**Китайський підхід до інформаційного протиборства**

Ще у трактаті Сунь-Цзи «Мистецтво війни» визначено різні способи впливу на психіку і поведінку супротивника. Сунь-Цзи зазначав, що мистецтво полководця полягає у досягненні перемоги над супротивником без застосування військової сили:

«У війні, як правило, найкраща політика зводиться до захоплення держави цілісною; зруйнувати її значно легше. Взяти у полон армію супротивника краще, ніж її знищити ... Підкорити супротивника без бою - ось вершина мистецтва».

Сунь-Цзи виокремив такі способи психологічного впливу на супротивника:

" розкладайте все гарне, що є в країні вашого супротивника";

"втягуйте провідних представників вашого супротивника у злочинну діяльність";

"використовуйте співробітництво самих підлих і мерзенних людей";

"розпалюйте сварки й зіткнення серед громадян ворожої країни";

"підбурюйте молодь проти старих";

"заважайте всіма способами діяльності уряду";

"перешкоджайте всіма способами оснащенню, забезпеченню й наведенню порядку в збройних силах";

"послаблюйте волю супротивника безглуздими, піснями і музикою";

"знецінюйте всі традиції ваших ворогів";

"будьте щедрі на пропозиції та подарунки для покупки інформації та спільників".

 Сучасна концепція ведення інформаційних операцій почала розроблятися в Китаї у 90-х роках 20 століття.

Ключовими відомствами, що відповідають за планування і реалізацію ІО є Міністерство оборони та Міністерство державної безпеки.

У Народно-визвольної армії Китаю (НВАК) за ведення ІО відповідає Головне політичне управління НВАК. ГПУ розробляє способи і форми ведення пропаганди як всередині країни, так і за її межами.

Координація діяльності з проведення комп’ютерних мережевих операцій покладено на управління радіоелектронної боротьби Генерального штабу НВАК. Йому підпорядковані спеціалізовані центри, що займаються вивченням можливості доступу до інформаційних мереж супротивника і захистом власних мереж.

З 2006 року в структурі управління зв'язку Генштабу НВАК функціонує навчальний центр з підготовки до ведення ІО. До його складу, зокрема, входить Ханкоуський навчальний центр, який є основним навчальним полігоном для відпрацювання форм і способів ведення інформаційного протиборства.

У широкому значенні суть інформаційного протиборства полягає у тому, що обидві сторони ведуть боротьбу одна проти одної у політичній, економічній, культурній, науковій, соціальній та технологічній сферах. Боротьба ведеться за інформаційний простір та ресурси.

Основна мета – інформаційне домінування, яке означає здатність захищати свою інформацію й руйнувати/атакувати інформаційну інфраструктуру супротивника.

Зміст ІО полягає у боротьбі за здобуття і збереженні ініціативи в отриманні, контролі та використанні інформації.

ІО спрямовані, насамперед, на системи управління супротивника, аби підірвати готовність осіб, що приймають рішення, чинити опір.

Директор департаменту комунікацій Народно-визвольної армії Китаю генерал Dai Qingmin визначає інформаційну операцію як «комплекс операцій в інформаційному середовищі, націлених на воєнну інформацію та інформаційну систему, які проводяться зазвичай у формі електронної війни і комп’ютерної мережевої війни». Такі операції засновані на знаннях і стратегіях. До таких стратегій зокрема відносяться:

* Саботування ворожої інформації чи інформаційної системи;
* Послаблення ворожих можливостей проводити інформаційну боротьбу;
* Розсіювання сил ворога з одночасною концентрацією власних військ;
* Відволікання уваги ворога і створення сприятливих бойових можливостей для себе;
* Створення у ворога помилкового враження, що супроводжується раптовою інформаційною атакою на нього;
* Спонукання ворога повірити, що правда- це брехня, а брехня – це правда;
* Спонукання ворога до помилкового судження або дії.

Слід відмітити, що китайські експерти запозичили низку положень американської концепції інформаційних операцій. Це стосується основної мети ІО (інформаційне домінування) і структурних елементів.

Так, основними компонентами ІО за китайською концепцією, є:

1. *Фізичні атаки*, в яких використовується високоточна зброя для знищення інформаційної інфраструктури супротивника
2. *Радіоелектронна боротьба* - застосування електронних засобів придушення або електромагнітної зброї для впливу на системи збору інформації та розвідданих.
3. *Комп’ютерні мережеві операції*, що проводяться у таких формах як кібер та хакерські атаки, а також віртуальної війни – засоби введення в оману супротивника за допомогою симульованих неправдивих команд.
4. *Психологічні операції та введення в оману*, що передбачає поширення інформації або дезінформації для впливу на емоції, погляди та поведінку цільової аудиторії.

Водночас, китайський підхід має низку **специфічних рис**, а саме:

1. Прагнення до більшого впливу при мінімальних витратах. Головною метою ІО є не перемога над супротивником будь-якою ціною, а досягнення панування, виживання і процвітання власного народу. Супротивник не знищується, а його ресурси та можливості використовуються для задоволення державних інтересів і потреб.
2. Замість нарощування потужності технічних засобів Китай докладає зусиль для досягнення сприятливого розвитку подій та їхнього позитивного результату. Пріоритетними напрямами діяльності Китаю є накопичення значущої інформації, захист власної інформацію, осіб, які приймають рішення, та національної єдності.
3. Китай намагається приховати свої власні наміри від світової громадськості.
4. Поєднання концепції «народної війни» з інформаційною війною.

Народна війна – це воєнно-політична стратегія, сформульована Мао Дзедуном. Основна ідея – заручитися підтримкою населення, затягти ворога у глибокий тил, де населення вимотає його партизанською війною.

Народна війна передбачає уникнення прямих зіткнень із сильним ворогом, натомість надається перевага стратегії затяжної війни з ретельним вибором поля бою, на якому можна здобути перемогу. Бойова група, яка проводить народну війну, починає з віддалених районів з гористою місцевістю, де ворог стає уразливим. Група встановлює опорні пункти і розширює свій вплив на ту місцевість, де може перетворитися на керівний орган.

Ідея поєднання народної війни з інформаційною втілюється у життя у півторамільйонних резервних силах Китаю. Народно-визвольна армія Китаю перетворює резервні сили деяких районах на міні полка ІО.

Так, в окрузі Ечен, провінція Хубей, НВАК створила резервний полк мережевих операцій, об'єднавши в нього близько 20 міських управлінь. У 2003 році в Гуанчжоу були сформовані загони «міської міліції» з ІО, куди набирали не лише висококваліфікованих ІТ-фахівців, а й усіх, хто мав навички роботи з комп'ютером.

1. Особливе значення надається використанню мережі Інтернет. Офіційний рупор Народно-визвольної армії Китаю (НВАК) опублікував статтю, в якій визначено п'ять основоположних принципів досягнення перемоги в "мережевих війнах", а саме:
* *Позбавлення живлення головного комп'ютера мережі супротивника.*
* *Удар по ключовим точкам*. Об'єктами атаки є такі основні сегменти мережі управління театром воєнних дій, як система дистанційної розвідки, система зв'язку, система обробки даних, система управління військами та зброєю, система забезпечення бойових дій.
* *Перевантаження мережі супротивника помилковими і застарілими даними.*
* *Зараження мережі супротивника вірусами.*
* *Таємне проникнення у мережу супротивника*. Проникнення не передбачає прямої участі людини, діє через простір і час. При цьому для збереження і передачі інформації використовуються електронні носії.
1. Використання стратагемних принципів.

Стратагема - це хитрість, призначена, щоб ввести в оману або застати ворога зненацька. Мистецтво стратагем – вміння представляти попередні стратегічні розрахунки й плани у формі пасток. Відмінною рисою хитрості служить не «обман» і «шахрайство», а «незвичайне». У трактаті Сунь-Цзи сказано: «При зустрічі з супротивником військо стає непереможним завдяки поєднанню незвичайних і регулярних дій ... Загалом, у бою супротивника зустрічають регулярною позицією, а перемагають його нерегулярним маневром».

Залежно від цілей, дослідники поділяють китайські стратагеми на такі категорії:

1. *Стратагеми підробки*. Суть - створення ілюзорної дійсності.

Наприклад, стратагема № 7. Витягти щось з нічого. Це стратагема містифікатора. Суть – представити вигадку реальністю; поширювати чутки; проводити брехливі, наклепницькі кампанії.

1. *Стратагеми приховування*. Суть – певні реальні обставини приховуються від ворога. Наприклад, стратагема №1 «Обдурити імператора, щоб він переплив море». Суть стратагеми - маскування цілі, шляху чи напрямку. Часто використовується у сучасних ІО. Так, військова операція у Лівії 201 року проводилась під гаслом захисту лівійських громадян. Насправді цілі були іншими – зменшити впливу М.Каддафі в Африці, доступ до нафтових ресурсів тощо.

Інший приклад – стратагема №8 «Начебто лагодити дерев’яні містки, а потай виступити у Ченьцан. Суть – приховувати за звичайними діями щось незвичайне; приховувати справжній напрям дії.

1. *Дезінформаційні стратагеми*. Суть – повідомлення про невідоме як про щось відоме. Наприклад, стратагема № 13 «Бити по траві, щоб сполохати змію». Це стратагема провокації. За допомогою цієї стратагеми можна змусити супротивника розкрити свої карти, можна розпалити міжнародні суперечки, а також сильні негативні емоції у громадян тієї чи іншої країни.
2. *Стратагеми отримання вигоди*. Суть – швидке виявлення і використання сприятливих обставин. Наприклад, стратагема №9 «Спостерігати за пожежею з протилежного берега». Суть – спостерігати за супротивником, що опинився у кризовій ситуації, не надаючи допомоги, поки ситуація не буде розвиватись у сприятливому напрямі.

Стратагема №19 «Витягати хмиз з-під котла». Суть – не виступати проти самої загрози, а усунути її причину; вибити грунт з-під ніг; позбавити опори. В інформаційних операціях це може бути використання шкідливих програм для виведення з ладу комп’ютерних мереж/систем або підрив морального духу військ супротивника.

1. *Стратагеми втечі*. Суть – ухилення від несприятливих обставин. Наприклад, стратагема №36 «Втеча – кращий варіант». Суть – якщо перемога супротивника неминуча, і битися з ним немає можливості, то потрібно або здатися, або домовлятися про мир, або втекти. Здатися означає поразку. Переговори про мир - поразка наполовину. Втеча не є поразкою. Уникнути поразки дуже важливо, бо це дасть змогу здобути перемогу у майбутньому.

2003 року була затверджена і у 2010 році скоригована **концепція «Трьох воєн»**, що визначає принципи та основні умови досягнення переваги в інформаційному протиборстві. Під трьома війнами мається на увазі медійна війна (public opinion warfare), психологічна війна (psychological warfare) та правова війна (legal warfare).

***Медійна війна*** передбачає використання громадської думки як зброї шляхом пропаганди через різні ЗМІ, щоб послабити «волю супротивника до боротьби», одночасно забезпечуючи силу волі та єдність між цивільними та військовими всередині країни. Медійна війна має допомогти деморалізувати супротивника, встановити контроль над ситуацією та уникнути жертв.

***Психологічна війна*** має на меті підірвати військову міць супротивника, здатність приймати правильні рішення, шляхом загострення внутрішніх протиріч, внесення розколу у ряди супротивника. Акцент зроблено на необхідності інтеграції психологічних атак з військовими діями, одночасній реалізації наступальних і оборонних дій тощо.

***Правова війна*** передбачає використання всіх аспектів права, включаючи національне законодавство, міжнародне право та закони війни, щоб забезпечити правову перевагу та делегітимізувати супротивника. Тобто мова йде про легітимізацію власних дій, здобуття підтримки з боку міжнародної спільноти.

Як зазначає дослідник Dean Cheng, психологічна війна є найбільш далекосяжною. Психологічні операції можуть направлятися на ворожі і на дружні, на зовнішні і на внутрішні, на військові і цивільні аудиторії, на лідерів і населення країн загалом, на союзників і на весь світ, здійснюватися різними методами і засобами.

Застосування методів психологічної війни у мирний час передбачає вплив та зміну поглядів опонента, щоб зробити його більш сприйнятливим до примусу. ПсО дають змогу сформувати позитивний національний імідж та здобути симпатії і підтримку політики країни з боку зарубіжних аудиторій.

У воєнний час психологічні операції мають за мету посіяти розгубленість, сумніви, тривогу, страх і відчуття виснаженості у супротивника. ПсО воєнного часу також спрямовані на формування почуття невизначеності та нерішучості на всіх рівнях, тим самим погіршуючи процеси прийняття рішень супротивника.

Аналітики Народно-визвольної армії КНР виокремили 4 типи ПсО: примусові операції, оманливі операції, операції відчуження (alienating) , оборонні операції.

* ***Примусові операції*** націлені на деморалізацію супротивника. Такі операції спрямовані на те, щоб змусити противника відмовитися від своїх планів або від опору шляхом формування у нього переконання в тому, що опір не має сенсу. Мета такої операції досягається демонстрацією переваги у військовій могутності, в інформаційних технологіях, бойової та психологічної підготовки військ, стратегічної позиції, а також уразливостей супротивника. Успішне примус дозволяє уникнути військового конфлікту. До таких операцій відносяться зокрема китайські хакерські атаки.
* ***Оманливі операції*** передбачають дезорієнтацію супротивника, формування помилкових вражень, оцінок, рішень та дій. Йдеться про вплив за допомогою ЗМІ та різних Інтернет-технологій на когнітивні процеси супротивника, з метою їх спотворення, уповільнення, блокування. При цьому акцент робиться на непомітному вбудовуванні помилок в існуючі вірування і системи цінностей супротивника. Реалізується принцип «сміття в смітті»: використання помилкової інформації при прийнятті рішення веде до прийняття помилкових рішень. Важливим елементом оманливих операцій є використання «підтверджувального упередження», тобто схильності людей шукати та надавати більше значення інформації, що підтверджує їхні існуючі переконання, відкидаючи інформацію, яка їм суперечить.
* ***Операції відчуження*** націлені на привнесення у табір супротивника підозр, розбіжностей, непорозумінь і відчуження, на порушення зв'язків між населенням і керівництвом, між керівниками, між союзниками, між військовими і цивільним населенням. Для реалізації принципу «фортеці краще захоплювати зсередини», на думку китайських фахівців, потрібно добре знати і враховувати індивідуальну і групову психологію супротивника, його слабкості і уразливі місця.
* ***Оборонні операції*** покликані протидіяти спробам противника вести операції примусу, обману і відчуження проти власної країни. Вони передбачають формування духовної, ідейної та соціальної єдності нації, «імунізацію» керівництва, населення, військовослужбовців проти ворожої пропаганди, утримання контролю за ЗМІ, з метою блокування деморалізуючих чуток і настроїв.

Сьогодні фахівцями Народно-визвольної армії Китаю (НВАК) розробляється нова концепція психологічних операцій – «cognitive domain operations».

Експерти НВАК виділили 6 технологій в рамках таких операцій:

* «Cognitive survey technology» переводить психологічні показники в кількісно вимірювані сигнали, щоб оцінити психологічну позицію противника - не лише сприйняття, а й мотивацію, емоції та потреби.
* «Cognitive interference technology*»* використовується для проведення атак на психологічний стан супротивника за допомогою летальних та не летальних засобів. Світлові хвилі, електромагнітні хвилі та мікрохвилі можуть завдати психологічної шкоди, викликати галюцинації, змусивши ворога діяти всупереч власним інтересам.
* *«*Cognitive strengthening technology*»* використовується для посилення власних когнітивних здібностей.
* *«*Subliminal information processing technology*»* використовується для збору та попередньої обробки контенту.
* «Subliminal information implantation technology» використовується для впровадження підсвідомих повідомлень у контент та створення «синтетичної інформації».
* «Subliminal information detection technology» використовується в оборонних цілях.

Національний університет оборонних технологій (NUDT) провів дослідження щодо використання підсвідомих повідомлень для зниження спротиву солдатів до індоктринації. Деякі тактики було протестовано на студентах унверситету. NDUT researched video manipulation during 2010-2011, and a December 2011 article proposed using “ audio-visual technology to imitate the voice of the national leadership and battlefield commanders to mislead the adversary’s decision-makers into wrong decisions.” This video editing required “sound-image synthesis technology” and seems to indicate the development of building blocks for deep fakes.

**Джерела інформації:**

1. Авраменко А., Старунский А. Психологические операции Народно-освободительной армии Китая. - http://psyfactor.org/lib/psywar37.htm
2. Vinod Anand Chinese Concepts and Capabilities of Information Warfare. - http://www.idsa.in/strategicanalysis/ChineseConceptsandCapabilitiesofInformationWarfare\_vanand\_1006
3. James Mulvenon The PLA and Information Warfare. - https://www.rand.org/content/dam/rand/pubs/conf\_proceedings/CF145/CF145.chap9.pdf
4. Зенгер Х. фон. Стратагемы. О китайском искусстве жить и выживать. ТТ. 1, 2. — М: Изд-во Эксмо, 2004. — 512 с, 1024 с.
5. Elsa Kania The PLA’s Latest Strategic Thinking on the Three Warfares. - https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/
6. Dean Cheng Winning Without Fighting: The Chinese Psychological Warfare Challenge. - https://www.heritage.org/global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge#\_ftn10
7. Nathan Beauchamp-Mustafaga Cognitive Domain Operations: The PLA’s New Holistic Concept for Influence Operations. - https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/
8. Кировец А. Органы пропаганды и информационной войны КНР. - http://factmil.com/publ/strana/kitaj/organy\_propagandy\_i\_informacionnoj\_vojny\_knr\_2013/59-1-0-284