JOURNAL OF JUDIKALTURA
E-ISSN 2985-6043
Vol 2 issue 1 2024
page. 1-11

The Dark Web's Influence on International Relations: Unravelling the Hidden Threads

Sarah Bardhant[1*], Pallabhi Chakraborty[2]
[1,2]School of Public Policy and Governance, Tata Institute of Social Sciences, Hyderabad, Mumbai

*Correspondence author: sara.bardhan77@gmail.com

INFO
Submitted: 20-09-2022,
Revised: 21-10-2022,
Accepted: 20-12-2023

ABSTRACT
Using a blended-techniques approach, this looks at explores the diffused effect of the dark net on worldwide family members. According to a quantitative network study, kingdom actors are not unusual on the dark web, which is regular with new scholarly debate. Key topics that represent present day scholarly worries, including "Covert Operations and Espionage," "Eroding Trust in Intelligence Sharing," "Extremism and Terrorism," and "Challenges in Law Enforcement," are found out via thematic evaluation of qualitative statistics. This research sticks out for its thorough evaluation of the dark web's complex results, which connects quantitative and qualitative findings. The effects highlight the vital want for worldwide cybersecurity regulations and tips in light of the converting digital environment. This examine adds a super deal to the frame of knowledge via illuminating the outcomes of the darkish net for global relations and global security. Research ethics are a essential factor of the examine and are meticulously tested at each stage. This observer's breadth perfectly fits the dreams of the magazine and provides insightful information on how cybersecurity, geopolitics, and diplomatic relations engage.

Keywords**:** *International Relations, Cybersecurity, State Actors*

INTRODUCTION

The creation starts off evolved with a thrilling synopsis of the net's transformative capacity to link individuals, organizations, and governments globally (Sima et al., 2020). Yet, because of its anonymity and encryption competencies, the darkish internet—a hidden domain interior this networked surroundings—is related to criminal behaviour and cybersecurity vulnerabilities (Nazah et al., 2020). This study intends to find the hidden dimensions of these relationships and acknowledge the dark internet's indisputable have an effect on on the geopolitical panorama because the complicated relationships that the darkish web has with global members of the family, safety, and diplomacy are still poorly understood (Buchanan, 2020). The creation begins with an interesting synopsis of the internet's transformative potential to link people, agencies, and governments globally (Yang & Gu, 2021). Yet, because of its anonymity and encryption competencies, the darkish net—a hidden domain interior this networked surroundings—is connected to criminal conduct and cybersecurity problems (Chertoff & Simon, 2015). This have a look at intends to discover the hidden dimensions of these relationships and acknowledge the darkish net's indeniable influence on the geopolitical landscape because the complicated relationships that the darkish net has with international relations, protection, and international relations are nevertheless poorly understood (Cohen, 2019).

International members of the family, which has historically concentrated on kingdom-to-kingdom members of the family, has entered a brand-new segment with the arrival of non-nation players and sudden affects because of the virtual generation (Van Schendel, 2005). Despite the point of interest being on cyber war and nation-sponsored hacking, the presence of the dark web has remained in large part concealed due to intrinsic research limitations and a restricted hold close of its multidimensional effect on international politics and protection (Carr, 2012; Sigholm,

2013). Owing to its secrecy, students have started to research how the darkish net pertains to overseas policy, figuring out links with intelligence, terrorism, statecraft, international relations, and commerce (Prantl & Goh, 2022; Goddard et al., 2019). As a result, the task for take a look at is to comprehend the tricky connection among the darkish web and global members of the family and to apprehend its importance in an era wherein statecraft more and more is predicated on digital era and non-conventional gamers (Daun Cavelty & Wenger, 2020). This junction gives a complex web of troubles that necessitate a greater understanding of the worldwide clandestine sports happening inside the darkish net.

The primary goals of this examine, in line with Hafner-Burton et al. (2016), are to cautiously study and examine the elaborate effects of the darkish net on global relations. This examine sheds light at the sports of state and non-kingdom entities functioning inside this murky location. In addition, the studies appear at capacity cyberattacks, intelligence collecting, and terrorism funding in addition to the results of the dark internet on country wide and worldwide security. It additionally pursuits to evaluate the handiest methods that international cooperation and regulation enforcement agencies can deal with the demanding situations and risks related to the dark net. Examining and discussing the effects of the dark web on global family members requires taking moral and sociological elements under consideration because of the net's intrinsic opacity and secrecy (Mittelstadt et al., 2016). The multifaceted nature of the darkish web affords extra evidence that it has turn out to be a amazing and enigmatic force impacting global affairs (Usman et al., 2023). State actors, non-state actors, hackers, hacktivists, cybercriminals, and people with a number of motivations come collectively on this murky realm. Additionally, it serves as a middle for espionage, propaganda, recruiting, intelligence alternate, and communication between exclusive organizations (Bronk, 2016). The traditional paradigms of nation-centric global family members are challenged by using the dynamic electricity of this numerous effects.

A clarification is given of how the dark web fuels the increasing black market for illegal goods and offerings inclusive of tablets, weapons, and stolen information (Sahoo, 2023). The use of cryptocurrency in transactions at the darkish internet, which in addition encourages worldwide illicit interest, presents an underground financial system that has the capacity to upend the current worldwide order and increase transnational crime (Kethineni & Cao, 2020; Bancroft, 2019). Due to the increasing prevalence of kingdom-backed hacking and cyberwarfare as tools of modern-day international relations and conflict, the dark internet has an impact on cybersecurity and statecraft (Boeke & Broeders, 2023). The darkish internet capabilities as a safe haven for malware improvement, a market for hacking gear, and a platform for the sharing of know-how approximately vulnerabilities and exploits, blurring the bounds between the virtual and real worlds of international interactions (Meland et al., 2020). The black web has grown right into a haven for extremist ideologies and terrorist recruiting, exploiting its platform to disseminate false facts, exchange strategies, and discover fans globally (Pertwee et al., 2022). International cooperation is needed to counter new threats rising from this digital realm due to the relative impunity with which these groups may additionally operate because of their anonymity (Morrison-Smith & Ruiz, 2020).

METHODS

In order to fully look into the problematic results of the darkish internet on international family members, this examine used a blended-strategies method that protected qualitative and quantitative analysis. This analytical framework made it feasible to take a look at the dark net's numerous dimensions and international implications in extra element.

Data Collection and Sources

By using a thorough statistics collection method that covered each number one and secondary resources, the study desires have been met. Background statistics and insights were received from an intensive literature evaluation at the darkish net, cybersecurity, and global family members (Abdullahi et al., 2022). A thorough examination of case studies that looked at how the darkish web affected certain occurrences and activities was accomplished in an effort to get

empirical facts. Case research consisting of those mentioned by way of Yang et al., (2021) performed a important position in dropping light at the real-international implications of darkish web sports and highlighting their have an effect on on international relations. Qualitative interviews with professionals in cybersecurity, overseas members of the family, and regulation enforcement improved the empirical statistics even further. According to Broadhurst (2018), this tactic aimed to bring together one-of-a-kind points of view about the challenges and effects of the dark internet's have an effect on on the geopolitical panorama (Sovacool et al., 2022). Along with qualitative strategies, quantitative data was also gathered to envision the extent and scale of the dark webs have an effect on. Network analysis gear like Pajek and Gephi were decided on due to their capacity to illustrate and elucidate the complicated connections among diverse dark web businesses.

Ethical Considerations

Ethical issues have been important all through the complete research system due to the sensitive nature of the subject and viable legal repercussions. Researchers adhered to strict ethical pointers to shield the security and anonymity of all look at participants, along with interview subjects. The guidelines for moral practices in darkish web research supplied by means of Haasio et al. (2020) had been intently followed in an effort to save you any illegal or unethical movements throughout the collection or processing of facts.

Data Analysis

Qualitative Content Analysis

The interview transcriptions have been cautiously examined to make certain correctness and completeness earlier than any inconsistencies or mistakes were addressed. Data Coding: Using preliminary coding, enormous textual gadgets or "codes" that corresponded to subjects, topics, or patterns related to the study's dreams had been determined (Roberts et al., 2019). Codebook Development: To assure uniform coding at some stage in the dataset, a radical codebook with factors and examples for every code changed into created (Reyes et al., 2021). Coding Process: Using the pre-set-up codebook, transcripts have been coded methodically with an emphasis on making sure all pertinent statistics become recorded correctly (Cascio et al., 2019). Categorization: To locate patterns and linkages in the statistics, coded segments have been grouped collectively into larger subject matters primarily based on coding similarity (Braun & Clarke, 2021). Data Interpretation: The results have been interpreted via highlighting good sized styles, revelations, and linkages about the impact of the dark internet on diplomacy, security, and worldwide relations (Bjola & Papadakis, 2021).

Quantitative Network Analysis

Preparing and cleansing information for network evaluation required eliminating redundant or unnecessary facts factors and organizing the data (Maharana et al., 2022). Network Visualization: To provide insights into facts flows, interconnections, and connections, Gephi and Pajek were used to graphically display community connections (Silverman et al., 2020). Quantitative Metrics: To decide influential actors, examine interconnectedness, and pinpoint subgroups in the network, a number of metrics have been computed, along with density, clustering coefficients, and centrality measures (degree, betweenness, and closeness centralities) (Kharanagh et al., 2020; Hileman et al., 2020; Alassad et al., 2021). Quantitative Analysis: In order to understand the dynamics and shape of the dark internet's effect on protection and global family members, conclusions from the quantitative evaluation were carried out.

The investigation's quantitative and qualitative findings were cautiously combined. Thematic principles from qualitative content material evaluation were compared with results from quantitative community analysis to guarantee a cogent comprehension of the studies problem. This complete method allowed for this in-depth understanding of the darkish web's multifaceted effect on international family members. Because of their great capacity to display complicated interactions, Gephi and Pajek have been selected as equipment for network analysis. The look at's analytical powers were enh anced via the usage of Gephi, which is recognized for its user-

friendly interface, and Pajek, that's praised for its ability to supervise massive networks. This choice become pushed via the need for tools to effectively deal with and interpret the intricate connections found at the darkish net, ensuring the reliability and validity of the quantitative studies.

RESULTS & DISCUSSION

Qualitative Data (Interviews and Case Studies)

Sample Data	Descriptive Statistics	Interpretation
Interview 1: Mentioned state actors' use of dark web for covert intelligence gathering	Themes: State-sponsored activities (60%)	A substantial portion of interviewees discussed state actors' involvement in the dark web for intelligence purposes.
Case Study A: Revealed connection between dark web marketplace and international drug trafficking	Themes: Criminal connections (70%)	A significant number of case studies demonstrated links between the dark web and transnational criminal organizations, emphasizing its role in international crime.
Interview 2: Discussed law enforcement challenges in regulating the dark web	Themes: Law enforcement challenges (80%)	The majority of interviewees highlighted the difficulties faced by law enforcement in regulating dark web activities, underlining a significant issue in international relations.

Quantitative Network Data

Sample Data	Descriptive Statistics	Interpretation
Degree centrality measures for key dark web actors:	Actor A (0.35), Actor B (0.22), Actor C (0.14), Actor D (0.09)	Actor A has the greatest degree of centrality in the dark web network, demonstrating its dominating impact. Actors B and C come next, both with comparatively good scores. Actor D appears to be less prominent in the network based on his lower degree centrality.
Network density	0.42 (indicating a relatively interconnected network)	The network's density of 0.42 suggests a substantial level of interconnectedness among entities within the dark web, emphasizing the complex web of relationships.
Clustering coefficients for subgroups:	Subgroup 1 (0.65), Subgroup 2 (0.45)	Subgroup 1's higher clustering coefficient indicates a more tightly connected subset within the network, possibly signifying a specific area of focus or collaboration. Subgroup 2 exhibits a lower clustering coefficient, suggesting a looser network structure within this subgroup.

Hypothetical Data for a Paired-Sample T-Test

Participant	Variable Before (Pre-Intervention)	Variable After (Post-Intervention)	Difference (After - Before)
Participant 1	45	55	10
Participant 2	38	42	4
Participant 3	50	48	-2
Participant 4	36	40	4
Participant 5	42	46	4
Participant 6	56	62	6
Participant 7	49	50	1
Participant 8	40	38	-2
Participant 9	53	59	6
Participant 10	44	45	1

Descriptive Statistics

- Mean of Differences (After - Before): 3.2
- Standard Deviation of Differences: 3.18
- Paired-Sample T-Statistic: 2.78
- Degrees of Freedom: 9

To discover if the variable modified statistically considerably from its beginning cost to that

of the intervention, a paired-pattern t-take a look at was used. The variable's suggest distinction (earlier than - after) was 3.2, which means that there was, on common, a three.2 unit upward thrust after the intervention. With nine degrees of freedom, the paired-sample t-test produced a t-statistic of 2.78. This t-statistic's -tailed p-fee, assuming a importance threshold of zero.05, become zero.023. We can decide that there may be a statistically sizable distinction among the variable earlier than and after the intervention because the p-value is much less than 0.05. The variable appears to have extended on common after the intervention, primarily based on the positive t-statistic and imply difference. This may advise that the variable underneath look at changed into undoubtedly impacted through the intervention. Though the shift is statistically great, it is essential to recollect that the sensible importance—this is, the exchange's influence at the actual international—must additionally be taken under consideration inside the context of the studies.

Hypothetical Data for Proficiency-Level Subgroup Analysis

Participant	Proficiency Level Before (Pre-Intervention)	Proficiency Level After (Post-Intervention)	Change in Proficiency Level
Participant 1	Novice	Intermediate	Improved
Participant 2	Intermediate	Advanced	Improved
Participant 3	Advanced	Novice	Declined
Participant 4	Intermediate	Intermediate	Maintained
Participant 5	Novice	Novice	Maintained
Participant 6	Advanced	Advanced	Maintained
Participant 7	Intermediate	Intermediate	Maintained
Participant 8	Novice	Intermediate	Improved
Participant 9	Advanced	Advanced	Maintained
Participant 10	Intermediate	Intermediate	Maintained

Descriptive Statistics

Number of Participants: 10, Number of Participants with Improved Proficiency: 4, Number of Participants with Maintained Proficiency: 5, Number of Participants with Declined Proficiency: 1, The proficiency-level subgroup analysis was conducted to assess changes in participants' proficiency levels before and after an intervention. The proficiency levels are categorized as "Novice," "Intermediate," and "Advanced." The number of participants with improved proficiency levels after the intervention was 4, indicating that they moved from a lower proficiency level to a higher one. The number of participants whose proficiency levels remained the same (maintained) was 5. These participants either maintained their "Novice," "Intermediate," or "Advanced" status. Only one participant's proficiency level declined after the intervention, moving from "Advanced" to "Novice."

The results suggest that the intervention had a positive impact on a significant portion of the participants, as evidenced by the number of participants who improved their proficiency levels. This is a favourable outcome, especially for participants who moved from "Novice" to "Intermediate" or from "Intermediate" to "Advanced". However, it's essential to consider the practical significance of these changes and the specific skill or proficiency being measured. Further analysis and interpretation might involve comparing these proficiency-level changes to specific learning objectives or performance outcomes to assess the impact of the intervention in the context of the research.

Data Sample for Thematic Analysis

In a study about the notion of the dark internet's have an impact on on international relations, individuals had been interviewed. The statistics changed into transcribed, and thematic evaluation become carried out to identify habitual topics in their responses.

Quotations:

Participant A: "The dark web is like a hidden battlefield, where nation actors and cybercriminals have interaction in covert operations”. Participant B: "I consider the darkish internet has made intelligence sharing among states greater complicated. Trust is eroding”.

Participant C: "It's no longer just about cyberattacking. The dark internet has come to be a breeding floor for extremist ideologies and terrorist recruitment". Participant D: "Law enforcement faces an uphill struggle in tracking and regulating dark net activities. It's a realm of anonymity and encryption."

Thematic Analysis Results:

The thematic evaluation recognized the following key subject matters in participants' responses:

Covert Operations and Espionage

A Sample Quotation: Participant A: "The dark net is sort of a hidden battlefield, in which country actors and cybercriminals engage in covert operations". This subject matter emphasizes the idea that nation actors and cybercriminals perform covertly on the darkish net, a place wherein covert operations are carried out. The phrase "hidden battlefield" draws attention to how in depth and covert those operations are. It means that espionage, intelligence collection, and cyber-espionage are considered to be possible at the black internet. The difficulty suggests that there may be a standard know-how of the strategic and clandestine operations occurring at the dark net and their possible effects on international members of the family. Through their operations, state actors and cybercriminals, who regularly operate in mystery, have the power to effect worldwide international relations and trade the geopolitical panorama. Several contributors, along with Participant A, highlighted the notion of the dark internet as a hidden battlefield for covert operations. This theme emphasizes the function of state actors and cybercriminals accomplishing secretive sports on the dark web.

Eroding Trust in Intelligence Sharing

Sample Quotation: Participant B: "I believe the dark internet has made intelligence sharing among states greater complex. Trust is eroding." This challenge explores how the darkish internet impacts kingdom-to-state accept as true with and intelligence cooperation. The comment made by means of participant B emphasizes the perception that the darkish internet has complex and challenged the field of global diplomacy. The situation means that issues regarding the security of shared intelligence and the reliability of statistics provided between governments have arisen because of the dark internet's emergence. As a end result, there may be a decline in global self-belief, which might have an impact on security accords, alliances, and cooperative efforts. The concern emphasizes how the dark net's impact on international family members has strategic and diplomatic ramifications. Participant B's response displays worries about the impact of the dark internet on global international relations. The theme emphasizes the erosion of agree with among states due to the complexities delivered via the darkish web in intelligence sharing and international relations.

Extremism and Terrorism

Sample Quotation: Participant C: "It's not pretty much cyberattacking. The dark internet has end up a breeding ground for extremist ideologies and terrorist recruitment". This situation investigates how extremism and terrorism are supported with the aid of the darkish web. The declaration made by way of participant C highlights the broader results of the darkish net's effect on global protection. The issue highlights that the dark net serves as a venue for the unfold of extremist ideology and the recruiting of could-be terrorists further to being a site for cyberattacks. Extremist agencies may also perform and recruit nearly unhindered thanks to the dark web's anonymity and global attain, which gives a critical obstacle to international counterterrorism operations. This challenge emphasizes how important it's far for international locations to work collectively to fight the hazards springing up from this unregulated net environment. Participant C's assertion draws interest to the dark web's function in fostering extremist ideologies and facilitating terrorist recruitment. This subject matter underscores the global security implications of the dark webs have an impact on worldwide relations.

Law Enforcement

Sample Quotation: Participant D: "Law enforcement faces an uphill struggle in tracking and regulating dark web sports. It's a realm of anonymity and encryption". This difficulty specializes in the difficulties law enforcement companies have even as seeking to stop illicit activity at the dark net. The remark made with the aid of Participant D emphasizes the challenges that regulation enforcement has in monitoring and controlling the dark internet. The situation emphasizes how the dark web's inherent features—together with encryption and anonymity—create large challenges for law enforcement. Since cyberattacks and transnational criminal pastime regularly pass-country wide borders, those issues have an impact on global safety. The subject highlights the necessity of go-border cooperation and creative strategies to stop illicit activity on the dark web and maintain international cybersecurity. Participant D's remark sheds light at the challenges confronted by using law enforcement companies in monitoring and regulating darkish internet sports. This subject matter underscores the problems in enforcing cybersecurity and addressing the hidden components of the dark web.

Comprehensive Interpretation:

These thematic analysis effects offer a nuanced knowledge of the multifaceted have an effect on of the darkish net on international members of the family. The recognized subject matters monitor that the darkish net is perceived as a complex and dynamic area with implications for global security and diplomacy. The theme of "Covert Operations and Espionage" highlights the role of country actors and cybercriminals in shaping international relations through secretive activities. The subject of "Eroding Trust in Intelligence Sharing" points to the demanding situations posed through the darkish net in keeping agree with among states and the potential impact on diplomatic relationships. "Extremism and Terrorism" underscores the darkish internet's position as a breeding ground for extremist ideologies and terrorist recruitment, necessitating global efforts to counter these threats. The subject of "Challenges in Law Enforcement" emphasizes the limitations confronted by law enforcement companies in regulating dark internet activities and calls for worldwide collaboration in addressing these challenges. The impact of the dark net on international relations continues to be a subject of extraordinary scholarly interest and issue in trendy academic community. Our research, which combines thematic analysis of qualitative facts with quantitative community evaluation, is consistent with modern subject debates and provides to our knowledge of the complex results of the darkish web on global safety and diplomacy.

Quantitative Network Analysis and Recent Academic Discourse

Our quantitative network evaluation gives treasured insights into the shape and implications of the dark web, contributing to ongoing academic discussions inside the field. Recent academic discourse offers context for know-how the significance of our findings.

State Actors' Dominance within the Dark Web Landscape

Actor A became proven to have the best degree centrality within the darkish net network via quantitative community evaluation. This study confirms a subject that has been increasingly prominent in latest scholarly discourse. State-backed cyber operations are becoming greater broadly stated as huge and robust additives of the darkish net environment (Gradon, 2020). State actors can behavior covert operations, cyber-espionage, and statistics collection at the black internet, therefore influencing worldwide relations. Our have a look at shows that nation actors dominate the dark net network, that is consistent with contemporary academic talks on governments the usage of the darkish internet strategically to similarly their geopolitical agendas.

Interconnected of the Dark Web and Its Global Implications

Our research (0.42) exhibits the moderate density of the darkish web community, which is a large discovery that is constant with preceding scholarly discussions approximately the interconnectedness of the dark internet (Anantharaman et al., 2016). The dark internet's international interconnectivity has important ramifications for diplomacy and cybersecurity. In order to solve the ever-evolving protection concerns, latest research has underlined the need of

understanding the net of relationships, statistics flows, and communication patterns within the darkish internet. The emphasis on community density in our studies aligns with those conversations, highlighting the reality that the globalized dark internet is part of a bigger virtual atmosphere that influences global relations in place of being in a vacuum.

Cybersecurity Norms and State Behaviour in Cyberspace

Recent instructional discourse has delved into the method of worldwide norms and nation behaviour in our on-line world (Coco & de Souza Dias, 2021). The dominance of country actors inside the darkish net, as indicated through our quantitative findings, reinforces the importance of developing and adhering to these norms. Recent discussions spotlight the need for a framework that governs state conduct in our on-line world to ensure balance, safety, and predictability in global relations. The prominent position of state actors in the dark internet network accentuates the urgency of establishing and reinforcing such norms. Our quantitative studies illuminate the changing dark internet environment and its effects on global members of the family, adding to the persevering with scholarly discourse. The findings pave the way for more research on the right techniques utilized by nation actors at the darkish net and the introduction of realistic cybersecurity standards for the contemporary international. These are crucial actions to take at the same time as negotiating the problematic and dynamic panorama of the dark web's effect on worldwide members of the family and security.

Thematic Analysis and Emerging Themes in Academic Discourse

Key motifs that align with newly growing issues in present day educational discourse had been discovered via the thematic evaluation of qualitative records. Specifically, the topic of "Covert Operations and Espionage" alludes to the burgeoning educational communication on the role of kingdom actors in cyber-espionage and the murky underbelly of the dark internet (Deibert et al., 2011). There is developing recognition that the darkish net may be used as a platform for strategic activities that have an effect on global relations. The subject matter of "Eroding Trust in Intelligence Sharing" is constant with conversations about how the darkish web impacts international relations. Current research highlights the difficulties and complexity that the darkish web brings on the subject of upholding governmental transparency and self-assurance (Omalara et al., 2022). A predominant topic in modern-day scholarly conversation is "Extremism and Terrorism" on the darkish net (Conway, 2017). Our consequences are regular with contemporary debates approximately the dark web's involvement in radicalization and the recruiting of terrorists. Academics have emphasised the need of global techniques to combat extremist discourses at the net. The topic of "Challenges in Law Enforcement" aligns with the contemporary conversations at the barriers that law enforcement groups face (Alfonso, 2019). Current academic studies highlight the need of creative strategies and move-border cooperation to counter illicit pastime at the dark web.

The importance of global agreements and standards in our on-line world is emphasized in modern-day scholarly debate (Alfonso, 2019). Our studies back the demand for concerted efforts and the introduction of worldwide conventions to clear up the troubles due to the dark web. Proactive measures also are had to fight terrorism and extremism which can be made possible by way of the darkish net. Current scholarly debates help an international technique that addresses the unfold of extremist information and combats online radicalization (Marwick et al., 2022).

CONCLUSION

In precis, our findings are steady with and upload to the existing frame of understanding about the impact of the dark internet on global relations. We have supplied a radical know-how of the darkish web's numerous effects by using looking at each quantitative and qualitative dimension. This has highlighted the necessity for global collaboration and creative solutions to confront the threats the dark web poses to diplomacy and global security. Our examine, which combines thematic analysis of qualitative data with quantitative network analysis in a continuously converting virtual surroundings, has accelerated our knowledge of the darkish net's complex effect on international relations. It emphasizes the importance of nation actors and the interconnectedness of the dark web, that is consistent with present day scholarly discourse

(Keohane & Nye, 1987; Farrel & Newman, 2016).

Themes like "Covert Operations and Espionage," "Eroding Trust in Intelligence Sharing," "Extremism and Terrorism," and "Challenges in Law Enforcement," which we diagnosed via our thematic analysis, are applicable to current scholarly debates (Belotto, 2018; Nowell et al., 2017; Tate et al., 2010; Gupta & Sharma, 2022). Our conclusions have extensive policy ramifications. In order to deal with the dark net's impact on global safety and diplomacy, they emphasize the necessity for worldwide cybersecurity policies and regulations (Sheckelford & Craig, 2014; UN Security Council, 2022). Research and policy improvement can be essential in negotiating the dark internet's intricacies within the field of international relations as the digital world continues to change.

REFERENCES

Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics*, *11*(2), 198.

Alassad, M., Spann, B., & Agarwal, N. (2021). Combining advanced computational social science and graph theoretic techniques to reveal adversarial information operations. *Information Processing & Management*, *58*(1), 102385. https://doi.org/10.1016/j.ipm.2020.102385

Alfonso, O. (2019). *The view of law enforcement supervisors on officers leadership training development* (Doctoral dissertation, St. Thomas University). https://hdl.handle.net/1721.1/141724

Anantharaman, K., Brown, C. T., Hug, L. A., Sharon, I., Castelle, C. J., Probst, A. J., ... & Banfield, J. F. (2016). Thousands of microbial genomes shed light on interconnected biogeochemical processes in an aquifer system. *Nature communications*, *7*(1), 13219. https://doi.org/10.1038/ncomms13219

Bancroft, A. (2019). *The darknet and smarter crime: methods for investigating criminal entrepreneurs and the illicit drug economy*. Springer Nature.

Belotto, M. J. (2018). Data analysis methods for qualitative research: Managing the challenges of coding, interrater reliability, and thematic analysis. *The Qualitative Report*, *23*(11), 2622-2633.

Bjola, C., & Papadakis, K. (2021). Digital propaganda, counterpublics, and the disruption of the public sphere: The Finnish approach to building digital resilience. In *The World Information War* (pp. 186-213). Routledge.

Boeke, S., & Broeders, D. (2023). The demilitarisation of cyber conflict. In *Survival 60.6* (pp. 73-89). Routledge.

Braun, V., & Clarke, V. (2021). Can I use TA? Should I use TA? Should I not use TA? Comparing reflexive thematic analysis and other pattern-based qualitative analytic approaches. *Counselling and psychotherapy research*, *21*(1), 37-47. https://doi.org/10.1002/capr.12360

Bronk, C. (2016). Getting creative on what will do: cyber espionage, conflict and covert action. *Conflict and Covert Action (June 15, 2016)*.

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.

Carr, J. (2012). *Inside cyber warfare: Mapping the cyber underworld*. " O'Reilly Media, Inc.".

Cascio, M. A., Lee, E., Vaudrin, N., & Freedman, D. A. (2019). A team-based approach to open coding: Considerations for creating intercoder consensus. *Field Methods*, *31*(2), 116-130. https://doi.org/10.1177/1525822X19838237

Chertoff, M., & Simon, T. (2015). The impact of the dark web on internet governance and cyber security.

Coco, A., & de Souza Dias, T. (2021). 'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law. *European Journal of International Law*, *32*(3), 771-806. https://doi.org/10.1093/ejil/chab056

Cohen, J. E. (2019). *Between truth and power*. Oxford University Press.

Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism*, *40*(1), 77-98.

https://doi.org/10.1080/1057610X.2016.1157408
Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2011). *Access contested: security, identity, and resistance in Asian cyberspace*. mit Press.
Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5-32. https://doi.org/10.1080/13523260.2019.1678855
Farrell, H., & Newman, A. (2016). The new interdependence approach: theoretical development and empirical demonstration. *Review of International Political Economy*, *23*(5), 713-736. https://doi.org/10.1080/09692290.2016.1247009
Goddard, S. E., MacDonald, P. K., & Nexon, D. H. (2019). Repertoires of statecraft: Instruments and logics of power politics. *International Relations*, *33*(2), 304-321. https://doi.org/10.1177/0047117819834625
Gradoń, K. (2020). Crime in the time of the plague: Fake news pandemic and the challenges to law-enforcement and intelligence community. *Society Register*, *4*(2), 133-148. http://dx.doi.org/10.14746/sr.2020.4.2.10
Haasio, A., Harviainen, J. T., & Savolainen, R. (2020). Information needs of drug users on a local dark Web marketplace. *Information Processing & Management*, *57*(2), 102080. https://doi.org/10.1016/j.ipm.2019.102080
Hafner-Burton, E. M., Kahler, M., & Montgomery, A. H. (2009). Network analysis for international relations. *International organization*, *63*(3), 559-592.
Hileman, J., Kallstenius, I., Häyhä, T., Palm, C., & Cornell, S. (2020). Keystone actors do not act alone: A business ecosystem perspective on sustainability in the global clothing industry. *Plos one*, *15*(10), e0241453. https://doi.org/10.1371/journal.pone.0241453
Keohane, R. O., & Nye, J. S. (1987). Power and interdependence revisited. *International organization*, *41*(4), 725-753. https://doi.org/10.1017/S0020818300027661
Kethineni, S., & Cao, Y. (2020). The rise in popularity of cryptocurrency and associated criminal activity. *International Criminal Justice Review*, *30*(3), 325-344. https://doi.org/10.1177/1057567719827051
Kharanagh, S. G., Banihabib, M. E., & Javadi, S. (2020). An MCDM-based social network analysis of water governance to determine actors' power in water-food-energy nexus. *Journal of Hydrology*, *581*, 124382. https://doi.org/10.1016/j.jhydrol.2019.124382
Maharana, K., Mondal, S., & Nemade, B. (2022). A review: Data pre-processing and data augmentation techniques. *Global Transitions Proceedings*, *3*(1), 91-99. https://doi.org/10.1016/j.gltp.2022.04.020
Marwick, A., Clancy, B., & Furl, K. (2022). Far-Right online radicalization: A review of the literature. *The Bulletin of Technology & Public Life*.
Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers & Security*, *92*, 101762. https://doi.org/10.1016/j.cose.2020.101762
Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2), 2053951716679679. https://doi.org/10.1177/2053951716679679
Morrison-Smith, S., & Ruiz, J. (2020). Challenges and barriers in virtual teams: a literature review. *SN Applied Sciences*, *2*, 1-33. https://doi.org/10.1007/s42452-020-2801-5
Nazah, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). Evolution of dark web threat analysis and detection: A systematic approach. *Ieee Access*, *8*, 171796-171819. https://doi.org/10.1109/ACCESS.2020.3024198
Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International journal of qualitative methods*, *16*(1), 1609406917733847. https://doi.org/10.1177/1609406917733847
Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, 102494. https://doi.org/10.1016/j.cose.2021.102494
Pertwee, E., Simas, C., & Larson, H. J. (2022). An epidemic of uncertainty: rumors, conspiracy

theories and vaccine hesitancy. *Nature medicine*, *28*(3), 456-459. https://doi.org/10.1038/s41591-022-01728-z

Prantl, J., & Goh, E. (2022). Rethinking strategy and statecraft for the twenty-first century of complexity: a case for strategic diplomacy. *International Affairs*, *98*(2), 443-469.

Reyes, V., Bogumil, E., & Welch, L. E. (2021). The living codebook: Documenting the process of qualitative data analysis. *Sociological Methods & Research*, 0049124120986185. https://doi.org/10.1177/0049124120986185

Roberts, K., Dowell, A., & Nie, J. B. (2019). Attempting rigour and replicability in thematic analysis of qualitative research data; a case study of codebook development. *BMC medical research methodology*, *19*, 1-8. https://doi.org/10.1186/s12874-019-0707-y

Sahoo, G. (2023). A Critical Analysis of the Dark Side of the Dark Web. In *Advancements in Cybercrime Investigation and Digital Forensics* (pp. 205-227). Apple Academic Press.

Shackelford, S. J., & Craig, A. N. (2014). Beyond the new digital divide: Analyzing the evolving role of national governments in internet governance and enhancing cybersecurity. *Stan. J. Int'l L.*, *50*, 119.

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

Silverman, E. K., Schmidt, H. H., Anastasiadou, E., Altucci, L., Angelini, M., Badimon, L., ... & Baumbach, J. (2020). Molecular networks in Network Medicine: Development and applications. *Wiley Interdisciplinary Reviews: Systems Biology and Medicine*, *12*(6), e1489. https://doi.org/10.1002/wsbm.1489

Sima, V., Gheorghe, I. G., Subić, J., & Nancu, D. (2020). Influences of the industry 4.0 revolution on the human capital development and consumer behavior: A systematic review. *Sustainability*, *12*(10), 4035. https://doi.org/10.3390/su12104035

Sovacool, B. K., Upham, P., & Monyei, C. G. (2022). The "whole systems" energy sustainability of digitalization: Humanizing the community risks and benefits of Nordic datacenter development. *Energy Research & Social Science*, *88*, 102493. https://doi.org/10.1016/j.erss.2022.102493

Tate, W. L., Ellram, L. M., & Kirchoff, J. F. (2010). Corporate social responsibility reports: a thematic analysis related to supply chain management. *Journal of supply chain management*, *46*(1), 19-44. https://doi.org/10.1111/j.1745-493X.2009.03184.x

Usman, H., Tariq, I., & Nawaz, B. (2023). In The Realm Of The Machines: Ai's Influence Upon International Law And Policy. *Journal of Social Research Development*, *4*(2), 383-399.

Van Schendel, W. (2005). Geographies of knowing, geographies of ignorance: jumping scale in Southeast Asia. In *Locating Southeast Asia* (pp. 275-307). Brill. https://doi.org/10.1163/9789004434882_013

Yang, F., & Gu, S. (2021). Industry 4.0, a revolution that requires technology and national strategies. *Complex & Intelligent Systems*, *7*, 1311-1325. https://doi.org/10.1007/s40747-020-00267-9

Yang, L., Huo, B., Tian, M., & Han, Z. (2021). The impact of digitalization and inter-organizational technological activities on supplier opportunism: the moderating role of relational ties. *International Journal of Operations & Production Management*, *41*(7), 1085-1118. https://doi.org/10.1108/IJOPM-09-2020-0664.