From Social Media Signals to Aerial Response: A Secure Drone Framework for Rapid Violent Crime Monitoring

Suhail Nassar
Faculty of Business and IT
University of Ontario Institute of Technology
Oshawa, Ontario
suhail.nassar@ontariotechu.net

Jeffrey Wong
Faculty of Applied Science and Engineering
University of Toronto
Toronto, Ontario
jeffreyy.wong@mail.utoronto.ca

Khalil El-Khatib
Faculty of Business and IT
University of Ontario Institute of Technology
Oshawa, Ontario
Khalil.El-Khatib@ontariotechu.ca

***Abstract*—Law enforcement agencies around the globe, facing budget cuts and increase in crime rates challenges, are turning to technologies to solve some of these challenges. Drones are viewed as a valuable complementary tool for traditional law enforcement agencies. They can be deployed for rapid responses to indications of criminal incidents, thereby freeing personnel for other duties. This paper presents a drone surveillance system for law enforcement agencies that quickly retrieves indications of violent crimes from social media posts and dispatches drones to reach areas highlighted in these posts or to conduct regular patrols near crime hotspots. The paper also includes a cybersecurity analysis of all system components and proposes mitigations to prevent exploitation by bad actors.**

Keywords—drones, cybersecurity, violence detection, machine learning, social media

I. Introduction

In Canada, violent crime has increased in recent years, particularly since the COVID-19 pandemic, and has become a major challenge for law enforcement agencies across the country. The crime severity index in Canada shows that violent crime has been increasing or remaining stable, even as other types of crimes decline [1]. However, because these relatively stable crime rates are adjusted for population, the actual volume of violent crimes has continued to increase [2].

In parallel, the number of law enforcement officers per capita in the country has also been steadily decreasing, with police strength declining by 2% in 2024 [3]. This trend may eventually lead to a situation in which there are insufficient law enforcement officers (LEOs) to effectively prevent or detect crime.

Surveillance technologies represent a significant step toward enhancing law enforcement through modern technology. Surveillance cameras are becoming increasingly affordable and easy to install, and many law enforcement agencies have the authority to access Closed Circuit Television (CCTV) footage from both public and private cameras. Some agencies, including those in Canada, have established surveillance centers that provide round-the-clock monitoring of CCTV cameras using both human and algorithmic methods to better support law enforcement operations [4]. However, surveillance cameras are not installed ubiquitously, nor do they usually provide a complete view of their surroundings, as they often have blind spots and are fixed in place. In addition, these cameras can be easily disabled through technological or physical means.

Drones offer a convenient way to address many of the limitations of surveillance cameras. They can move from one location to another, and do not require pre-installation. This allows them to reach areas where fixed surveillance cameras are unavailable and to monitor criminal activity across a much wider area. Moreover, disabling drones can be more difficult than disabling traditional surveillance cameras, if proper security measures are in place. Drones can also be dispatched almost instantaneously and can reach target areas more quickly than ground-based methods, such as vehicles, because they do not need to follow pre-built paths like roads. They can travel in straight lines, bypass obstacles by flying over or around them, and are not affected by traffic conditions.

In this paper, we present an automated drone-based surveillance system to support crime detection and prevention. The system uses social media feeds as trigger of crimes activity in an area [5]. Today, most people maintain at least one social media account, with easy access available through their smartphones. Social media platforms are commonly used to highlight and circulate information about noteworthy local incidents. For law enforcement agencies, these posts can serve as a valuable source of clues about criminal activities. Analyzing thousands of social media posts in real time using various AI models and identifying legitimate reports of crimes is well within the capabilities of current technology. Integrating drone surveillance with social media analysis can therefore lead to innovative solutions in modern policing.

The rest of the paper is organized as follows: Section II discusses related work. Section III presents the drone system and its architecture. Section IV presents a cybersecurity analysis of the system presented in Section III. Section V lists possible improvements and additions to the system.

II. Related Work

In [6], the authors employed the YOLO (You Only Look Once) algorithm for anomaly detection in human behaviour analysis. The UCF-Crime video dataset [7] was used for training and evaluation. For feature extraction, a hybrid LSTM–CNN

979-8-3195-0167-7/26/$31.00 ©2026 IEEE

(Long Short-Term Memory and Convolutional Neural Network) architecture was implemented. The LSTM component was utilized to capture temporal dependencies in the video sequences, while the CNN component was used to extract spatial features. The extracted features were subsequently passed to a modified YOLO model for real-time object detection. The system was further implemented to generate audible alerts through a sound system whenever a crime was detected in the monitored area. Experimental results demonstrated an accuracy of 91%. The authors noted that the accuracy could potentially be improved by employing a feature extraction approach that preserves a greater amount of relevant information, thereby reducing the model's false positive rate.

In [8], the authors employed a Region Proposal Network (RPN) in conjunction with a Faster Region-Based Convolutional Neural Network (Faster R-CNN) for object detection. Their study focused on surveillance cameras in Colombia operated by Command and Control Citizen Security Centres (C2IS), which are part of the law enforcement infrastructure. These cameras can pan, tilt, and zoom to capture different events; therefore, the authors aimed to develop a model capable of detecting criminal activity in live video while remaining robust to camera motion. The dataset used in the study was constructed by the authors using C2IS surveillance data and is not publicly available. AlexNet, a convolutional neural network architecture, was used within the RPN stage, while Faster R-CNN was applied for object detection and classification of different types of crime. Using this approach, the authors reported an accuracy of 71%. The results suggest that accuracy could potentially be improved by experimenting with alternative object detection algorithms and RPN architectures. However, such improvements would likely involve trade-offs among training time, computational requirements, and overall system performance. Given the authors' objective of developing a low-cost implementation with reasonable performance, the reported accuracy was considered acceptable.

Gandapur [9] proposed a model that combines the VGG-16 convolutional neural network architecture with Bidirectional Gated Recurrent Units (BiGRUs). The CAVIAR dataset [10] was used for training and evaluation. In this approach, the video data are first pre-processed into blocks of frames, which are subsequently down sampled. These processed frames are then passed to the VGG-16 network, which consists of multiple convolutional, pooling, and fully connected layers for feature extraction. The output of the final VGG-16 layer is then provided to the BiGRU module, which is well suited for modelling temporal dependencies, for the final classification stage. The proposed model achieved a detection and classification accuracy of approximately 99%. The authors also evaluated an alternative configuration in which the BiGRUs were replaced with Simple Recurrent Units (SRUs). This modification reduced the accuracy to approximately 98% but also lowered the computational cost of the model. The extent to which the choice of dataset influenced the reported accuracy remains unclear. Further evaluation of the model on additional datasets would provide greater insight into its generalizability and overall effectiveness.

In [11], the authors proposed a model that combines the VGG-16 architecture with Long Short-Term Memory (LSTM) layers. Because VGG-16 is a deep and computationally intensive convolutional neural network, transfer learning was employed to reduce training time by utilizing a pre-trained VGG-16 model. Two datasets were used for training and evaluation: a mini-drone video (MDV) dataset [12] and the University of Minnesota (UMN) dataset [13]. The model achieved an accuracy of approximately 72% when trained on the MDV dataset and greater than 99% accuracy on the UMN dataset. The authors suggested that this discrepancy in performance may be attributed to the relatively small number of videos in the MDV dataset and the lower complexity of the UMN dataset. The study also noted that supervised learning approaches may have limitations when applied to anomaly detection tasks. Nevertheless, the use of transfer learning was shown to be effective in reducing the time and computational resources required for training deep learning models.

In [14] the authors proposed a framework for utilizing social media data to task unmanned aerial vehicles (UAVs) in search and rescue operations. The framework monitors posts containing specific hashtags associated with events such as natural disasters and preprocesses them using Natural Language Processing (NLP) techniques. Semantic similarity between the content of a post and disaster-related concepts is evaluated using WordNet. If sufficient similarity is detected, the system extracts the reported location and determines an appropriate UAV task based on the content of the post. To prioritize operations, the framework performs clustering of posts using geographic information and additional parameters to assess task urgency. The authors also adapted the Vehicle Routing Problem (VRP) to address UAV scheduling and routing. Evaluation was conducted using a dataset consisting of social media posts from Hurricane Sandy. The results indicated that the proposed framework enabled UAVs to prioritize tasks and areas with greater need for assistance. However, the authors noted that the experiments were conducted in a laboratory environment, and that further validation using live data from active social media platforms would be necessary to fully assess the framework's effectiveness.

Although significant research has been conducted in the areas of violence detection, social media analysis, and unmanned aerial systems, these components have largely been studied in isolation. To the best of our knowledge, there is currently no fully integrated and autonomous system that combines these capabilities within a unified framework. This gap motivates the approach proposed in this work.

III. Violence Detection with Drones

To address the challenge of crime detection and prevention in large areas, this paper proposes a system called Violence Detection with Drones (VDD). The proposed system analyzes crime data collected over time using Geographic Information System (GIS) software to identify crime hotspots and generate waypoint missions (automated flight paths) corresponding to these locations. In addition, the system performs social media analysis to monitor online feeds for reports of violent incidents occurring near or within identified hotspots.

Based on this information, the VDD autonomously determines when to deploy, either conducting routine patrols in high-risk areas or responding to suspected violent incidents. Video and other media captured by the drones are subsequently analyzed using deep learning algorithms to detect and classify

violent activity. Fig 1. illustrates the overall architecture of the proposed VDD system.

Unlike traditional surveillance systems, which rely on fixed infrastructure, VDD is a dynamic framework that integrates patterns of violent crime, social media analysis, and automated aerial sensing. This integration enables targeted monitoring and more timely situational awareness in areas with elevated risk.

A. Crime Hotspot Mapping

Crime hotspots are defined as geographic areas exhibiting a high concentration of criminal activity. These hotspots can be identified by analyzing crime data collected over a period of time and applying techniques such as density analysis or clustering. Historical crime patterns in a region can often provide sufficient information to estimate the likelihood of future incidents; however, the data must be processed carefully. Proper data cleaning procedures are necessary, and potential biases in the data must be considered to avoid misleading conclusions. Temporal factors must also be incorporated when generating hotspots, as different types of crimes may occur at different times of the day or during specific periods. Additionally, the time span of the dataset should be carefully selected, since including outdated data may significantly distort the resulting hotspot maps and reduce their accuracy.

A variety of Geographic Information System (GIS) platforms are available for hotspot analysis. In the proposed system, ArcGIS Pro with the Crime Analysis solution [15] is used. Although ArcGIS Pro supports many types of analysis, its role in this work is limited to hotspot identification.

Several analytical methods may be employed to identify hotspots. The kernel density estimation tool generates hotspot maps by applying a kernel smoothing function to incident data; while effective, the results are sensitive to the choice of bandwidth. The 80–20 analysis tool can be used to identify areas with a disproportionately high number of incidents, based on the principle that a large proportion of incidents may occur within a relatively small number of locations. However, this approach may skew the results toward frequently targeted locations and neglect areas with lower, yet still meaningful, levels of criminal activity.

Density-based clustering methods, such as DBSCAN, can also be applied to identify clusters of incidents using machine learning techniques. When using such methods, parameters such as neighbourhood radius and minimum point density must be carefully selected, as they significantly influence the clustering results.

Hotspots should be recalculated at regular intervals, with the frequency determined by the relevant law enforcement authority. The recalculation period depends on the rate at which crime patterns change, which can be influenced by factors such as increased police presence or seasonal variations in criminal activity.

The number of identified hotspots directly impacts the number of drones required for effective patrol coverage; a higher number of hotspots necessitates a larger drone fleet. Certain hotspot identification tools, such as kernel density estimation, provide an intensity measure for each hotspot. This intensity

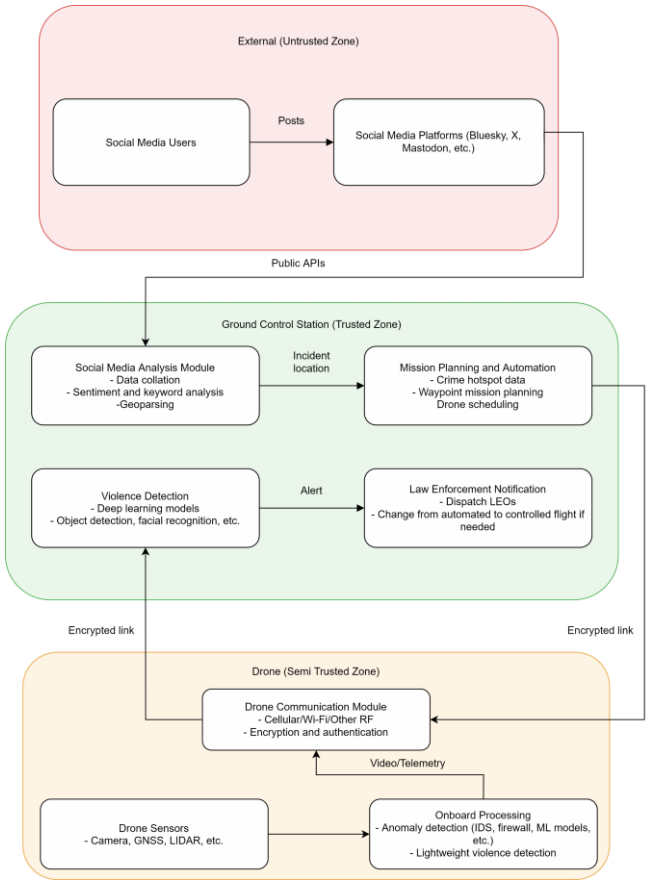


Fig. 1. General architecture of the system

information can be used to optimize drone deployment, including determining the frequency of revisits and the duration of time a drone should remain in a particular area during patrols.

B. Drone Waypoint Mission Creation

Drone waypoint missions must be planned using specialized software that ensures the flight paths are safe, obstacle-free, and provide adequate coverage of the target area. Several drone management platforms are available to perform these tasks [16], [17], [18]. The selected software must also support automated flight execution, either at predefined times or in response to specific triggers.

These capabilities are essential for the drone management system in the proposed VDD framework. The choice of platform depends on the drone model being deployed and the additional features required. Since different software platforms support different drone models, the selection of management software should be made only after the drone models for the VDD system have been finalized.

Supplementary features in drone management software can enhance system performance. For instance, some platforms allow manual remote control via keyboard and mouse, while others offer photogrammetry tools that enable law enforcement to collect accurate data for incident investigation. Additional functionalities may include live video streaming to officers on the ground, providing real-time aerial situational awareness, or

integration with traffic and navigation apps, such as Waze, to augment incident intelligence.

Several operational constraints must be considered when planning waypoint missions. These include adherence to no-fly zones, the drone's maximum range on a single battery charge, and regulatory restrictions such as altitude limits and rules regarding flights over people. Mission parameters must also account for camera resolution, ensuring that altitude and field of view allow sufficient visibility of incidents. Patrol speed, camera orientation, and other auxiliary settings can be configured within the drone management system to optimize surveillance coverage and data collection.

C. Violence Analysis Program

Media captured by the drone must be analyzed to determine whether a violent incident is occurring. In the proposed system, the media is streamed to a Ground Control Station (GCS) for processing. This analysis can be performed using various algorithms, typically deep learning models trained on appropriate datasets. While on-board analysis is possible, it generally requires enterprise-grade drones due to the high computational power and battery capacity needed to run deep learning models locally.

Effective violent incident detection often involves combining multiple deep learning techniques. Temporal analysis methods, such as Long Short-Term Memory (LSTM) or Gated Recurrent Units (GRU), are commonly used alongside object and human detection algorithms, such as YOLO (You Only Look Once).

The system can benefit from a two-tiered model architecture. The primary model, designed for low computational cost, can be deployed directly on drones capable of on-board processing. This model prioritizes rapid analysis over absolute accuracy, enabling near-real-time detection from the drone livestream. Its primary requirement is a low false negative rate to minimize missed incidents. False positives are less critical at this stage, as suspected events can be further verified by the secondary model. By performing fast preliminary analysis, the primary model also reduces the data transmission load to the GCS by only sending media flagged as potentially containing violent activity.

The secondary model prioritizes detection accuracy and may employ a different algorithm from the primary model. Once the primary model flags a potential incident, the secondary model analyzes the full video sequence captured by the drone to confirm the occurrence of a violent event. This two-tiered approach improves overall detection and classification accuracy while balancing computational efficiency and real-time responsiveness.

D. Social Media Analysis Program

Social media has become deeply integrated into modern life, with most people owning smart devices and regularly sharing updates about events, including violent occurrences. Multiple social media platforms can serve as real-time sources of information about such incidents, potentially providing faster alerts than traditional reporting methods, such as emergency phone calls [19]. Leveraging this timely information can reduce the response time for deploying drones to incident locations.

The proposed social media analysis system is illustrated in Fig 2. It performs continuous monitoring of feeds from multiple social media networks. For the proposed implementation, the Bluesky platform [20] is used to obtain incident-related data, although other platforms such as X (formerly Twitter), Mastodon, or Threads could also be utilized. Bluesky was selected due to its well-documented Software Development Kit (SDK) across multiple programming languages and the availability of public API endpoints, including the firehose.

Posts related to incidents can be retrieved using two primary methods: the social media firehose or tags/mentions. The firehose provides a live stream of all posts on the platform, offering comprehensive coverage but generating a large volume of data. Tags and mentions provide a more targeted approach, in which users include specific hashtags or directly reference law enforcement accounts, reducing the data that must be processed.

Retrieved posts are stored in a database, where sentiment analysis and keyword filtering are applied. Sentiment analysis, performed using machine learning and natural language processing techniques, categorizes posts as positive, neutral, or negative. Since reports of violent incidents are expected to carry a negative sentiment, only negatively classified posts are selected for further analysis. These posts are then filtered using relevant keywords, such as "violence" or "crime," to remove negative posts unrelated to actual incidents.

The filtered posts are subsequently processed by a geoparsing module, which extracts location information from free-form text. When available, location tags from social media posts can be directly retrieved via the platform API. Otherwise, geoparsing converts textual descriptions into geographic coordinates. Challenges such as ambiguous place names can arise; these can be mitigated by restricting the geoparsing scope to the operational area of the law enforcement agency and prioritizing addresses with the highest confidence scores. Retrieved addresses, expressed in plaintext or latitude/longitude, are then compared to the jurisdiction of the law enforcement agency. Verified locations are matched to existing drone flight paths, and a drone is dispatched to the closest patrol route.

Reliance on community-generated content introduces potential vulnerabilities. Malicious actors could send false reports or use botnets to flood the system with spurious data, while misinformation campaigns could divert drones to non-existent incidents. To mitigate these risks, spam and bot detection mechanisms should be integrated, alongside trustworthiness metrics for users. Accounts with a history of legitimate reporting can be assigned higher trust values, while users who repeatedly submit false reports can be penalized or blocked. Cross-validation using multiple sources of data further increases the reliability of incident detection.

This workflow ensures that LEOs are only deployed when a violent incident is confirmed, reducing unnecessary in-person responses and allowing drones to perform initial verification. As a result, the system alleviates the operational burden on an already stretched police force while improving the efficiency and timeliness of law enforcement interventions.

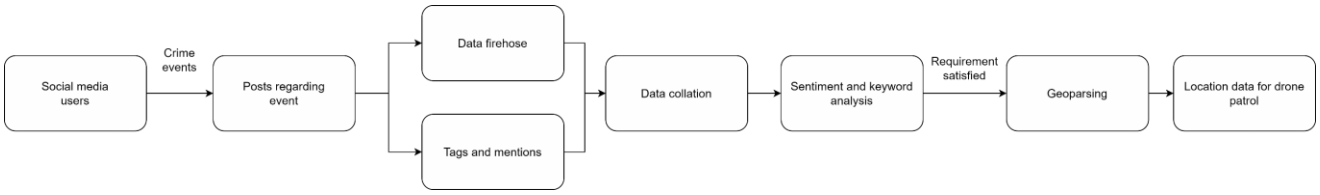


Fig. 2. Social media analysis flowchart

IV. Cybersecurity Analysis

Any technological system is inherently vulnerable to attacks, and the proposed drone surveillance system is no exception. The system comprises three main components: (1) the drones, which capture media for violence detection; (2) the communication link between drones and the Ground Control Station (GCS); and (3) the GCS, which controls and manages the drones while also performing social media analysis and violence detection (Fig. 3). Each component contains multiple sub-components and must be analysed for potential vulnerabilities, with appropriate mitigation and prevention strategies applied.

Drones rely on multiple sensors, including GPS, for navigation, geofencing, automated flights, and return-to-home operations [21]. Public GPS signals are unencrypted and unauthenticated, making them vulnerable to spoofing and jamming attacks [22], [23]. Spoofing can redirect drones from waypoint missions, while jamming can cause loss of position or crashes. Sensor redundancy, using Inertial Measurement Units (IMUs), LIDAR, and multi-constellation GNSS (e.g., Galileo, GLONASS, BeiDou), can enhance resilience. Sensor fusion techniques, combined with machine learning models, have been shown to detect GPS anomalies with high accuracy [24], [25].

Supply chain attacks targeting firmware or hardware also pose significant risks, potentially enabling attackers to bypass all security measures if undetected. Preventive measures include secure software development, patch management, zero trust architectures, employee cybersecurity training, physical access controls, and tamper-evident packaging. Open network ports on drones can also be exploited; proper firewall configurations, port management, and encryption are critical to limit unauthorized access.

Drones equipped with Automatic Dependent Surveillance–Broadcast (ADS-B) can receive updates on nearby aircraft to avoid collisions [26]. However, ADS-B signals are also unencrypted and unauthenticated, leaving them vulnerable to spoofing and jamming attacks. Malicious actors could manipulate drone flight paths or cause collisions by falsifying ADS-B data. Mitigation strategies include sensor redundancy, directional antenna arrays, and machine learning-based anomaly detection to identify spoofed messages [27], [28], [29].

Communication links between drones and the GCS, including Wi-Fi, cellular networks, and proprietary protocols (e.g., OcuSync, Lightbridge), are susceptible to man-in-the-middle attacks, de-authentication attacks, protocol downgrades, and denial-of-service (DoS) attacks [30], [31], [32], [33]. Wi-Fi networks can be protected through WPA3 encryption and Protected Management Frames, while cellular communications require updated protocols and IMSI-catcher detection tools, such as Rayhunter [34]. Rate limiting, authenticated access, and fail-safe measures (e.g., return-to-home functionality) can mitigate DoS attacks.

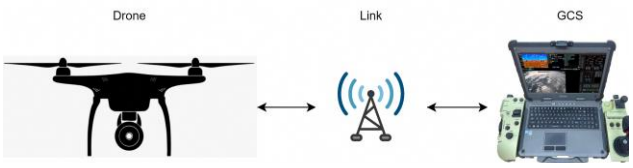


Fig. 3. Drone components

Ground Control Stations are central to system operations, controlling drones and performing analysis. They are vulnerable to software exploits, hardware vulnerabilities, and supply chain attacks [35]. Compromise of the GCS could allow attackers to modify flight paths, disrupt automated patrols, or gain access to sensitive media streams. Security measures include secure-by-design software, regular patches, vulnerability audits, bug bounty programs, and robust access controls.

In conclusion, ensuring the security of drone-based surveillance systems requires a comprehensive approach addressing sensor vulnerabilities, secure communications, supply chain integrity, and GCS protection. Proper mitigation strategies enhance the resilience and reliability of autonomous systems deployed for violence detection and law enforcement support.

V. Conclusions and Future Research

Drones offer a valuable tool for surveillance in areas with high crime density, particularly where fixed cameras are absent. By integrating deep learning models with social media analysis, the proposed system can detect violent incidents in such areas and automate portions of law enforcement tasks, thereby reducing the operational workload for officers. However, as with any technological system, potential vulnerabilities exist; a comprehensive cybersecurity assessment is therefore essential, along with the implementation of robust prevention and mitigation strategies to safeguard system integrity.

Several enhancements and extensions could further improve system performance. Incorporating audio analysis could complement visual data for more accurate violence detection. LIDAR sensors on drones could capture precise spatial information of the environment, aiding in scene reconstruction and preventing tampering. Flying Ad-hoc Networks (FANETs) could enable distributed processing across a drone swarm, reducing dependency on the Ground Control Station (GCS) for decision-making. Additional data sources, such as 911 calls, could augment social media feeds to trigger drone deployment. Large Language Models (LLMs) could be employed to replace both the sentiment analysis and geoparsing modules within the social media analysis pipeline, potentially improving accuracy and efficiency.

Privacy considerations remain critical and were not explored in detail in this work. To mitigate privacy risks, measures such as automatic blurring of faces, deletion of collected data after a defined retention period, and the application of homomorphic encryption [36] can be implemented to ensure the protection of individual privacy while maintaining system functionality.

ACKNOWLEDGMENT

The authors would like to thank Shaun Hildebrand of ESRI for their help with the ArcGIS software, and Rob Williamson of Durham Regional Police Service for providing the crime data for the Durham region.

REFERENCES

[1] S. C. Government Of Canada, *Police-reported Crime Severity Indexes, Canada, 1998 to 2024,* 2025.

[2] S. C. Government Of Canada, *Police-reported crime rates, Canada, 1962 to 2024,* 2025.

[3] S. C. Government of Canada, *The Daily — Police resources in Canada, 2023,* 2024.

[4] M. Lukacs, "Canadian police expanding surveillance powers via new digital "operations centres"," April 2025. [Online]. Available: https://breachmedia.ca/canadian-police-expanding-surveillance-powers-via-new-digital-operations-centres/.

[5] P. Siriaraya, Y. Zhang, Y. Wang, Y. Kawai, M. Mittal, P. Jeszenszky and A. Jatowt, "Witnessing Crime through Tweets," 2019.

[6] K. Ganagavalli and V. Santhi, "YOLO-based anomaly activity detection system for human behavior analysis and crime mitigation," *Signal Image and Video Processing,* vol. 18, p. 417–427, April 2024.

[7] "Real-world Anomaly Detection in Surveillance Videos," [Online]. Available: https://www.crcv.ucf.edu/projects/real-world/.

[8] J. Suarez-Paez, M. Salcedo-Gonzalez, A. Climente, M. Esteve, J. A. Gómez, C. E. Palau and I. Pérez-Llopis, "A novel low processing time system for criminal activities detection applied to command and control citizen security centers," *Information,* vol. 10, p. 365, November 2019.

[9] M. Q. Gandapur, "E2E-VSDL: End-to-end video surveillance-based deep learning model to detect and prevent criminal activities," *Image and Vision Computing,* vol. 123, p. 104467, April 2022.

[10] "CAVIAR test case scenarios," [Online]. Available: https://homepages.inf.ed.ac.uk/rbf/CAVIARDATA1/.

[11] J. Henrio and T. Nakashima, "Anomaly detection in videos recorded by drones in a surveillance context," *2022 IEEE International Conference on Systems, Man, and Cybernetics (SMC),* p. 2503–2508, October 2018.

[12] "Mini-drone video dataset," [Online]. Available: https://www.epfl.ch/labs/mmspg/downloads/mini-drone/.

[13] "Monitoring human activity - Detection of events," [Online]. Available: https://mha.cs.umn.edu/proj_events.shtml#crowd.

[14] M. Terzi, P. Kolios, C. Panayiotou and T. Theocharides, "Towards a Social-media Driven Multi-Drone Tasking platform," 2020.

[15] "Introduction to Crime Analysis—ARCGIS Solutions | Documentation," [Online]. Available: https://doc.arcgis.com/en/arcgis-solutions/latest/reference/introduction-to-crime-analysis.htm.

[16] "Litchi for DJI drones," [Online]. Available: https://flylitchi.com/.

[17] "Home - DroneSense," [Online]. Available: https://www.dronesense.com/.

[18] "Autonomous Drone Operations Management Software Platform features," [Online]. Available: https://www.flytbase.com/features.

[19] "#Westgate tweets: A detailed study in information forensics," November 2013. [Online]. Available: https://irevolutions.org/2013/11/18/westgate-information-forensics/.

[20] "Bluesky," [Online]. Available: https://bsky.app/.

[21] "GPS | GPS.gov," [Online]. Available: https://www.gps.gov/gps.

[22] "GPS under attack as crooks, rogue workers wage electronic war," August 2016. [Online]. Available: https://www.nbcnews.com/news/us-news/gps-under-attack-crooks-rogue-workers-wage-electronic-war-n618761.

[23] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," *Texas ScholarWorks (Texas Digital Library),* p. 2314–2325, January 2018.

[24] U. Kröner, C. Bergonzi, J. Fortuny-Guasch, R. Giuliani, F. Littmann, D. Shaw and D. Symeonidis, "Hardening of GNSS based trackers Final Report," 2010.

[25] M. Y. Alzahrani, "Enhancing drone security through Multi-Sensor anomaly detection and machine learning," *SN Computer Science,* vol. 5, June 2024.

[26] "Automatic Dependent Surveillance Broadcast - Airservices," June 2025. [Online]. Available: https://www.airservicesaustralia.com/industry-info/resources/ads-b/.

[27] M. R. Manesh and N. Kaabouch, "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system," *International Journal of Critical Infrastructure Protection,* vol. 19, p. 16–31, October 2017.

[28] S. Rudys, J. Aleksandravicius, R. Aleksiejunas, A. Konovaltsev, C. Zhu and L. Greda, "Physical layer protection for ADS-B against spoofing and jamming," *International Journal of Critical Infrastructure Protection,* vol. 38, p. 100555, August 2022.

[29] Q. A. Al-Haija and A. Al-Tamimi, "Secure Aviation Control through a Streamlined ADS-B Perception System," *Applied System Innovation,* vol. 7, p. 27, March 2024.

[30] Samyk, "GitHub - samyk/skyjack: A drone engineered to autonomously seek out, hack, and wirelessly take full control over any other Parrot or 3DR drones within wireless or flying distance, creating an army of zombie drones under your control.," [Online]. Available: https://github.com/samyk/skyjack.

[31] M. Hooper, Y. Tian, R. Zhou, B. Cao, A. P. Lauf, L. Watkins, W. H. Robinson and W. Alexis, "Securing commercial WiFi-based UAVs from common security attacks," *MILCOM 2016 - 2016 IEEE Military Communications Conference,* November 2016.

[32] Riverloopsec, "GitHub - riverloopsec/killerbee: IEEE 802.15.4/ZigBee Security Research Toolkit," [Online]. Available: https://github.com/riverloopsec/killerbee.

[33] C. Bender, "DJI drone IDs are not encrypted," *arXiv (Cornell University),* July 2022.

[34] C. Q. Greenberg and Will, "Meet Rayhunter: A New Open Source Tool from EFF to Detect Cellular," April 2025. [Online]. Available: https://www.eff.org/deeplinks/2025/03/meet-rayhunter-new-open-source-tool-eff-detect-cellular-spying.

[35] Darknavy, "Fatal vulnerabilities compromising DJI control devices," March 2025. [Online]. Available: https://www.darknavy.org/blog/fatal_vulnerabilities_compromising_dji_control_devices/.

[36] W. Ao and V. N. Boddeti, "CryptoFace: End-To-End Encrypted Face Recognition," *IEEE Conference on Computer Vision and Pattern Recognition 2025,* p. 19197–19206, June 2025.