Artem Yevlampiiev, Postgraduate Student
National Academy of the Security Service of Ukraine
Kyiv, Ukraine
ORCID: https://orcid.org/0009-0001-6082-2220

DOI: https://doi.org/10.30525/978-9934-26-650-8-4

A COMPARATIVE ANALYSIS OF MODELS FOR THE USE OF DIGITAL TECHNOLOGIES IN SPECIAL INFORMATION OPERATIONS: FROM DATA-DRIVEN MANAGEMENT TO COGNITIVE DOMINANCE

ПОРІВНЯЛЬНИЙ АНАЛІЗ МОДЕЛЕЙ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЯХ: ВІД DATA-DRIVEN УПРАВЛІННЯ ДО КОГНІТИВНОГО ДОМІНУВАННЯ

Сучасні спеціальні інформаційні операції (СІО) дедалі більше трансформуються з інструменту ситуативного інформаційного впливу на системну управлінську функцію, інтегровану у стратегічне планування державної безпеки [1]. Ця трансформація зумовлена розвитком цифрових технологій – аналізу великих даних, алгоритмічних систем обробки соціальних сигналів, штучного інтелекту та синтетичних медіа, які докорінно змінюють як інструментарій СІО, так і архітектуру їх управління [1; 2]. Фактично, СІО перестають бути сукупністю окремих кампаній, перетворюючись на керовані соціотехнічні системи з алгоритмізованими циклами управління, де цифрові інструменти забезпечують повний ланцюг від збору даних до оцінки когнітивних ефектів [1; 3]. Спільним інваріантом для провідних держав, таких як США, КНР, РФ та Україна, є саме вбудовування цифрового компонента безпосередньо в організаційно-управлінські комплекси, проте спосіб цієї інтеграції глибоко відображає політичну філософію, стратегічну культуру та інституційні рамки кожної з них, формуючи якісно різні типові моделі.

Інституціоналізовано-нормативна модель США сформувалася в умовах жорсткого правового регулювання та демократичного цивільного контролю над сектором безпеки, що накладає визначені обмеження, зокрема заборону впливу на внутрішню аудиторію. Вона інтегрована у концепцію багатодоменних операцій, де

інформаційний і когнітивний домени розглядаються як рівноправні з традиційними військовими просторами [3; 9]. Організаційно модель будується навколо чіткої координації між військовими структурами, такими як Командування спеціальних операцій (USSOCOM) та Кіберкомандування (USCYBERCOM), і цивільними агенціями на чолі з ЦРУ. Визначальною рисою є високий рівень алгоритмізації управління, досягнутий завдяки програмам DARPA та IARPA [4; 5]. Системи на кшталт Integrated Crisis Early Warning System (ICEWS) забезпечують безперервний моніторинг відкритих джерел і соціальних мереж для раннього попередження про кризи, трансформуючи масиви інформації у формалізовані індикатори ризику [4]. Платформа Plan X дозволяє планувати та синхронізувати кібер- й інформаційні операції в реальному часі, поєднуючи технічний і когнітивний вплив у єдиному інтерфейсі [5]. Крім того, програми на кшталт Anomaly Detection at Multiple Scales та Math for Social Networks забезпечують виявлення нетипової поведінки та моделювання динаміки соціальних мереж. У сукупності це формує високоефективну data-driven архітектуру СІО, яка, проте, функціонує в жорстких нормативних рамках, що водночас забезпечує легітимність та обмежує оперативну свободу.

Централізовано-партійна модель КНР якісно відрізняється логікою тотальної інституціоналізації та повною відсутністю подібних правових обмежень. Вона ґрунтується на доктрині когнітивної війни, що еволюціонувала з концепції «трьох війн» (війни громадської думки, психологічної та правової війни), і спрямована на довгострокове формування сприйняття та поведінки цільових аудиторій [6]. Організаційно цифровий компонент зосереджений у Силах інформаційної підтримки НВАК КНР та технічних управліннях Генштабу, але ключовим механізмом виступає інституціоналізоване військово-цивільне злиття. Цей механізм інтегрує державні органи з приватними технологічними корпораціями (Huawei, Baidu, Tencent, Alibaba) в єдину екосистему збору даних і розробки алгоритмів, де комерційні платформи та дані системи соціального кредиту стають джерелом для мікротаргетингу [6]. Масове використання big data, генеративного ШІ та deepfake-технологій дозволяє реалізовувати персоналізований когнітивний вплив у масштабах, недоступних децентралізованим моделям. Паралельно розвиток нейротехнологічних програм, зокрема масштабного China Brain Project, окреслює подальший перехід СІО від інформаційного впливу до технологічно

опосередкованого контролю когнітивних процесів, що вказує на прагнення до абсолютного технократичного домінування в сфері свідомості.

Гібридно-деструктивна модель РФ походить від радянських «активних заходів» і концепції рефлексивного управління, адаптованих до цифрового середовища. На відміну від китайського підходу, російська модель орієнтована не на довгостроковий контроль, а на хаотизацію інформаційного простору, руйнування довіри до інститутів та дестабілізацію суспільств супротивника. Її теоретичним підґрунтям слугує так звана «доктрина Герасимова», яка акцентує перевагу невійськових методів. Організаційним ядром стали Війська інформаційних операцій, створені в 2017 році, проте характерною ознакою є використання складної проксі-екосистеми: кіберзлочинних угруповань, бот-мереж та напівформальних структур, які поєднують технічний злам з інформаційним впливом, забезпечуючи заперечення причетності держави. Синтетичні медіа та масові дезінформаційні кампанії, що координуються через спеціалізовані програмні комплекси керування «фабриками тролів», застосовуються як інструмент швидкої дестабілізації. Ця модель, орієнтована на керований хаос, дозволяє швидко досягати тактичних ефектів, але внутрішньо суперечлива та знижує потенціал стратегічного наративного домінування через відверту деструктивність.

Адаптивно-мережева модель України сформувалася в умовах реальної гібридної агресії та обмежених ресурсів, що зумовило її оборонний характер, високу практичну апробацію та унікальну структуру. Її доктринальною основою стали Стратегії інформаційної, воєнної та кібербезпеки, що закріпили концепцію всеохоплюючої оборони [7; 8]. Ключовою рисою є інтеграція державних інституцій (Сили інформаційно-психологічних операцій ЗСУ, СБУ, ГУР МО) із мережевими ініціативами громадянського суспільства – волонтерськими OSINT-спільнотами, IT-активістами та міжнародними партнерами. Це забезпечує високу швидкість реагування, резилієнтність інформаційного простору та здатність до швидкого навчання. Використання цифрових технологій охоплює три ключові функції: 1) кіберзахист і протидія дезінформації через стійку інфраструктуру; 2) розвідка й аналітика на основі масового OSINT, геоаналітики та алгоритмів ШІ; 3) власне інформаційний вплив через координацію кампаній у соцмережах з бойовими діями за допомогою платформ на кшталт «Кропива» чи GIS Arta.

Український досвід демонструє, що ефективність СІО в умовах асиметрії може досягатися не лише через технологічну перевагу, а й через довіру суспільства, гнучкість інституцій, соціальну мобілізацію та потужну мережеву координацію.

Отже, порівняльний синтез виявляє спільний data-driven цикл управління СІО, однак ключові відмінності зумовлені архітектурою управління, рівнем правового регулювання та характером міжвідомчої та державно-громадянської взаємодії. США та КНР, орієнтовані на стратегічний довгостроковий вплив, реалізують технократичні моделі, але в діаметрально протилежних правових полях – обмеженого демократичного контролю та тотального партійного керівництва відповідно. РФ та Україна діють у логіці оперативної адаптації в умовах активного конфлікту, проте їхні цілі принципово різняться: перша прагне руйнування через хаос, друга – побудови стійкості через довіру та мережеву солідарність. Таким чином, цифрові технології не лише підсилюють інструментарій СІО, а й визначають тип управлінської моделі, яка, будучи продуктом політичної системи, безпосередньо впливає на ефективність впливу в когнітивному домені. Майбутнє інформаційного протиборства, ймовірно, визначатиметься саме протистоянням між моделями технократичного контролю та моделями мережевої резилієнтності, що спираються на громадянську участь, як це наочно демонструє український досвід, сформований у реальній війні.

Література:

1. NATO. MC 0422/6 NATO Military Policy for Information Operations. Brussels : NATO, 2019.
2. NATO. Allied Joint Doctrine for Information Operations (AJP-3.10). Brussels : NATO Standardization Office, 2015.
3. U.S. Department of the Army. FM 3-0 Operations. – Washington, DC : Department of the Army, 2022.
4. DARPA. Integrated Crisis Early Warning System (ICEWS): Program Overview. 2010. URL: https://www.darpa.mil/program/integrated-crisis-early-warning-system (дата звернення: 15.12.2025).
5. DARPA. Plan X: Cyber and Information Operations Platform. 2012. URL: https://www.darpa.mil/program/plan-x (дата звернення: 15.12.2025).
6. Beauchamp-Mustafaga N. Cognitive Warfare and China’s Concept of Intelligentized Warfare. Washington, DC : RAND Corporation, 2023.
7. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки України»: Указ Президента України № 685/2021.

8. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України»: Указ Президента України № 121/2021.

9. NATO StratCom Centre of Excellence. Measuring the Effectiveness of Strategic Communications. Riga : NATO StratCom COE, 2019.