماعی را برای گروهی از کشورهای صاحب فنّاوری به همراه داشته است، قدرت اجتماعی که در مقولهٔ مؤلفهٔ قدرت کشور ملت‌ها بررسی می‌شود به دلیل هزینهٔ کمتر و تأثیرگذاری بیشتر مورد توجه خیل عظیمی از کشور و ملت‌ها قرارگرفته است (متقی دستنائی و همکاران، ۱۴۰۱).

ژئوپلیتیک و قدرت سایبری

ژئوپلیتیک یک علم میان رشته‌ای بوده که به تأثیر عوامل جغرافیایی در مقوله‌ها و موضوعات سیاسی و روابط بین‌المللی می‌پردازد. با خلق فضای سایبری حوزهٔ جغرافیایی سایبری نیز در کانون توجه تصمیم سازان و بازیگران دنیای سیاست قرار گرفت و فضای سایبری در ابعاد مختلفی چون؛ تحول در فضای مورد رقابت در ژئوپلیتیک؛ همگرایی و همکاری میان ملل دنیا، تحول در ماهیت قدرت و توسعهٔ عناصر دخیل در تکوین قدرت، فرآیند کنترل و مدیریت فضای سایبری؛ تحول در روابط حاکمان با شهروندان و منازعات در حوزهٔ سایبری در گسترهٔ جهانی، صحنه گردانان عرصهٔ سیاست داخلی و بین‌المللی را به چالش واداشته است. طوریکه امروزه فضای سایبری به اندازهٔ فضای واقعی مهم بوده و در تکوین و تحول جریانات ملی و بین‌المللی مؤثر است (عنابی، ۱۴۰۱).

در بسیاری از تحلیل‌های استفاده از قدرت سایبری در سیاست بین‌الملل و سیاست خارجی آمده است که ژئوپلیتیک واقع‌گرا دیگر اهمیتی ندارد. حتی وقتی در چنین تحلیلی از واژهٔ ژئوپلیتیک استفاده می‌شود، گویی جغرافیا از سیاست جدا شده است. در حالیکه بدون شک فضای سایبری به دلیل زیرساخت فیزیکی آن از رایانه‌های شبکه‌ای، کابل‌ها و ماهواره‌ها پایه‌ای جغرافیایی دارد، به طور گسترده فرض می‌شود که موقعیت جغرافیایی هیچ ارتباطی با استفادهٔ سیاسی از قدرت سایبری توسط دولت‌ها و بازیگران

غیردولتی ندارد. در حالیکه فضای سایبری زمان و مکان را به روش‌های آشکار کوچک می‌کند، تنظیمات جغرافیایی همچنان در استفاده از قدرت سایبری اهمیت دارد. علاوه بر این، درک ژئوپلیتیک قدرت سایبری می‌تواند به سیاست‌گذاران و تحلیل‌گران کمک کند تا هویت، انگیزه‌ها و مقاصد افراد را درک کنند (Sheldon, 2014).

جغرافیا و کارکرد فضای سایبر

به طور معمول اگرچه جغرافیا بر مبنای عناصر طبیعی و ارتباطات متقابل آن با انسان معنا می‌یابد، اما فارغ از کارکردها و نقش‌آفرینی این عناصر، امروزه، دامنه‌های جدیدی از فضا شکل گرفته که با توجه به ارتباط آن با گسترهٔ جغرافیایی بیانگر شمای جدیدی از فضای جغرافیایی می‌باشد. تلاش انسان برای پدید آوردن جهانی به موازات جهان طبیعی به دلیل آنکه انسان و محیط یا از طریق آزمون و خطا و یا از طریق تجارب و علم با یکدیگر در ارتباط می‌باشند، باعث شد تا ساختارهای مبتنی بر شبیه سازی مدنظر محققان و دانشمندان قرار گیرد، تا از صرف هزینه‌های مادی، معنوی و زمانی در پیشبرد هرچه سریع‌تر علم جلوگیری شود. از این‌رو، فضای مجازی از علم سایبرنتیک یعنی مناسبات میان انسان و ماشین منبعث شده که در شکل پیشرفته‌تر آن به وجود آوردندهٔ واقعیت‌های مجازی، الگوهای شبیه سازی مجازی و فضای سایبر می‌باشد (کریمی پاشاکی، ۱۳۹۳). نتایج پژوهش کریمی پاشاکی و همکاران (۱۳۹۳) نشان داد که میان توسعهٔ تکنولوژی ارتباطی و جغرافیا، ارتباط معناداری وجود دارد که منجر به رشد دامنه‌های فضای شبکه‌ای و توسعهٔ تحلیل‌های فضایی در جغرافیای فضای سایبر می‌گردد. بنابراین با توجه به رشد کارکردی فضای مجازی، کلیهٔ گرایش‌های جغرافیا تحت تأثیر آن قرار گرفته و منجر به شکل‌گیری چشم‌انداز داده‌های اطلاعاتی در این عرصه می‌شود.

فعالیت‌های زیانبار ارتباطات فضای سایبری

منشأ جرایم سایبری را می‌توان به روزهای اولیهٔ فناوری رایانه جستجو کرد. از آنجایی که رایانه‌ها در دسترس‌تر و به هم مرتبط می‌شوند، افراد با نیت مخرب شروع به سوء استفاده از آسیب‌پذیری‌ها برای منافع شخصی کردند. در نتیجه، اصطلاح «هک» برای توصیف دسترسی غیرمجاز به سیستم‌های رایانه‌ای با موارد قابل توجهی مانند حملهٔ موریس کرم در سال ۱۹۸۸ که تأثیر بالقوهٔ جرایم سایبری را نشان می‌دهد، پدیدار شد (اندرسون، ۲۰۲۰).

گسترش اینترنت و پیشرفت‌های فناوری منجر به توسعهٔ نرم‌افزارهای مخرب پیچیده (بدافزار) و سوء استفاده‌ها شد. ظهور ویروس‌ها، کرم‌ها، تروجان‌ها و سایر اشکال بدافزار تهدیدات قابل‌توجهی برای افراد و سازمان‌ها در سرتاسر جهان ایجاد کرد (سدهاکر و کومار، ۲۰۲۰). موارد قابل توجهی مانند ویروس ILOVEYOU و کرم Conficker عواقب مخرب فعالیت‌های مجرمانهٔ آنلاین را نشان دادند (Raff & Nicholas, 2020).

با گسترش تراکنش‌های آنلاین و سیستم‌های مالی دیجیتال، مجرمان سایبری بر کلاهبرداری و سرقت هویت متمرکز شدند. تکنیک‌هایی مانند فیشینگ، کلاهبرداری‌های آنلاین و کلاهبرداری از کارت اعتباری رایج شدند که باعث خسارات مالی قابل توجهی شد و اطلاعات شخصی را به خطر انداخت (هولت، ۲۰۲۳). موارد پُرمخاطب، از جمله نقض داده‌های Target و Yahoo، بزرگی کلاهبرداری سایبری و تأثیر آن بر افراد و شرکت‌ها را برجسته کرد (Gundur et al, 2021).

روش پژوهش

این پژوهش از نظر هدف، کاربردی و در زمرهٔ تحقیقات توصیفی – پیمایشی قرار می‌گیرد. جامعهٔ آماری شامل تمامی اساتید مطرح حوزهٔ برنامه‌ریزی و مدیریت دانشگاه فرهنگیان تهران است. ابتدا با استفاده از روش نمونه‌گیری هدفمند تعداد ۱۵ نفر از اساتید به عنوان نمونه‌ای که در سال تحصیلی ۱۴۰۳-۱۴۰۲ در دانشگاه فرهنگیان تهران مشغول به تدریس بودند، انتخاب شدند.

ابزار پژوهش شامل پرسشنامهٔ محقق ساختهٔ سنجش تأثیر شاخص‌های حوزهٔ جغرافیایی مدیریت فضای مجازی است که بر اساس پژوهش لشکری (۱۳۹۵) است و دارای ۶ بعد (وابستگی هرچه بیشتر الکترونیک به شبکهٔ سایبر، مرکزیت حضور موتورهای

اصلی جستجو، قابلیت اثرگذاری بر ساختارهای سیاسی کشور، قابلیت دستیابی به اطلاعات حکومتی و فردی، مدیریت تولید نرم‌افزارها، دگرگونی ساختار قوای نظامی و ارتشی سایبری) و ۲۴ سؤال می‌باشد. در این تحقیق برای تعیین طیف پاسخ‌ها از مقیاس پنج گزینه‌ای لیکرت استفاده شد. که دارای ۵ گزینهٔ خیلی زیاد، زیاد، متوسط، کم و خیلی کم بوده است که به ترتیب نمرهٔ ۵ تا ۱ دریافت می‌کنند.

در پژوهش حاضر سعی بر آن بود که متغیرها و سؤالات ابزار کاملاً قابل فهم و محرز باشد؛ بنابراین با تعریف دقیق گویه‌ها، معیار سنجش و مقیاس اندازه‌گیری، روایی محتوای انتخاب شده تعیین شد و تأیید اساتید متخصص رسید. پایایی پرسشنامه با روش ضریب آلفای کرونباخ ۰/۷۶ به دست آمد و مورد تأیید واقع شد.

با توجه به ماهیت سؤالات پژوهش حاضر از آزمون‌های آماری متفاوتی استفاده شده است. پس از جمع‌آوری پرسشنامه‌ها، داده‌ها کدگذاری و پس از آن وارد نرم‌افزار Spss25 شد. جهت تجزیه و تحلیل داده‌ها از آمار توصیفی (کمینه، بیشینه، میانگین و انحراف معیار متغیرهای پژوهش) و استنباطی (آزمون‌های کفایت حجم نمونه (KMO) و آزمون کرویت بارتلت و کولموگوروف – اسمیرنوف و نرمال بودن متغیرهای پژوهش، آزمون فریدمن) استفاده شده است.

یافته‌های تحقیق

بر اساس نتایج پژوهش بیشترین افراد نمونهٔ آماری دارای سابقهٔ خدمت ۱۵ سال به بالا (۹ نفر) و کمترین افراد نمونهٔ آماری پژوهش دارای سابقهٔ خدمت زیر ۵ سال (۴ نفر) بوده‌اند. همچنین رتبهٔ علمی ۶ نفر از اساتید استادیار و ۷ نفر دانشیار و ۲ نفر استاد بود.

جدول ۱. مقادیر کمینه، بیشینه، میانگین و انحراف معیار شاخص‌های حوزهٔ جغرافیایی مدیریت فضای مجازی مؤثر بر جلوگیری از فعالیت‌های زیانبار ارتباطات فضای سایبری از دیدگاه اساتید دانشگاه

آماره / متغیر	کمینه	بیشینه	میانگین	انحراف معیار	واریانس
وابستگی هرچه بیشتر الکترونیک به شبکهٔ سایبر	۱	۵	۴.۶	۰.۴۸۹۹	۰.۲۴
مرکزیت حضور موتورهای اصلی جستجو	۱	۵	۳.۱۳۳۳	۰.۸۸۴۴	۰.۷۸۲۲
قابلیت اثرگذاری بر ساختارهای سیاسی کشور	۱	۵	۳.۶	۰.۸۷۹۴	۰.۷۷۳۳
قابلیت دستیابی به اطلاعات حکومتی و فردی	۱	۵	۴.۲۶۶۷	۰.۷۷۱۷	۰.۵۹۵۶
مدیریت تولید نرم‌افزارها	۱	۵	۳.۲۶۶۷	۰.۹۹۷۸	۰.۹۹۵۶
دگرگونی ساختار قوای نظامی و ارتشی سایبری	۱	۵	۳.۸	۰.۸۳۲۷	۰.۶۹۳۳

بر اساس نتایج جدول بالا بیشترین میانگین شاخص‌های حوزهٔ جغرافیایی مدیریت فضای مجازی مؤثر بر جلوگیری از فعالیت‌های زیانبار ارتباطات فضای سایبری از دیدگاه اساتید دانشگاه به ترتیب وابستگی هرچه بیشتر الکترونیک به شبکهٔ سایبر۴.۶، قابلیت دستیابی به اطلاعات حکومتی و فردی ۴/۲۶، دگرگونی ساختار قوای نظامی و ارتشی سایبری ۳/۸؛ قابلیت اثرگذاری بر ساختارهای سیاسی کشور ۳/۶، مدیریت تولید نرم‌افزارها ۳/۲۶، مرکزیت حضور موتورهای اصلی جستجو ۳/۱۳ بوده است.

مقدار KMO، ۰/۹۲ به دست آمده و مقدار خی‌دو (X^2) ۳۰۹/۲۰۱ به دست آمده است. با توجه به اینکه سطح معنی‌داری آزمون بارتلت کمتر از مقدار ۰/۰۵ می‌باشد (۰/۰۵ ≥≤) می‌توان گفت حجم نمونهٔ پژوهش حاضر از کفایت لازم برخوردار می‌باشد. همچنین با توجه به اینکه سطح معناداری تمامی متغیرها بیشتر از مقدار ۰/۰۵ می‌باشد، فرض نرمال بودن متغیرهای مورد بررسی در پژوهش تأئید می‌گردد.

به ترتیب کدام یک از شاخص‌ها و مؤلفه‌های کارکردی حوزهٔ جغرافیایی مدیریت فضای مجازی بر جلوگیری از فعالیت‌های زیانبار ارتباطات فضای سایبری مؤثر است؟

جدول ۲. نتایج آزمون فریدمن برای رتبه‌بندی میزان اهمیت هر یک از شاخص‌های کارکردی حوزهٔ جغرافیایی مدیریت فضای مجازی بر جلوگیری از فعالیت‌های زیانبار ارتباطات فضای سایبری

ردیف	ابعاد	میانگین	رتبهٔ میانگین	خی‌دو	درجه آزادی	سطح معناداری
۱.	وابستگی هرچه بیشتر الکترونیک به شبکهٔ سایبر	۴.۶	۲/۱۲	۲۸/۴۸۶	۲	۰/۰۰۱
۲.	مرکزیت حضور موتورهای اصلی جستجو	۳.۱۳	۱/۷۱			
۳.	قابلیت اثرگذاری بر ساختارهای سیاسی کشور	۳.۶	۱/۴۷			
٤.	قابلیت دستیابی به اطلاعات حکومتی و فردی	۴.۲۶	۱/۹۴			
۵.	مدیریت تولید نرم‌افزارها	۳.۲۶	۱/۳۹			
٦.	دگرگونی ساختار قوای نظامی و ارتشی سایبری	۳.۸	۱/۵۱			

جدول بالا مربوط به رتبه‌بندی میزان اهمیت هر یک از شاخص‌های کارکردی حوزهٔ جغرافیایی مدیریت فضای مجازی بر جلوگیری از فعالیت‌های زیانبار ارتباطات فضای سایبری بر اساس آزمون فریدمن می‌باشد. با توجه به اینکه مقدار خی‌دو (۲۸/۴۸۶) با درجه آزادی (۲) در سطح ۰/۰۵ معنادار می‌باشد، می‌توان گفت بین شاخص‌های کارکردی حوزهٔ جغرافیایی مدیریت فضای مجازی از نظر رتبه‌بندی اختلاف معناداری وجود دارد. بر اساس نتایج حاصل شده، طبق نظر اساتید دانشگاه فرهنگیان تهران از بین عوامل مؤثر به ترتیب عامل «وابستگی هرچه بیشتر الکترونیک به شبکهٔ سایبر، دگرگونی ساختار قوای نظامی و ارتشی سایبری، قابلیت اثرگذاری بر ساختارهای سیاسی کشور، مدیریت تولید نرم‌افزارها، مرکزیت حضور موتورهای اصلی جستجو» بیشترین تأثیر را بر جلوگیری از فعالیت‌های زیانبار ارتباطات فضای سایبری دارند.

نتیجه‌گیری

هدف از انجام پژوهش حاضر ارزیابی و رتبه‌بندی شاخص‌های حوزهٔ جغرافیایی مدیریت فضای مجازی مؤثر بر جلوگیری از فعالیت‌های زیانبار ارتباطات فضای سایبری از دیدگاه اساتید دانشگاه فرهنگیان تهران بود. نتایج نشان داد که بین شاخص‌های حوزهٔ جغرافیایی از نظر رتبه‌بندی اختلاف معنی‌داری وجود دارد. اکنون فضای مجازی نه تنها به عنوان جدیدترین حوزهٔ جنگ، بلکه به عنوان فضایی حیاتی برای توسعهٔ اقتصادی، آموزشی و فرهنگی برای همهٔ کشورها شناخته می‌شود. با در نظر گرفتن شاخص‌های حوزهٔ جغرافیایی جهت مدیریت فضای مجازی، محققان، سیاست‌گذاران و سازمان‌های مجری قانون می‌توانند پویایی سایبری، عوامل مؤثر بر پیشگیری از آسیب‌های سایبری و فعالیت‌های زیانبار آن را بهتر درک کنند. تأثیرات و چالش‌های نظارتی مرتبط با جرایم سایبری می‌تواند مداخلات و استراتژی‌های هدفمند را برای پیشگیری و کاهش مؤثر فعالیت‌های مجرمانهٔ سایبری ارائه دهد. علاوه بر این، درک فعالیت‌های مجرمانهٔ سایبری و جمعیت شناسی این گروه‌ها در ایجاد سیاست‌ها و استراتژی‌های سیاسی برای رسیدگی به جرایم سایبری و جنگ سایبری ضروری می‌شود.

بر اساس یافته‌های پژوهش حاضر جامعهٔ امروزی به اینترنت و فضای سایبری وابستگی شدیدی دارد که بر اساس نظر اساتید فعال در این زمینه، این وابستگی منجر به ایجاد فعالیت‌های زیانبار سایبری شده و کنترل این وابستگی نیز عامل مهمی جهت پیشگیری از جرائم سایبری است. از طرفی ؛ مداخله در تولید نرم‌افزارها توسط دولت و ایجاد تغییر در وزارت اطلاعات و ارتباطات نیز عامل مهمی جهت کنترل و جلوگیری از جرائم سایبری هستند. از آن جهت که جرائم سایبری عامل اثرگذار بر فعالیت‌های اینترنتی است بنابراین ساختار سیاسی کشور باید به گونه‌ای برنامه‌ریزی شود که امنیت سایبری در جامعه وجود داشته باشد. همچنین عوامل جغرافیایی مؤثر بر جرائم سایبری مشخص گردد و سیاستمداران و برنامه‌ریزان اجتماعی و اقتصادی ابعاد مختلف این علائم را بررسی کرده و قوانین خاصی را برای آن تبیین کنند. بنابراین تدوین راهبردهای پیشگیری و بکارگیری مفاهیم جرم‌شناسی محیطی در مبارزه با جرایم و فعالیت‌های زیانبار ارتباطات فضای سایبری ضروری است.

منابع

۱. حیدری، حسن و علیرضا میلانی (۱۴۰۱). بررسی تطبیقی جایگاه صلاحیت سرزمینی در رسیدگی به جرائم سایبری با تکیه بر نظام کیفری ایران. مجلهٔ علمی حقوق و مطالعات نوین، ۳(۴)، ۱-۲۲.

۲. عنابی، علیرضا (۱۴۰۱). ژئوپلتیک و فضای سایبری، سومین کنفرانس ملی پدافند سایبری، مراغه، https://civilica.com/doc/1493938

۳. کریمی پاشاکی، سجاد، و زهرا پیشگاهی‌فرد (۱۳۹۳). چشم‌انداز جغرافیایی در تحلیل کارکرد فضای سایبر. فضای جغرافیایی، ۱۴(۴۷)، ۲۵۶-۲۳۳. SID. https://sid.ir/paper/91461/fa

۴. متقی دستنائی، افشین، احمدی نوحدانی، سیروس و بابک شفیعی (۱۴۰۰). فضای سایبر بستری جدید برای اعمال قدرت اجتماعی. مطالعات توسعهٔ اجتماعی ایران، ۱۴(۱)، ۲۷۱-۲۸۶. SID. https://sid.ir/paper/1063648/fa

5. Chen, M., Claramunt, C., Çöltekin, A., Liu, X., Peng, P., Robinson, A. C., ... & Lü, G. (2023). Artificial intelligence and visual analytics in geographical space and cyberspace: Research opportunities and challenges. Earth-Science Reviews, 241, 104438.
6. Fuerlinger, G., & Garzik, L. (2022). Silicon Valley Innovation System. Successful Innovation Systems: A Resource-oriented and Regional Perspective for Policy and Practice, 225-247.
7. Gao, S., Chen, H., Luo, W., Hu, Y., & Ye, X. (2018). Spatio-temporal-network visualization for exploring human movements and interactions in physical and virtual spaces. Human Dynamics Research in Smart and Connected Communities, 67-80.

8. Gundur, R. V., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L. Y.-C., & Mejía, D. D. (2021). Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context. In CrimRxiv. https://doi.org/10.21428/cb6ab371.5f335e6f.
9. Hall, T., Sanders, B., Bah, M., King, O., & Wigley, E. (2021). Economic geographies of the illegal: The multiscalar production of cybercrime. Trends in Organized Crime, 24(2), 282–307. https://doi.org/10.1007/s12117-020-09392-w
10. Khan, M., Wu, X., Xu, X., & Dou, W. (2017, May). Big data challenges and opportunities in the hype of Industry 4.0. In 2017 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.
11. Lee, R., Wakamiya, S., & Sumiya, K. (2015). Exploring geospatial cognition based on location-based social network sites. World Wide Web, 18, 845-870.
12. Raff, E., & Nicholas, C. (2020). A Survey of Machine Learning Methods and Challenges for Windows Malware Classification (arXiv:2006.09271). arXiv.
13. Roth, C., Mazières, A., & Menezes, T. (2020). Tubes and bubbles topological confinement of YouTube recommendations. PloS one, 15(4), e0231703.
14. Sheldon, J. B. (2014). Geopolitics and cyber power: Why geography still matters. American Foreign Policy Interests, 36(5), 286-293.
15. Wright, D. C. S. (2023). Geographical Aspects of Cybercrime: A Literature Review. Available at SSRN 4521486.