International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

Digital Sentinels: A Quantitative Content Analysis of Unintentional Information Exposure among Defence Personnel and Their Families on Social Media

Arya A
Independent Researcher, Kerala, India

Abstract- Social media platforms enable defence personnel and their families to share their everyday routines, travel, family moments and, personal milestones with a large audience. But information that appears routine or harmless in isolation may reveal sensitive contextual details when viewed collectively. This study examines potential information exposure in publicly available social media content associated with defence personnel and their families. A quantitative content-analysis method was applied to 100 publicly available content items consisting of vlogs, short-form videos, and posts from Facebook and Instagram collected for the study. Each content was evaluated using nine parameters: Location Information, Travel and Movement Details, Workplace Information, Personal Identification, Vehicle Information, Family Information, Equipment Information, Routine and Activity Patterns, and Textual Information Disclosure. Each parameter was assigned as 0 (not present) or 1 (present), producing an exposure score from 0 to 9. For this analysis, scores of 0–2 were classified as Low Risk, 3–5 as Medium Risk and 6–9 as High Risk. The analysis found that Textual Information Disclosure was present in 99% of the content, followed by Location Information (80%), Personal Identification (73%) and Routine and Activity Patterns (71%). The analysis also showed that 4% of content was classified as Low Risk, 63% as Medium Risk and 33% as High Risk. These results indicate that unintentional sensitive information leakage is a major concern and the need for greater OPSEC awareness among defence personnel and their families to promote safer social media sharing practices. Keywords: OSINT, Digital Footprint Aggregation, Operational Security (OPSEC), Social media privacy, defence personnel, content analysis, risk classification.

Keywords- ***OSINT, Digital Footprint Aggregation, Operational Security (OPSEC), Social media privacy, defence personnel, content analysis, risk classification.***

1. INTRODUCTION

Social media has become an important medium to share personal experiences, photographs, videos, family activities, professional events and day-to-day activities with a large audience. Platforms such as YouTube, Instagram and Facebook provide continuous sharing of content, which provides economic benefits. But, the accumulation of everyday details, when viewed collectively can lead to unintended information exposure.

These risks become evident when social media content is examined through an intelligence analysis lens. Open-Source Intelligence (OSINT) involves the systematic collection and analysis of publicly available information to identify meaningful patterns. A photograph or video containing location tag, timestamp, organizational caption, vehicles, uniforms, workplaces, routines, movements, family member identification may appear harmless, but when these details are combined can construct a detailed profile.

Operation Security (OPSEC) provides the framework for protecting the sensitive data. The core process of OPSEC identifying what information requires protection and implementing practices to prevent its disclosure to unintended observers. Information leakage on social media typically results not from intentional disclosure, but from normal, well-intentioned behaviors: user sharing personal moments, documenting life experiences, or participating in online communities. While using social media, defence-associated families may face particular challenges in maintaining privacy. Family members routinely share content depicting daily life, accommodation details, vehicles, uniform, identification badges, routine patterns and travel experiences. Although, these posts reflect normal family activities, they accumulate information that, from an OSINT perspective, creates exploitable intelligence. The fundamental issue is whether the collective body of publicly available information creates comprehensive exposure of sensitive details.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

In this study, a structured content-analysis approach was used to examine 100 publicly available social media content items related defence-associated individuals. Each item was evaluated against 9 core security parameters: Location Information, Travel and Movement Details, Workplace Information, Personal Identification, Vehicle Information, Family Information, Equipment Information, Routine and Activity Patterns, and Textual Information Disclosure. A risk classification framework categorized each item as low-risk, medium-risk and high risk.

The research objectives are:

• To identify different forms of potentially sensitive information exposed through publicly available social media content.

• To measure the frequency of each identified information-exposure parameter.

• To classify analyzed content into Low, Medium and, High potential exposure categories.

• To identify the most frequently observed forms of information exposure.

• To provide a practical coding framework for social media privacy and security awareness.

This study examines unintentional information exposure in publicly available content associated with defence families by analyzing multiple parameters and classifying into low, medium and high risk. The study also investigates what type of information is commonly exposed and finding aims to enhance awareness among defence personnel and their families about the potential risk associated with sharing information on social media.

2. RELATED WORK

Social media is now widely used by military personnel and their families for communication, sharing experiences and staying connected with others. While these platforms offer benefits like monetization but unintentionally sometimes reveal sensitive information. Prior studies have examined this issue from different angles, including social media privacy, military operational security, OSINT and the analysis of publicly available content.

Research on privacy in social media suggests that users do not fully recognize that publicly shared content may contain sensitive information. [1] Bioglio and Pensa developed a coding framework to distinguish between sensitive and non-sensitive content, highlighting that publicly accessible posts may contain privacy concerns. [2] Wood and Gray et al. carried out a study on how military families uses social media and stay connected during deployment and separation. The review highlighted that social media helps families to stay connected and also concern related to operational security. However, the study mainly focused on family communication rather than examining the information that could be revealed through publicly available social media content.

Second, military-security research demonstrates that seemingly ordinary social media information can create operational-security and personal-security risks.[3] Dressler and Bronk et al. examined publicly available information from U.S. military members and used content analysis and machine-learning methods to assess vulnerability. The researchers used content analysis and machine techniques to assess the information available online and classified individuals according to their level of vulnerability. Their findings highlighted the importance of cumulative data collected which cause privacy issues. [4] Lee and Park et al. subsequently demonstrated the use of OSINT techniques for searching social media sources for military information, names and personal identification information. They collected data from platforms such as Facebook and Instagram using OSINT collection technique and analysis of information using OSINT techniques rather than evaluating individual social media content.

Recent research has also examined privacy risks in social media content. [5] Meng and Zhang et al. studied the privacy risks that may arises from videos shared on social media. The study found that videos can reveal details such as location, personal characteristics and daily activities. The study mainly looked at user‟s opinions about AI inference rather than analyzing the information. [6] Tay, Subbaraj and Kandappu developed a deep-learning model designed to identify sensitive information in images. The model tries to identify where the sensitive information is located so that area can be blurred before sharing. [7] Vit, Aronson et al. examined Instagram images and applied deep-learning methods to identify six types of confidential objects. The findings showed that sensitive information can appear even in the background of an ordinary image. This paper examines about different types of information exposure and classifies the content into low, medium or high risk.

Overall, the existing research shows that social media is useful for communication, but sometimes create privacy and risks, especially in military-related contents. Earlier studies mainly looked at military OPSEC, OSINT or particular types of sensitive information. There is comparatively less research that examines publicly available social media content related to defence personnel and their families and considers different types of information exposure together. To address this gap, the present study

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

focused on an analysis of 100 publicly available social media contents using 9 predefined parameters associated with defence families. This study also identifies which types of information are most leaked and assess the overall level of risk as low, medium and high risk.

3. RESEARCH QUESTIONS

1. What types of sensitive information are shared in publicly available social media content associated with defence personnel and their families, and how frequently do they occur?

2. Which information-exposure parameters occur most frequently?

3. What privacy and OPSEC- related concerns can be identified from these patterns?

4. METHODOLOGY

4.1 Research Design

A quantitative descriptive content-analysis approach was used to evaluate the publicly available social media content and each post was considered as one unit of analysis. The study was designed to identify what kind of information are shared rather than determining whether any post has resulted in actual security incident. Only publicly available content was considered for the study and, no private accounts or non-public information was accessed.

4.2 Dataset

The dataset contains only 100 publicly available social media content, selected using hash-tags(#army, #quarter, #navy, #airforce, #bsf, #cisf, #crpf, #itbp) were analyzed. The spreadsheet included content type, postdate, channel name, source URL and nine coding parameters. The analyzed content comprised vlogs, short-form videos and posts from publicly accessible social media sources. Source URLs were kept in the research spreadsheet for reference but not included in the paper.

4.3 Content Distribution

Content Type	Frequency	Percentage
Vlogs	55	55.0%
Shorts-Form Videos(Shorts/ Reels)	33	33.0%
Facebook Posts	7	7.0%
Instagram Posts	5	5.0%

4.4 Coding Framework

Parameter	Operational definition
Location Information	Specific or identifiable locations, landmarks, signboards, geotags or surroundings that may reveal where the content was recorded.
Travel and Movement Details	Travel routes, destinations, excise, departure/arrival information, movement plans, posting movements or travel-related details.
Workplace Information	Information revealing a workplace, station, unit/formation, office, camp or identifiable duty environment.
Personal Identification	Names, identification cards, badges, rank/name plates, service numbers or other information that can identify an individual.
Vehicle Information	Vehicle registration numbers, markings, identifiable service vehicles or other vehicle-related information.
Family Information	Information about family members, relationships, children, family locations,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

	schools, workplaces or other identifiable family details.
Equipment Information	Visible military/service equipment, communication devices, technical equipment, documents or other potentially sensitive equipment.
Routine & Activity Patterns	Regular timings, duty schedules, recurring activities, predictable movements or patterns that could indicate when or where activities occur.
Textual Information Disclosure	Potentially sensitive information disclosed through captions, descriptions, hash-tags or text appearing within the content.

4.5 Coding Procedure

Each parameter was assigned a value of 0 indicated not present and 1 indicated present. A content item could receive a value of 1 for more than one parameter. Therefore, parameter frequencies represent the number of content items containing each type of exposure and are not mutually exclusive.

4.6 Risk Classification

An exposure score was calculated by summing the nine binary parameter values for each content item. The theoretical score range was 0–9. For this study, a transparent three-level screening rule was applied: 0–2 = Low Risk, 3–5 = Medium Risk and 6–9 = High Risk. This classification represents the number of observed exposure categories and should not be interpreted as a validated probability of a real-world security incident.

4.7 Data Analysis

Descriptive statistics were used. Frequencies and percentages were calculated for each parameter, and the distribution of Low, Medium and High Risk content was determined. Because the sample size was 100, a frequency of x corresponds to x%. The mean exposure score was 5.06, the median was 5, and observed scores ranged from 2 to 8.

5. RESULTS

5.1 Parameter-wise Frequency

Parameter	**Frequency (n=100)**	**Percentage**
Textual Information Disclosure	99	99.0%
Location Information	80	80.0%
Personal Identification	73	73.0%
Routine & Activity Patterns	71	71.0%
Family Information	46	46.0%
Workplace Information	45	45.0%
Equipment Information	32	32.0%
Vehicle Information	30	30.0%
Travel & Movement Details	30	30.0%

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

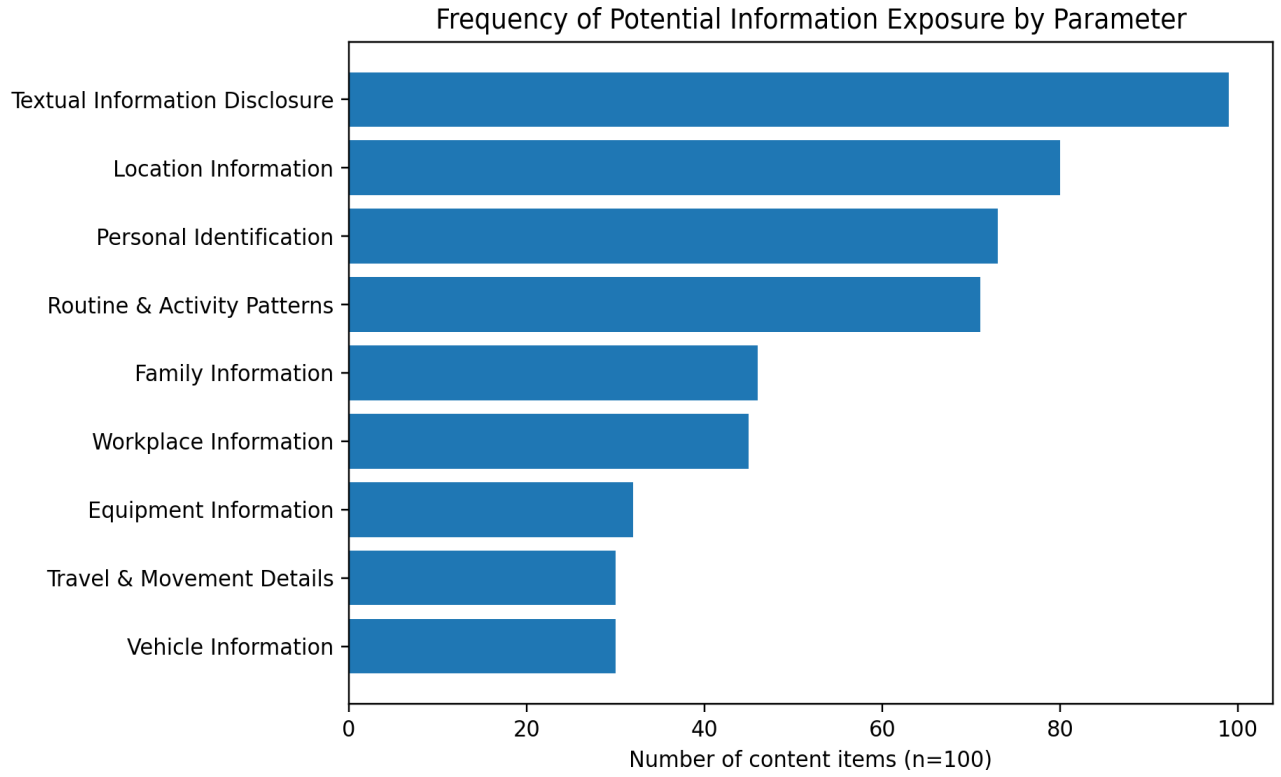

Fig. 1 Frequency of observed potential information-exposure parameters.

5.2 Risk Classification

Risk Category	Frequency (n=100)	Percentage
Low Risk	4	4.0%
Medium Risk	63	63.0%
High Risk	33	33.0%

The analysis classified 4 content items (4%) as Low Risk, 63 items (63%) as Medium Risk and 33 items (33%) as High Risk. Thus, 96% of the analysed items fell into the Medium or High Risk screening categories under the nine-parameter scoring rule.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

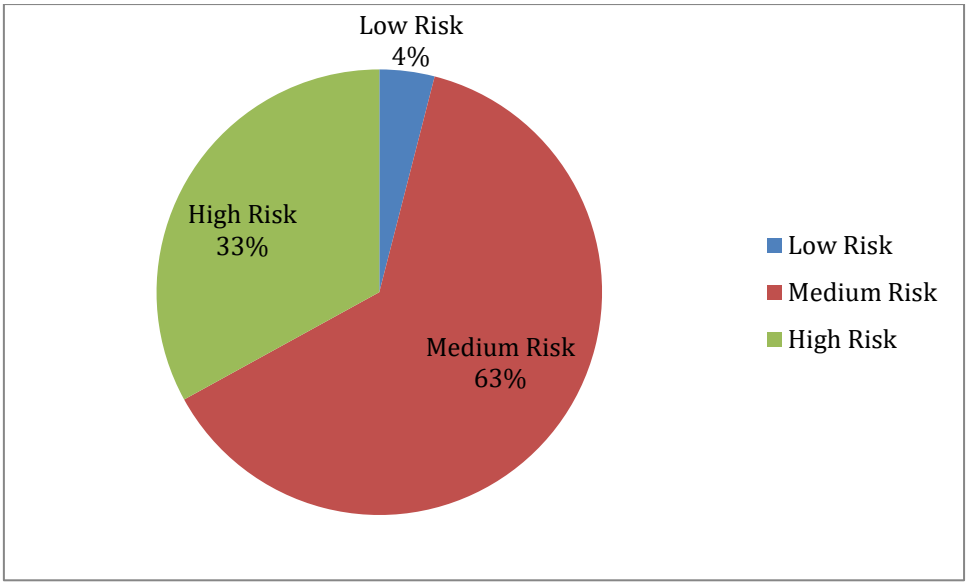

Fig.2 Distribution of content by potential information-exposure risk category.

5.3 Exposure Score Distribution

Exposure Score	Frequency	Percentage
2	4	4.0%
3	9	9.0%
4	24	24.0%
5	30	30.0%
6	12	12.0%
7	15	15.0%
8	6	6.0%

The observed exposure scores ranged from 2 to 8. The most common score was 5, recorded for 30% of the content, followed by a score of 4 for 24%. Scores of 2, 3, 6, 7 and 8 were observed in 4%, 9%, 12% and 6% of the dataset, respectively.

6. DISCUSSION

The findings demonstrate that information can be exposed on social media even when there is no intention to share sensitive details. The exposure doesn't come from a single post but when multiple posts such as high occurrence of textual information (99%), location information (80%) and personal identification (73%) are viewed together can reveal sensitive information. The result indicates that 33% of the analyzed content was classified as high risk further highlights the need for greater awareness of social media use. These findings also suggest that individual awareness alone may not be sufficient. While users should be encouraged to review the information what they share, institutional awareness programs should be organized. The study also supports the value of multimodal analysis in identifying risk exposure. Potential exposure can be visible in images or video, audible or contextual in the content, and explicit in captions or hash-tags. Future automated systems could combine OCR, object detection, speech-to-text and natural-language processing to identify these categories at large scale.

7. IMPLICATIONS

- Social media awareness programs should emphasize how isolated details become threats combined.
- Users should review captions, hash-tags, visible backgrounds, identification items, travel details and routine information before posting.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

- Family education programs for defence-associated families should use simple parameter framework with real social media examples.
- Future systems can automate using AI, OCR, object detection and speech analysis, geo-location to evaluate risk.

8. COUNTERMEASURES

- Location services and geo-tagging should be disabled before posting.
- Set defence personnel and their family accounts to private, and periodically review who has accessed.
- Review previously shared contents and delete post that disclose sensitive information.
- Families avoid accepting requests from unknown persons or sharing information.
- Conduct regular awareness program to understand risk of information shared publicly online.
- Remove metadata from photographs and videos before uploading them to YouTube.
- Promote safe-sharing practices and remove service related data such as vehicle numbers, identity cards, name and, uniforms.

9. LIMITATIONS

- The sample size was limited to 100 content items and therefore may not represent all YouTube content associated with defence families.
- The dataset was not evenly distributed across platforms; Vlogs and Shorts formed the majority of the sample.
- The coding framework uses binary presence/absence coding and does not assign different weights to different types of exposure.
- Risk categories are a study-specific screening model and have not been externally validated against actual security incidents.
- The study identifies potential exposure but does not establish that any analysed content resulted in an actual security compromise.

10. CONCLUSION

Social media provides defence personnel and their families to communicate and share everyday experiences to outside world. But careless sharing can also expose information that may cause privacy and OPSEC implications. The study highlights the importance of what contents to be shared and double check the contents before posting. Sensitive information such as locations, uniforms, badges, workplaces and other information shouldn't be revealed. Promoting OPSEC awareness and safe social media practices can help individuals make safer decisions about what they share publicly.

11. REFERENCES

[1] L. Bioglio and R. G. Pensa, "Analysis and Classification of Privacy-Sensitive Content in Social Media Posts," in EPJ Data Science, vol.11, no.12, 2022.
[2] A. Wood, L. Gray, J.B. Angermann, P. Gibson, M.Fossey and L. G. McBard, "Social media and Internet-based communication in military families during separation: An International Scoping Review," in New Media & Society, 1802-1823, 2023.
[3] J. C. Dressler, C. Bronk, and D. S. Wallach, "Exploiting military OpSec through open-source vulnerabilities," in Proc. IEEE Military Communications Conference (MILCOM), pp. 450–458, 2015.
[4] Y. J. Lee, S. J. Park, and W. H. Park, "Military Information Leak Response Technology through OSINT Information Analysis Using SNSes," in Security and Communication Networks, 9962029, 2022.
[5] W. Meng and X. Zhang,"Study of the Leakage of „Top Secret" Documents in the United States of America," in International Journal of Advances in Engineering and Management, vol. 5, no. 12, 2023.
[6] C. Tay, V. Subbaraju, and T. Kandappu, "PrivObfNet: A Weakly Supervised Semantic Segmentation Model for Data Protection," in CVF Winter Conference on Applications of Computer Vision, 2410-2420, 2024.
[7] A. P. Vit, Y.Aronson, R. Fraidenberg, and R. Puzis, "Visual Censorship: A Deep Learning-Based Approach to Preventing the Leakage of Confidential Content in Images," in Applied Science, vol. 17, no.17, 2024