



## Theoretical and Experimental Framework for Estimating Cyber Victimization Risk in a Hybrid Physical-Virtual World

Ling Wu, Suphanut Jamonnak, Xinyue Ye, Shih-Lung Shaw, Nitesh Saxena & Kyung-Shick Choi

To cite this article: Ling Wu, Suphanut Jamonnak, Xinyue Ye, Shih-Lung Shaw, Nitesh Saxena & Kyung-Shick Choi (2025) Theoretical and Experimental Framework for Estimating Cyber Victimization Risk in a Hybrid Physical-Virtual World, Journal of Applied Security Research, 20:2, 219-243, DOI: [10.1080/19361610.2024.2368969](https://doi.org/10.1080/19361610.2024.2368969)

To link to this article: <https://doi.org/10.1080/19361610.2024.2368969>



Published online: 17 Jun 2024.



Submit your article to this journal [↗](#)



Article views: 203



View related articles [↗](#)



View Crossmark data [↗](#)



Citing articles: 2 View citing articles [↗](#)



# Theoretical and Experimental Framework for Estimating Cyber Victimization Risk in a Hybrid Physical-Virtual World

Ling Wu<sup>a</sup>, Suphanut Jamonnak<sup>b</sup>, Xinyue Ye<sup>c</sup> , Shih-Lung Shaw<sup>d</sup>, Nitesh Saxena<sup>e</sup>, and Kyung-Shick Choi<sup>f</sup>

<sup>a</sup>Department of Justice Studies, Prairie View A&M University, Prairie View, TX, USA; <sup>b</sup>Institute of Data Science, Texas A&M University, College Station, TX, USA; <sup>c</sup>Department of Landscape Architecture and Urban Planning & Center for Geospatial Sciences, Applications and Technology, Texas A&M University, College Station, TX, USA; <sup>d</sup>Department of Geography and Sustainability, The University of Tennessee, Knoxville, TN, USA; <sup>e</sup>Department of Computer Science & Engineering, Texas A&M University, College Station, TX, USA; <sup>f</sup>Cybercrime Investigation and Cybersecurity Graduate Program, Boston University, Boston, TX, USA

## ABSTRACT



This study proposes a framework integrating Routine Activities Theory into a hybrid physical-virtual space. Utilizing a space-time path metaphor, it explores phishing susceptibility in relation to daily activities in the hybrid physical-virtual environments. The mixed-method approach includes surveys and experiments, such as simulated phishing emails, to assess response patterns in both settings and investigate travel behavior's impact on cyber victimization. This hybrid model seeks to understand how physical and virtual interactions affect cybercrime vulnerability, aiding in developing prevention strategies. Additionally, the research underscores the role of visual analytics in cybersecurity, turning complex data into visual forms for effective threat analysis.

## KEYWORDS

Routine activities theory; human dynamics; visual analytics; cyber-physical systems

## Introduction

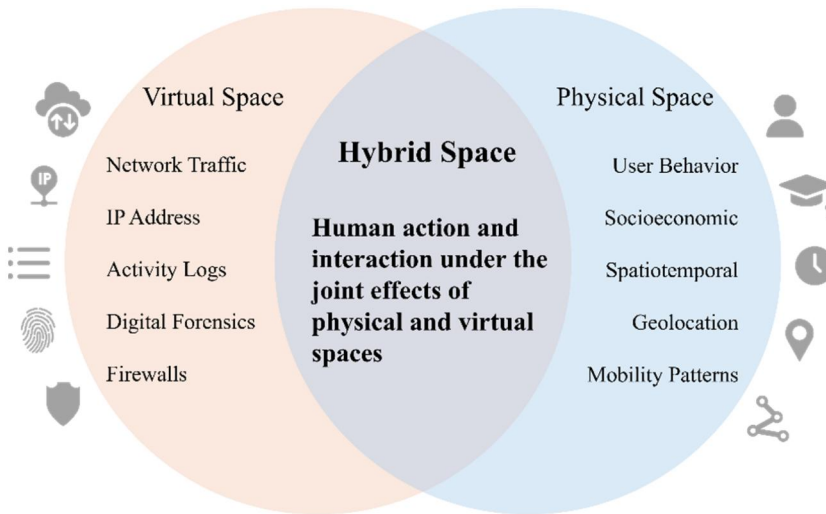
In an era increasingly defined by the interplay between emerging technologies and criminal activities, understanding the complexities of crimes in the digital age has become more crucial than ever. This research delves into the intersection of physical-world crimes and cybercrimes, realms traditionally studied in isolation. While significant attention has been given to either physical or virtual spaces, the reality of crimes existing in a hybrid physical-virtual space has often been overlooked. Social scientists have studied a wide range of cybercrimes, as classified into four-categories: (1) cyber-trespass, (2) cyber-deception/theft, (3) cyber-porn and obscenity, and (4) cyberviolence.

**CONTACT** Xinyue Ye  [xinyue.ye@tamu.edu](mailto:xinyue.ye@tamu.edu), [xinyue.ye@gmail.com](mailto:xinyue.ye@gmail.com)  Department of Landscape Architecture and Urban Planning & Center for Geospatial Sciences, Applications and Technology, Texas A&M University, College Station, TX, USA.

The classification has been instrumental in shedding light on the risks, dynamics, and prevention of various cyber-offending and victimization behaviors. In the realm of cybersecurity, limited research in the social sciences concerning victimization creates a notable gap in understanding the susceptibility of users to cybersecurity threats (Payne & Hadzhidimova, 2020) and (Baki & Verma, 2021), particularly in the context of phishing. Phishing attacks have undergone significant evolution, employing advanced social engineering techniques (Jansson & von Solms, 2013) across various channels such as email, voice calls (vishing), SMS (smishing), and fraudulent websites (Furnell et al., 2019; Griffin & Rackley, 2008; Yeboah-Boateng & Amanor, 2014). These sophisticated attacks often bypass security measures by mimicking trusted entities, leading victims to reveal sensitive information (Cui et al., 2020; Ramzan, 2010). Moreover, phishing attacks target users across diverse ecologies and environments in physical space (Wu et al., 2023).

Classical Routine Activities Theory (RAT) was first proposed to provide a robust framework for understanding physical space crimes by analyzing the convergence of three elements: a motivated offender, a suitable target, and the absence of capable guardianship (Cohen & Felson, 2010). When applied to cybercrime, RAT principle remains the same, but shifts focus to the virtual space (Choi, 2008) by utilizing structural equation modeling in computer-crime victimization. However, such studies do not consider the effect of physical space. Therefore, this research acknowledges the coexistence of real-world crimes and cybercrimes within the hybrid physical-virtual Splatial concept (Shaw & Sui, 2020) and presents a theoretical framework to adapt RAT for this complex environment.

Figure 1 illustrates our research approach considering the intricate relationship between physical and virtual spaces. For example, the physical context like a crowded event or the trajectory of individuals, ranging from routine to social active lifestyles, could influence the likelihood of cyber victimization. We propose an integrated ontology aligned with the hybrid space concept, aiming to gain insights into how routine activities in both realms impact cyber victimization risks. This approach highlights the interplay between behavioral patterns in physical spaces and the characteristics of these spaces (such as events, design, population density, and facility quality) in relation to cyber victimization. Furthermore, the widespread use of technologies like mobile phones and online social networks, which significantly shape individual behaviors, is a salient factor in the landscape of cybercrimes (Wu et al., 2022). This research represents a pioneering effort in developing a theoretical framework that combines physical and cyber routine activities, using the metaphor of the space-time path to elucidate



**Figure 1.** A graphical model of our research approach in hybrid space. This hybrid environment represents human actions and interaction under the joint effects of physical and virtual spaces.

cyber victimization risks in today's interconnected world. The metaphor of the space-time path used in this research aims to understand the structure and dynamics of routine activities (when, where, and why) that could lead to victimization. To validate the theoretical framework, we propose an experimental design incorporating mixed methods and a survey focused on both virtual and physical activities of individuals. Additionally, we present a concept of visual analytics (VA) system for a comprehensive understanding of activities in both realms. In summary, our main contributions are as follows:

- A theoretical framework aimed at adapting the traditional Routine Activities Theory (RAT) from its conventional application in physical space to the realm of virtual space. We introduce a novel theoretical framework to extend the traditional Routine Activities Theory into the hybrid physical-virtual space, providing a holistic view of cybercrime risks. This innovative approach enables the simulation, analysis, and visualization of potential risks associated with cybercrimes, thereby enhancing our understanding of security dynamics in the digital environment.
- We outline an experimental design for practical validation, including collaboration with IT departments to create real-world scenarios, such as phishing simulations, to test the framework's applicability.
- A Visual Analytics (VA) system is proposed to enable effective data visualization and analysis, bridging the gap between physical and virtual spaces, and enhancing decision-making in cybersecurity.

In summary, we present a theoretical framework that extends the traditional Routine Activities Theory (RAT) to virtual space, offering a comprehensive understanding of cybercrime risks in the hybrid physical-virtual environment. Our approach includes a validation method involving real-world simulations of phishing scenarios. Additionally, we propose a visual analytics methodology to enhance decision-making in both physical and virtual spaces. We believe that our theoretical framework has the potential to bridge the gap between users and cybersecurity threats by applying visual analytics methods to illustrate modern cybersecurity challenges.

## Related work

The application of Routine Activity Theory (RAT) and its variations, such as Lifestyle-Routine Activity Theory (LRAT), to cybercrime has been extensively explored in recent literature. Several surveys have investigated the role of RAT in understanding cybervictimization. For instance, Marcum et al. (2010) revealed significant insights into online victimization, emphasizing the impact of internet behaviors. Hawdon et al. (2017) focused on online conflict management's effect on cybervictimization, while Wick et al. (2017) studied predictors of cyber-harassment among students. Additionally, Mustaine and Tewksbury (1998) used RAT to predict victimization risks through demographic variables, and Holtfreter et al. (2008) combined RAT and self-control theory to explain online fraud victimization. Bossler and Holt (2009) applied RAT to study data loss from malware infections in college samples. Similarly, Pratt et al. (2010) integrated RAT with consumer behaviors, revealing that online routines and personal characteristics expand opportunities for cyber-fraud. Henson et al. (2010) examined the impact of structured and unstructured routine activities on adolescent violent victimization, while Ngo and Paternoster (2011) assessed the effects of individual and situational factors on cyber victimization. Reyns (2013) linked online routines with identity theft, showcasing RAT's applicability without physical proximity. Leukfeldt and Yar (2016) further evaluated RAT's analytical utility in cybercrime, highlighting visibility as a crucial factor. Vakhitova et al. (2016) examined spatial and temporal factors that might disconnect RAT from the cybercrime environment, and Räsänen et al. (2016) identified significant factors in youth victimization through online hate. Williams et al. (2019) provided a criminological analysis of corporate insider victimization through RAT.

Researchers have also applied RAT to various types of cybervictimization. In phishing victimization, Hutchings and Hayes (2009) and Leukfeldt (2014) emphasized routine activities and personal background in susceptibility to cybercrimes. Holt and Bossler (2008) explored RAT's limitations

and adapted it to examine online harassment. Wilsem (2011, 2013) addressed risk factors and compared digital and traditional threats, linking RAT to online harassment, while Bossler et al. (2012) studied online harassment among juveniles. Näsi et al. (2017) used RAT to predict online harassment victimization, focusing on socio-demographic factors. In cyberbullying, Navarro and Jasinski (2013) explored gender differences in online behaviors and cyberbullying risks, and Choi et al. (2019) proposed a cyber-routine activities theory to explain cyberbullying victimization.

In the context of Lifestyle-Routine Activity Theory (LRAT), Schreck and Fisher (2004) highlighted family attachment's role in effective guardianship. McNeeley (2015) reviewed the theoretical and empirical status of LRAT, discussing its utility for policy and practice. Reyns et al. (2016) emphasized offline guardianship in mitigating cyberstalking risks, with earlier work in 2011 confirming that online behaviors predict cyberstalking victimization. Van Ouytsel et al. (2018) adopted an LRAT perspective to study online romantic partner monitoring and cyber dating abuse, considering factors such as gender, age, and relationship length. Ngo et al. (2020) integrated LRAT to examine the relationships between online frequency, activity, and posting in cybercrime victimization. Akdemir and Lawless (2020) investigated human factors influencing cyber-dependent and cyber-enabled crimes through LRAT, while Culatta et al. (2020) explored how sexual victimization influences substance use and depressive symptoms, leading to revictimization. Guerra and Ingram (2022) found that online victimization significantly influences LRAT behaviors, suggesting a dynamic relationship between behavior and victimization.

Despite the extensive exploration of RAT and LRAT in both physical and virtual spaces, there is a notable gap in the examination of hybrid spaces, where physical and virtual environments intersect. Existing studies typically focus on one domain without considering the complex interactions that occur in hybrid environments. Furthermore, the literature lacks visual analytic tools that could enhance the understanding and interpretation of data related to cybercrime in these hybrid spaces. Therefore, our research will focus on examining hybrid spaces and employing visual analytic tools to provide a more comprehensive understanding of cybercrime dynamics. This approach aims to bridge the gap in current research and offer new insights into the prevention and analysis of cybercrime in contemporary environments.

## **Theoretical framework**

Routine Activities Theory (RAT), as an ecological approach to crime causation, fundamentally considers the spatial and temporal localization of

persons, objects, and activities as essential to understanding crime dynamics. This theory, proposed by Cohen and Felson in 1979, hinges on the etiological formula where the convergence of an offender, a suitable target, and the absence of a capable guardian in the same space and time leads to a crime. This framework is particularly insightful in explaining and anticipating crime patterns, including those in cyberspace. The RAT formula provides a structured way to understand and analyze the potential for cybercrimes based on crime likelihood with the combination of three critical elements illustrated as follows.

$$\text{Crime Likelihood} = k \cdot (MO) \times (ST) - (AG) \quad (1)$$

Where, *CL* represents Crime Likelihood and *k* is the proportionality constant, which could include other environmental or contextual factors not explicitly covered by *MO*, *ST*, and *AG*. To be more specific, *MO* (Motivated Offender) represents the presence of individuals who are willing to commit crimes. *ST* (Suitable Target) refers to the presence of potential targets that are attractive and accessible to the offender. Lastly, *AG* (Absence of Capable Guardian) indicates a lack of effective guardianship or supervision that could deter potential offenders.

Therefore, in virtual space, crime is more likely when a motivated offender encounters a suitable target without the presence of a capable guardian. Adjustments to the variables and constant *k* can further tailor the formula to specific situations or empirical studies. Moreover, the application of RAT extends to the development of prevention and intervention strategies against cybercrimes. For example, organizations can leverage this understanding to enhance cybersecurity measures when users are more vulnerable in specific locations prone to cyber threats. In the context of urban planning, the principles of RAT can inform the design of spaces to reduce cybercrime vulnerability. A city park layout strategically designed with well-lit pathways, open communal spaces, and interactive installations can encourage public engagement in safer zones, simultaneously deterring crimes in both physical and virtual realms. The inclusion of technology such as surveillance cameras and Wi-Fi hotspots in these areas not only enhances safety but also serves as a deterrent to potential cyber threats.

To extend the RAT formula for the development of prevention and intervention strategies against cybercrimes, we can incorporate factors specific to cybercrime prevention and urban planning strategies. This holistic approach emphasizes both physical and virtual safety, integrating traditional RAT principles with contemporary urban and cybersecurity measures. In cybersecurity, three elements from RAT can be denoted as  $MO_{cyber}$ ,  $ST_{cyber}$ , and  $AG_{cyber}$  respectively.

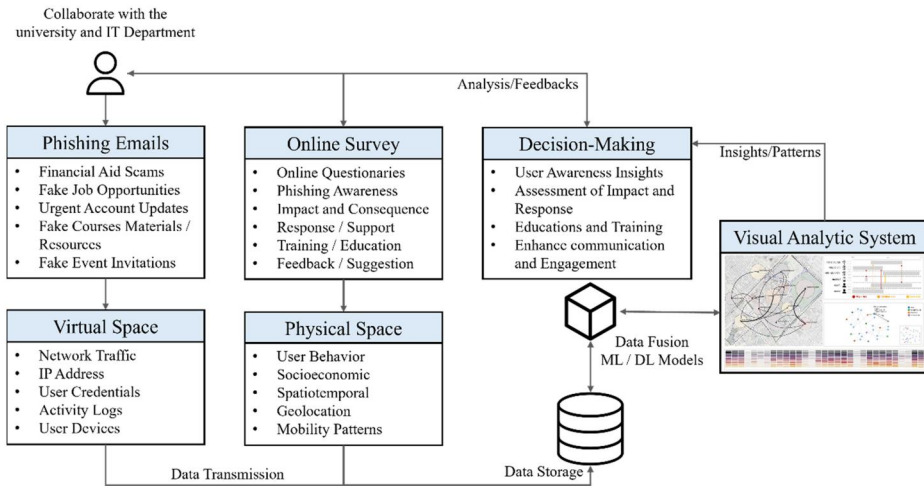
*Cybercrime Prevention Likelihood*

$$= k \cdot \frac{AG_{cyber} \times CSM \times PSM}{MO_{cyber} \times ST_{cyber} \times TEO \times VT \times ECF} \quad (2)$$

Where, *CSM* (Cybersecurity Measures) and *PSM* (Physical Cybersecurity Measures) has inverse relationship as more measures can reduce crime likelihood. Other variables and factors are represented as *TEO* (Technical Expertise of the Offender), *VT* (Vulnerability of the Target), and *ECF* (Environmental and Contextual Factors). These prevention strategies and insights gained from applying RAT can guide institutions in identifying and addressing vulnerabilities in hybrid physical environments susceptible to cybercrime. This knowledge is crucial in enhancing place-based network security design and shaping organizational training. For instance, a university might apply these findings to improve the security of the users of outdoor Wi-Fi networks, while a corporate office could incorporate these insights into comprehensive employee security training programs, covering both the physical and virtual facets of cybersecurity. This adaptive approach, rooted in the principles of RAT, enables institutions to strengthen their defenses against potential cyber threats. By continuously applying RAT's spatial and temporal analysis, organizations can develop more effective strategies to tackle the dynamic nature of cybercrime, thus ensuring a higher level of security in an increasingly interconnected world.

### Experimental framework

The experimental design outlined in this research seeks to enhance our understanding of how phishing opportunities are shaped by people's routine activities in both physical and virtual spaces (Ghazi-Tehrani & Pontell, 2021). This multifaceted approach involves collecting and analyzing data from various sources to construct a comprehensive context where these routine activities occur and examining individual vulnerabilities to phishing attacks. Figure 2 illustrates our experimental framework and our workflow. First, the experimental design focuses on assessing individual susceptibility to phishing attacks. This involves the collaboration with IT departments to create simulated spear and generic phishing emails. These emails will be strategically sent to subjects (students and employees) during specific events (e.g., football games, spring breaks, final exams) over a two-month period to capture temporal variations. The 'click-rate' of these emails will be monitored, encompassing actions like replying, clicking links, or opening attachments in the email. We aim to build a profile of individual "victims" and identify patterns among repeat victims (i.e., those who respond to phishing emails more than once), documenting the time and IP address of their



**Figure 2.** Experimental framework and workflow, including collaboration with the university to send out phishing emails, data collection and preprocessing, integrate both physical and virtual data sources, develop visual analytics platform, and design security protocol.

responses. These simulated emails will be designed to simulate common phishing scenarios, such as fake password reset requests or urgent financial alerts. In addition, the constructed phishing email will include subtle indicators that can help users to recognize suspicious emails effectively.

Following the experiment, a comprehensive survey will be conducted. This survey will delve into the subjects' virtual and physical routine activities and their specific interactions with phishing emails. The survey instrument aims to cover various scenarios, differentiating between those who responded to the emails and those who did not. The survey questions will focus on the contextual factors of their responses, such as their mental state, mood, and physical location at the time of interaction with the phishing email. To integrate response from virtual space to physical space, we can extract a range of data sources to gather information on POIs (Points of Interests) and human activities. This includes information from long-term analysis of Tweets, SafeGraph data (<https://www.safegraph.com/>), and web crawled images to construct the contextual environment where physical and virtual routine activities occur. Furthermore, a physical activity survey will be conducted to gather statistical data on trip characteristics (e.g., trip length, trip frequency, trip purpose). This will offer insights into the travel patterns and behaviors of individuals, which may correlate with their vulnerability to cyber victimization.

The survey will question the impact of victimization on subjects, including their physical, mental, and behavioral reactions. It will explore the subsequent actions taken by subjects after interacting with the phishing emails, such as reporting the incident, sharing information with peers, or

enhancing their cybersecurity measures. This aspect of the survey will help understand the under-reporting of cyber victimization and inform the development of enhanced support systems for crime victims in the future. Through this comprehensive experimental design, we aim to bridge the gap between physical and virtual spaces in the study of cybercrimes, providing a nuanced understanding of individual vulnerabilities and responses to phishing attacks. The insights gained will be invaluable in designing more effective situational crime prevention techniques and supporting cybercrime victims.

## Methodology

In the development of our proposed theoretical and experimental frameworks, addressing the challenges of processing and interpreting large datasets is pivotal, especially considering that these datasets are often textual and can be cumbersome for human behavioral analysis. To mitigate this, we advocate for the transformation of these textual datasets into visual representations. Visualizations not only enhance the accessibility and interpretability of complex textual information but also provide a more intuitive means for comprehending patterns and trends. In addition, visualizations offer an array of benefits, as outlined by Marty (2008), including the ability to quickly answer and generate questions about the data, uncover insights, make more accurate and faster decisions, enhance data analysis efficiency, and inspire the adoption of novel visualization methods. In cybersecurity, visualization plays a critical role in rapidly identifying malicious activities, trends, relationships, and anomalies (Shiravi et al., 2011). To realize this vision, our approach involves three key steps: identifying key tasks in cybersecurity, reviewing existing visual analytic tools in this domain, and then proposing a novel hybrid physical-virtual visual analytics system tailored to these tasks.

## Data collection

In real-world physical space, the data sources encompass various human activities and behaviors, such as people tracking, object monitoring, and event logging. Conversely, for data sources in virtual spaces, we rely on digitized data forms such as log files, network activity records, DNS data, and malware information. These data sources, when referenced with temporal data types, establish a vital link between physical and virtual environments, a connection especially crucial in cybersecurity where timing and location of activities are vital factors. One of two primary tasks is *Forensic Analysis*, which involves scrutinizing incidents to understand the threats and their origins (McClain et al., 2015). *Threat Analysis* is another primary

security task that uses visualization to identify, analyze, and prioritize potential security threats to systems (Tuma et al., 2018).

Various tools have emerged to aid forensic analysts. Examples include MalViz, which assists in real-time malware behavior analysis (Nguyen et al., 2018), Eventpad for simplifying malware analysis in network traffic (Cappers et al., 2018), a web-based tool for visualizing network packet captures (PCAPs) (Ulmer et al., 2019), and FIMETIS which provides streamlined views of file system records, event timelines, and data clusters (Beran et al., 2020). These tools, however, primarily focus on analyzing specific data types or single data sources and do not facilitate a comprehensive connection between diverse physical and virtual data sources. By combining these elements, our visual analytic tool will offer a more holistic view of cybersecurity threats, enabling users to effectively analyze data from multiple sources and dimensions. This integrated approach is essential for advancing our understanding of and response to complex cybersecurity challenges. Therefore, our proposed visual analytic tool aims to bridge this gap by integrating various data types from both physical and virtual environments. This necessitates processes for data transformation and manipulation. We define the data terminology and attributes used in our research (as detailed in Tables 1 and 2) to ensure clarity and uniformity in our approach.

In our databases, our approach focuses on storing and organizing specific terms related to cybersecurity events in an efficient and structured manner. Each term corresponds to a unique entry in our database, with each row representing a distinct event. These events encapsulate critical information categories such as user, event, policy, anomalous activity, alert, and endpoint, offering a comprehensive overview of each incident. Furthermore, the information in the “Event” and “Alert” attributes, as shown in Table 2, is collected from two primary channels:

- *Online Survey*: These surveys are meticulously designed to extract insights on various aspects of an event, including the identities of the involved parties (user), the nature of the incident (event), the timing and location (when and where), and the rationale or motive behind the malicious action (why). The survey data provides a rich, human-centric perspective on each event, contributing to a deeper understanding of the behaviors and motivations in cybersecurity incidents.
- *Activity Logs*: Complementing the survey data, activity logs serve as another crucial source of information. These logs are systematically analyzed to extract similar data points as the surveys—detailing the “who,” “what,” “when,” “where,” and “why” of each event. The activity log data provides a more technical and objective view of the incidents, capturing real-time data on system interactions, user activities, and network behaviors.

**Table 1.** Glossary.

Term	Description
User	A real person can access more than one user account (victims), and more than one person could access the same user account (attackers). User accounts can contain encrypted personal information (i.e., user profile, activity patterns, and personal devices).
Event	An action performed by a <i>user</i> such as sending phishing email, opening or closing a file, or forwarding email to potential victims. An event generally contains the endpoint (or location), user, time, and application.
Endpoint	A <i>device</i> on which an <i>event</i> has occurred (i.e., computers, servers, and mobile phones). Endpoint consists of spatial information (latitude and longitude).
Policy	A predefined <i>rule</i> that an <i>event</i> can be judged against it. It may contain multiple and disjoint clauses (AND/OR).
Anomalous Alert	An <i>event</i> that is markedly different from normal given a <i>user's</i> past activity patterns. An <i>event</i> that is <i>anomalous</i> or satisfies a policy definition leading to such alerts. A consecutive sequence of events that fall into this alert are grouped into one anomalous event.

**Table 2.** Event and alert attributes.

Event Attributes	
Who	User
What	Application, Resource & Activity
When	Start & End Time
Where	Endpoint
Alert Attributes	
What	One or more Events
When	Alert Time
Why	Policy or Tag & Confidence (AI Detection)

The combination of these two data sources offers a robust, multi-dimensional view of cybersecurity events. By aggregating data from both surveys and activity logs, we gain a comprehensive understanding of human characteristics and behaviors in both physical and virtual spaces. This dual-source approach is instrumental in painting a complete picture of each event, encompassing both the subjective human elements and the objective technical details.

### **Design requirements**

The development of visual analytics systems tailored to cybercrimes and victimization has emerged as a promising approach. In this context, we outline the design requirements for a visual analytics system aimed at answering key questions about cybercrime incidents. These requirements are essential for enabling stakeholders, including law enforcement agencies, cybersecurity professionals, and policymakers, to identify patterns, attribute attacks, profile victims, and analyze temporal trends in cybercrime activity.

*R1: Geographic Distribution of Cybercrime Activity* focuses on visualizing the geographic distribution of cybercrime activity, enabling stakeholders to understand where malicious actions are occurring. By mapping the locations of cyberattacks, compromised devices, and victim origins, users can

identify hotspots of cybercrime activity and patterns of victim targeting across different regions or countries.

*R1.1: Locate Malicious Activity:* Provide a visual representation of the geographical distribution of cybercrime incidents, indicating where malicious actions have occurred. This includes mapping the locations of cyberattacks, compromised devices, and affected organizations or individuals.

*R1.2: Identify Victim Origins:* Display the geographic origins of cybercrime victims, highlighting regions or countries from which victims originate. This helps identify patterns of victim targeting and may reveal trends in cybercrime activity across different geographical areas.

*R2: Attribution of Cyber Attacks and Victim Identification* involves visualizing the identities of cyber attackers, including known threat actors, and attributing malicious actions to specific individuals, groups, or entities. Additionally, the requirement entails profiling cybercrime victims by providing insights into their demographics, affiliations, and roles within organizations.

*R2.1: Identify Perpetrators:* Visualize the identities of cyber attackers and attribute malicious actions to specific individuals, groups, or entities. This includes tracking the origins of cyberattacks, such as IP addresses, domains, or known threat actors.

*R2.2: Victim Profiling:* Provide insights into the demographics and characteristics of cybercrime victims, including their affiliations, income levels, and roles within organizations. This helps understand the targeted demographics and potential motives behind cyberattacks.

*R2.3: Device Identification:* Display information about the devices used in cybercrime incidents, including the types of devices (e.g., computers, mobile devices) and their operating systems. This enables users to identify vulnerable devices and potential entry points for cyberattacks.

*R2.4: Identify Peak Attack Times:* Visualize temporal patterns of cybercrime activity, highlighting spikes or surges in malicious actions over time. This includes identifying peak hours, days, weeks, or months when cyberattacks are most prevalent, such as during public events or crowded periods.

*R3: Victim Background and Affiliation* focuses on providing detailed information about the backgrounds and affiliations of cybercrime victims. It includes demographic data such as age, gender, occupation, and socioeconomic status, as well as information about victims' affiliations with organizations, industries, or communities. Understanding victim backgrounds and affiliations helps contextualize cybercrime incidents and identify potential motives behind attacks.

*R3.1: Victim Demographics:* Provide demographic information about cybercrime victims, including their backgrounds, affiliations, and socioeconomic characteristics. This helps contextualize cybercrime incidents and understand the diverse range of individuals and organizations affected.

*R4: Global Temporal Views* involves coordinating and synchronizing temporal views of cybercrime events across different time intervals, such as hours, days, weeks, and months. It enables users to analyze temporal patterns of cybercrime activity, including identifying peak attack times, trends over time, and correlations with external events or factors. Global temporal views provide stakeholders with valuable insights into the timing and frequency of cyberattacks, facilitating effective incident response and mitigation strategies.

*R4.1: Coordinated Temporal Analysis:* Coordinate and synchronize temporal views of cybercrime events and user activities across different time intervals, such as hours, days, weeks, and months. This enables users to analyze trends and correlations in cybercrime activity over time and across various temporal scales.

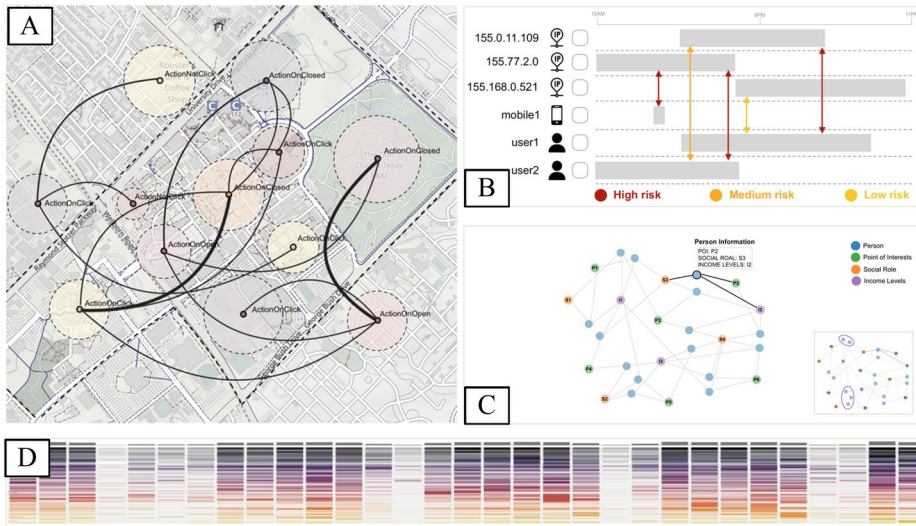
By addressing these design requirements, a visual analytics system for cybercrimes and victimization can provide valuable insights into the spatial, temporal, and demographic aspects of cybercrime events, empowering stakeholders to understand, respond to, and mitigate cyber threats effectively.

## **Visual analytic system**

The visualizations and requirements are designed to support the seamless integration of data from both physical and virtual data sources, denoted as ( $P + V$ ). Consequently, our visual analytic tool in [Figure 3](#), consists of four primary components: (1) Behavioral Map, (2) Incident Reports, (3) Ontology Graph, and (4) Temporal Events. Furthermore, these various components are designed to interact and coordinate with each other seamlessly. When users interact with one component, it can dynamically filter or change the display of information in other components based on specific threshold criteria. This interactive design ensures that users can explore and analyze integrated data effectively, promoting a deeper understanding of the relationship between physical and virtual spaces.

### **Behavioral map**

To support *R1*, [Figure 3\(A\)](#) presents a map-based visualization known as the “behavioral map.” This visualization displays the spatiotemporal path of human activity information in physical space. This data is extracted from various sources, including Tweets, SafeGraph data, and web-crawled images. Furthermore, specific geographic regions are aggregated based on information such as county codes, zip codes, or spatial boundaries. Each of these regions contains multiple instances of malicious events and points of interest (POIs). Different types of actions are represented by color-coding. For example, yellow circles indicate instances where individuals did not

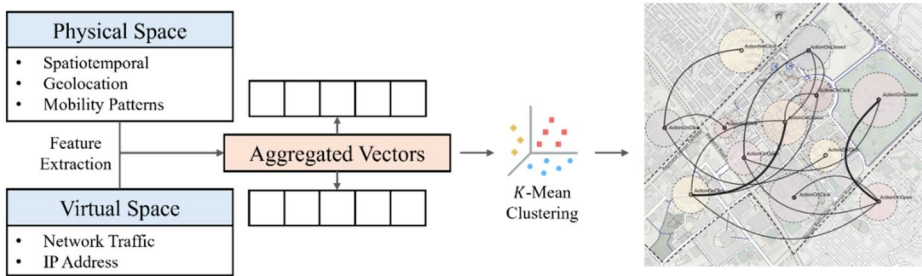


**Figure 3.** Visual Analytic (VA) System with coordinated views such as (A) Behavioral Map for travel patterns and travel frequencies (B) Incident Reports with activity logs (C) Ontology Graph visualize user profile and background, and (D) Temporal Events that summarize malicious events in a global temporal view.

click (“ActionNotClick”) on a phishing email. On the other hand, red circles represent individuals who did click (“ActionOnClick”) on a phishing email. The visualized path and trajectory provide statistical insights into trip characteristics, such as trip length, trip frequency, and trip pattern. This information helps us better understand individuals’ travel patterns and behaviors. Importantly, the visualization in this component can be dynamically filtered. Users have the flexibility to apply different temporal constraints, allowing them to gain various insights on behavioral patterns based on their specific queries (Figure 4).

### **Incident report**

The visualization proposed in Figure 3(B) is specifically designed to offer a detailed exploration of malicious actions between victims and attackers (R2). In this visualization, each row in the table represents a specific activity. It also indicates which device initiated the action and the duration of each action. To provide insights into the severity of the relationships between different devices, the arrows are color-coded based on their risk levels. This color scheme helps users quickly identify the level of risk associated with each connection. Furthermore, to protect user privacy, device information is encoded with pseudo-IP addresses and user accounts. This encoding ensures that the identities of users and devices remain confidential and protected (Figure 5).



**Figure 4.** The development of Behavioral Map, by extracting and aggregating feature vectors from both physical and virtual spaces. The applied clustering method is to group different behavior with different color coded.

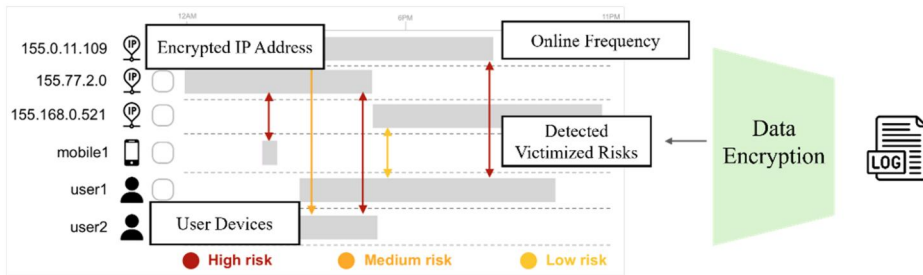
### **Ontology graph**

The ontology graph is designed to support R3, illustrated in Figure 3(C). In this visualization, people (victims) are denoted by blue nodes. These nodes serve as the focal points of the graph, representing people within the dataset. To enrich the representation of this complex network, various attributes are introduced and are depicted using nodes of different colors. Green nodes signify Points of Interests (POIs), providing information about specific locations or places. Orange nodes represent social roles, indicating individuals' roles in social contexts.

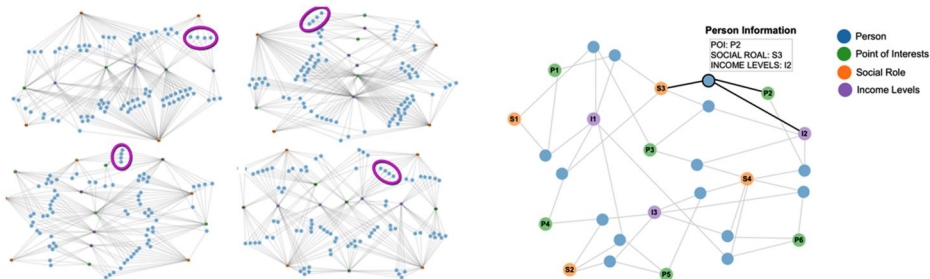
Additionally, purple nodes denote income levels, offering insights into the economic status of individuals. The relationships between individuals and attributes are conveyed through edges that connect people to attribute nodes. These edges establish connections, signifying that a person is associated with particular attributes, such as a POI, a specific social role, or an income bracket. These connections allow for the representation of personal information within the ontology graph, enabling a comprehensive understanding of individuals and their associated attributes. To make the ontology graphs more informative and visually appealing, Figure 6 shows various visual parameters which can be adjusted. Similar to conventional graph representations, visual elements like node size scaling, node shapes, and node thickness can be adjusted. These adjustments enable users to customize the visualization to suit their specific analytical needs, enhancing the interpretability of the graph and providing deeper insights into the relationships between individuals and their associated attributes.

### **Temporal visualization**

The temporal visualization in Figure 3(D) is designed to seamlessly integrate data from both physical and virtual spaces into a unified and visually informative colored heat map (R4). Within this visualization, each color block represents attacker activities and is intricately linked with a detailed



**Figure 5.** Incident Report combines and encrypt users' activities logs into different timeline sequences. All sensitive information such as users IP address, name of devices, and activity are encrypted to preserve users' privacy.

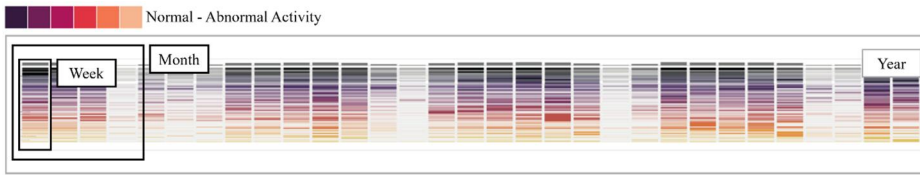


**Figure 6.** Ontology graph visualization, which includes clusters of individual nodes in different categories.

timeline, which is segmented into hours, days, and weeks, providing a multi-layered temporal perspective. What sets this visualization apart is its interactivity; hovering over each color block in the temporal visualization reveals specific incidents generated by the attackers. This interactive feature empowers analysts to explore the dataset in greater detail, enabling a thorough examination of the actions taken by the attackers over time. By integrating data from both physical and virtual realms into a single heat map, this visualization in Figure 4 offers a holistic view of the evolving landscape of attacker activities, aiding in the identification of patterns, trends, and anomalies. More importantly, it assists analysts in making informed decisions and formulating effective security strategies, thereby enhancing the overall security of the system or the environment being analyzed (Figure 7).

### Case studies and evaluation design

To illustrate the potential benefits of such systems, we present hypothetical case studies that demonstrate how visual analytics can help identify patterns, attribute attacks, profile victims, and analyze temporal trends in cybercrime activity. These examples highlight how visualization can



**Figure 7.** Temporal Visualization: illustrating the malicious activities with color encodings ranging from black (normal) to orange (abnormal). Each block in the heatmap of temporal visualization is sorted by days (365 days per year).

enhance decision-making and response strategies for various types of cyber-crime incidents, providing valuable insights to law enforcement agencies, cybersecurity professionals, and policymakers.

### ***Case study 1: mitigating a ransomware attack on a healthcare network***

A regional healthcare network was targeted by a sophisticated ransomware attack that encrypted patient records and disrupted critical healthcare services. The attack originated from a group of known cybercriminals operating internationally. To address this, the healthcare network employed a visual analytics system tailored to cybercrimes and victimization. The system first visualized the geographic distribution of the ransomware activity, enabling stakeholders to understand where the malicious actions were occurring. By mapping the locations of compromised devices across multiple hospitals, the system highlighted the initial infection point and the subsequent spread across facilities. It also displayed the geographic origins of the victims, revealing that the network was primarily targeted in a specific state, with further insights indicating the spread to neighboring regions. This helped identify the geographic scope of the attack and the areas most affected.

Next, the visual analytics system helped attribute the cyberattacks to specific perpetrators. It traced the origins of the attack back to an Eastern European hacking group by visualizing the IP addresses and domains involved, allowing the security team to identify and attribute the attack to the group. The system also provided demographic insights about the affected victims, including the types of departments most impacted (e.g., emergency, oncology), which helped prioritize the restoration of critical services. Additionally, it displayed information about the types of devices compromised, including older operating systems that were particularly vulnerable, enabling the IT team to focus on securing and updating these systems first. Temporal analysis revealed that the attack peaked during a shift changeover, exploiting reduced monitoring periods. This insight helped the healthcare network adjust their monitoring schedules to prevent future attacks. By utilizing the visual analytics system, the healthcare network

effectively mitigated the ransomware attack, restored critical services, and enhanced their cybersecurity protocols to prevent future incidents.

### ***Case study 2: protecting an educational institution from phishing campaigns***

A prominent university experienced a surge in phishing emails targeting faculty, staff, and students, attempting to steal credentials and financial information. To combat this, the university deployed a visual analytics system to analyze and respond to the phishing campaigns. The system mapped the origins of the phishing emails to several international locations, with a concentration in Southeast Asia, providing a clear view of the geographic distribution of the phishing sources. It also revealed that the victims were predominantly located in specific departments and student housing areas, indicating targeted attacks. By visualizing these patterns, the university could better understand the scope and focus of the phishing campaigns.

The visual analytics system also helped attribute the phishing attacks to specific perpetrators. By analyzing the patterns and content of the emails, the system linked the campaign to a known group that frequently targeted educational institutions. The system provided insights into the demographics of the victims, including their roles within the university and their susceptibility to phishing attempts based on their access levels. It displayed that most phishing emails were opened on personal devices such as smartphones and tablets, highlighting a need for improved mobile security measures. Temporal analysis showed that the phishing attacks were most frequent at the beginning of the semester and during registration periods, exploiting times of increased communication and administrative activity. With this information, the university implemented targeted cybersecurity training for high-risk groups, enhanced email filtering, and introduced multifactor authentications for all accounts. These measures significantly reduced the success rate of phishing attempts and protected sensitive information.

By implementing these case studies, the visual analytics system demonstrated its practical applications and effectiveness in various real-world scenarios, showcasing its value in combating cybercrimes and supporting victims.

## **Discussion**

### ***Data privacy***

collecting detailed data about victims of cybercrimes in both virtual and physical spaces present significant challenges, primarily due to privacy

concerns and regulatory constraints. Victims' data, such as personal demographics, device information, and geographic locations, are sensitive and protected by various data protection laws and regulations. These privacy concerns make it difficult for researchers and cybersecurity professionals to access real-world data necessary for thorough analysis and effective response to cyber threats. An alternative approach involves the use of Machine learning (ML) and Deep learning (DL) techniques to generate synthetic data. Synthetic data can be created to mimic the properties and patterns of real-world data without exposing sensitive information. This approach offers several advantages. For instance, synthetic data can protect individual privacy, as it does not contain real personal information. This allows researchers and analysts to work with data that simulates real-world scenarios without risking breaches of privacy. Furthermore, with synthetic data, there are no legal restrictions on data sharing and usage, enabling broader collaboration and innovation in cybersecurity research and development. This availability is crucial for testing and improving algorithms and systems designed to combat cyber threats. Synthetic data can be tailored to represent a wide range of scenarios and attack patterns, providing a comprehensive testing ground for cybersecurity measures. It allows the simulation of various cyberattack vectors and victim profiles, helping to develop robust defense mechanisms. However, there are also limitations to consider. Synthetic data may not fully capture the complexity and unpredictability of real-world cyber incidents. The effectiveness of models trained on synthetic data needs to be validated with real-world data to ensure their applicability and reliability. Moreover, generating high-quality synthetic data requires sophisticated techniques and deep domain knowledge to ensure its relevance and utility.

### ***Scalability***

Another critical aspect of developing a visual analytics system for cyber-crimes and victimization is ensuring its scalability. Scalability refers to the system's ability to handle increasing amounts of data and a growing number of users without compromising performance. For such a system to be effective on a large scale, several factors must be considered. First, the system must be capable of integrating data from various sources, including logs, sensors, and third-party databases, in real-time. This requires robust data management frameworks that can handle large volumes of data efficiently. Scalable systems must leverage distributed computing and cloud-based resources to process and analyze data rapidly. This involves using parallel processing, load balancing, and other techniques to ensure that the system remains responsive under heavy loads. As the system scales, the

user interface must be designed to accommodate a wide range of users, from cybersecurity experts to policymakers.

### **Ethical considerations**

Ethical considerations are critical when developing and deploying a visual analytics system for cybercrimes and victimization. Even with the use of synthetic data to mitigate privacy concerns, it is essential to handle all data ethically and responsibly. This includes obtaining necessary consents, anonymizing data where possible, and maintaining transparency about data practices. Additionally, it is crucial to regularly review and audit the system's algorithms to identify and mitigate any biases that could lead to unfair or inaccurate outcomes. Ensuring fairness in data representation and analysis helps maintain trust in the system and its outputs, making it a reliable tool for cybersecurity efforts. Addressing these ethical considerations not only aligns with legal and regulatory standards but also upholds the integrity and effectiveness of the system.

### **Limitation**

Despite the potential benefits of a visual analytics system for cybercrimes and victimization, several limitations must be acknowledged. One significant limitation is the reliance on the quality and completeness of input data; inaccuracies or gaps in the data can lead to misleading insights and ineffective responses. Additionally, while synthetic data can mitigate privacy concerns, it may not fully capture the complexity and unpredictability of real-world cyber incidents, potentially limiting the system's effectiveness in practical applications. The development and maintenance of such a system also requires substantial financial and technical resources, which may be challenging for smaller organizations to sustain. Moreover, the system's effectiveness depends on the users' ability to interpret and act on the visualized data correctly, necessitating ongoing training and education. Finally, the rapid evolution of cyber threats means that the system must continuously adapt to new attack vectors and methodologies, requiring regular updates and potential redesigns to stay relevant and effective.

### **Conclusion & future work**

In summary, our research introduces a novel framework extending Routine Activities Theory (RAT) into a hybrid space that blends physical and virtual realms. By addressing the intersection of real-world physical crime and cybercrime, our study focuses on cyber victimization risk influenced by individuals' activities across both domains. Leveraging a space-time path

metaphor, our aim is to dissect the dynamics of phishing susceptibility in relation to everyday activities in these dual realms, thus bridging the knowledge gap between social science and computer science in cybersecurity. Our methodology employs a mixed-method approach, featuring an experimental design that includes a detailed survey of participants' virtual and physical behaviors. Data sourced from varied avenues will map human activities, providing a comprehensive context for analyzing routine activities. Our experiment framework on simulated phishing emails to evaluate individuals' responses based on their activity patterns in both physical and virtual settings. Additionally, a physical activity survey will explore travel behaviors and their impact on cyber victimization. Integrating RAT into a hybrid model, our study aims to reveal how the interplay of physical and virtual environments shapes cybercrime vulnerability. This approach promises not only to enhance understanding of cybercrime causation but also to aid in developing targeted crime prevention strategies for today's interconnected reality. Furthermore, our research highlights the importance of visual analytics in cybersecurity, emphasizing the conversion of complex data into visual formats for efficient threat detection and trend analysis. This visual analytics system, bridging physical and virtual data, is poised to revolutionize cybersecurity tasks, including forensic and threat analysis. Overall, our research marks a vital advancement in understanding and mitigating cyber victimization in the hybrid digital-physical sphere.

In the future, our vision is to see this visual analytics system become a cornerstone in cybersecurity strategies. By bridging the gap between physical and virtual realms, it promises to transform how organizations and individuals understand and respond to cyber threats. Our future work will focus on several key areas to further enhance and validate the proposed system. While the current study uses hypothetical scenarios to demonstrate the system's capabilities, future research will involve applying the system to real-world case studies. This will help validate the system's effectiveness in practical settings and provide concrete evidence of its utility in identifying and mitigating cyber threats. Additionally, we aim to integrate more advanced machine learning and artificial intelligence algorithms that can enhance the system's ability to detect and predict cyber threats. These algorithms can improve anomaly detection, threat prediction, and response strategies, making the system even more robust. In addition, continuously gathering feedback from users will be crucial in refining the system. By iterating based on user experiences and requirements, we can ensure that the system remains user-friendly and meets the evolving needs of its stakeholders. Lastly, we want to encourage collaboration between different organizations and sectors. Developing secure mechanisms for information sharing will enable collective defense strategies and a more unified approach to cybersecurity. Through these efforts, we aim to

continually enhance the visual analytics system, making it an indispensable tool in the fight against cybercrime.

## ORCID

Xinyue Ye  <http://orcid.org/0000-0001-8838-9476>

## References

- Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, 30(6), 1665–1687. <https://doi.org/10.1108/INTR-10-2019-0400>
- Baki, S., & Verma, R. (2021). Sixteen years of phishing user studies: What have we learned? arXiv preprint arXiv:2109.04661
- Beran, M., Hrdina, F., Kouřil, D., Ošlejšek, R., & Zákopčanová, K. (2020, October). Exploratory analysis of file system metadata for rapid investigation of security incidents. In *2020 IEEE Symposium on Visualization for Cyber Security (VizSec)* (pp. 11–20). IEEE. <https://doi.org/10.1109/VizSec51108.2020.00008>
- Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, 3(1): 400–420.
- Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment victimization among a juvenile population. *Youth & Society*, 44(4), 500–523. <https://doi.org/10.1177/0044118X11407525>
- Cappers, B. C., Meessen, P. N., Etalle, S., & Van Wijk, J. J. (2018, October). Eventpad: Rapid malware analysis and reverse engineering using visual analytics. In *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)* (pp. 1–8). IEEE. <https://doi.org/10.1109/VIZSEC.2018.8709230>
- Cohen, L. E., & Felson, M. (2010). Social change and crime rate trends: A routine activity approach (1979). In *Classics in environmental criminology* (pp. 203–232). Routledge.
- Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, 2(1): 308–333.
- Choi, K. S., Cho, S., & Lee, J. R. (2019). Impacts of online risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimization among Korean youth: Application of cyber-routine activities theory with latent class analysis. *Computers in Human Behavior*, 100, 1–10. <https://doi.org/10.1016/j.chb.2019.06.007>
- Cui, X., Ge, Y., Qu, W., & Zhang, K. (2020). Effects of recipient information and urgency cues on phishing detection. In *HCI International 2020-Posters: 22nd International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings, Part III 22* (pp. 520–525). Springer International Publishing.
- Culatta, E., Clay-Warner, J., Boyle, K. M., & Oshri, A. (2020). Sexual revictimization: A routine activity theory explanation. *Journal of Interpersonal Violence*, 35(15–16), 2800–2824. <https://doi.org/10.1177/0886260517704962>
- Furnell, S., Millet, K., & Papadaki, M. (2019). Fifteen years of phishing: Can technology save us? *Computer Fraud & Security*, 2019(7), 11–16. [https://doi.org/10.1016/S1361-3723\(19\)30074-0](https://doi.org/10.1016/S1361-3723(19)30074-0)

- Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). Phishing evolves: Analyzing the enduring cybercrime. *Victims & Offenders*, 16(3), 316–342. <https://doi.org/10.1080/15564886.2020.1829224>
- Griffin, S. E., & Rackley, C. C. (2008, September). Vishing. In Proceedings of the 5th Annual Conference on Information Security Curriculum Development (pp. 33–35). <https://doi.org/10.1145/1456625.1456635>
- Guerra, C., & Ingram, J. R. (2022). Assessing the relationship between lifestyle routine activities theory and online victimization using panel data. *Deviant Behavior*, 43(1), 44–60. <https://doi.org/10.1080/01639625.2020.1774707>
- Hawdon, J., Costello, M., Ratliff, T., Hall, L., & Middleton, J. (2017). Conflict management styles and cybervictimization: Extending routine activity theory. *Sociological Spectrum*, 37(4), 250–266. <https://doi.org/10.1080/02732173.2017.1334608>
- Henson, B., Wilcox, P., Reyns, B. W., & Cullen, F. T. (2010). Gender, adolescent lifestyles, and violent victimization: Implications for routine activity theory. *Victims & Offenders*, 5(4), 303–328. <https://doi.org/10.1080/15564886.2010.509651>
- Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30(1), 1–25. <https://doi.org/10.1080/01639620701876577>
- Holtfreter, K., Reising, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, 46(1), 189–220. <https://doi.org/10.1111/j.1745-9125.2008.00101.x>
- Hutchings, A., & Hayes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the ‘net’? *Current Issues in Criminal Justice*, 20(3), 433–452. <https://doi.org/10.1080/10345329.2009.12035821>
- Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, 32(6), 584–593. <https://doi.org/10.1080/0144929X.2011.632650>
- Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior and Social Networking*, 17(8), 551–555. <https://doi.org/10.1089/cyber.2014.0008>
- Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3), 263–280. <https://doi.org/10.1080/01639625.2015.1012409>
- Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, 31(5), 381–410. <https://doi.org/10.1080/01639620903004903>
- Marty, R. (2008). *Applied security visualization*. Addison-Wesley Professional.
- McClain, J., Silva, A., Emmanuel, G., Anderson, B., Nauer, K., Abbott, R., & Forsythe, C. (2015). Human performance factors in cyber security forensic analysis. *Procedia Manufacturing*, 3, 5301–5307. <https://doi.org/10.1016/j.promfg.2015.07.621>
- McNeeley, S. (2015). Lifestyle-routine activities and crime events. *Journal of Contemporary Criminal Justice*, 31(1), 30–52. <https://doi.org/10.1177/1043986214552607>
- Mustaine, E. E., & Tewksbury, R. (1998). Predicting risks of larceny theft victimization: A routine activity analysis using refined lifestyle measures. *Criminology*, 36(4), 829–858. <https://doi.org/10.1111/j.1745-9125.1998.tb01267.x>
- Näsi, M., Räsänen, P., Kaakinen, M., Keipi, T., & Oksanen, A. (2017). Do routine activities help predict young adults’ online harassment: A multi-nation study. *Criminology & Criminal Justice*, 17(4), 418–432. <https://doi.org/10.1177/1748895816679866>

- Navarro, J. N., & Jasinski, J. L. (2013). Why girls? Using routine activities theory to predict cyberbullying experiences between girls and boys. *Women & Criminal Justice*, 23(4), 286–303. <https://doi.org/10.1080/08974454.2013.784225>
- Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, 5(1), 773.
- Ngo, F. T., Piquero, A. R., LaPrade, J., & Duong, B. (2020). Victimization in cyberspace: Is it how long we spend online, what we do online, or what we post online? *Criminal Justice Review*, 45(4), 430–451. <https://doi.org/10.1177/0734016820934175>
- Nguyen, V. T., Namin, A. S., & Dang, T. (2018, July). MalViz: An interactive visualization tool for tracing malware. In *Proceedings of the 27th ACM SIGSOFT International Symposium on Software Testing and Analysis* (pp. 376–379). <https://doi.org/10.1145/3213846.3229501>
- Payne, B. K., & Hadzhidimova, L. (2020). Disciplinary and interdisciplinary trends in cybercrime research: An examination. *International Journal of Cyber Criminology*, 14(1), 81–105.
- Ramzan, Z. (2010). Phishing attacks and countermeasures. In *Handbook of information and communication security* (pp. 433–448). Springer.
- Räsänen, P., Hawdon, J., Holkeri, E., Keipi, T., Näsi, M., & Oksanen, A. (2016). Targets of online hate: Examining determinants of victimization among young Finnish Facebook users. *Violence and Victims*, 31(4), 708–726. <https://doi.org/10.1891/0886-6708.VV-D-14-00079>
- Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, 47(3), 267–296. <https://doi.org/10.1177/0022427810365903>
- Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, 50(2), 216–238. <https://doi.org/10.1177/0022427811425539>
- Reyns, B. W., Henson, B., & Fisher, B. S. (2016). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine activity theory as it applies to online forms of victimization. *Journal of Contemporary Criminal Justice*, 32(2), 148–168. <https://doi.org/10.1177/1043986215621378>
- Schreck, C. J., & Fisher, B. S. (2004). Specifying the influence of family and peers on violent victimization: Extending routine activities and lifestyles theories. *Journal of Interpersonal Violence*, 19(9), 1021–1041. <https://doi.org/10.1177/0886260504268002>
- Shaw, S.-L., & Sui, D. (2020). Understanding the new human dynamics in smart spaces and places: Towards a spatial framework. *Annals of the American Association of Geographers*, 110(2), 339–348. <https://doi.org/10.1080/24694452.2019.1631145>
- Shiravi, H., Shiravi, A., & Ghorbani, A. A. (2011). A survey of visualization systems for network security. *IEEE Transactions on Visualization and Computer Graphics*, 18(8), 1313–1329. <https://doi.org/10.1109/TVCG.2011.144>
- Tuma, K., Calikli, G., & Scandariato, R. (2018). Threat analysis of software systems: A systematic literature review. *Journal of Systems and Software*, 144, 275–294. <https://doi.org/10.1016/j.jss.2018.06.073>
- Ulmer, A., Sessler, D., & Kohlhammer, J. (2019, October). Netcapvis: Web-based progressive visual analytics for network packet captures. In *2019 IEEE Symposium on Visualization for Cyber Security (Vizsec)* (pp. 1–10). IEEE. <https://doi.org/10.1109/Vizsec48167.2019.9161633>
- Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*, 32(2), 169–188. <https://doi.org/10.1177/1043986215621379>

- Van Ouytsel, J., Ponnet, K., & Walrave, M. (2018). Cyber dating abuse victimization among secondary school students from a lifestyle-routine activities theory perspective. *Journal of Interpersonal Violence*, 33(17), 2767–2776. <https://doi.org/10.1177/0886260516629390>
- Wilsem, J. V. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, 8(2), 115–127. <https://doi.org/10.1177/1477370810393156>
- Wick, S. E., Nagoshi, C., Basham, R., Jordan, C., Kim, Y. K., Nguyen, A. P., & Lehmann, P. (2017). Patterns of cyber harassment and perpetration among college students in the United States: A test of routine activities theory. *International Journal of Cyber Criminology*, 11(1), 24–38.
- Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior*, 40(9), 1119–1131. <https://doi.org/10.1080/01639625.2018.1461786>
- Wilsem, J. V. (2013). Hacking and harassment—do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, 29(4), 437–453. <https://doi.org/10.1177/1043986213507402>
- Wu, L., Peng, Q., Lemke, M., Hu, T., & Gong, X. (2022). Spatial social network research: A bibliometric analysis. *Computational Urban Science*, 2(1), 21. <https://doi.org/10.1007/s43762-022-00045-y>
- Wu, L., Peng, Q., & Lemke, M. (2023). Research trends in cybercrime and cybersecurity: A review based on web of science core collection database. *International Journal of Cybersecurity Intelligence & Cybercrime*, 6(1), 5–28. <https://doi.org/10.52306/2578-3289.1154>
- Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, 5(4), 297–307.