8. Розвиток автоматизованих систем розпізнавання осіб та транспортних засобів: Застосування систем, які аналізують дані з камер спостереження та ідентифікують обличчя або транспортні засоби, що фігурують у злочинах, дозволить оперативно виявляти зловмисників.

9. Аналіз поведінкових моделей злочинців: Використання великих обсягів даних для створення моделей поведінки злочинців, що дозволить прогнозувати їхні дії та місця вчинення нових злочинів, сприяючи попередженню злочинів.

10. Законодавча адаптація до нових технологій: Оновлення нормативної бази, що дозволить офіційно застосовувати новітні технології та методи роботи з криміналістичними обліками під час розслідування злочинів, забезпечуючи їхню юридичну силу та захист прав людини.

Список використаних джерел

1. Єфімов М.М. Типові слідчі ситуації при розслідуванні кримінальних правопорушень проти моральності. *Прикарпатський юридичний вісник*. 2018. Вип. 1 (22), т. 5, ч. 2, С. 111–115.

2. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «СЛІД» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України: Наказ Міністерство внутрішніх справ України від 16.03.2020 № 257 станом на 14 серп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/z0319-20#Text.

3. Сайт Межа: Новини URL: https://mezha.net/ua/bukvy/za-dopomohoiu-systemy-rozpiznavannia-oblych-prykordonnyky-vstanovyly-ponad-10-tysiach-osib-prychetnykh-do-voiennykh-zlochyniv/.

Стрілецький Максим Олександрович,
начальник 2-го відділу (аналітики воєнних злочинів) 4-го управління (ситуаційного аналізу) Департаменту кримінального аналізу Національної поліції України

РОЛЬ OSINT У ДОКУМЕНТУВАННІ ВОЄННИХ ЗЛОЧИНІВ В УКРАЇНІ

Open-source Intelligence – це розвідка на основі відкритих джерел. Але така назва не є звичною для кіберсвіту, тому зазвичай вживається формулювання «OSINT».

Сама назва говорить про те, що під час проведення розвідки використовуються виключно відкриті джерела, які доступні усім. Тим паче, що зараз в Інтернеті можна зібрати величезні масиви даних і без застосування методів, що акумулюють інформацію у незаконний спосіб.

Термін OSINT також охоплює інформацію, яку можна знайти в різних форматах медіа. Попри те, що ми зазвичай асоціюємо його з текстом, до цього поняття також включають зображення, відео, вебінари, публічні виступи та конференції.

Для чого OSINT в умовах сьогодення?

Протокол Берклі – це практичний посібник з ефективного використання цифрової інформації з відкритим вихідним кодом при розслідуванні порушень міжнародного кримінального права, права людини та гуманітарного права.

Це перший набір глобальних керівних положень щодо використання цифрових даних, які є у відкритому доступі, як доказів у міжнародних розслідуваннях щодо порушень прав людини.

Документ містить стандарти знаходження, збирання, зберігання, перевірки та аналізу контенту із соцмереж та інших відкритих джерел.

Які навички необхідні для OSINT?

Привабливість OSINT полягає в тому, що він може бути використаний, як для технічних процесів, так і загалом для розвитку людини. Стосовно навичок, то по-перше – це базове розуміння використання програмного забезпечення (мінімально браузер). По-друге – це звісно посидючість, тому що збір інформації потребує часу. Ще один важливий момент. Має бути присутня креативність, адже я часто в своїй роботі стикався із ситуаціями, коли ти робиш все правильно, застосовуєш правильні інструменти, але все одно не можеш добратися до суті.

Тоді потрібно знаходити креативні підходи, шукати дотичні об’єкти або події, що неопосередковано стосуються цього об’єкта. Ну і звісно бажання розвиватися, тому що цифровий світ розвивається дуже активно і створюються нові програмні рішення, нові підходи до збору інформації. Це потребує базових навичок у програмуванні, хоча вони не є ключовим і, в принципі, можуть прокачуватись паралельно.

Наскільки важливим є наявність технічного бекграунду у людини? Знання в програмуванні, налаштуванні відповідних систем?

Все залежить від задач, що стоять перед дослідниками. Для більш простіших нам може бути достатньо лише смартфону. Якщо ж ми говоримо про якийсь більш серйозний підхід, то тут дійсно потрібно прокачувати технічні навички, але, як я вже сказав, це можна робити паралельно. Тобто наявність або відсутність технічного бекграунду критично не впливає на роботу, але якщо це приватний детектив, якому потрібно все зробити для того, щоб провести розвідку обережно і без розкриття себе, то тут потрібен хоча б мінімальний технічний бекграунд.

Хто використовує OSINT?

OSINT використовується різними людьми та організаціями для різних цілей. Ось кілька прикладів:

Розвідувальні організації використовують OSINT для збору інформації про потенційні цілі, такі як конкуренти або вороги.

Кібербезпекові фахівці використовують OSINT для виявлення кіберзагроз, таких як фішингові атаки, розвідка і зломи.

Журналісти використовують OSINT для розслідування новинних історій.

Бізнесмени використовують OSINT для дослідження ринку, конкурентів і потенційних клієнтів.

OSINT також використовується окремими людьми для різних цілей, таких як:

Вивчення історії або культури.

Знаходження інформації про продукти або послуги.

Розслідування злочинів.

Етапи розвідувального процесу

Підготовка: На цьому етапі визначаються потреби та вимоги завдання, такі як визначення цілей і вибір найкращих джерел для пошуку необхідної інформації.

Збір: Це ключовий етап, під час якого здійснюється первинний збір даних та інформації з різних джерел.

Обробка: На цьому етапі зібрані дані організовуються, перевіряються та зіставляються для подальшого аналізу.

Аналіз та обробка: Цей етап включає інтерпретацію зібраної інформації з метою виявлення закономірностей та створення висновків. Підготовка звіту містить відповідь на розвідувальне питання та рекомендації для подальших дій.

Поширення: На останньому етапі результати представляються перед зацікавленими сторонами у вигляді

письмових звітів, графіків, рекомендацій і т. д. Вони відповідають на розвідувальні запитання та надають інформацію для подальших дій.

Пасивний та активний OSINT

Пасивний підхід передбачає, що ви не взаємодієте активно з об'єктом дослідження. Ви лише збираєте інформацію з відкритих джерел, використовуючи загальнодоступні дані. Важливо розуміти, що на пасивному етапі ви не вступаєте в активний контакт з особами в онлайні, такими як коментування, обмін повідомленнями, додавання в друзі тощо.

Приклади пасивного OSINT:

Пошук інформації в Інтернеті за допомогою пошукових систем.

Аналіз соціальних мереж.

Читання новинних статей.

Отримання доступу до публічних баз даних.

Активний підхід передбачає пряму взаємодію з об'єктом дослідження, таку як додавання до списку друзів на соціальних мережах, коментування публікацій, відправлення повідомлень іт. д.

Приклади активного OSINT:

Використання інструментів для збору інформації з соціальних мереж.

Спілкування з людьми в Інтернеті.

Використання інструментів для виявлення прихованої інформації.

Вибір між пасивним та активним OSINT залежить від ваших конкретних потреб. Якщо ви шукаєте інформацію, яка вже доступна публіці, пасивний OSINT є хорошим варіантом. Якщо вам потрібна інформація, яка недоступна публіці, активний OSINT може бути більш ефективним.

ВАЖЛИВІСТЬ «OSINT» У ДОКУМЕНТУВАННІ

В умовах війни доступ до окупованих або тимчасово неконтрольованих територій обмежений, а документування ймовірних порушень там – небезпечне, або й неможливе. Слідчим, прокурорам, адвокатам і суддям може бракувати досвіду роботи з деякими особливими категоріями надтяжких порушень, як-то воєнні злочини або злочини проти людяності.

Саме в цьому випадку аналітики воєнних злочинів допомагають встановити низку важливих деталей, зокрема:

1. **Військові підрозділи та їхня активність**. Чи видно на відео чи фотографіях військовослужбовців у формі. Чи можливо ідентифікувати форму, відзнаки, техніку.

2. **Можливі військові цілі**. Після визначення місця проведення військової операції, інформація з відкритих джерел може допомогти встановити, чи були там або поруч можливі військові цілі. З належними навичками ви можете визначити військові цілі з використанням картографічних інструментів і супутникових знімків високої роздільної здатності, перевіряючи наявність військових об'єктів або споруд, а також визначаючи крупну військову техніку: вантажівки, танки, бронетехніку та літальні апарати.

3. **Активність цивільних**. Куди саме припав удар – у житловий район, точку евакуації, багатоквартирний будинок, лікарню чи деінде? Чи видно десь цивільних осіб, наприклад, дітей або літніх людей? Що вони роблять? Чи дозволяють відкриті джерела візуально порахувати кількість цивільних осіб – живих або мертвих?

4. **Ідентифікація озброєння**. Постраждалі, які знімали місце подій, часто оприлюднюють зображення залишків зброї або іншої військової техніки онлайн. До них відносяться уламки ракет або снарядів, гільзи, касетні боєприпаси, упаковки тощо. Ідентифікація цієї зброї може допомогти встановити, чи був удар непропорційним або невибірковим та в подальшому допомогти встановити безпосередньо виконавців вказаного злочину (командирів підрозділу).

Список використаних джерел

1. Dehtiarova Y. Як OSINT впливає на війну в Україні? [Електронний ресурс] / Yuliana Dehtiarova // itedu.cente. – 2022. – Режим доступу до ресурсу: https://itedu.center/ua/blog/articles/osint/?srsltid=AfmBOooGkcfk0Cb_A5SDyxlzlsWzJPrA8FZTxGNgx2luA1fyOGcdwiHV.

2. Старосек А. OSINT в Україні: хто і як допомагає фронту під час війни? [Електронний ресурс] / Артем Старосек // Українська правда. – 2023. – Режим доступу до ресурсу: https://www.pravda.com.ua/columns/2023/01/23/7386112/.

3. ECOFCC. OSINT і його роль у сучасному світі [Електронний ресурс] / ECOFCC // EUROPEAN CENTER OF FINANCIAL CRIME COUNTERACTION – Режим доступу до ресурсу: https://ecofcc.org/2023/08/21/osint-earth/.