Методи зберігання даних для інформаційно-аналітичного забезпечення органів влади та управління (ІАЗ ОУВ) в умовах сучасного конфлікту

Розділ 1: Дата-центричне поле бою: Стратегічна роль ІАЗ у російсько-українській війні

1.1. Вступ: Інформація як вирішальний домен ведення війни

Сучасна війна, яскравим прикладом якої є російсько-український конфлікт, трансформувала інформацію з допоміжного інструменту на самостійний домен бойових дій, що стоїть на одному рівні із землею, морем, повітрям, космосом та кіберпростором. Застаріле кліше "дані — це нова нафта" поступається місцем більш точному військовому аналогу: дані — це нова "панівна висота". Це та вирішальна ділянка місцевості, з якої здійснюється командування та управління всіма іншими операціями. Контроль над інформаційним ландшафтом забезпечує перевагу в темпі, точності та, зрештою, у досягненні стратегічних цілей.

Аналіз перших 72 годин повномасштабного вторгнення слугує хрестоматійним прикладом інформаційної асиметрії. Російське військово-політичне керівництво діяло на основі хибних, застарілих даних та фундаментально неправильної оцінки суспільно-політичної ситуації в Україні. Їхні розвідувальні дані, що малювали картину слабкого опору та швидкої капітуляції, призвели до катастрофічних операційних провалів: розтягнутих і незахищених колон постачання, висадки десанту без належної підтримки та загальної

втрати ініціативи. Водночас українська сторона продемонструвала виняткову здатність до швидкого генерування, обробки та розповсюдження точної ситуаційної обізнаності. Ця здатність, що спиралася на поєднання даних від збройних сил, розвідувальних органів, цивільного населення та міжнародних партнерів, стала критичним фактором в успішній обороні Києва та зриві початкового плану бліцкригу.

Ця динаміка демонструє, що перевага в конфлікті визначається не лише кількістю танків чи артилерійських систем, але й здатністю швидше та ефективніше перетворювати сирі дані на actionable intelligence — розвідувальну інформацію, що спонукає до дії. Сторона, яка швидше проходить цикл "спостереження — орієнтація — рішення — дія" (цикл OODA полковника Джона Бойда), отримує вирішальну перевагу в темпі. У цьому контексті архітектура зберігання та обробки даних перестає бути суто технічним питанням IT-департаменту. Вона стає фундаментальним компонентом бойової потужності держави. Затримка у виконанні запиту до бази даних може буквально означати різницю між успішним ураженням пріоритетної цілі та втраченою можливістю, що вимірюється життями та стратегічними наслідками.

1.2. Визначення ІАЗ ОУВ у контексті воєнного часу

Інформаційно-аналітичне забезпечення органів влади та управління (ІАЗ ОУВ) в умовах тотальної війни зазнає фундаментальної трансформації. Це вже не просто процес збору даних та підготовки звітів для бюрократичного апарату. В умовах екзистенційної загрози ІАЗ перетворюється на когнітивний двигун національного спротиву — нервову систему, що поєднує сенсори на полі бою з центрами прийняття рішень та ефекторами.

У сучасному розумінні ІАЗ — це замкнений та безперервний цикл:

1. **Збір:** Дані надходять з незліченної кількості джерел — від тактичного безпілотника на лінії зіткнення, повідомлення цивільної особи у чат-боті, знімка комерційного супутника до перехопленої радіограми.
2. **Обробка та зберігання:** Сирі дані передаються до систем зберігання, де вони очищуються, структуруються, збагачуються метаданими та готуються для аналізу. Саме на цьому етапі вибір правильної архітектури зберігання є критичним.
3. **Аналіз:** Аналітики (або все частіше — алгоритми машинного навчання) виявляють у даних патерни, зв'язки та аномалії, перетворюючи їх на знання.
4. **Прийняття рішення:** Синтезована інформація у вигляді чіткої оперативної картини, аналітичної записки чи цілевказівки доставляється до центру прийняття рішень — командира бригади, міністра оборони, керівника військової адміністрації або Президента.
5. **Дія:** Рішення трансформується у конкретну дію — наказ артилерійському підрозділу, дипломатичний демарш, публічну комунікацію для протидії дезінформації або

гуманітарну операцію.
6. **Зворотний зв'язок:** Результати дії знову стають даними, які надходять у систему, замикаючи цикл і дозволяючи адаптуватися в режимі реального часу.

Ефективність, швидкість та стійкість цього циклу безпосередньо залежать від базової архітектури зберігання та управління даними. Неспроможність системи швидко обробити потік даних з БПЛА означає запізнілу реакцію артилерії. Неможливість надійно зберігати та каталогізувати докази воєнних злочинів унеможливлює майбутнє правосуддя. Повільна або вразлива система є гальмом для всього оборонного механізму держави.

1.3. Еволюція від підтримки даними до операцій, керованих даними

До 2014 року інформаційні системи в секторі безпеки та оборони України значною мірою успадкували радянську модель: жорсткі, ієрархічні, ізольовані ("силосні") системи, що часто покладалися на паперовий документообіг. Дані розглядалися як статичний ресурс, що надавався *на підтримку* вже прийнятих рішень. ІАЗ виконував функцію обслуговування, а не формування операцій.

Події 2014 року стали каталізатором змін, але повномасштабне вторгнення 2022 року спричинило справжню революцію. Необхідність протистояти значно переважаючому противнику змусила Україну здійснити стрибок до нової парадигми — операцій, керованих даними (data-driven operations). У цій моделі ІАЗ перестає бути лише *підтримуючою* функцією і стає *рушійною* силою. Дані, завдяки автоматизованому аналізу та спільній ситуаційній обізнаності, самі *визначають* та *скеровують* операції.

Яскравим втіленням цього парадигмального зсуву є національна система ситуаційної обізнаності "Дельта". Це не просто карта, на яку наносяться дані. Це комплексна екосистема, що інтегрує інформаційні потоки від десятків джерел у режимі реального часу, надаючи єдину, достовірну та актуальну оперативну картину для всіх рівнів командування. Успішні удари по високоцінних російських цілях, таких як командні пункти, склади боєприпасів та засоби ППО, часто є результатом не одного джерела розвідки, а швидкого синтезу даних у таких системах. Цей синтез — поєднання даних радіоелектронної розвідки, супутникових знімків, інформації від агентурних мереж та OSINT-аналізу — стає можливим лише за наявності інформаційної архітектури, здатної приймати, обробляти та надавати доступ до різнорідних типів даних у режимі, близькому до реального часу. Таким чином, інвестиції в сучасні платформи даних, хмарну інфраструктуру та відповідні методи зберігання є не просто проектом з IT-модернізації; це пряма інвестиція в летальність, оперативну ефективність та національну стійкість.

Розділ 2: Анатомія даних воєнного часу: від стрічок OSINT до потоків SIGINT

2.1. Таксономія даних у сучасному конфлікті

Для ефективного управління даними в умовах війни необхідно вийти за межі традиційної класифікації за розвідувальними дисциплінами (HUMINT, SIGINT, IMINT тощо) і запровадити класифікацію за структурою, швидкістю та форматом. Цей підхід дозволяє правильно обирати технології зберігання та обробки для кожного типу інформації.

- **Структуровані дані (Structured Data):** Це високоорганізовані дані, що мають жорстку, заздалегідь визначену схему і легко піддаються пошуку та аналізу за допомогою стандартних інструментів. Вони зазвичай зберігаються у реляційних базах даних.
    - *Приклади:* Бази даних втрат військової техніки противника (з полями: тип, модель, дата, місце, статус); логістичні таблиці (номенклатура, кількість, місцезнаходження, статус доставки); офіційні реєстри внутрішньо переміщених осіб (ВПО); бази даних оцінки пошкоджень об'єктів критичної інфраструктури.
- **Напівструктуровані дані (Semi-Structured Data):** Ці дані не відповідають жорсткій схемі реляційної бази даних, але містять теги, маркери або інші семантичні елементи, що дозволяють структурувати інформацію. Вони часто представлені у форматах JSON, XML або YAML.
    - *Приклади:* Дані з сенсорів БПЛА (координати, висота, швидкість, дані з камери у форматі JSON); метеорологічні звіти, що передаються через API; дані з систем радіоелектронної боротьби; розвідувальні донесення, розмічені за стандартною формою.
- **Неструктуровані дані (Unstructured Data):** Це дані у своєму первинному, "сирому" форматі, без заздалегідь визначеної моделі чи схеми. Вони складають переважну більшість (за оцінками, понад 80%) даних, що генеруються під час війни, і становлять найбільший виклик для зберігання та аналізу.
    - *Приклади:* Відеопотоки з розвідувальних дронів та камер спостереження; перехоплені аудіозаписи розмов; тексти з соціальних мереж та месенджерів (Telegram, Twitter, Facebook); супутникові знімки високої роздільної здатності; фотографії з поля бою; текстові звіти агентів у вільній формі.

Ключовим завданням сучасного ІАЗ є не просто зберігання цих трьох типів даних, а створення архітектури, яка дозволяє їх поєднувати та аналізувати разом. Саме на перетині структурованих, напівструктурованих та неструктурованих даних народжується

найцінніша розвідувальна інформація.

2.2. "3 V" в українському контексті: Volume, Velocity та Veracity

Класична модель "Великих даних" (Big Data), що описується трьома "V" — Volume (Об'єм), Velocity (Швидкість) та Variety (Різноманітність), — набуває в умовах російсько-української війни особливої гостроти. До цих трьох необхідно додати четверте, найважливіше "V" — Veracity (Достовірність).

- **Volume (Об'єм):** Масштаб даних, що генеруються, є безпрецедентним. Це петабайти супутникових знімків, що надходять щодня від комерційних та державних партнерів. Це мільйони щоденних повідомлень, фото та відео у соціальних мережах, що стосуються війни. Це безперервні потоки даних з тисяч сенсорів на лінії фронту. Архітектура зберігання повинна бути здатною масштабуватися для поглинання цих величезних об'ємів без втрати продуктивності.
- **Velocity (Швидкість):** Дані генеруються і старіють з надзвичайною швидкістю. Розвіддані про переміщення колони ворожої техніки актуальні протягом годин, якщо не хвилин. Координати цілі, отримані з БПЛА, вимагають обробки та передачі до артилерійського розрахунку за секунди. Система ІАЗ повинна бути спроектована для обробки даних у режимі, близькому до реального часу (near real-time), оскільки затримка безпосередньо впливає на бойову ефективність.
- **Variety (Різноманітність):** Як описано вище, система повинна одночасно працювати з десятками різних форматів: від структурованих таблиць SQL до сирих відеофайлів H.264, геопросторових даних у форматі GeoJSON та текстових повідомлень. Нездатність уніфіковано зберігати та обробляти таку різноманітність призводить до створення ізольованих "силосів" даних та унеможливлює їх ефективний синтез.
- **Veracity (Достовірність):** Це найкритичніший аспект в умовах конфлікту, що характеризується безпрецедентними за масштабом російськими інформаційно-психологічними операціями (ІПСО) та поширенням дезінформації. Завдання полягає не просто у зберіганні даних, а у зберіганні їх разом із метаданими про джерело, час отримання, рівень достовірності та історію перевірки. Кожен елемент даних у системі ІАЗ повинен мати чіткий "паспорт", що дозволяє аналітику оцінити його надійність. Архітектура зберігання повинна підтримувати такий рівень деталізації метаданих та забезпечувати незмінний аудиторський слід для боротьби з дезінформацією та внутрішніми загрозами.

2.3. Глибокий аналіз джерел даних з прикладами

- **OSINT (Open-Source Intelligence / Розвідка на основі відкритих джерел):** Аналіз геолокованих фото та відео з соціальних мереж (Telegram, TikTok, Twitter) став одним з ключових інструментів для відстеження переміщень російських військ, ідентифікації та верифікації втрат техніки, а також для виявлення воєнних злочинів. Платформи, особливо Telegram, перетворилися на справжній "водоспад" інформації. З точки зору архітектури, це вимагає наявності масивних, масштабованих та відносно дешевих сховищ, таких як озера даних (data lakes), здатних "вбирати" цей потік сирої, неструктурованої інформації для подальшої обробки та аналізу.
- **IMINT (Imagery Intelligence / Видова розвідка):** Обробка комерційних супутникових знімків (наприклад, від компаній Maxar, Planet, ICEYE) та тактичних відео з БПЛА є основою для планування операцій та цілевказування. Виклик тут подвійний: по-перше, необхідно зберігати величезні об'єми файлів зображень та відео (терабайти на добу). По-друге, що важливіше, потрібно видобувати з цих зображень структуровані дані (наприклад, за допомогою моделей комп'ютерного зору) і зберігати їх як метадані. Результат роботи моделі, наприклад, "танк Т-72Б3 за координатами 48.123,37.456 на знімку ID_XYZ від 14:32 UTC", є набагато ціннішим для швидкого пошуку, ніж сам файл зображення.
- **SIGINT (Signals Intelligence / Радіоелектронна розвідка):** Управління перехопленими комунікаціями (радіо, телефонними, інтернет-трафіком) є одним з найчутливіших напрямків. Ці дані вимагають рішень для зберігання з найвищим рівнем безпеки, включаючи наскрізне шифрування, гранулярний контроль доступу (щоб аналітик бачив лише те, що йому дозволено) та надійні протоколи управління ключами шифрування.
- **GEOINT (Geospatial Intelligence / Геопросторова розвідка):** Це фундаментальний шар, який об'єднує всі інші типи даних. Практично кожен елемент інформації у війні має географічну прив'язку. Це вимагає використання спеціалізованих геопросторових баз даних (наприклад, PostgreSQL з розширенням PostGIS). Такі системи оптимізовані для виконання складних просторових запитів з високою швидкістю, наприклад: "Показати всі ворожі підрозділи РЕБ в радіусі 30 км від позиції нашої артилерійської батареї, які були активні за останні 6 годин" або "Знайти всі мости через річку, що здатні витримати вагу танка і не були пошкоджені, згідно з останніми даними IMINT".

Справжня сила сучасного ІАЗ полягає у здатності до "тріангуляції" даних — підтвердження інформації з одного джерела даними з двох або більше незалежних джерел різного типу. Наприклад, повідомлення в Telegram (OSINT) про скупчення техніки стає набагато ціннішим, коли воно підтверджується супутниковим знімком (IMINT) та перехопленою радіограмою (SIGINT) з того ж району. Аналітик, що працює з ізольованими системами, змушений вручну запитувати кожну з них, експортувати дані та намагатися їх зіставити. Це повільно, неефективно та схильно до помилок. Сучасна архітектура повинна автоматизувати цей процес. Це вимагає переходу від традиційних, розрізнених баз даних до уніфікованої архітектури, такої як модель "Lakehouse". Ця модель поєднує масштабованість та гнучкість озера даних (для зберігання сирих,

неструктурованих даних) з функціями управління та транзакційними можливостями сховища даних (для структурованої, перевіреної інформації). Така система, спроектована для синтезу даних "з нуля", значно зменшує когнітивне навантаження на аналітика і прискорює цикл виробництва розвідданих, що є прямим мультиплікатором сили для розвідувальної спільноти.

Розділ 3: Архітектури стійкості: Порівняльний аналіз моделей зберігання даних для ОВУ

3.1. Фундаментальні принципи: Безпека, стійкість та інтероперабельність

Перед тим, як порівнювати конкретні технологічні моделі, необхідно встановити непорушні критерії, яким повинна відповідати будь-яка архітектура даних воєнного часу. Ці принципи є не опціями, а обов'язковими вимогами для виживання та ефективного функціонування держави в умовах повномасштабного конфлікту.

- **Безпека за задумом та нульова довіра (Security by Design & Zero Trust):** Базовим припущенням має бути те, що мережа вже скомпрометована. Не можна покладатися на концепцію безпечного "периметра". Кожен запит до даних, незалежно від його походження, повинен проходити автентифікацію та авторизацію. Дані мають бути зашифровані як під час зберігання (at rest), так і під час передачі (in transit). Архітектура "нульової довіри" означає, що довіра ніколи не є неявною і повинна постійно перевірятися.
- **Стійкість та резервування (Resilience & Redundancy):** Система повинна бути спроможною пережити як фізичні атаки на інфраструктуру (ракетні удари по дата-центрах), так і складні кібератаки (віруси-шифрувальники, DDoS-атаки). Це вимагає географічного розподілу інфраструктури, автоматизованих механізмів переключення на резервні системи (failover), а також надійних і регулярно тестованих протоколів резервного копіювання та відновлення (backup and recovery).
- **Інтероперабельність (Interoperability):** Дані повинні бути доступними для обміну між різними видами та родами військ, державними установами та, що критично важливо, міжнародними партнерами. Це унеможливлює використання пропрієтарних, закритих форматів та систем. Архітектура повинна базуватися на відкритих стандартах, API-орієнтованому підході до доступу та, за можливості, відповідати стандартам НАТО (наприклад, STANAGs) для забезпечення безшовної

взаємодії з союзниками.

3.2. Порівняльний аналіз моделей зберігання

Кожна модель зберігання даних має свої переваги та недоліки, які необхідно оцінювати крізь призму вищезазначених принципів та реалій війни.

- **Локальні сервери (On-Premise Servers):**
  - *Опис:* Традиційна модель, за якої сервери та системи зберігання даних розміщуються у власних або орендованих дата-центрах на території країни.
  - *Аналіз:* Ця модель забезпечує максимальний фізичний контроль над обладнанням та даними. Однак у контексті війни це перетворюється на її найбільшу слабкість. Централізований дата-центр стає очевидною та пріоритетною ціллю для ракетних ударів та диверсійних дій. Приклади ударів по урядових будівлях та об'єктах критичної інфраструктури в Києві та інших містах доводять цю вразливість. Масштабування таких систем є повільним, дорогим і вимагає значних капіталовкладень. Ця модель може бути виправданою лише для невеликих, повністю ізольованих (air-gapped) систем, що зберігають найсекретнішу інформацію, яка ніколи не повинна підключатися до зовнішніх мереж.
- **Приватна хмара (Private Cloud, напр., на базі OpenStack):**
  - *Опис:* Хмарне середовище, розгорнуте для ексклюзивного використання однією організацією. Воно може бути розміщене як у власному дата-центрі, так і в дата-центрі довіреного стороннього провайдера.
  - *Аналіз:* Пропонує кращу гнучкість, автоматизацію та ефективність використання ресурсів порівняно з традиційними локальними серверами. Однак вона все ще страждає від обмеженої географічної стійкості, якщо не спроектована спеціально для цього (що є дуже дорогим). Навантаження на управління та підтримку такої інфраструктури залишається значним. Приватна хмара може бути проміжним рішенням, але вона не вирішує фундаментальної проблеми фізичної вразливості в межах однієї країни.
- **Публічна хмара (Public Cloud, напр., AWS, Microsoft Azure, Google Cloud):**
  - *Опис:* Використання інфраструктури та сервісів глобальних хмарних провайдерів.
  - *Аналіз:* Ця модель стала справжнім "гейм-чейнджером" для стійкості української держави. Вона пропонує практично необмежену масштабованість за вимогою, неперевершений рівень географічного резервування (можливість зберігати дані та запускати сервіси в десятках регіонів по всьому світу) та надзвичайно складний і багаторівневий захист, який будь-якій окремій державі вкрай важко і дорого відтворити. Стратегічне рішення про міграцію критично важливих

державних реєстрів та систем у публічні хмари на початку вторгнення стало одним з ключових факторів забезпечення безперервності функціонування уряду. Це рішення змусило переосмислити саму концепцію "суверенітету даних". Традиційно він асоціювався з фізичним розташуванням сервера в межах кордонів країни. Війна довела, що такий підхід є вразливістю, а не силою. Справжній суверенітет — це безперервна здатність контролювати свої дані та отримувати до них доступ. Дані, що зберігаються в зашифрованому вигляді в дата-центрі у Франкфурті, доступ до яких маєте лише ви, є більш "суверенними", ніж дані на сервері в Києві, який може бути знищений ракетою. Цей зсув парадигми має величезні наслідки для національної IT-політики, міжнародного права та оборонного планування, роблячи міжнародні канали зв'язку та цифрові ланцюги постачання елементами національної безпеки.

- **Гібридна хмара (Hybrid Cloud):**
  - *Опис:* Комбінація локальної інфраструктури (або приватної хмари) з публічною хмарою, де обидва середовища працюють узгоджено.
  - *Аналіз:* Це найбільш реалістична, гнучка та ефективна модель для ІАЗ ОУВ. Вона дозволяє досягти оптимального балансу між безпекою та стійкістю. Найбільш чутливі дані (наприклад, дані про агентурні мережі) можуть зберігатися в високозахищеній локальній системі, тоді як публічна хмара може використовуватися для завдань, що вимагають великих обчислювальних потужностей та масштабування (наприклад, обробка OSINT, тренування моделей ШІ), для розміщення публічних сервісів, а також як платформа для аварійного відновлення (Disaster Recovery).

3.3. Глибокий аналіз технологій баз даних

Вибір конкретної технології бази даних залежить від типу даних та завдань, які необхідно вирішити.

- **Реляційні (SQL, напр., PostgreSQL):** Найкращий вибір для структурованих даних, що вимагають суворої узгодженості (consistency) та транзакційної надійності (ACID).
  - *Сценарій використання:* Управління кадровим обліком військовослужбовців, облік матеріально-технічних засобів, ведення офіційних реєстрів пошкодженого майна, фінансові системи.
- **NoSQL - Документні (напр., MongoDB):** Ідеально підходять для напівструктурованих даних, схема яких може часто змінюватися. Дозволяють зберігати складну, вкладену інформацію в одному документі (наприклад, у форматі JSON).
  - *Сценарій використання:* Зберігання розвідувальних звітів, де кожен звіт може мати різний набір полів; каталогізація даних з різних сенсорів.

- **NoSQL - Ключ-значення (напр., Redis):** Використовуються для високошвидкісного кешування та додатків, що вимагають мінімальної затримки.
    - *Сценарій використання:* Зберігання тимчасових тактичних даних у системах управління боєм для забезпечення миттєвого доступу; кешування часто запитуваних даних для зменшення навантаження на основну базу даних.
- **Графові (напр., Neo4j):** Спеціалізовані бази даних для аналізу зв'язків та відносин між об'єктами. Вони розглядають дані не як таблиці, а як мережу вузлів та ребер.
    - *Сценарій використання:* Побудова та аналіз російських командних структур (хто кому підпорядковується); виявлення ключових вузлів у мережах впливу та дезінформації; відстеження ланцюгів постачання компонентів для ворожої військової техніки.

Таблиця 3.1: Матриця відповідності моделей зберігання даних для завдань ІАЗ у воєнний час

Модель зберігання	Масштабованість	Безпека (Контроль)	Латентність (Затримка)	Стійкість (до фіз. атак)	Інтероперабельність (НАТО)	Вартість (ТСО)	Основний сценарій використання в ІАЗ
Локальні сервери (On-Premise)	Низька, повільна	Максимальна (фізична)	Низька (локальна)	Дуже низька	Низька (ізольовані системи)	Висока	Зберігання даних особливої державної таємниці в ізольованих (air-gapped) системах.

Приватна хмара	Середня	Висока	Низька-середня	Низька (якщо в межах країни)	Середня	Дуже висока	Захищене середовище для обробки чутливих даних відомств, що вимагає гнучкості хмари.
Публічна хмара (GovCloud)	Дуже висока, еластична	Висока (логічна, криптографічна)	Середня (залежить від регіону)	Дуже висока (глобальна інфраструктура)	Висока (стандартизовані API)	Середня (Pay-as-you-go)	Основна платформа для державних реєстрів, аналітики Big Data (OSINT), аварійного відновлення.
Гібридна хмара	Висока	Оптимальний баланс	Гнучка	Висока	Висока	Гнучка	Найбільш універсальна

							модель: чутливі дані локально, масштабовані обчислення та стійкість у хмарі.
Озеро даних (на S3/Blob)	Практично безмежна	Висока (через IAM, шифрування)	Висока (для сирих даних)	Дуже висока	Висока	Низька (за зберігання)	Централізоване сховище для всіх типів сирих даних (OSINT, IMINT, SIGINT) для подальшої обробки.
Графова БД (у хмарі)	Висока	Висока	Низька (для запитів зв'язків)	Дуже висока	Висока	Середня	Аналіз мереж, командних структур, ланцюгів постач

							ання та виявлення прихованих зв'язків.

Розділ 4: Практичні кейси з передової: Застосування принципів зберігання даних в бойових та стратегічних операціях

Теоретичні моделі набувають сенсу лише тоді, коли їх можна застосувати до реальних операційних завдань. Наступні кейси з досвіду російсько-української війни ілюструють, як правильний вибір архітектури зберігання даних безпосередньо впливає на ефективність на полі бою та стійкість держави.

4.1. Тактична перевага: Екосистема "Кропива" та "Дельта"

- **Проблема:** Забезпечення спільної, актуальної та достовірної картини поля бою на тактичному рівні (відділення, взвод, рота, батальйон) в умовах нестабільного або відсутнього зв'язку.
- **Дані та архітектура:** Цей кейс є блискучим прикладом гібридної, дворівневої архітектури, що поєднує децентралізовану стійкість на "краю" (edge) з централізованою аналітичною потужністю в ядрі.
    - **"Кропива":** Ця система працює на планшетах та смартфонах окремих підрозділів. Дані (позиції ворога, виявлені цілі, розташування дружніх сил) зберігаються локально на пристрої, найчастіше у простій та надійній вбудованій базі даних, такій як SQLite. Обмін даними між пристроями відбувається напряму (peer-to-peer) через тактичні радіостанції з низькою пропускною здатністю. Це децентралізована модель, оптимізована для роботи в умовах відключення від глобальної мережі (disconnected environments). Вона є надзвичайно стійкою, оскільки вихід з ладу одного елемента не впливає на роботу інших.
    - **"Дельта":** Ця система виконує роль центральної нервової системи та

стратегічного ядра. Вона агрегує дані, що надходять з окремих інсталяцій "Кропиви" (коли з'являється зв'язок), а також з безпілотників, супутників, радарів та інших джерел. Ці дані завантажуються у хмарну інфраструктуру, де зберігаються у централізованій базі даних (ймовірно, комбінації PostGIS для геопросторових даних та NoSQL бази даних для іншої розвідувальної інформації). "Дельта" надає єдину оперативну картину для вищих рівнів командування, дозволяючи проводити аналіз та планування на оперативно-стратегічному рівні.

- **Урок щодо зберігання даних:** Ця екосистема демонструє ідеальну реалізацію гібридної архітектури. Стійкий, децентралізований "край" для тактичних користувачів, який періодично синхронізується з масштабованим, централізованим хмарним ядром для стратегічного аналізу. Це дозволяє поєднати тактичну автономність та швидкість з централізованим командуванням та контролем.

4.2. Синтез OSINT: Ідентифікація та ураження високоцінних цілей

- **Проблема:** Як перетворити інформаційний "шум" з мільйонів повідомлень у соціальних мережах на перевірену, точну ціль для удару високоточною зброєю, наприклад, HIMARS.
- **Дані та архітектура:** Цей процес ілюструє багатошарову стратегію зберігання даних, де кожен шар виконує свою функцію.
    1. **Поглинання (Ingestion):** Потужний конвеєр даних (data pipeline) автоматично збирає повідомлення, фото та відео з тисяч Telegram-каналів, пабліків у Twitter та інших відкритих джерел. Ці сирі, неструктуровані дані завантажуються "як є" у хмарне озеро даних (наприклад, AWS S3 або Azure Blob Storage). Це дешеве та безмежно масштабоване сховище.
    2. **Обробка (Processing):** На даних в озері запускаються моделі штучного інтелекту та машинного навчання (AI/ML). Вони виконують розпізнавання іменованих сутностей (виявляють номери військових частин, типи техніки, імена), аналіз тональності та, що найважливіше, намагаються визначити геолокацію за характерними ознаками на фото чи відео.
    3. **Синтез та верифікація (Fusion & Verification):** Видобуті напівструктуровані дані (наприклад, "ймовірно, ЗРК 'Бук' в районі з координатами X, Y") завантажуються в аналітичну базу даних. Аналітик-людина виконує запити до цієї бази, перевіряючи дані OSINT з іншими джерелами: замовляє супутниковий знімок цього району (IMINT), що зберігається в тому ж озері даних, та перевіряє наявність даних SIGINT з цього району, що зберігаються в окремій, високозахищеній базі даних.
    4. **Розповсюдження (Dissemination):** Після того, як ціль верифікована з високим рівнем впевненості, "пакет цілі" (точні координати, час виявлення, тип цілі, рівень

достовірності) зберігається у базі даних з низькою затримкою (low-latency database), до якої мають доступ системи управління вогнем.
- **Урок щодо зберігання даних:** Цей кейс демонструє абсолютну необхідність багатошарової архітектури: озеро даних для дешевого зберігання сировини, аналітичні бази даних для кураторської, обробленої інформації, та високошвидкісні бази даних для передачі оперативних даних. Він також підкреслює дилему "Достовірність-Швидкість" (Veracity-Velocity): швидка обробка OSINT є важливою, але без ретельної верифікації вона може призвести до фатальних помилок.

4.3. Цивільний фронт: Управління ВПО та пошкодженнями інфраструктури

- **Проблема:** Надання соціальних послуг мільйонам внутрішньо переміщених осіб та систематичний збір і облік даних про пошкодження майна та інфраструктури для майбутніх репарацій та відбудови.
- **Дані та архітектура:** Ключовим прикладом тут є державний застосунок "Дія". Громадяни можуть подавати повідомлення про пошкоджене майно, додаючи фотографії, документи та геолокаційні дані. Ця інформація є юридично значущою та містить персональні дані. Тому вона повинна зберігатися у високозахищеній, транзакційній базі даних (найімовірніше, хмарній інстанції PostgreSQL або аналогічної реляційної СУБД).
- **Урок щодо зберігання даних:** Не всі дані воєнного часу призначені для ураження цілей. Для завдань цивільної адміністрації пріоритетами є цілісність даних, безпека, захист персональних даних та можливість повного аудиту. Традиційна реляційна база даних, з її гарантіями ACID (Atomicity, Consistency, Isolation, Durability — Атомарність, Узгодженість, Ізольованість, Довговічність), є абсолютно правильним вибором для таких завдань. Це доводить, що не існує єдиного "найкращого" рішення для зберігання; вибір технології завжди повинен диктуватися конкретним завданням.

4.4. Кіберстійкість: Виживання після атаки на Viasat та подальші кроки

- **Проблема:** Забезпечення безперервності операцій (continuity of operations), коли комунікаційна та інформаційна інфраструктура перебуває під прямими кінетичними та кібератаками.
- **Дані та архітектура:** Масована кібератака на супутникову мережу Viasat на самому початку повномасштабного вторгнення, яка вивела з ладу системи зв'язку

українських військових, стала жорстоким уроком про вразливість централізованих систем. Урок полягає в необхідності архітектурної стійкості на всіх рівнях, включаючи зберігання даних.

- **Урок щодо зберігання даних:** Цей кейс фокусується на оборонних стратегіях зберігання даних, які є критично важливими для виживання:
    - **Незмінні резервні копії (Immutable Backups):** Використання функцій хмарних сховищ (таких як S3 Object Lock або Azure Immutable Blob Storage) для створення резервних копій за принципом "один раз записати, багато разів читати" (WORM - Write-Once-Read-Many). Такі копії неможливо змінити або видалити (навіть адміністратором) протягом встановленого періоду, що робить їх невразливими до вірусів-шифрувальників.
    - **Географічний розподіл (Geographic Distribution):** Реплікація критично важливих баз даних та сховищ у кількох географічно віддалених регіонах (наприклад, Центральна Європа, Західна Європа, Північна Америка). Це гарантує, що вихід з ладу або недоступність одного регіону (через технічний збій, кібератаку або навіть пошкодження магістральних кабелів) не призведе до повної втрати доступу до даних.
    - **Регулярні знімки та тренування з відновлення:** Важливо не просто мати резервні копії, а й регулярно тестувати процес відновлення з них. Необхідно проводити навчання (disaster recovery drills), щоб переконатися, що у кризовій ситуації процедури відновлення спрацюють, а персонал знає, що робити.

Розділ 5: Зміцнення цифрового тилу: Найкращі практики для безпечного та інтероперабельного управління даними

Створення стійкої та ефективної системи ІАЗ вимагає не лише правильного вибору архітектури, але й дотримання суворих операційних процедур та найкращих практик на кожному етапі життєвого циклу даних.

5.1. Життєвий цикл даних у ворожому середовищі

Безпека повинна бути інтегрована в кожен етап роботи з даними, від моменту їх створення до моменту їх знищення.

- **Безпечне поглинання (Secure Ingestion):** Дані повинні бути зашифровані на самому джерелі (наприклад, на БПЛА або пристрої агента) і передаватися до сховища через захищені канали з використанням наскрізного шифрування (end-to-end encryption). Це унеможливлює їх перехоплення та прочитання під час передачі.
- **Безпечна обробка (Secure Processing):** Для аналізу надзвичайно чутливих даних слід розглядати технології конфіденційних обчислень (confidential computing). Ці технології дозволяють обробляти дані в зашифрованому вигляді навіть в оперативній пам'яті сервера, створюючи захищений анклав, до якого не має доступу навіть хмарний провайдер.
- **Безпечне зберігання (Secure Storage):** Шифрування даних при зберіганні (encryption at rest) з використанням надійних алгоритмів (наприклад, AES-256) є обов'язковим. Ключовим елементом є надійне управління ключами шифрування (Key Management System, KMS). Ключі повинні зберігатися окремо від даних і мати суворий контроль доступу.
- **Безпечне розповсюдження (Secure Dissemination):** Доступ до даних повинен надаватися за принципом мінімальних привілеїв. Необхідно впроваджувати моделі контролю доступу на основі ролей (Role-Based Access Control, RBAC) та атрибутів (Attribute-Based Access Control, ABAC). RBAC визначає доступ на основі ролі користувача (наприклад, "аналітик", "оператор"), тоді як ABAC дозволяє створювати більш гранулярні правила (наприклад, "дозволити доступ аналітику з 93-ї бригади лише до даних, що стосуються його зони відповідальності та мають гриф не вище 'Таємно'").
- **Безпечне архівування та знищення (Secure Archival & Deletion):** Необхідно мати чіткі політики щодо термінів зберігання різних категорій даних. Після закінчення терміну зберігання дані повинні бути не просто видалені, а криптографічно знищені (crypto-shredding), коли видаляється ключ шифрування, що робить зашифровані дані невідновними.

5.2. Впровадження архітектури нульової довіри

Перехід від застарілої моделі "фортеці та рову", де все всередині периметра вважається довіреним, до моделі нульової довіри (Zero Trust) є критично важливим. Нульова довіра базується на принципі "ніколи не довіряй, завжди перевіряй".

- **Ідентифікація та управління доступом (Identity and Access Management, IAM):** Кожен користувач, пристрій та додаток повинен мати унікальну цифрову ідентичність. Доступ до ресурсів, включаючи бази даних, надається на основі суворих політик IAM.
- **Багатофакторна автентифікація (Multi-Factor Authentication, MFA):** MFA має бути обов'язковою для доступу до всіх чутливих систем та баз даних. Одного лише пароля

недостатньо.

- **Мікросегментація мережі (Network Micro-segmentation):** Мережа розбивається на невеликі, ізольовані сегменти. Навіть якщо зловмисник отримує доступ до одного сегмента, він не зможе вільно пересуватися по всій мережі та отримати доступ до баз даних в інших сегментах.
- **Безперервний моніторинг:** Усі дії з даними (запити, зміни, видалення) повинні реєструватися та аналізуватися в режимі реального часу для виявлення аномальної поведінки.

5.3. Досягнення інтероперабельності з партнерами

Ефективна співпраця з міжнародними партнерами є мультиплікатором сили. Для цього необхідно забезпечити технічну можливість безшовного та безпечного обміну даними.

- **Стандартизовані формати даних:** Використання загальновизнаних, не пропрієтарних форматів даних (таких як JSON, XML, GeoJSON) спрощує інтеграцію.
- **Безпечні API (Application Programming Interfaces):** Розробка добре документованих та захищених API є сучасним стандартом для обміну даними між системами. Це дозволяє партнерам отримувати доступ до необхідних даних, не отримуючи прямого доступу до внутрішніх баз даних.
- **Дотримання стандартів НАТО:** Адаптація до релевантних стандартів НАТО (STANAGs) у сферах обміну тактичними даними (напр., Link 16), форматування повідомлень та геопросторових даних є ключовим для забезпечення інтероперабельності на полі бою.

Розділ 6: Майбутнє інформаційного домінування: Новітні технології та стратегічні імперативи

Війна є каталізатором технологічних інновацій. Методи та технології, що сьогодні є передовими, завтра стануть стандартними. Для збереження інформаційної переваги Україна повинна не лише впроваджувати існуючі найкращі практики, але й дивитися у майбутнє.

6.1. ШІ/МЛ та майбутнє автоматизованого аналізу

Величезні масиви даних, зібрані під час війни, є безцінним ресурсом для тренування наступного покоління моделей штучного інтелекту та машинного навчання (AI/ML). Ці моделі зможуть автоматизувати значну частину аналітичної роботи:

- **Автоматичне розпізнавання цілей (Automated Target Recognition, ATR):** Моделі, натреновані на мільйонах супутникових знімків та відео з БПЛА, зможуть в режимі реального часу ідентифікувати типи ворожої техніки з високою точністю.
- **Предиктивний аналіз:** Аналізуючи історичні дані про переміщення військ, логістику та комунікації, ШІ зможе прогнозувати ймовірні напрямки майбутніх атак противника.
- **Виявлення дезінформації:** Моделі зможуть автоматично аналізувати інформаційні потоки для виявлення скоординованих кампаній ІПСО, фейкових новин та ботоферм.
- **Вимоги до зберігання:** Це вимагатиме ще більш масштабованих та високопродуктивних рішень для зберігання, таких як паралельні файлові системи (напр., Lustre) або об'єктні сховища з високою пропускною здатністю, які будуть розташовані поруч з потужними GPU-кластерами для тренування моделей.

6.2. Федеративне навчання та децентралізована розвідка

Однією з найбільших проблем у співпраці розвідок є небажання ділитися сирими, чутливими даними через ризик компрометації джерел. Технологія федеративного навчання (Federated Learning) пропонує революційне вирішення цієї проблеми. Вона дозволяє кільком організаціям (або навіть країнам-союзникам) спільно тренувати одну модель ШІ, не передаючи одна одній свої дані. Кожна сторона тренує модель на своїх локальних даних, а потім до центрального сервера надсилаються лише оновлення ваг моделі, а не самі дані. Це дозволяє створити значно потужнішу модель, використовуючи колективний досвід, при цьому зберігаючи повну конфіденційність первинної інформації.

6.3. Квантова загроза та постквантова криптографія

Хоча повноцінні квантові комп'ютери, здатні зламати сучасні алгоритми шифрування (такі як RSA та ECC), ще не створені, ця загроза є реальною в довгостроковій перспективі. Зловмисник може вже сьогодні перехоплювати та зберігати зашифровані дані, розраховуючи розшифрувати їх у майбутньому, коли з'являться відповідні технології. Це становить особливу загрозу для даних, які повинні залишатися секретними протягом десятиліть (дані про агентурні мережі, стратегічні плани, розробки озброєнь). Тому вже

сьогодні необхідно починати планування переходу на алгоритми постквантової криптографії (Post-Quantum Cryptography, PQC) — криптографічні системи, які вважаються стійкими до атак як класичних, так і квантових комп'ютерів.

6.4. Стратегічні імперативи для України

На основі проведеного аналізу можна сформулювати низку високорівневих стратегічних рекомендацій для органів влади та управління України:

1. **Інвестувати в людський капітал:** Найсучасніші технології є марними без кваліфікованих аналітиків, інженерів даних та фахівців з кібербезпеки, які можуть їх ефективно використовувати. Необхідно розбудовувати національну систему підготовки та утримання таких фахівців.
2. **Дотримуватися стратегії "Cloud-First", але "Hybrid-by-Design":** Продовжувати активно використовувати стійкість, масштабованість та інноваційність глобальних публічних хмар, але робити це продумано. Зберігати суверенний контроль над найбільш критичними даними та процесами, реалізуючи гнучку гібридну модель.
3. **Сприяти культурі обміну даними:** Руйнувати інституційні та відомчі "силоси", що перешкоджають обміну інформацією. Успіх на полі бою залежить від міжвідомчого та міждоменного синтезу даних. Необхідно створювати як технічні, так і організаційно-правові механізми для безпечного та ефективного обміну даними.
4. **Планувати для наступної війни:** Інформаційна війна не закінчиться з припиненням бойових дій. Противник буде вчитися та адаптуватися. Україна, яка продемонструвала світові приклад інновацій та стійкості, повинна продовжувати експериментувати, впроваджувати нові технології та розвивати свої асиметричні переваги, щоб зберегти та зміцнити своє інформаційне домінування.