Article

Cyber Attack Motivations: Connecting Actors with Event Types

Thanasis Pseftelis * and Gregory Chondrokoukis

Posted Date: 13 May 2025

doi: 10.20944/preprints202505.1003.v1

Keywords: cybersecurity; data; policy

Article

Cyber Attack Motivations: Connecting Actors with Event Types

Thanasis Pseftelis * and Gregory Chondrokoukis

University of Piraeus; University of Piraeus

* Correspondence: psesftelis@unipi.gr

Abstract: This study examines the various motivations that drive cyberattacks, focusing on correlations with the types of actors and the types of events they execute. The rise of digitization, especially post-COVID-19, has intensified the threat landscape, making it critical to understand the factors influencing these attacks. Using the University of Maryland's Cyber Events Database (2014-2024), the research uses chi-squared tests to identify significant correlations between different actor categories-such as cybercriminals, state-sponsored entities, and activist groups-and their motivations, which include financial gain, espionage, protest, and sabotage. The results indicate that ideology-driven actors often engage in disruptive events, while cybercriminals focus primarily on exploitative actions aimed at economic gain. These findings underscore the urgent need for multifaceted cybersecurity strategies that adapt to changing dynamics in the threat landscape, foster cross-sector collaboration, and support informed policymaking to strengthen defenses against diverse cyber risks. The study lays the groundwork for future research into the linkages between actor motivations and their operational impacts, thereby contributing to improved cybersecurity practices and resilience.

Keywords: cybersecurity; data; policy

1. Introduction

In recent years, particularly following the advent of the COVID-19 pandemic, there has been an unrelenting acceleration in the process of digitization that pervades all facets of our lives. Concurrently, the proliferation of cyber threats has escalated, resulting in the compromise of various systems and data. The motives underlying cyberattacks are multifaceted, encompassing a broad spectrum of factors, including economic interests and various ideological beliefs. It is imperative for professionals engaged in the realm of cybersecurity to comprehend these motivations, as this knowledge is instrumental in enhancing their contributions to cybersecurity measures and more effectively countering cyber-attacks.

It is imperative to acknowledge that disparate actors—be they individuals or groups of individuals—operate with a diverse array of motivations. These motivations significantly influence the methods employed to exploit vulnerabilities and achieve desired outcomes. For instance, actors motivated by ideology primarily seek to disseminate or project messages that align with their ideological framework, often without prioritizing economic gain. Furthermore, they perceive themselves as contributing to the justice or desired change they are promoting, vis-à-vis entities or situations that perceive them as opponent [1,2]. A close examination of the extant literature reveals that the motivations of attackers vary according to the prevailing socio-political context. In particular, the pursuit of material gain or reputation appears to be a less significant factor in certain circumstances.

Conversely, cyberattacks driven by financial motives represent an emerging threat to organizations and individuals. The proliferation of cybercrime can be attributed to the increasing prevalence of financial transactions conducted online. Ransomware and phishing attacks are frequently employed by attackers due to their effectiveness against online transactions. This phenomenon can be attributed to the growing vulnerabilities of digital infrastructures, which renders businesses and organizations susceptible to exploitation [3]. In the contemporary landscape of cybersecurity, the integration of artificial intelligence (AI) has profoundly transformed the landscape of cyberattacks, rendering traditional defense techniques increasingly obsolete. This paradigm shift underscores the imperative for the development of innovative, cutting-edge defense methodologies.

Furthermore, the role of state actors, whether directly or indirectly, in cyber espionage or the dissemination of disinformation, introduces an additional layer of complexity to the motivations underlying cyberattacks. The objectives of the aforementioned assailants are commensurate with the realms of national security or industrial espionage, with the objective of acquiring classified information and attaining an advantage over competitors [4] [5] .

This research study examines the existence, if any, of relationships between the motives of the attackers and the motives of the attacks. The data from past attacks (2014–2024) are utilized to draw safe conclusions by employing the chi-square test [6], a widely used statistical method for examining relationships between categorical variables. The corroboration of these relationships has the potential to enhance defense mechanisms and improve security policies, as it facilitates the generation of knowledge derived from real-world events.

2. Materials and Methods

In order to develop a more profound comprehension of the threats posed by cybercrime, it is imperative to undertake a thorough investigation into the motivations that underpin the actions of both the perpetrators and the attacks themselves. The conventional classification of hackers into two categories, namely ethical hackers, who seek to identify vulnerabilities in various systems in a timely manner, and black hackers, who exploit existing vulnerabilities, is insufficient to comprehensively understand the motivations behind their actions.

The issue of motivation must be approached with a multifaceted and nuanced perspective, especially in the dynamic and ever-evolving field of cybersecurity. It is essential to conduct analyses that consider motivations related to incidents and those related to different types of actors. To better assess them, a review of the literature is sought in accordance with the type of cyber incidents, the different types of actors and their motivations, based on the interaction they have with each other.

2.1. Cyber Events Database: University of Maryland NIS360 [7,8]

The University of Maryland's database, which has been in operation since 2014, systematically documents various cyber incidents that occur in different countries. A comprehensive internet scan was conducted to identify sources that highlight cyberattacks. These sources were then confirmed and systematically categorized to map the current state of cyber security issues.

The following variables are distinguished among the elements contained in the database:

- Actor Type: The actor type is a critical factor in distinguishing the perpetrators of cyberattacks. These perpetrators include criminal organizations, nation-state actors, terrorist groups, hacktivists, and hobbyists. This categorization facilitates the discernment of potential motives and methods employed by the actors in question by cybersecurity researchers and policymakers.
- Motive: The motivation behind each cyberattack is a critical factor in its classification. The motives can be categorized into four distinct groups: economic gain, espionage, protest, and sabotage. The utilization of this categorization facilitates the identification of potential trends and patterns that may emerge in future analyses, thereby providing a framework for anticipating future outcomes.
- Mixed: Cyber incidents are classified into three categories: disruptive, exploitative, or mixed. This categorization facilitates comprehension of the repercussions that cyberattacks have on various organizational systems and the consequences that ensue from these events.

2.2. A Profile of Actor Types in Cyber Threats

An analysis of the various types of actors reveals the following classification:

- Cybercriminals are individuals or associations of individuals who commit illegal acts in cyberspace with the primary objective of financial gain. These actors leverage vulnerabilities to compromise the security of systems, with the aim of perpetrating financial fraud, stealing the identity of their victims, and obtaining sensitive personal data or confidential information [9–11]. A marked increase in cyber activity has been observed, accompanied by the implementation of advanced methodologies involving ransomware and phishing attacks [10,11].
- Actors operating under the auspices of a state entity, either directly or indirectly, seek to gather intelligence for the purpose of espionage and to inflict a blow against other state entities [12,13]. Furthermore, these actors frequently pursue acts of sabotage against critical infrastructure and surveillance systems in matters of geopolitical concern [14,15]. The primary objective of the aforementioned actions is to diminish national security and to acquire a technological superiority over states that are antagonistic towards them.
- Terrorist groups are non-state entities that seek to alter political situations through the instigation of fear. These actors leverage cyberspace to launch attacks against various institutions and beyond. The tactics employed by these actors pose a significant threat to national security and the prestige of the state entity in question. These threats manifest through attacks on critical information systems or infrastructure, which can severely compromise the entity's ability to function effectively [16,17]. The subjects' objectives are driven by a specific ideological framework that guides their actions. These actions are intended to instill fear, modify political circumstances, and, in general, radicalize protest movements.
- Hacktivists who adhere to political or social criteria employ cyberattacks as a medium to articulate their protest against situations that they deem to be in violation of their sense of justice. The objective of these actors is to create problems in the operations of organizations or state entities, thereby promoting their message in specific situations [18,19]. The objective of cyberattacks is twofold: to exploit and to disrupt various services.
- Hobbyists are individuals who engage in activities for the sake of personal interest and enjoyment, often driven by a desire to satisfy their curiosity and receive acknowledgment for their pursuits. While their actions in cyberspace are not inherently malicious, they may unintentionally engage in practices that compromise cybersecurity [20,21]. While not necessarily driven by the same motivations as cybercriminals, the actions of these entities can potentially result in the exploitation of vulnerabilities or service disruption.

2.3. Motives Underlying Cyber Events

A multitude of factors underpin the motivations, which, to enhance comprehension of the subject matter, are delineated as such in light of extant literature.

- Financial Gain: The primary motivation for cybercriminals is typically economic gain. This is achieved through data breach or data theft attacks, or ransomware [22,23]. These actors employ sophisticated methods to exploit vulnerabilities, guided by the pursuit of optimal economic gain [24]. Cyberattacks driven by economic gain can be categorized as exploitative in nature, as they focus on targeting data that is being utilized for economic gain.
- Espionage: Espionage is the prevailing motive for state entities, with the objective being the collection of information and the procurement of classified data, ultimately leading to the attainment of a strategic advantage [25,26]. The phenomenon under consideration combines both disruptive and exploitative cyber events.
- Protest: The impetus behind the various activists seeking the shutdown of online services is protest, which is motivated by socio-political reasons [27,28]. These actors typically engage in actions directed towards governments or corporate entities, often achieving their objectives through the orchestration of disruptive cyber events. In recent years, there has been an observed increase in the use of exploitative cyber events [29,30].

- Sabotage: Sabotage is typically characterized as either ideologically motivated or a tactic employed by state entities to neutralize systems or networks [31,32]. The cyber events that achieve this objective are classified as disruptive cyber events, with the aim of either inflicting a loss of reputation or imposing a significant financial burden.

2.4. The Interaction of Cyber-Events with Motives and Actors

The classification of cyber events, as delineated by contemporary literature, enables the discernment of distinct categories based on the actors involved and their respective motivations. This systematic approach facilitates the identification of cyber events into the following categories:

- Disruptive Events: Disruption events are defined as those that deliberately seek to interrupt or hinder the functioning of various systems or services. These events are often initiated by hacktivists, terrorists, and similar actors, with the primary objective being to either influence public opinion or to instill fear [33,34]. Beyond the mere disruption of services, the objectives of these actors frequently entail the extensive damage of existing services and functions, as well as the reputation of their targets [35].
- Exploitative Events: Exploitative events are those that primarily stem from cybercriminals seeking financial gain through theft or ransom [36,37]. Given the sophisticated tactics employed to achieve their objectives, it is imperative to implement continuous updates to cybersecurity protocols across all industry sectors [38,39].
- Mixed Events: The proliferation of cyber-events, encompassing both disruptive and exploitative elements, such as ransomware, necessitates the establishment of a distinct category that incorporates the existing classifications [40,41]. It is evident that the occurrence of such events can lead to the implementation of service disruptions and the exploitation of economic resources.

2.5. Methodology

According to the previously articulated framework, the present research study is designed to investigate the presence or absence of any potential relationships between the following:

- The actors and the motives.
- The event types and the motives.

Research Questions:

RQ1: Is there a correlation between the type of actor and the type of motive?

RQ2: Is there a correlation between the event type and the motive?

The University of Maryland's Cyber Events database [42] is regarded as an appropriate dataset for this investigation, as it can contribute to the study of our research questions. The database under consideration contains more than 14,000 cyberattack incidents, spanning the period from 2014 to 2024. Among the variables examined, three were identified as the most pertinent to the research interests under investigation. In the context of this study, the following variables warrant particular consideration:

Actor Type (actor_type):

- Criminal
- Nation-State
- Terrorist
- Hacktivist
- Hobbyist

Event Type (event_type)

- Disruptive
- Exploitive
- Mixed

Motive (motive):

- Protest

doi:10.20944/preprints202505.1003.v1

- Sabotage
- Espionage
- Financial

The initial records of the set exceeded 14,000. For the variables actor, actor_type, industry, motive, event_type, event_subtype, country, and actor_country, the respective values with the indication "undetermined" or with a similar reference were excluded. The database was formed with 2,728 records. This decision is made consciously in an effort to mitigate the ambiguity inherent in the data and to optimally address the research questions at hand.

3. Results

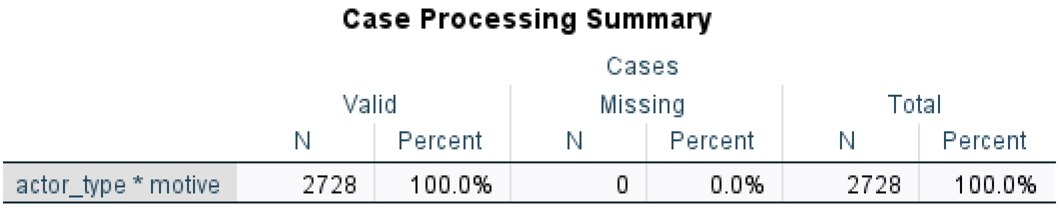
In light of the aforementioned considerations, the ensuing findings are hereby presented:

RQ1: Is there a correlation between the type of actor and the type of motive?

The null hypothesis (H0) and the alternative hypothesis (H1) of the chi-square independence test are formulated as follows for the pair of variables (actor_type, motive):

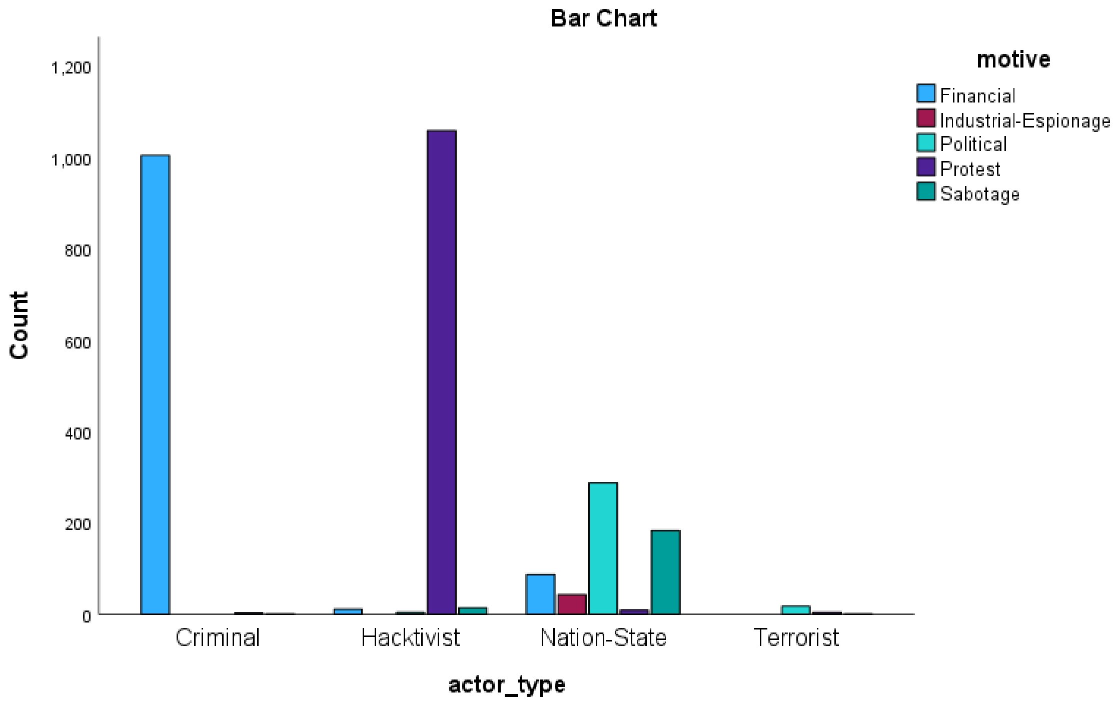
- H0: The null hypothesis posits that "Actor Type is independent of Motive."
- H1: The alternative hypothesis posits that "Actor Type is not independent of Motive."

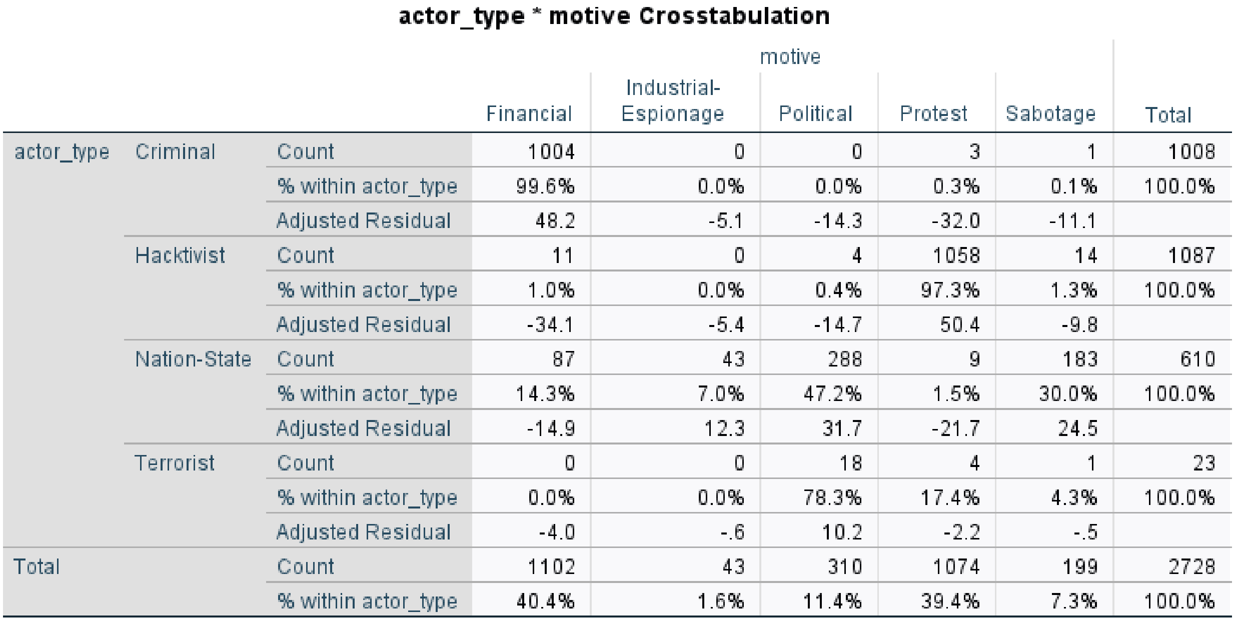
Our first research question was examined using the chi-square test. The categorical variables employed in this study included actor type and event type. Both are nominal variables and include the categories presented above. The following contingency table enumerates the observations that fall into each combination.



Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
actor_type * motive	2728	100.0%	0	0.0%	2728	100.0%

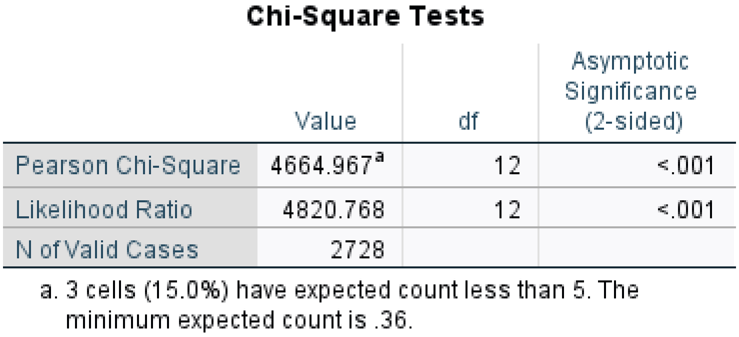




actor_type * motive Crosstabulation

			motive					
			Financial	Industrial-Espionage	Political	Protest	Sabotage	Total
actor_type	Criminal	Count	1004	0	0	3	1	1008
		% within actor_type	99.6%	0.0%	0.0%	0.3%	0.1%	100.0%
		Adjusted Residual	48.2	-5.1	-14.3	-32.0	-11.1	
	Hacktivist	Count	11	0	4	1058	14	1087
		% within actor_type	1.0%	0.0%	0.4%	97.3%	1.3%	100.0%
		Adjusted Residual	-34.1	-5.4	-14.7	50.4	-9.8	
	Nation-State	Count	87	43	288	9	183	610
		% within actor_type	14.3%	7.0%	47.2%	1.5%	30.0%	100.0%
		Adjusted Residual	-14.9	12.3	31.7	-21.7	24.5	
	Terrorist	Count	0	0	18	4	1	23
		% within actor_type	0.0%	0.0%	78.3%	17.4%	4.3%	100.0%
		Adjusted Residual	-4.0	-.6	10.2	-2.2	-.5	
Total		Count	1102	43	310	1074	199	2728
		% within actor_type	40.4%	1.6%	11.4%	39.4%	7.3%	100.0%

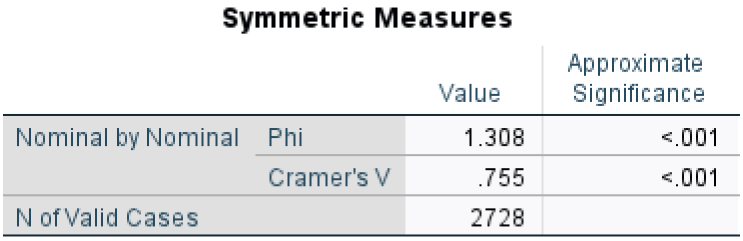
The chi-square test yielded a statistic of $\chi^2 = 4664.967$ with 12 degrees of freedom (df = 12), p < 0.001. This finding suggests the presence of a statistically significant correlation between the variables under study.



Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4664.967[a]	12	<.001
Likelihood Ratio	4820.768	12	<.001
N of Valid Cases	2728		

a. 3 cells (15.0%) have expected count less than 5. The minimum expected count is .36.



Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	1.308	<.001
	Cramer's V	.755	<.001
N of Valid Cases		2728	

All the test criteria were met specifically, the following conditions were satisfied:

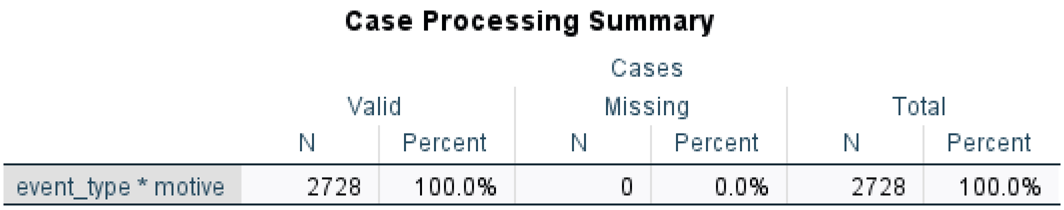
- The expected cell frequencies all met the required conditions (80% of the cells are greater than or equal to 5).
- There are more than two categories of categorical variables.
- The sample size is large.

RQ2: Is there a correlation between the event type and the motive?

The null hypothesis (H0) and the alternative hypothesis (H1) of the chi-square independence test are formulated as follows for the pair of variables (event_type, motive):

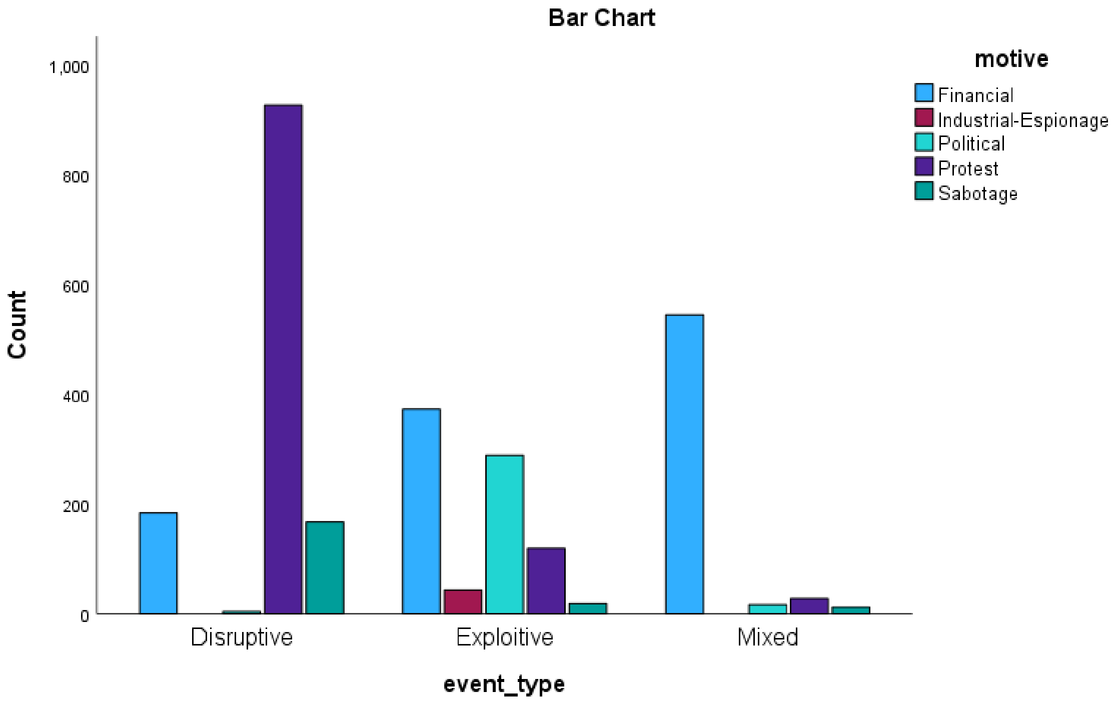
- H0: The null hypothesis posits that "Event Type is independent of Motive."
- H1: The alternative hypothesis posits that "Event Type is not independent of Motive."

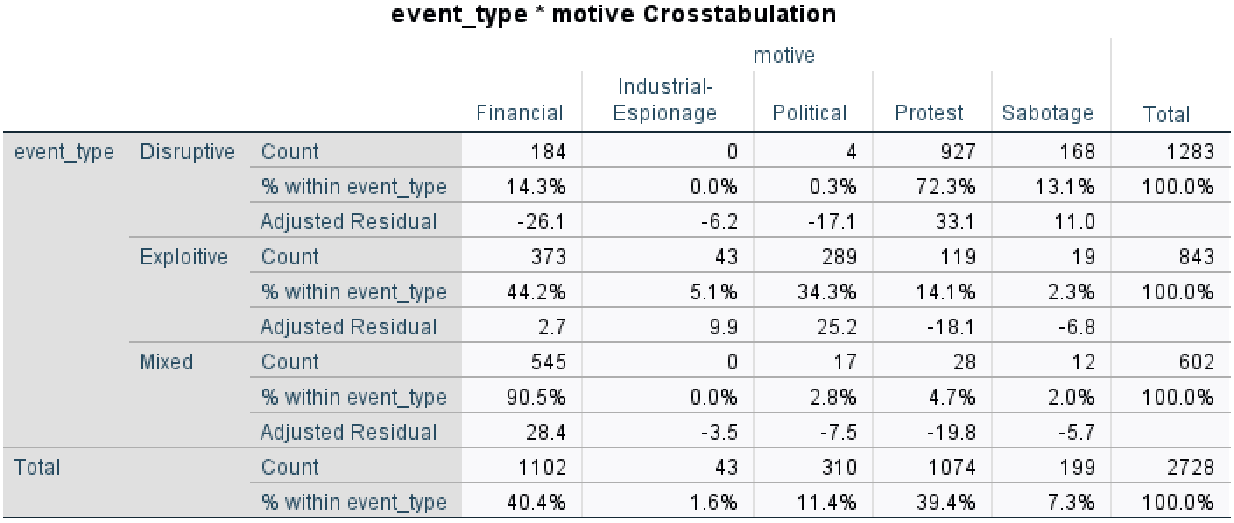
Our second research question was examined using the chi-square test. The categorical variables employed in this study included event type and motive. Both are nominal variables and include the categories presented above. The following contingency table enumerates the observations that fall into each combination.



Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
event_type * motive	2728	100.0%	0	0.0%	2728	100.0%

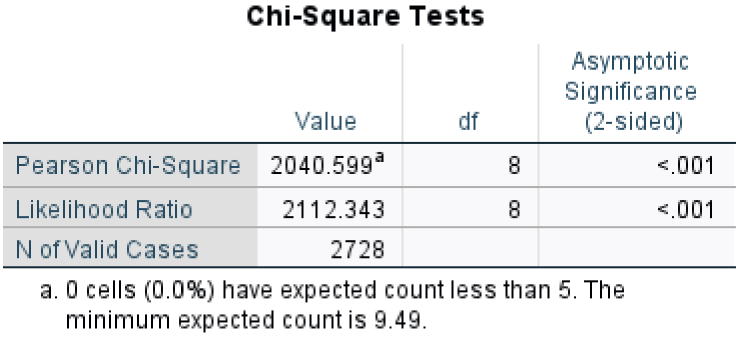




event_type * motive Crosstabulation

			motive					
			Financial	Industrial-Espionage	Political	Protest	Sabotage	Total
event_type	Disruptive	Count	184	0	4	927	168	1283
		% within event_type	14.3%	0.0%	0.3%	72.3%	13.1%	100.0%
		Adjusted Residual	-26.1	-6.2	-17.1	33.1	11.0	
	Exploitive	Count	373	43	289	119	19	843
		% within event_type	44.2%	5.1%	34.3%	14.1%	2.3%	100.0%
		Adjusted Residual	2.7	9.9	25.2	-18.1	-6.8	
	Mixed	Count	545	0	17	28	12	602
		% within event_type	90.5%	0.0%	2.8%	4.7%	2.0%	100.0%
		Adjusted Residual	28.4	-3.5	-7.5	-19.8	-5.7	
Total		Count	1102	43	310	1074	199	2728
		% within event_type	40.4%	1.6%	11.4%	39.4%	7.3%	100.0%

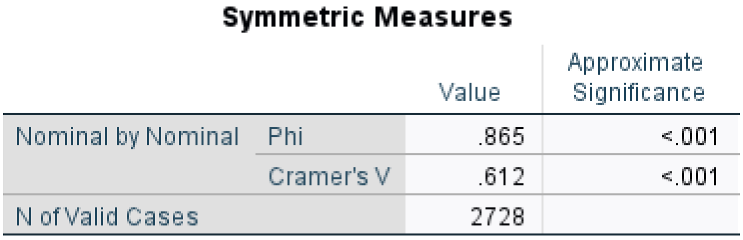
The chi-square test yielded a statistic of $\chi^2 = 2040.599$ with 8 degrees of freedom (df = 8), $p < 0.001$. This finding suggests the presence of a statistically significant correlation between the variables under study.



Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2040.599[a]	8	<.001
Likelihood Ratio	2112.343	8	<.001
N of Valid Cases	2728		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 9.49.



Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	.865	<.001
	Cramer's V	.612	<.001
N of Valid Cases		2728	

All the test criteria were met; specifically, the following conditions were satisfied:

- The expected cell frequencies all met the required conditions (80% of the cells are greater than or equal to 5).
- There are more than two categories of categorical variables.
- The sample size is large.

4. Discussion

This research contributes to a more nuanced understanding of cyber actors, their motivations, and the cyber attacks they carry out. A multifactorial approach to the analysis of cyber-security incidents is deemed necessary, as cyber-threats evolve simultaneously with various technologies and changing socio-political realities. The confirmation of statistically significant correlations through chi-square tests, with regard to actor types and motives and event types and motives, once again highlights the necessity of employing integrated analytical frameworks. These frameworks are capable of enhancing prediction and response to cyber threats.

The results of the study indicate that the various actors involved in cybercrime, including nation-state actors and hacktivists, typically operate in accordance with specific motives. For instance, cybercriminals seek financial gain through ransomware and phishing attacks. The advent of the Internet has led to a substantial increase in financial transactions, thereby creating new avenues for exploitation [43]. Moreover, the digital transition of various organizations has led to the emergence of vulnerabilities that can be exploited by perpetrators for financial gain [44].

Cyber actors operating under the auspices of a state entity are driven by espionage and sabotage objectives, seeking to compromise national security or disrupt industrial activity. Given the severity of these threats, it is imperative for respective state entities to maintain constant vigilance and to enhance national strategies against various cyber threats. The various geopolitical tensions related to cyberspace require further academic investigation in the light of improving existing policies [45,46].

Through this research, the existence of a relationship between event types and motivation is highlighted. Disruptive events are most associated with hacktivists and fear-mongering groups, whose motivations are based on socio-political causes. The present findings are consistent with the existing literature, highlighting that these actors, through cyber attacks seek to influence public opinion or cultivate a sense of fear in the targeted societies [47]. As a result, the categorization of events into disruptive, exploitative and mixed allows for easier consolidation of the consequences of these attacks.

Mixed events, such as ransomware attacks, exemplify the intricate nature of emerging cyber threats. In their occurrence, these phenomena achieve two objectives: the disruption of services and the pursuit of financial gain. Due to their inherent characteristics, they render a number of conventional approaches to cybersecurity obsolete, thereby underscoring the necessity to recalibrate various cyber strategies [48].

In the aforementioned points, it would be remiss to neglect to mention the use of artificial intelligence in the domain of cybersecurity. This development poses a challenge to existing defense mechanisms, but it also facilitates the enhancement of cyber protection. A significant component of the research should entail the evaluation of defense strategies through the utilization of artificial intelligence, with the objective of intercepting emerging cyber threats [49,50]. This is particularly salient in the context of de facto actors leveraging artificial intelligence to engineer novel forms of cyberattacks.

The utilization of artificial intelligence in the analysis of cyber actors' motivations and behaviors has the potential to enhance the efficacy of personalized training programs for various organizations and communities. This approach can contribute to the cultivation of a robust cybersecurity culture, as well as the proactive identification and mitigation of potential cyber threats [51,52].

Given the dynamic nature of cyber threats, further exploration of the relationships identified in this study is necessary. In the near future, it would be advisable for research to concentrate on exploring other datasets and/or utilize poetic methods to further enrich the findings presented. A regional and/or broader focus on specific areas has the potential to illuminate the motivations and tactics influenced by these individual characteristics.

In order to enhance the protection of cyberspace, it is imperative to facilitate the exchange of information among the various stakeholders, particularly those responsible for formulating cybersecurity policies. It is imperative that there be as much cooperation between the public and private sectors as possible.

5. Conclusions

This study contributes to our understanding of the intricate relationship between the motivations of cyber actors and the typology of cyber events. Utilizing a comprehensive dataset from the University of Maryland Cyber Events Database, which spans the period from 2014 to 2024, and employing rigorous chi-squared analyses, the study uncovers statistically significant associations between both actor types and their corresponding motivations, as well as between event types and their inherent motivations. These findings underscore the necessity for multifaceted analytical frameworks that can capture the inherent dynamism and complexity of today's cyber threat landscape.

The results indicate that a diverse array of cyber actors—ranging from financially motivated cybercriminals to ideologically motivated hacktivists and state-sponsored entities—demonstrate distinct motivational profiles that directly influence the nature of cyber events they perpetrate. A critical aspect of understanding the operational impact of cyber events is the classification of these events into distinct categories, namely disruptive, exploitative, and mixed types. This classification provides a nuanced perspective, allowing for a more comprehensive analysis of the operational consequences of these incidents. For instance, the occurrence of a ransomware attack, a type of blended event, results in the disruption of services and the exploitation of economic vulnerabilities, thereby challenging the efficacy of traditional cybersecurity defenses.

Despite the contributions of this research, several limitations must be acknowledged. The study's reliance on secondary data and the exclusion of ambiguous or indeterminate cases may introduce selection bias and limit the generalizability of the findings. Consequently, future research endeavors would benefit from the incorporation of additional and more diverse data sources, longitudinal analyses, and the exploration of regional variations in cyber operations. Furthermore, the accelerating integration of artificial intelligence into both offensive and defensive cyber strategies signifies an emerging frontier that merits further scholarly exploration.

In summary, the present study establishes a critical foundation for future research endeavors aimed at elucidating the intricate interplay between the motivations of cyber actors and the typology of events. The statistically significant correlations identified in this study provide compelling evidence for the necessity of enhanced inter-sectoral collaboration—spanning the public, private, and academic domains—and the development of more resilient, adaptive cybersecurity frameworks. In the contemporary context of a constantly evolving threat landscape, characterized by increasing interconnectedness, such integrative efforts are imperative for the protection of digital infrastructures.

Supplementary Materials: The following supporting information can be downloaded at the website of this paper posted on Preprints.org.

References

1. Banerjee, S., Swearingen, T., Shillair, R., Bauer, J. M., Holt, T. J., & Ross, A. (2021). Using machine learning to examine cyberattack motivations on web defacement data. Social Science Computer Review, 40(4), 914-932. https://doi.org/10.1177/0894439321994234
2. Holt, T. J., Freilich, J. D., & Chermak, S. M. (2017). Exploring the subculture of ideologically motivated cyber-attackers. Journal of Contemporary Criminal Justice, 33(3), 212-233. https://doi.org/10.1177/1043986217699100
3. Nedeljković, N., Vugdelija, N., & Kojić, N. (2020). Use of "owasp top 10" in web application security. Fourth International Scientific Conference ITEMA Recent Advances in Information Technology, Tourism, Economics, Management and , 25-30. https://doi.org/10.31410/itema.2020.25
4. Heering, M. S., Travaglino, G. A., Abrams, D., & Goldsack, E. (2020). "if they don't listen to us, they deserve it": the effect of external efficacy and anger on the perceived legitimacy of hacking. Group Processes &Amp; Intergroup Relations, 23(6), 863-881. https://doi.org/10.1177/1368430220937777
5. Pärn, E. and Edwards, D. J. (2019). Cyber threats confronting the digital built environment. Engineering, Construction and Architectural Management, 26(2), 245-266. https://doi.org/10.1108/ecam-03-2018-0101
6. https://libguides.library.kent.edu/spss/chisquare
7. Harry, C., & Gallagher, N. (2018). Classifying Cyber Events. Journal of Information Warfare, 17(3), 17-31 https://cissm.umd.edu/sites/default/files/2019-07/Cyber-Taxonomy-101918.pdf
8. https://cissm.umd.edu/cyber-events-database
9. Pseftelis, T. and Chondrokoukis, G. (2025). Understanding cyber incident dynamics in the european union: a study of actor types and sector vulnerabilities.. https://doi.org/10.20944/preprints202504.2169.v1
10. Pawlicka, A., Choraś, M., & Pawlicki, M. (2021). The stray sheep of cyberspace a.k.a. the actors who claim they break the law for the greater good. Personal and Ubiquitous Computing, 25(5), 843-852. https://doi.org/10.1007/s00779-021-01568-7
11. Mihai, I. (2022). Untitled. International Journal of Information Security and Cybercrime, 11(1). https://doi.org/10.19107/ijisc.2022.01
12. Alda, E. and Sala, J. L. (2014). Links between terrorism, organized crime and crime: the case of the sahel region. Stability: International Journal of Security &Amp; Development, 3(1). https://doi.org/10.5334/sta.ea
13. Sukhodolia, O. (2018). Implementation of the concept of critical infrastructure protection in ukraine: achievements and challenges. Information &Amp; Security: An International Journal, 40(2), 107-119. https://doi.org/10.11610/isij.4008
14. Alkharman, J. and Hassan, I. (2023). Cyberterrorism and self-defense in the framework of international law. Journal of Law and Sustainable Development, 11(8), e1430. https://doi.org/10.55908/sdgs.v11i8.1430
15. Raghuwanshi, P. (2024). Ai-driven identity and financial fraud detection for national security. Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023, 7(01), 38-51. https://doi.org/10.60087/jaigs.v7i01.294
16. Chang, H. and Hawamdeh, S. (2020). Cybersecurity for information professionals.. https://doi.org/10.1201/9781003042235

17. Cantika, S. and Umniyah, A. (2023). Analysis of the australian government's security strategy in countering the potential threat of terrorism groups through cyber terrorism instruments. Insignia: Journal of International Relations, 10(2), 214. https://doi.org/10.20884/1.ins.2023.10.2.9376
18. KOVACI, P. (2024). Threat actors seeking to exploit ai capabilities. types and their goals. Strategic Impact, 89(4), 53-63. https://doi.org/10.53477/1842-9904-23-21
19. Sigholm, J. (2013). Non-state actors in cyberspace operations. Journal of Military Studies, 4(1), 1-37. https://doi.org/10.1515/jms-2016-0184
20. Rizal, M. and Yani, Y. M. (2016). Cybersecurity policy and its implementation in indonesia. JAS (Journal of ASEAN Studies), 4(1), 61. https://doi.org/10.21512/jas.v4i1.967
21. Sigholm, J. (2013). Non-state actors in cyberspace operations. Journal of Military Studies, 4(1), 1-37. https://doi.org/10.1515/jms-2016-0184
22. Maimon, D. and Louderback, E. R. (2019). Cyber-dependent crimes: an interdisciplinary review. Annual Review of Criminology, 2(1), 191-216. https://doi.org/10.1146/annurev-criminol-032317-092057
23. Habermayer, H. and Schröfl, J. (2014). Genese und wesentliche inhalte der österreichischen strategie für cyber sicherheit (öscs). Sicherheit &Amp; Frieden, 32(1), 28-36. https://doi.org/10.5771/0175-274x-2014-1-28
24. Garty, A. (2023). The digital frontier: defending the public sector against cyberthreats. Network Security, 2023(9). https://doi.org/10.12968/s1353-4858(23)70041-x
25. Petrich, K. (2021). The crime–terror nexus. Oxford Research Encyclopedia of International Studies. https://doi.org/10.1093/acrefore/9780190846626.013.608
26. Batueva, E. (2014). Virtual reality: u.s. information security threats concept and its international dimension. MGIMO Review of International Relations, (3(36)), 128-136. https://doi.org/10.24833/2071-8160-2014-3-36-128-136
27. Rasmussen, M. L. and Erickson, C. M. (2025). From elements to effects: the strategic imperative to understand "national cyber power". International Conference on Cyber Warfare and Security, 20(1), 86-92. https://doi.org/10.34190/iccws.20.1.3365
28. Albahar, M. A. (2017). Cyber attacks and terrorism: a twenty-first century conundrum. Science and Engineering Ethics, 25(4), 993-1006. https://doi.org/10.1007/s11948-016-9864-0
29. Kautwima, P., Haiduwa, T., Sai, K. O. S., Hashiyana, V., & Suresh, N. (2021). System end-user actions as a threat to information system security. International Journal of Network Security &Amp; Its Applications, 13(6), 71-83. https://doi.org/10.5121/ijnsa.2021.13606
30. Beretas, C. P. (2024). The most important types of cyber attacks that france is expected to face in the future and the cyber security measures it must implement to protect critical infrastructure, telecommunication networks and personal data. Universal Library of Engineering Technology, 01(01), 01-12. https://doi.org/10.70315/uloap.ulete.2024.0101001
31. Malec, N. (2024). Sztuczna inteligencja a bezpieczeństwo państwa. Prawo I Bezpieczeństwo, (1 (2024)), 20-24. https://doi.org/10.4467/29567610pib.24.002.19838
32. Judijanto, L. (2024). National security strategies amidst increasing global cyber threats: a multilateral approach. Synergisia, 1(2), 11-18. https://doi.org/10.62872/2wph4p15
33. Morris, A. and Meloy, J. R. (2020). A preliminary report of psychiatric diagnoses in a scottish county sample of persons of national security concern. Journal of Forensic Sciences, 65(5), 1638-1645. https://doi.org/10.1111/1556-4029.14471
34. Lehto, M. (2022). Apt cyber-attack modelling: building a general model. International Conference on Cyber Warfare and Security, 17(1), 121-129. https://doi.org/10.34190/iccws.17.1.36
35. Rath, S. K. (2016). South asia's cyber insecurity: a tale of impending doom. Qatar Foundation Annual Research Conference Proceedings Volume 2016 Issue 1. https://doi.org/10.5339/qfarc.2016.ictpp1054
36. Heinl, C. H. (2021). Technology. The Oxford Handbook of Cyber Security, 201-220. https://doi.org/10.1093/oxfordhb/9780198800682.013.11
37. Olszewski, B. (2018). Advanced persistent threats as a manifestation of states' military activity in cyber space. Scientific Journal of the Military University of Land Forces, 189(3), 57-71. https://doi.org/10.5604/01.3001.0012.6227

38. Turunen, M. and Kari, M. J. (2020). Cyber deterrence and russia's active cyber defense. Proceedings of the 19th European Conference on Cyber Warfare. https://doi.org/10.34190/ews.20.038
39. Florido-Benítez, L. (2024). The types of hackers and cyberattacks in the aviation industry. Journal of Transportation Security, 17(1). https://doi.org/10.1007/s12198-024-00281-9
40. Стригунов, К. С. (2023). Hybridization of international terrorism and transnational crime at the present stage. Istoriya, 14(4 (126)), 0. https://doi.org/10.18254/s207987840020330-2
41. Grytsyshen, D. (2020). Methodology of implementation of the state criminal policy in the field of prevention and counteraction to economic crime in the context of interaction with other types of state policy. Public Administration Aspects, 8(5), 97-106. https://doi.org/10.15421/152098
42. https://cissm.umd.edu/research-impact/publications/cyber-events-database-home
43. Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Almuhaisen, H. A., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. Sensors, 23(16), 7273. https://doi.org/10.3390/s23167273
44. Cheung-Blunden, V., Cropper, K., Panis, A., & Davis, K. (2019). Functional divergence of two threat-induced emotions: fear-based versus anxiety-based cybersecurity preferences.. Emotion, 19(8), 1353-1365. https://doi.org/10.1037/emo0000508
45. Chimezie, O., Akagha, O. V., Dawodu, S. O., Anyanwu, A., Onwusinkwue, S., & Ahmad, I. A. I. (2024). Comprehensive review on cybersecurity: modern threats and advanced defense strategies. Computer Science &Amp; IT Research Journal, 5(2), 293-310. https://doi.org/10.51594/csitrj.v5i2.758
46. Bocharova, A. (2024). Information security and cybersecurity policy. World Economy and International Relations, 68(4), 121-130. https://doi.org/10.20542/0131-2227-2024-68-4-121-130
47. Gombár, M., Vagaská, A., Korauš, A., & Račková, P. (2024). Application of structural equation modelling to cybersecurity risk analysis in the era of industry 4.0. Mathematics, 12(2), 343. https://doi.org/10.3390/math12020343
48. Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Cybersecurity awareness and education programs: a review of employee engagement and accountability. Computer Science &Amp; IT Research Journal, 5(1), 100-119. https://doi.org/10.51594/csitrj.v5i1.708
49. Mavroeidis, V., Hohimer, R. E., Casey, T., & Jesang, A. (2021). Threat actor type inference and characterization within cyber threat intelligence. 2021 13th International Conference on Cyber Conflict (CyCon), 327-352. https://doi.org/10.23919/cycon51939.2021.9468305
50. Holding, A. C., Barlow, M., Koestner, R., & Wrosch, C. (2019). Why are we together? a dyadic longitudinal investigation of relationship motivation, goal progress, and adjustment. Journal of Personality, 88(3), 464-477. https://doi.org/10.1111/jopy.12503
51. Sundjaja, A. M., Ridwan, A., Robbani, D., & Soemantri, R. A. (2024). Impact of 'don't know? kasih no!' campaign on cybersecurity awareness: unraveling the links to user satisfaction, trust, and commitment. International Journal of Safety and Security Engineering, 14(5), 1577-1589. https://doi.org/10.18280/ijsse.140525
52. Srivast, A., Hussain, M. M., Sadanandan, S. K., Sarwari, A. R., & Reece, R. (2023). Building cyber-attack immunity in electric energy system inspired by infectious disease ecology.. https://doi.org/10.21203/rs.3.rs-3376693/v1

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.