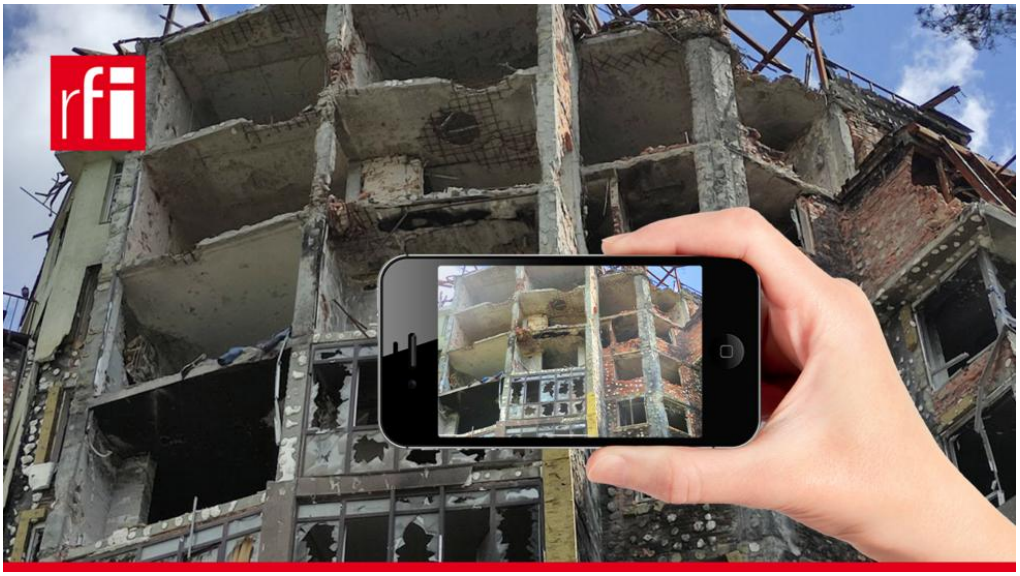
Через канали, чати та ігри. Хто і як вербує українських підлітків під час війни

Вони вербують українських підлітків і обіцяють гроші за фотографії та геолокацію стратегічних об'єктів й адміністративних будівель. А в Польщі збиралися платити криптовалютою за диверсії на залізничних шляхах, якими мала йти гуманітарна та військова допомога в Україну. Так працюють спецслужби РФ. Українська редакція RFI дізнавалась про популярні методи вербування дітей і про те, як убезпечити їх від ворожого впливу.



Через канали, чати та ігри. Хто і як вербує українських підлітків під час війни © RFI
Автор:Оксана Козлова

Наприкінці липня в Польщі викрили російську розвідувальну мережу. Про це повідомила Gazeta Polska. За інформацією Національної прокуратури та Агентства внутрішньої безпеки, це була найбільша російська розвідувальна мережа в історії країни. За звинуваченням у шпигунстві на користь російської розвідки затримали 15 осіб, яким загрожує до 10 років позбавлення волі. Учасники цієї мережі — росіяни, білоруси та українці.

Серед наших співвітчизників були й підлітки. Про цю деталь повідомила українка, яка проживає у Польщі, — голова правління Stand with Ukraine Foundation Наталія Панченко (*орфографія та пунктуація автора допису збережена. — Ред.*):

— З того, що мені відомо, серед учасників групи були неповнолітні українці. Припускаю, що завербували їх онлайн, і вони просто бігали робили якісь «маленькі задачки» за біткойни. Батьки одного з хлопців, якого тоді затримали, просили їм допомогти, бо не вірили у його причетність до справи, адже, за їх словами, їх син це: «спокійна дитина, мухи не обідить, з хати майже не виходив, за комп'ютером сидів». Коли я дізналась, у чому його звинувачують, відмовила. Бо знала, що при затриманні забрали всі його девайси, і розуміла, що якщо раптом його затримали випадково, то скоро випустять, якщо ж не випадково, то мені в цій справі робити нічого.

У травні правоохоронці викрили 17-річного жителя Харківської області, якого ще у січні завербував працівник ФСБ РФ. За його завданнями підліток збирав та передавав інформацію про пересування сил та засобів ЗСУ, що дислокуються у місті Вовчанськ.

А на початку серпня УСБУ в Харківській області затримало двох хлопців 18 та 20 років, які теж були інформаторами та корегувальниками РФ і наводили удари по Харкову.

Двох хлопців затримали у Харкові, вони збирали дані про українських військових © СБУ / Facebook

«Вони переміщувалися по території Харкова на велосипедах і знімали місця, де, на їхню думку, дислокуються українські військовослужбовці. У подальшому фігуранти відмічали ці локації на гугл-карті та відправляли скріншоти з відмітками до свого куратора з РФ. Співробітники СБУ затримали обох учасників групи «на гарячому» під час збору даних про дислокацію одного з підрозділів Сил оборони», — говорить речник управління СБУ в Харківській області Владислав Абдула.

Цим хлопцям повідомили про підозру. Їм загрожує до 12 років тюрми.

Цікавляться росіяни ще й станом адміністративних та військових споруд, їх обороноздатністю. За інформацією також відправляють дітей. Такий випадок стався у Київській області у травні. Там правоохоронці виявили неповнолітнього, якого завербував співробітник ФСБ РФ. Дитина, виконуючи завдання, які отримувала у Telegram, фотографувала військові та адміністративні споруди та передавала світлини.

Затриманим загрожує 12 років позбавлення волі © СБУ / Facebook

Прийоми і засоби спецслужб РФ

В СБУ говорять, що агресор робить багато спроб завербувати українців до збору розвідданих, організації диверсій на фронті та провокацій у тилу. Робити вони це можуть використовуючи тортури і шантаж, підкуп, втягування у співпрацю «втемну», і це працює як для дітей, так і для дорослих.

«Останній спосіб — особливо поширений для пошуку потенційних зрадників серед жителів умовно мирних областей. В такому випадку перший контакт із російським «рекрутером» може відбуватися у соціальній мережі або під час телефонної розмови. Вербувальник зазвичай видає себе за іншу особу, навіть може створювати враження справжнього патріота, який вільно спілкується українською мовою та доволі непогано обізнаний з нашою культурою і традиціями», — пояснюють в СБУ.

Зазвичай, непідготовлена людина не може розпізнати в новому знайомому співробітника спецслужби. Вербуванням займаються переважно досвідчені маніпулятори, які вміють грати на людських почуттях та слабкостях. Спочатку вони будуть схиляти співрозмовників до надання безневинних послуг, а потім вже поступово будуть їх підбурювати до злочинних дій, говорять в СБУ.

Як підлітки потрапляють в агентурну мережу

Варіантів затягнути до агентурних мереж у російських спецслужб може бути багато. Інколи вони можуть діяти через мобільні ігри та додатки і в ігровій формі виманювати геолокації та дані стратегічних об'єктів.

Наприклад, у травні минулого року українським дітям пропонували «пограти в квест». Учасники шукали так звані «коробки», в яких були віртуальні призи, що можна було обміняти на електронні гроші. В СБУ пояснили правила такої «гри»:

— Під час проходження маршруту діти здійснюють фотофіксацію місцевості, у тому числі об’єктів військової та критичної інфраструктури на території різних населених пунктів. Усю інформацію з геолокацій учасники квесту завантажують у базу ігрового додатку. При цьому доступ до адміністрування цього застосунку має підконтрольна спецслужбам рф ІТ-компанія, яка зареєстрована в одній з європейських країн і займається розповсюдженням інтерактивних платформ. Таким чином ворог «втемну», тобто без їх відома, використовував українських дітей для збору інформації про розташування стратегічно важливих об’єктів.

Тоді спецслужбам вдалося затримати двох підлітків із Жовтих Вод, що на Дніпропетровщині. Вони в Кіровоградській області фотографували блок-пости, елеватори та транспортні шляхи.

А от зараз дуже популярний спосіб вербування — це соціальні мережі, анонімні чати в месенджерах. Про це розповіла RFI Аліна Бондарчук, керівниця департаменту збору та моніторингу інформації Центру протидії дезінформації робочого органу РНБО України:

— Перше, на що варто звертати увагу і батькам, і підліткам, які вже, в принципі, самі за себе відповідають, це на месенджери, які мають анонімні канали, анонімні джерела інформації. Наприклад, той же Telegram — це небезпечна мережа, з якою ми радимо завершувати співпрацю. До 2020 року він був заблокований в РФ, та 18 червня 2020 року Роскомнадзор офіційно розблокував Telegram і у той час активно почали створюватись анонімні канали, канали пропаганди та воєнкорів. Тоді ж вони говорили, що «позитивно оцінюють висловлену засновником Telegram готовність протидіяти тероризму та екстремізму». Говорячи про тероризм, вони звичайно ж мали на увазі Україну.

Аліна Бондарчук, керівниця департаменту збору та моніторингу інформації Центру протидії дезінформації робочого органу РНБО України © Особистий архів Аліни Бондарчук

Потрапити у халепу дитина може, коли буде шукати спосіб заробити гроші. За словами Аліни Бондарчук, приваблюють дітей повідомлення на кшталт «робота 2000 доларів, навички не потрібні, тільки ваш телефон і час». І якщо дорослі розуміють усю абсурдність оголошення, то діти можуть відгукнутись на нього, бо до кінця не усвідомлюють, яку шкоду можуть завдати і собі, і оточуючим.

І якщо на мобільний додаток може відреагувати функція «батьківський контроль» та й вербувальник може залишити сліди у мережі, пройшовши різні етапи реєстрації, то в месенджерах зловмисник може залишитись абсолютно анонімним.

Де і навіщо відбувається вербування

Небезпека бути завербованим існує у будь-якому регіоні України. Але частіше ці випадки трапляються на прифронтових територіях, на прикордонні та в окупації. За словами Аліни Бондарчук, там ворогу потрібно володіти інформацією про ситуацію 24 години на добу. А от вербування українців в інших умовно безпечних регіонах можуть збільшуватись в залежності від інформації, якою володіє ворог, пояснює пані Аліна:

— Все залежить від задачі, яка поставлена РФ. Наприклад, там отримали інформацію, що до нас буде йти партія зброї, шлях пролягає конкретними регіонами України. Отже буде запит на людей в тих областях.

Запит — це пошук людей через чати, оголошення про роботу чи «звичайне» спілкування, яке начебто ні до чого не зобов'язує. Але в результаті людину вербують. А інколи ворог може прямо говорити, що йому потрібно. Як розповідає пані Аліна, одне зі своїх завдань спецслужби РФ у Запорізькій області намагалися виконати два місяці тому, розсилаючи повідомлення «міняємо ЗСУ на долари»:

— Так, пропонували людям здавати позиції наших ЗСУ. Цю інформацію ми зафіксували і передали. Але ж ми розуміємо, що на пропозицію міг хтось і погодитись.

Поради з кібербезпеки

Директор компанії з кібербезпеки 10Guards Віталій Якушев говорить, що, користуючись мобільною грою, соціальною мережею чи месенджером, користувач відкриває доступ до інформації у своєму смартфоні — до фото, листувань, геолокацій, контактів. А нею користуються спецслужби країн, на території яких зареєстровані ці застосунки, соцмережі чи мобільні ігри, пояснює фахівець:

— Соцмережі — це дуже складні додатки. Для повноцінної роботи вони запитують доступ майже до всього. Це може бути як мінімум доступ до галереї, доступ до файлової системи взагалі, до ваших контактів, до камери, до мікрофона, до інтернет-з'єднань, до інформації про телефон. Ми встановлюємо умовні «Однокласники» або «ВКонтакті» собі на телефон, заходимо — і віддаємо інформацію про себе, щоб користуватися цим додатком. Що заважає цьому додатку ці фотографії закачувати собі в службову територію, про яку ви навіть не знаєте, і потихеньку передавати на сервери. Або ваші контакти, які ви віддали, вони повинні віддавати (*спецслужбам. — Ред.*), тому що так місцеві закони працюють. І це не тільки про диктаторські країни, такі як Росія. Навіть у європейських країнах спецслужби мають доступ до серверів компаній, які розміщені на їхній території. Якщо ми кажемо про

Facebook, Instagram, WhatsApp, Signal — це американські компанії. І вони вимушені, за законом Сполучених Штатів, надавати доступ спецслужбам своєї країни. Якщо ми кажемо про «ВКонтакті», то це російські ресурси. І згідно їх законів, спецслужби мають доступ до всього, що є всередині.

Фахівець із кібербезпеки Віталій Якушев © Особистий архів Віталія Якушева

Віталій Якушев певен, що все заборонити неможливо, а тим паче дітям та підліткам, які діятимуть наперекір батькам і все одно зареєструються, щоби користуватись застосунками. На його думку, саме тому важливо говорити з дітьми про всі можливі загрози, опікуватися кібергігієною:

— Проблема не в дитині і в іграх, а у вихованні, у тому, що батьки або близькі не приділяють уваги дитині. І заборона ігор або соцмереж може стати додатковим каталізатором. Месенджер або соцмережа не промиває мізки. Промиває мізки той, хто публікує контент, хто керує ним… Слід обов'язково проводити на рівні держави інформаційні кампанії про медіагігієну, пояснювати людям, яка інформація є секретною і її не можна розголошувати, хто б її не запитував (*у мережі. — Ред.*) — чи ГУР, чи СБУ, чи ССО або хтось із ЗСУ.

Секретну інформацію, навіть якщо ти її знаєш, можна повідомляти, лише офіційним каналом комунікації. Наприклад, тим, що вказані на сайті правоохоронного органу. Потрібно говорити, що є інформація державного характеру. І це необхідно забивати в голову методично плакатами на вулицях, білбордами, соціальною рекламою по телевізору, банерами в інтернеті, у соцмережах, через лідерів думок. І тоді це буде працювати.

Аліна Бондарчук вважає, що не мають залишатись осторонь і батьки. Вони повинні пояснювати дитині, що шкодить не тільки їй, а й державі, а також перевіряти, із ким донька чи син спілкується. І робити це варто з повагою до їхнього особистого простору та думок.

Куди можна звернутися

Сьогодні кібер- та загрози із вербування виявляють правоохоронці та СБУ. Але вони просять про допомогу й українців: можна долучитись до блокування телеграм- та ютюб-каналів, фейсбук-груп, інстапрофілів, які поширюють дезінформацію, а також дані про місця дислокації ЗСУ.

Для цього варто звернутись у чатбот StopRussia | MRIYA, надіслати відомості про виявлені ресурси, щоби їх перевірили та заблокували.

Має чатботи і СБУ. В один із них, «Знайди зрадника», можна надсилати інформацію про людей, які співпрацюють із російськими загарбниками, про інтернет-агентів, що передають ворогові інформацію чи поширюють контент на його підтримку.