Сунгурова Саломе Романівна

Політико-інформаційна війна: інструментально-функціональний аспект

УДК 327.8
DOI https://doi.org/10.24195/2414-9616.2021-6.11

Сунгурова Саломе Романівна
ад'юнкт кафедри військової політології
Військового інституту
Київського національного університету
імені Тараса Шевченка
вул. Ломоносова, 81, Київ, Україна

Актуальність статті пов'язана з тим фактом, що сьогодні стрімко розвивається інформаційно-комунікаційне поле глобалізованого світу, держави поринули в активне удосконалення інформаційно-комунікаційної інфраструктури. Інформаційна війна вийшла чи не на перше місце серед засобів нефізичного впливу на людину зокрема та спільноту загалом. Поза іншим, інформаційна війна широко застосовується у сучасних політичних протистояннях між політичними акторами різних рівнів та масштабів.

Як предмет наукового дослідження інформаційна війна комплексно вивчається як українськими науковцями, так і їх зарубіжними колегами через високий рівень прикладної значущості цієї теми. Сьогодні ґрунтовно досліджені різні аспекти інформаційної війни – сутність, функції, наслідки тощо. Однак інструментально-функціональний вимір висвітлений недостатньо. Саме тому мета цієї статті полягає у дослідженні інструментів політико-інформаційної війни і деталізується реалізацією таких завдань, як розкриття функціонального навантаження кожного інструменту та з'ясування ролі цих засобів за реалізації атакувальної та захисної стратегій.

Провідним методом даного наукового пошуку став діалектичний підхід, який дозволив врахувати суперечливу природу інформаційної війни, бінарний характер її інструментів. Окрім цього, ми покладалися на структурно-функціональний метод, який допоміг у вичленуванні функцій окремих інструментів.

У результаті дослідження були виділені та проаналізовані такі інструменти, як збір, передача, захист, маніпулювання, порушення, деградація та заперечення. Окрім цього, був деталізований їх зміст як за атакувальної, так і захисної стратегії ведення політико-інформаційної війни. Інструменти інформаційної війни (інформаційна зброя) використовуються задля викрадення, спотворення чи знищення інформації, обмеження чи припинення доступу до неї, порушення роботи або виведення з ладу телекомунікаційних мереж та комп'ютерних систем, маніпулювання свідомістю окремих суспільних груп тощо. Інформаційна зброя, попри психологічну спрямованість дії, може мати не менш деструктивні для суспільства наслідки, ніж інструменти традиційної війни, що спираються на фізичне насилля.

Ключові слова: *інформаційна війна, інструменти, інформаційна зброя, маніпулювання, збір інформації, захист, напад.*

Вступ. Сучасний цифровий світ демонструє одночасно і звершення, і вади суспільства. З одного боку, поглиблюється арсенал знань, удосконалюються технології, а з іншого боку, усі ці досягнення почасти використовуються для дестабілізації, пошкодження та руйнації. Стрімко розвивається інформаційно-комунікаційне поле глобалізованого світу, держави поринули у активне удосконалення інформаційно-комунікаційної інфраструктури. Інформаційна війна вийшла чи не на перше місце серед засобів нефізичного впливу на людину зокрема та спільноту загалом. Поза іншим, інформаційна війна широко застосовується у сучасних політичних протистояннях між політичними акторами різних рівнів та масштабів.

Як предмет наукового дослідження інформаційна війна комплексно вивчається як українськими науковцями, так і їх зарубіжними колегами через високий рівень прикладної значущості цієї теми. Серед експертів найвищого ґатунку доцільно згадати А. Еріксона [6], А. Кампена [5], М. Лойда [8], Г. Салівана [9] тощо. Завдяки напрацюванням цих науковців та великої кількості інших досліджені різні аспекти інформаційної війни – сутність, функції, наслідки тощо. Однак інструментально-функціональний вимір, на нашу думку, висвітлений недостатньо у науково-дослідній літературі.

Мета та завдання. Мета статті полягає у дослідженні інструментів політико-інформаційної війни і деталізується реалізацією таких завдань, як розкриття функціонального навантаження кожного інструменту та з'ясування ролі цих засобів під час реалізації атакувальної та захисної стратегій.

Методи дослідження. Провідним методом даного наукового пошуку став діалектичний підхід, який дозволив врахувати суперечливу природу інформаційної війни, бінарний характер її інструментів. Окрім цього, ми покладалися на структурно-функціональний метод, який допоміг у вичленуванні функцій окремих інструментів.

Результати. Отже, інформаційна війна у політичній площині застосовується задля досягнення політичних цілей за рахунок використання інформаційного інструментарію. Комплексний аналіз інформаційної війни як засобу політичного насилля передбачає дослідження прикладних аспектів, зокрема інструментів, за допомогою яких відповідне протистояння може здійснюватися. Інструментальний арсенал інформаційної війни – це інформаційна зброя.

Т. Андрусова і Ю. Гомонова зазначають: «Інформаційна зброя – це сукупність засобів та методів, що дозволяють викрадати, спотворювати чи знищувати інформацію, обмежувати чи припиняти доступ до неї законних користувачів, порушувати роботу або виводити з ладу телекомунікаційні мережі та комп'ютерні системи, що використовуються у забезпеченні життєдіяльності суспільства та держави. Також інформаційна зброя здатна змінювати свідомість людей, змушує їх неадекватно сприймати реальність, жити у світі ілюзій та робити згубні для себе вчинки» [1].

«Інформаційну зброю від звичайної відрізняють такі ознаки: прихованість — можливість досягнення мети без видимої підготовки та оголошення війни; масштабність — можливість завдавати невиправних збитків, не визнаючи державних кордонів і суверенітетів, без обмеження простору в усіх середовищах; універсальність — можливість багатоваріантного використання країною, що нападає, проти як воєнних, так і цивільних об'єктів країни ураження», – стверджує група вітчизняних дослідників на чолі з І. Харченком [3].

Отже, які інструменти можуть бути зараховані до арсеналу інформаційної зброї? На нашу думку, за найбільш узагальнюючого підходу можна виділити такі категорії, як збір, передача, захист, маніпулювання, порушення, деградація та заперечення. Деталізуємо їх зміст у подальшому аналізі.

Збір інформації є одним із інструментів інформаційної війни, оскільки та сторона протистояння, яка знає більше, у результаті матиме вирішальні переваги. Ідея полягає в тому, що чим більше у людини інформації, тим вищою є її обізнаність про ситуацію, що веде до кращого планування бою та кращих результатів. А. Сін зазначає: «Недавно знання свого положення та позиції дружніх сил саме по собі було величезним завданням. Технології точного визначення місцезнаходження, такі як навігація на основі глобальної системи позиціонування (GPS), значною мірою полегшили ці проблеми. Знання позиції противника також стало певною мірою можливим завдяки застосуванню технологій розвідки та спостереження» [10]. Далі він зазначає, що «функції розвідки та спостереження <...> рухаються до використання датчиків із спектрів, таких як інфрачервоний, ультрафіолетовий, нюховий, слуховий, зоровий, сейсмічний тощо, і об'єднання даних з них для формування всеосяжної картини» [10]. В інформаційній війні збір інформації є набагато менш небезпечним і більш повним, оскільки ці технології можна використовувати для проникнення в ситуації та збору точної інформації з мінімальною втратою достовірності.

Збір великої кількості вичерпної інформації, безумовно, є хорошою практикою, але він не має великої цінності, якщо інформація зберігається в сховищі й не використовується. Таким чином, здатність своєчасно передавати інформацію в руки тих, хто її потребує, є ще одним важливим аспектом інформаційної війни. Інструменти, які використовуються в цій галузі, – це не зовсім зброя, а радше цивільні технології, які використовуються у військових ситуаціях. Найважливішим з цих інструментів є комунікаційна інфраструктура, що складається з мереж комп'ютерів, маршрутизаторів, телефонних ліній, оптоволоконного кабелю, телефонів, телевізорів, радіоприймачів та інших технологій і протоколів транспортування даних. Без цих технологій можливість транспортування інформації в режимі реального часу, що вимагається за сучасними стандартами, була б неможливою.

У даному контексті хотілося б звернути увагу на аспект введення терміна «мережа» до військової лексики. Упродовж сотень років для поширення інформації військові покладалися на ієрархії, а не на мережі. Цивільні досягнення в комунікаційних технологіях дотримуються мережевої парадигми, що може серйозно змінити уявлення про командування і контроль у військових колах. Перехід до мережевих структур може вимагати децентралізації командування та контролю. Але децентралізація — це лише частина картини. Нова технологія також може забезпечити кращий «пригляд» і центральне розуміння загальної картини, що покращує управління у складній ситуації. З огляду на це стає очевидним, що навіть, здавалося б, базові зміни в технології транспортування інформації можуть зробити війну інформаційної епохи абсолютно відмінною від її аналога індустріальної епохи.

Одним із найбільш широко узгоджених аспектів інформаційної війни є необхідність мінімізувати обсяг інформації, до якої має доступ опонент. Значна частина цього завдання пов'язана з захистом інформації, яку ви маєте утримати від захоплення іншою стороною. Зброя, яка використовується для захисту інформації, поділяється на два класи. По-перше, це ті технології, які фізично захищають життєво важливі засоби зберігання даних, комп'ютери та транспортні механізми, включаючи бомбо- та куленепробивні кожухи та механізми запобігання проникненню, такі як замки та сканування відбитків пальців. По-друге, і, можливо, важливіше, це технології, які запобігають видимості та перехопленню фрагментів інформації ворогом. Це, безумовно, стосується основних технологій комп'ютерної безпеки, таких як паролі, а також більш складні технології, тобто шифрування. За словами М. Лібіцкі, «заплутуючи власні повідомлення та розшифровуючи повідомлення іншої сторони, кожна сторона виконує квінтесенцію інформаційної війни, захищаючи власний погляд на реальність, одночасно принижуючи погляд іншої сторони» [7].

Наступний широко уживаний інструмент – це інформаційні маніпуляції. У контексті інформаційної війни – це зміна інформації з метою спотворити картину реальності опонента. Це можна зробити за допомогою низки технологій, зокрема комп'ютерного програмного забезпечення для редагування тексту, графіки, відео, аудіо та інших форм передачі інформації. Розробка маніпульованих даних зазвичай виконується вручну, щоб ті, хто командує, мали контроль над тим, яке зображення стає доступним ворогу, але вищезгадані технології переважно використовуються для пришвидшення процесу фізичного маніпулювання після визначення вмісту.

Кінцевими аспектами інформаційної війни є порушення, деградація та заперечення. Усі три прийоми є засобами для досягнення однієї і тієї ж загальної мети – запобігання отриманню ворогом повної правильної інформації. Через їхню схожість багато однакових видів зброї використовується для досягнення однієї або кількох цілей, тому є сенс обговорити їх разом. Деякі з найбільш популярних видів зброї, які використовуються для ведення цих видів інформаційної війни, — це підробка, введення шуму, заглушення та перевантаження [7].

Підробка – це техніка, яка використовується для погіршення якості інформації, що надсилається ворогу. Потік інформації ворога порушується введенням у цей потік підробки, тобто підробленого повідомлення. Ця техніка працює, оскільки вона дозволяє надавати неправдиву інформацію системам збору інформації цільових конкурентів, щоб спонукати їх приймати погані рішення на основі цієї помилкової інформації.

Інший спосіб порушити інформацію, яку отримує опонент, – це ввести шум на частоту, яку він використовує. Фоновий шум заважає противнику відокремити фактичне повідомлення від шуму. Ця техніка є особливо корисною, якщо ворог використовує бездротовий зв'язок, оскільки ці частоти можна використовувати без необхідності під'єднання до фізичної мережі кабелів.

Заглушення – це техніка, яка використовується для досягнення заперечення та включає перехоплення сигналів, надісланих між двома каналами зв'язку або між датчиком і каналом. Сигнал перехоплюється, потім заглушується або зупиняється від подальшого просування до цільового призначення. Здебільшого той самий сигнал зберігається захоплюючою стороною як розвідувальна інформація і використовується для визначення погляду противника на його власну позицію в протистоянні.

Нарешті, перевантаження – це техніка, яка використовується для відмови ворогу в інформації як у військових, так і в цивільних умовах. Надсилаючи в комунікаційну систему противника об'єм даних, який є занадто великим для того, щоб він міг його обробити, сторона конфлікту спричиняє збій або серйозне погіршення здатності системи передавати інформацію. Система настільки зайнята боротьбою з перевантаженням, що не в змозі надати важливу інформацію тим, хто її потребує. Цю тактику називають атакою «відмова в обслуговуванні». Вона є легкою та ефективною.

О. Зозуля зазначає: «Інформаційно-технічний вплив є цілеспрямованим виробництвом і поширенням спеціальної інформації, яка справляє безпосередній вплив на функціонування та розвиток інформаційно-технічного середовища суспільства. Комп'ютери, засоби зв'язку і програмне забезпечення відіграють роль зброї масового збою, за допомогою якої можна проникати до комп'ютерних систем і порушувати їх роботу» [2].

Перераховані вище методи та зброя, безумовно, можуть завдати серйозної шкоди воєнно-політичним операціям, що залежать від інформації. Сучасний контекст інформаційного суспільства робить держави та інших політичних акторів, особливо у країнах з високорозвиненою інформаційно-комунікаційною інфраструктурою, з одного боку, найбільш дієвими, а з іншого боку, найбільш уразливими. Як же тоді захищатися? Існує кілька способів, де використовуються ті самі прийоми, які задіяні за атакувальної стратегії. Отже, розглянемо також доступні контрзаходи для кожного з озвучених інструментів інформаційної війни.

Захищатися від атак збору інформації означає не дати ворогам можливості зібрати інформацію про себе та/або про конфліктну ситуацію. Це передбачає захист власної інформації від перехоплення та запобігання потраплянню інформації до об'єктів збору ворога. Таким чином, доступним контрзаходом для захисту від збору інформації є та сама зброя, яка була визначена раніше для використання для захисту, підробки, заглушення та перевантаження. Зокрема, використання шифрування, підробки, введення шуму, заглушення та перевантаження є особливо корисним для зведення до мінімуму збору інформації ворогом.

Оскільки транспортування інформації сильно залежить від інфраструктури, найефективнішим контрзаходом для запобігання передачі й отриманню інформації є знищення інфраструктури противника. Цей конкретний контрзахід «потребує знання того, як спілкується інша сторона» [7]. Із цими знаннями захист може бути відносно легким. Якщо архітектура транспортування інформації будується на дротах та вузлах, останні легко ідентифікуються та виводяться з ладу. Як і командні центри, системи зв'язку можуть бути пошкоджені внаслідок атак на генератори, підстанції та трубопроводи подачі палива. Якщо архітектура є електромагнітною, часто ключові вузли видно. Якщо супутники використовуються для передачі та сигналізації, то лінії зв'язку можуть бути заглушені або збиті.

Атака на інфраструктуру противника як протидія транспортуванню інформації може бути не тільки особливо легкою, а й може мати далекосяжні наслідки для всієї ворожої інформаційної системи. У своїй книзі «Захисна інформаційна війна» Д. Альбертс зауважує про це явище: «Два різних сценарії служать для ілюстрації хаотичного характеру атак на інфраструктуру. У першому випадку конкретна атака на інфраструктуру може викликати низку приблизних наслідків, які важко передбачити і які значно посилюють наслідки атаки. У другому випадку серія атак демонструватиме хаотичну поведінку, коли сума їх кумулятивного ефекту значно перевищуватиме суму індивідуальних впливів серії незалежних подій» [4].

Щоб протидіяти спробам ворога захистити власну інформацію, треба мати можливість обійти ворожі механізми захисту. Як зазначалося раніше, основною технологічною зброєю для захисту власної інформації є шифрування. На жаль, нещодавнє зростання складності криптографії дуже ускладнило контрзаходи. М. Лібіцкі зазначає: «Декодування повідомлень, створених комп'ютером, усе більше ускладнюється. Комбінація таких технологій, як стандарт потрійного цифрового шифрування для передачі повідомлень за допомогою закритих ключів і шифрування з відкритим ключем для передачі приватних ключів за допомогою відкритих ключів, ймовірно, буде переможена найкращими комп'ютерами, що розшифровують код» [7]. Це означає для тих, хто бажає протидіяти захисту інформації, що їхні зусилля згодом стануть марними. А ось спроби зламати коди за допомогою потужних комп'ютерів, імовірно, принесуть найкращі результати.

Хоча криптографія є найефективнішою, вона не є єдиним інструментом захисту інформації. Зокрема, паролі є набагато більш поширеною технікою для захисту інформаційних систем від несанкціонованого доступу. Однак, на жаль, системи паролів залежать від людей, які відстежують і вводять коди, що створює для них значну вразливість. Якщо є можливість фізичного доступу до системи або тих, хто її використовує, отримання або вгадування паролів може бути неймовірно простим і дуже ефективним засобом для отримання доступу до захищеної інформації.

Як тільки ворог отримає інформацію, запобігти маніпулюванню нею буде надзвичайно складно. З огляду на це існує лише два контрзаходи для захисту від такого роду атак. Зокрема, можна працювати над тим, щоб не допустити перехоплення інформації ворогом. Найефективнішими тут є методи захисту інформації, оскільки вони не дозволяють ворогу отримати доступ до інформації або зрозуміти її у початковій формі.

Другий, і, можливо, більш важливий ключ у захисті від маніпуляцій з даними — це запобігання повторному введенню змінених даних у потік реальної інформації. На щастя, для цього існує кілька методів, найпоширенішим з яких є резервування.

М. Лібіцкі називає інформаційну маніпуляцію семантичною атакою і зазначає, що «система під семантичною атакою функціонує і буде сприйматися як така, що працює правильно, але вона генеруватиме відповіді, що відрізняються від реальності <...>» [7]. Це відбувається, тому що ці системи залежать від якогось джерела інформації, яке дослідник називає датчиком для отримання інформації про реальний світ. Якщо датчики можна обдурити, то і системи можна обдурити. Щоб протидіяти семантичній атаці, захист від збою може полягати, скажімо, у датчиках, надлишкових за типами та розподілами, і у мудрому розподілі влади для прийняття рішень між людьми та машинами. Збираючи ту саму інформацію з кількох альтернативних джерел, система збільшує ймовірність того, що правильна інформація пройде. Навіть якщо ворогу вдасться зіпсувати ці дані на одній лінії зв'язку, можна легко виявити погані дані, оскільки вони відрізнятимуться від картини, намальованої рештою ваших джерел.

Захист від порушення інформації, деградації та заперечення вимагає застосування багатьох із згаданих контрзаходів. Будь-який з видів зброї для здійснення цих типів атак вимагає доступу до каналів зв'язку противника, тому механізми захисту інформації та резервні канали можуть бути ефективними для підтримки деяких ліній зв'язку, на які потенційні зловмисники не впливають. Д. Альбертс зазначає: «Наша колекція застарілих систем забезпечує певну частку притаманної надійності та стійкості <…> Вони вказують на перекриття та дублювання в цих системах і стверджують, що комусь було б дуже важко повністю порушити певний порядок» [4].

Існує також кілька доступних методів, спеціально розроблених для протидії описаній зброї. М. Лібіцкі пише: «Комунікатори рухаються до технологій стрибкоподібної зміни частоти, широкого спектру та множинного доступу з кодовим поділом (CDMA), які важко заглушити та перехопити. Зв'язок із відомих місць <...> може використовувати цифрові технології для фокусування на фронтальних сигналах та відкидання глушіння, яке виникає з боків. Методи цифрового стиснення разом із надлишковістю сигналу означають, що бітові потоки можна відновити неушкодженими, навіть якщо великі частини знищені» [7]. Ці методи, а також тисячі інших, які зараз розробляються в дослідницьких центрах у всьому світі, полегшують кожен день відновлення після спроб знищити та заблокувати інформацію, коли вона потрапляє до цільового призначення.

Висновки. З огляду на зазначене легко побачити, що інформаційна війна є не менш складною, ніж традиційна. Вона включає багато різних стратегій, технік, видів зброї та захисту. Аналіз інструментального набору ведення інформаційної війни може допомогти у розробці реальних планів щодо того, як боротися з загрозами, які перманентно виникають у політико-інформаційному полі. Окрім цього, важливо пам'ятати, що більшість інструментів, проаналізованих у даному дослідженні, дає змогу втілювати не тільки ефективну атакувальну стратегію, але й захисну.

ЛІТЕРАТУРА:

1. Андрусова Т., Гомонова Ю. Информационное оружие и информационные войны. URL: file:///C:/Users/908/Downloads/informatsionnoe-oruzhie-i-informatsionnye-voyny.pdf.

2. Зозуля О. Інформаційна зброя як геополітичний чинник та інструмент силової політики. URL: http://academy.gov.ua/ej/ej18/PDF/12.pdf.

3. Основні засоби інформаційного протиборства та інформаційної війни як явища сучасного міжнародного політичного процесу / І. Харченко, С. Сапогов, В. Шамраєва, Л. Новікова. URL: file:///C:/Users/908/Downloads/9974-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-19803-1-10-20171219.pdf.

4. Alberts D. Defensive Information Warfare. URL: http://www.dodccrp.org/files/Alberts_Defensive.pdf.

5. Campen A. The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War. Fairfax, VA, AFCEA International Press, 1992.

6. Eriksson A. Viewpoint: Information Warfare: Hype or Reality? URL: https://www.nonproliferation.org/wp-content/uploads/npr/erikss63.pdf.

7. Libicki M. What is Information Warfare? Washington, National Defense University, 1995.

8. Lloyd M. The Art of Military Deception. London, Leo Cooper, 1997.

9. Sullivan G. War in the Information Age. URL: https://www.files.ethz.ch/isn/109690/War_Information_Age.pdf.

10. Singh A. Information Warfare: Reshaping Traditional Perceptions. URL: http://www.idsa-india.org/an-mar-4.html.

REFERENCES:

1. Andrusova, T., Gomonova, Yu. (2010) Informacionnoe oruzhie i informacionnye vojny [Information weapons and information wars]. URL: file:///C:/Users/908/Downloads/informatsionnoe-oruzhie-i-informatsionnye-voyny.pdf.

2. Zozulya, O. (2013) Informacijna zbroya yak geopolity`chny`j chy`nny`k ta instrument sy`lovoyi polity`ky` [Information weapons as a geopolitical factor and a tool of power policy]. URL: http://academy.gov.ua/ej/ej18/PDF/12.pdf.

3. Kharchenko, I., Sapogov, S., Shamrayeva, V., Novikova, L. (2017) Osnovni zasoby` informacijnogo proty`borstva ta informacijnoyi vijny` yak yavy`shha suchasnogo mizhnarodnogo polity`chnogo procesu [The main means of information confrontation and information warfare as a phenomenon of modern international political process]. URL: file:///C:/Users/908/Downloads/9974-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-19803-1-10-20171219.pdf.

4. Alberts, D. (1996) Defensive Information Warfare. URL: http://www.dodccrp.org/files/Alberts_Defensive.pdf.

5. Campen, A. (1992) The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War. Fairfax, VA, AFCEA International Press.

6. Eriksson A. Viewpoint: Information Warfare: Hype or Reality? URL: https://www.nonproliferation.org/wp-content/uploads/npr/erikss63.pdf.

7. Libicki, M. (1995) What is Information Warfare? Washington, National Defense University.

8. Lloyd, M. (1997) The Art of Military Deception. London, Leo Cooper.

9. Sullivan, G. (1994) War in the Information Age. URL: https://www.files.ethz.ch/isn/109690/War_Information_Age.pdf.

10. Singh, A. (2006) Information Warfare: Reshaping Traditional Perceptions. URL: http://www.idsa-india.org/an-mar-4.html.

Political and information war: instrumental and functional aspect

Sunhurova Salome Romanivna

PhD Student at the Department of Military Political Science
Military Institute
Taras Shevchenko National University of Kyiv
Lomonosova str., 81, Kyiv, Ukraine

The actuality of the article is since today the information and communication field of the globalized world is developing rapidly, the states are immersed in the active improvement of information and communication infrastructure. Information warfare has come out on top among the means of non-physical influence on people in particular and the community in general. Among other things, information warfare is widely used in modern political confrontations between political actors of various levels and scales.

As a subject of scientific research, information warfare is comprehensively studied by both the Ukrainian scientists and their foreign colleagues due to the high level of applied significance of this topic. Today, various aspects of information warfare have been thoroughly studied: the essence, functions, consequences, etc. However, the instrumental-functional dimension is insufficiently covered. Therefore, the purpose of this article is to study the tools of political information warfare and is detailed with the implementation of such tasks as disclosing the functional load of each tool, as well as clarifying the role of these tools in offensive and defensive strategies.

The leading method of this scientific research was the dialectical approach, which allowed to consider the contradictory nature of information warfare, the binary nature of its tools. In addition, we relied on the structural-functional method, which helped to indicate the functions of individual instruments.

As a result of the study, tools such as collection, transfer, protection, manipulation, violation, degradation, and denial were identified and analyzed. In addition, their content was detailed in both the offensive and defensive strategies of political and information warfare. Information warfare tools or information weapons are used to steal, distort, or destroy information, restrict or stop access to it, disrupt or disable telecommunications networks and computer systems, manipulate the consciousness of certain social groups, and so on. Information weapons, despite their psychological orientation, could have no less destructive consequences for society than the tools of traditional warfare based on physical violence.

Key words: *information warfare, tools, information weapons, manipulation, information collection, defense, attack.*