ПУБЛІЧНА БІБЛІОТЕКА ПО ВІЙСЬКОВІЙ ТЕХНІЦІ ПРОТИВНИКА ДЛЯ НАУКОВИХ ДОСЛІДЖЕНЬ

С.Є. Євсеєв
Івано-Франківський національний технічний університет нафти і газу
sergiy@yevseyev.ua

Повномасштабна агресія проти України знову підкреслила значущість та важливість захисту критичної інфраструктури від безпілотних літальних апаратів (БПЛА) різного типу: як керованих, так і таких, що працюють у повністю автоматичному режимі.

До лютого 2022 року вже було зафіксовано декілька значущих атак за допомогою БПЛА на промислові та військові об'єкти:

Атаки на нафтові об'єкти Саудівської Аравії (2019 рік). У вересні 2019 року була вчинена масштабна атака на об'єкти нафтової компанії Saudi Aramco. Було пошкоджено об'єкти в Абкаїку та Хурайсі. Хоча спочатку заяви вказували на інвольованість БПЛА, пізніше стало відомо, що було використано як безпілотники, так і крилаті ракети. Відповідальність за атаку взяли на себе йеменські хусити, але багато країн вважали, що Іран стоїть за цією операцією.

Атаки на військові бази в Сирії. Під час громадянської війни в Сирії БПЛА були активно використані для проведення розвідки та нанесення ударів по різноманітних цілях. В основному такі атаки відбувалися на військові бази, що контролювалися силами президента Асада або російськими військовими.

*Атаки на військові об'єкти в Вірменії та Азербайджані (2020 рік)***.** Під час конфлікту в Нагірному Карабасі у 2020 році обидві сторони активно використовували безпілотники. Особливо ефективною виявилася ударна авіація Азербайджану, яка завдала серйозних втрат військовим Вірменії.

Ці та інші атаки БПЛА демонстрували, наскільки ці технології можуть бути ефективними та небезпечними в сучасних військових конфліктах і як вони можуть змінювати баланс сил під час активних бойових дій

Наша війна виключенням не стала: супротивник активно використовує різні типи апаратів, які люди вже прозвали «дронами», «мопедами» та ін. Особливо грізною стали баражуючі боєприпаси типу «Shahed 136», «Ланцет», «Куб-БЛА», БПЛА систем управління тактичної ланки типу «Орлан», «Картограф», «Форпост», ударні «Оріони» та ін.

Росте номенклатура безпілотників, змінюються і практичні засоби їх застосування: від простого спостереження до «виманювання» ППО. Залучають їх і до безпосередніх атак, і до допомоги пораненим (коли з малих БПЛА скидають ліки для поранених бійців та показують безпечний маршрут відходу) та ін.

Відповідно, має змінюватись і технологія ідентифікації та знищення БПЛА, як зазначав український вчений С. О. Перепеліцин ще у 2020 році [1]. Він вказав на необхідність використання блоків нейромережевого аналізу для протистояння загроз БПЛА, оскільки розвиток т.з. «нейромереж» набув в останні роки неабиякого значення – на це вплинуло, звичайно, зростання обчислювальних потужностей та зниження їх вартості.

Нейромережі навчились виконувати складні завдання: від підтримки спілкування на рівні, близьким до людського, генерації картинок по текстовому опису до постановки діагнозів хворим чи грі на біржі.

Відповідно, виникає очевидне бажання використати їх у військовій справі. По всьому світу [2, 3, 4, 5] вчені досліджують різні методи ідентифікації та

знешкодження БПЛА, але використовують або математичні абстракції (моделі), або досліджують 1-2 типи відомих БПЛА.

Будь-який нейромережевий аналіз можливий лише коли у дослідника існує доступ до спеціальним чином підготовленого масиву даних. Наприклад, відоме комерційне LLM-рішення, ChatGPT від компанії OpenAI використовувало величезний масив даних для навчання. Цей масив містить текст з різних джерел з Інтернету: книги, веб-сайти, статті та інше. Точні деталі та об'єми цього масиву є комерційною таємницею OpenAI, але він був настільки обширний, що дозволив навчити модель різним мовам, фактам, контексту та іншим аспектам комунікації на різні теми і навіть проходити тест Тьюрінга.

За оцінками видання Medium [6], розмір датасету (бази для навчання) поточної версії GPT, GPT 4, склав біля 1 ПБ даних та 1.8 трильйону параметрів.

Як відомо, нейромережі складаються з великої кількості «нейронів», які з'єднані між собою. Кожне з'єднання має вагу, а кожен нейрон може мати своє зміщення (bias). Ці ваги та зміщення називаються «параметрами» нейромережі.

Під час процесу навчання мета полягає в оптимізації цих параметрів таким чином, щоб нейромережа могла найкраще відтворювати бажаний вихід на основі вхідних даних. Наприклад, якщо у нас є нейромережа, яка намагається розпізнати котів на фотографіях, параметри нейромережі будуть коригуватися таким чином, щоб коли мережа бачить фотографію кота, вона видає відповідь, що це кіт, а не собака або який-небудь інший предмет чи живий організм.

Оптимізація параметрів здійснюється за допомогою алгоритмів, таких як градієнтний спуск, які поступово коригують вагу та зміщення на основі помилок, які робить мережа протягом навчання.

Україна, яка знаходиться у гострій (активній) фазі бойових дій з супротивником, котрий переважає кількісно, має віднаходити способи протидії ворожим силам. Наразі найбільш поширеним використанням БПЛА у ЗСУ є:

Ідентифікація ворожих сил. БПЛА пролітає заданим маршрутом і оператор отримує відеозапис чи набір фотографій, по яких або в ручному, або напівавтоматичному режимі бійці пробують визначити, чи є по маршруту ворог, чим він оснащений (кількість та чим саме);

Ураження військових сил за допомогою людини-оператора. Ударний дрон виводиться на ціль вручну, ідентифікації об’єкта та прийняття рішення про знищення приймає людина;

Ураження військових сил в автоматичному режимі. Ударний дрон виводиться на ціль автоматично та рішення по ураження приймає бортова автоматика (в переважній більшості – по заходу на потрібні координати чи візуальну ідентифікацію);

Нейромережі можуть використані в *ідентифікації* цілей (або індивідуальної цілі дрона), але виникає потреба в «сирих» (raw) даних, з яких дослідник може згенерувати датасет для навчання.

І в цьому в українських дослідників є колізія: ім дуже важко (або, навіть, неможливо) отримати достатню кількість різнопланових даних (аудіо- та візуальних) для аналізу, оскільки монополістом таких даних є держава та її відповідні органи.

Дослідникам (особливо з непрофільних навчальних закладів) доводиться звертатись до Міністерства оборони або до Міністерства цифрової трансформації, очікувати підтвердження запитів, проходити численні перевірки – що затягує час

аналізу і не факт, що запит буде задоволений або отримані дані підійдуть для конкретного дослідження.

Відповідно, лише нечисленні «профільні» структури мають доступ до даних та можуть використовувати їх у власних розробках, що дуже звужує можливості національної ІТ-галузі по продукуванню рішень для потреб військових. Але чи правильно це? Може, Державі треба зайняти більш проактивну позицію, відкрити публічну (доступну для громадян України, ВНЗ відповідної акредитації) електронну бібліотеку з аудіовізуальними та / або РЛС-даними по живій силі та техніці (які вже не становлять військової таємниці).

Звичайно, підготовка такої бібліотеки на національному рівні вимагатиме ресурсів, часу та якісного регулярного оновлення. Чому це важливо:

Тільки держава має доступ до всіх даних, які збирають Збройні сили у всіх їх повноті. Відповідно, лише держава здатна забезпечити сталий розвиток такої бібліотеки з даними, які будуть нести наукову цінність;

Використання великої кількості попередньо класифікованих даних *дозволяє вийти на наступний якісний рівень* як спеціалізованих нейромереж для військових, так і для непрофільних, може, навіть, часом і аматорских рішень.

Постійне оновлення даних буде корисне і «профільним» освітнім закладам та підприємствам, оскільки *дозволить підвищити точність розпізнавання військової техніки*, дозволить ідентифікувати «прогалини» у власних датасетах та коригувати наповнення в майбутньому.

Аматорські рішення теж не треба відкидати – так, звичайно, багато з них будуть викликати посмішку у професійних військових розробників або думку: «Ну, ми вже це проходили». Може, і проходили, але волонтерів в ІТ – величезна кількість і у них відсутній обмін досвідом з закритими державними інституціями. Вони не мають доступу на полігони, спілкуються лише з друзями з військових частин, але мають відповідні знання, аби пропонувати щось нове. Навіть якщо з 100 запропонованих «аматорами» ідей 99 виявиться сміттям, а 1 – гарною та втіленою у життя, це вже буде маленькою перемогою, оскільки держава не витрачатиме на R&D ані копійки.

Наприклад, можливість для «аматорів» поглянути на проблему візуальної ідентифікації БПЛА по його відеозображенню, ще і в умовах дощу / туману, з дешевих камер (наприклад, 3-4 ракурси одночасно), у поєднанні з інфрачервоним зображенням може призвести до прориву у певній предметній області.

Які ж саме дані варто включити до бібліотеки:

Зображення об’єкта з багатьох ракурсів, при різних погодних умовах на один тип об’єктива;

Зображення об’єкта з різних типів об’єктивів;

Аудіо-відбиток об’єкта;

Інфрачервоний відбиток об’єкта;

Дані про електромагнітне випромінювання (якщо воно є), можливість перехоплення керування;

Традиційне застосування об’єкта (наприклад, якщо система помилково визначить БПЛА, як танк у повітрі – такого не може бути);

Зображення об’єкту з різних відстаней, під час руху, маскування та ін.

Тактико-технічні характеристики об’єкта, типові обмеження та супутні об’єкти (наприклад, якщо виявлено пускові установки від ЗРК – десь має бути і командний пункт)

Відомі (відкриті для публікації) моделі, на базі яких можна створити власну або покращити існуючу.

Держава має віддати належне простому факту, що у талановитих людей єдина зброя, якою вони володіють на професійному рівні – це комп'ютер та вміння програмувати. Вже менша кількість здатна втілити якісь рішення «в залізі» і ще менша – побудувати щось, що дійсно буде працювати і приносити користь. Відповідно, і прогрес в цьому випадку, в першу чергу, буде йти зі сторони розробки програмного забезпечення, комплексів систем управління, особливо для індивідуальних дронів чи систем протидії «роям» дронів.

Вже існують ідеї по ідентифікації «роїв» дронів на базі ефекту Доплера [4], вчені пробують використати математичну модель «переслідування» [5], але ці теоретичні моделі досить відірвані від практики, відповідно – потребують перевірки. Традиційний науковий ланцюжок пізнання «теорія – серія експериментів – практичні підтвердження або спростування теорії» під час активних бойових дій є дуже важким у реалізації, оскільки потребує ресурсів, яких може не бути у пересічного дослідника.

Тому, крім аудіовізуальної чи радіолокаційної інформації слід ще зберігати і практичну інформацію по всім взірцям ворожої техніки: практичний запас ходу, швидкість, дальність, можливість контролю, специфіку елементів керування, у випадку з наземною технікою – варіанти кустарних модифікацій (приварені «мангали» та ін), сліди від траків – все те, що може спотворити аналіз та призвести до неефективних рішень.

Список літературних джерел

1 С. О. Перепеліцин. Система захисту від загроз удару БПЛА із використанням блоків нейромережевого аналізу // Наукоємні технології № 1(45), 2020, DOI: 10.18372/2310-5461.45.14579

2 Simeon Okechukwu Ajakwe. Radicalization of Airspace Security: Prospects and Botheration of Drone Defense System Technology / Simeon Okechukwu Ajakwe, Dong-Seong Kim, Jae-Min Lee // Journal of Intelligence, Conflict, and Warfare and Simon Fraser University, 2023. URL: https://journals.lib.sfu.ca/index.php/jicw/article/view/5274/4492

3 Kejie Yang. A Multi-drones Target Tracing Strategy Based on the Pursuit-Evasion Game Formula / Kejie Yang, Ming Zhu, Xiao Guo // 2022 China Automation Congress (CAC), DOI: 10.1109/CAC57257.2022.10054992

4 Megha Katana. Simulation of micro-doppler signatures of drones / Megha Katana, Brejesh Lall // 2023 IEEE International Conference on Acoustics, Speech, and Signal Processing Workshops (ICASSPW), DOI: 10.1109/ICASSPW59220.2023.10193632

5 Jennifer Simonjan. Reinforcement Learning-based Countermeasures against Attacking UAV Swarms / Jennifer Simonjan, Kseniia Harshina, Melanie Schranz // 2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSSIoT), DOI: 10.1109/DCOSS-IoT58021.2023.00103

6 GPT-4: Everything you want to know about OpenAI's new AI model // Medium.com, 2023. URL: https://medium.com/predict/gpt-4-everything-you-want-to-know-about-openais-new-ai-model-a5977b42e495