

ПОЛІТИЧНІ НАУКИ

УДК 32.1.321.01:355

Бірюков Д. С.,
кандидат технічних наук, завідувач сектору,
Національний інститут стратегічних досліджень
(Україна, Київ), dmytro.biriukov@niss.gov.ua

КОНЦЕПТУАЛІЗАЦІЯ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В СУЧАСНИХ БЕЗПЕКОВИХ ДОСЛІДЖЕННЯХ

Розглядається питання про формування політологічної концепції захисту критичної інфраструктури як способу розуміння, пояснення та дослідження процесів перетворень в системах забезпечення національної безпеки сучасних держав. Визначено предмет, для якого дана концепція є «способом розуміння», сформульована її «керівна ідея». В прикладному полі концепції розробляються питання операціоналізації національних інтересів, встановлення балансу інтересів в трикутнику «держава–суспільство–бізнес», політизації (сек'юритизації) безпекових проблем та ін.

Ключові слова: національна безпека, критична інфраструктура, політологічна концепція, прикладні політологічні дослідження.

Протягом останньої чверті століття в світі відбулися кардинальні геополітичні зміни, утворилося принципово нове турбулентне безпекове середовище, якому характерний широкий спектр невоєнних загроз, підвищення ролі недержавних акторів, розмиття національних границь. Ці перетворення були усвідомлені та відображені в численних наукових працях в рамках такого міждисциплінарного напрямку як безпекові дослідження [1]. В Україні становлення і розвиток теорії національної безпеки пов'язаний із роботами таких відомих науковців та практиків як В. П. Горбулін, С. І. Пирожков, О. С. Бодрук, О. В. Литвиненко, О. М. Гончаренко, Б. О. Парахонський. Грунтовним дослідженням безпекових питань в окремих сферах (зовнішньополітична, економічна, гуманітарна, інформаційна, екологічна, тощо) були присвячені роботи Г. М. Перепелиці, О. С. Власюка, М. М. Розумного, А. І. Сухорукова, Я. А. Жаліла, В. М. Гейця, М. А. Ожевана, Д. В. Дубова, А. Б. Качинського, та ін.

Термін критична інфраструктура останніми роками стає все більш звичним для вітчизняних теоретиків і практиків в сфері національної безпеки. Сприяє цьому робота НІСД зі поступового обґрунтування необхідності введення даного підходу в систему забезпечення національної безпеки [2; 3].

Нині «інформаційну базу» досліджень з питань захисту критичної інфраструктури становлять нормативно-правові документи провідних країн світу та їх об'єднані (див. посилання в [3, с. 6–10, 11–19]), аналітичні звіти урядових установ (наприклад, Рахункової палати США), офіційні документи Європейської комісії, звіти неурядових аналітичних центрів, монографії та збірники доповідей спеціалізованих конференцій, численні публікації в профільних наукових журналах. Однією з найвідоміших праць з питань захисту критичної інфраструктури є книга *Тедда Л'юїса*, яка має підзаголовок: «захищаючи націю, що з'єднана мережею» [4]. В ній американський дослідник розглядає еволюцію розвитку системи захисту критичної інфраструктури в Сполучених Штатах, країні, в якій цей

напрямок був започаткований і, пройшовши декілька етапів нормативно-інституційного вдосконалення, досяг нині найбільш розвинутої форми в організаційному плані.

Через свій міждисциплінарний характер завдання забезпечення безпеки та стійкості критичної інфраструктури, як відзначає *Ян Мецгер*, розглядається в різноманітних аспектах, таких як економічний, технологічний, правовий, безпековий (зокрема, забезпечення правопорядку, оборона та цивільний захист) [5, с. 201]. Проте, не зважаючи на поширення терміну «критична інфраструктура», впровадження підходів до захисту критичної інфраструктури в багатьох країнах світу, на нашу думку, не можна стверджувати про сформованість політологічної концепції критичної інфраструктури. Підтверджує цю тезу аналіз публікацій, зроблених в двох спеціалізованих міжнародних міждисциплінарних наукових журналах, результатом якого було визначення частоти представлених в них тематик [3, с. 28].

Дана робота розглядає захист критичної інфраструктури на предмет його спроможності бути політологічною концепцією, а, отже, метою є критичний аналіз, визначення концептуальних засад захисту критичної інфраструктури в рамках безпекових досліджень.

Як правило, концепцією (від лат. *conceptio* – розуміння, система) називають «певний спосіб розуміння, трактування деякого предмету, явища, процесу, основна точка зору на предмет або явище, керівна ідея для їхнього систематичного висвітлення» [6]. Цей термін вживається для позначення системи поглядів на явище в світі, природі, чи суспільстві, головного задуму, конструктивного принципу в науковій, художній, політичній та інших видах діяльності.

В першу чергу, визначимо «предмет, явище, процес», для якого дана концепція є «способом розуміння». На нашу думку, ним є процес розвитку системи забезпечення національної безпеки. Так, в США захист критичної інфраструктури є невід'ємною частиною політики «внутрішньої» безпеки (англ., *homeland security*), яку почали розбудовувати в цій країні у відповідь на асиметричні безпекові загрози ХХІ століття, передусім – загрози глобального тероризму [4]. Інший приклад – формування загальноєвропейського безпекової архітектури і запровадження захисту критичної інфраструктури як на наднаціональному рівні, так і в окремих країнах ЄС [7].

Далі, щодо «основної точки зору» чи «керівної ідеї» концепції захисту критичної інфраструктури, то її можна спрощено сформулювати таким чином: в системі забезпечення національної безпеки особливу увагу (встановлювати особливі вимоги, перерозподіляти ресурси тощо) слід звертати на ті об'єкти, що забезпечують надання товарів та послуг, які є найважливішими для життєдіяльності суспільства, функціонування економіки та державного управління. При цьому ідентифікація критичної інфраструктури, визначення пріоритетів та переліку заходів із її захисту здійснюється на основі

оцінки на національному (загальнодержавному рівні) широкого спектра загроз [2, с. 15–26].

Якщо ж розглядати концепцію захисту критичної інфраструктури як *конструктивну ідею* в теорії національної безпеки, то можна вказати низку можливостей для практичного застосування даної концепції. Зокрема, на нашу думку, ця концепція дозволяє піднімати та досліджувати такі питання як операціоналізація національних інтересів, залучення всіх стейкхолдерів (в т.ч. недержавних акторів забезпечення безпеки), врахування «м'яких» (нетрадиційних) загроз, децентралізація та приватизація безпекових функцій, пріоретизація дій та розподіл ресурсів.

Нині панівною в теорії національної безпеки є триада понять: «національна безпека», «національні інтереси», «загрози національним інтересам». Хоча на такій понятійній основі побудовано теорію національної безпеки, вона є слабо прийнятною для операціоналізації. Тобто на практиці важко визначати, яким чином ті чи інші державні рішення впливають на досягнення цілей, що обумовлені національними інтересами. Цей недолік певною мірою усуває критична інфраструктура, оскільки її стабільне функціонування є передумовою досягнення таких цілей [3, с. 29–30].

Піднімаючи питання про концептуалізацію захисту критичної інфраструктури в рамках сучасних безпекових досліджень, потрібно зауважити, що він природним чином відображає трансформацію безпеки у чотирьох вимірах, які описала *Емма Ротшильд*: від безпеки держав до безпеки груп та окремих індивідуумів; від безпеки окремої держави до міжнародної безпеки; з суто військової в інші форми (економічна, енергетична, екологічна т.і.); розширилася політична відповідальність за забезпечення безпеки як для держави, так і інших акторів (в т.ч. громадських організацій, міжнародних організацій) [8].

Політика держави щодо захисту критичної інфраструктури аргументується через необхідність забезпечення першорядного надання життєво важливих товарів та послуг населенню та суб'єктам національної економіки. Наприклад, така аргументація прослідковується в робочому документі апарату Європейської Комісії відмічається [9, с. 2]: «забезпечуючи високий рівень захисту інфраструктури в ЄС та підвищуючи її стійкість (проти всіх загроз та небезпек), ми можемо мінімувати наслідки втрат сервісів для суспільства в цілому». Цей підхід є характерним для скандинавських країн, зокрема, заслуговує уваги звіт «Захист критичної інфраструктури та критичні функції суспільства в Норвегії», підготовлений в 2006 році комісією при уряді Норвегії [10]. У ньому з-поміж нових викликів, пов'язаних із безпекою суспільства, були названі технологічні зміни (зокрема поширення інформаційних технологій), підвищення економічної конкуренції, зменшення обсягу державних послуг та здійснення приватними компаніями державних замовлень. Ці проблеми, поряд із появою «м'яких» загроз, таких як тероризм, організована злочинність чи зміни клімату в багатьох розвинених країнах світу докорінно змінили пріоритети та акценти в державній політиці щодо захисту критичної інфраструктури.

Концепція захисту критичної інфраструктури фокусує увагу на таких питаннях розвитку нормативних та організаційних основ безпекової політики сучасної держави [3, с. 5, 14–15]: координація та взаємодія між відомствами

сектору безпеки і оборони; розвиток державно–приватного партнерства в сфері безпеки; використання комплексного (так званого, all-hazard) ризик–орієнтовного підходу для управління надзвичайними ситуаціями (на всіх етапах: попередження, реагування мінімізація наслідків).

Нині складовою безпекової політики розвинених держав, як це відмічають *Джеймс Брасет та Нік Воган–Уїліамс* (Університет Уорвіку, Велика Британія), є побудова більш стійкого суспільства до надзвичайних ситуацій різної природи [11]. Отже до вирішення безпекових проблем залучаються всі зацікавлені сторони (суспільство, бізнес, держава), а недержавним акторам делегуються більш широкі права та обов'язки щодо забезпечення безпеки. Це вкрай важливо, з огляду на домінуючу роль приватного сектору в економіках розвинених країн. Наприклад, в США доля приватного сектору оцінюється на рівні 85% [4]. Так само в багатьох країнах ЄС, такі інфраструктурні мережі як водопостачання, електроенергетика, залізничний транспорт, які ще 20–30 років тому перебували в державній власності, нині приватизовані. Водночас навіть в розвинутих країнах Західної Європи відмічається проблема, що пов'язана із відсутністю як досвіду, так і самих засобів моніторингу та контролю за функціонуванням критичної інфраструктури приватного сектору [12].

В Україні приватизація багатьох підприємств (в основному це стосується тих, що надавали послуги населенню із забезпеченням електроенергією, телефонним зв'язком та ін.), створення нових, від самого початку приватних компаній (провайтери телекомунікаційних послуг, мобільний зв'язок, Інтернет), також актуалізує питання державно–приватного партнерства в безпековій сфері. Нині питома вага державного сектору вітчизняної економіки, підрахована за методикою Мінекономрозвитку, становить 16,2%. І хоча методика не визначає даний показник категорій об'єктів, що можуть бути віднесені до критичної інфраструктури, наприклад, підприємств, що мають стратегічне значення для економіки та оборони держави (див. [2, с. 32]), можна припустити, що для них показник буде вищий. Водночас в Україні багато об'єктів, що надають послуги із життєзабезпечення населення вже знаходяться в приватній власності, що утворює соціально–політичні ризики [3, с. 77].

На цю проблему державної політики вказує відомий вітчизняний фахівець *Володимир Горбулін*: «З огляду на те, що нині більшість суб'єктів господарювання в енергетичному секторі є приватними, відповідальність за забезпечення захисту критичної інфраструктури країни мають нести як відповідні органи державної влади, так і приватний сектор (оператори енергетичної інфраструктури). При цьому інші зацікавлені суб'єкти, зокрема місцеві органи влади та населення, також мають залучатися до діяльності у цій сфері» [13]. Так само в галузі телекомунікацій та зв'язку, яка бурхливо розвивається, актуальним є питання щодо державного контролю та забезпечення інформаційної безпеки: «інфраструктура, що існує і розвивається де-факто у вельми ліберальному правовому полі, має чимало проблем... і правові і технічні ..., технологічні... але ключовою ... є відсутність цілісної системи управління» [14, с. 128].

В більш широкому плані можна казати про те, що концепція критичної інфраструктури дозволяє

досліджувати взаємовідносини економічної та політичної влади, наслідки цих відносин для стану національної безпеки. Тут значну роль відіграють такі недержавні актори як транснаціональні компанії та локальні (національні чи регіональні) фінансово-промислові групи. Причому в умовах ринкової економіки навіть для багатьох європейських країн їх діяльність суттєво впливає на національну безпеку, а темною стороною виборювання економічних інтересів окремих компаній стає лобювання та корупція [15, с. 19–29].

Можна також говорити про критичну інфраструктуру як про індикатор розмежування безпекових функцій між центральною та місцевою виконавчою владою в державі. Тобто певні безпекові функції мають залишатися суто за центральною владою, оскільки вони пов'язані із гарантіями безпечного функціонування об'єктів критичної інфраструктури. При цьому *Тед Люїс* наголошує на нерівномірності розподілу ресурсів, формулюючи правило «80–20%», за яким 80% інвестицій на забезпечення безпеки критичної інфраструктури здійснюються для 20% території країни [4, с. 18].

Поряд з можливостями, що надає критична інфраструктура для розвитку економіки та підвищення рівня суспільних благ, існують і загрози, пов'язані з можливими аваріями на об'єктах такої інфраструктури, зокрема, хімічної промисловості, нафто- та газо-транспортних мереж, гідротехнічних споруд тощо. Це обґрунтовує необхідність окремо вивчення питань сек'юритизації для подібних об'єктів. Тобто розгляду загроз таким об'єктам як екзистенціальних для суспільства, економіки чи держави. Наприклад, *Клаудія Арайдо* (Відкритий університет, Мілтон Кейнс, Велика Британія) розглядає взаємозв'язок процесів сек'юритизації та захисту критичної інфраструктури від можливих терористичних посягань [16].

Нині практика ведення гібридної війни проти України наочно демонструє, що змиваються межі між проявами жорстких (воєнних) та м'яких (невоєнних) загроз. В таких умовах, з одного боку, об'єктивно підвищується важливість забезпечення захисту критичної інфраструктури (через їх виняткову важливість і масштаб можливих наслідків для економіки та соціального благополуччя населення), а, з іншого, все очевиднішим стає необхідність впровадження в державній безпековій політиці спеціальних підходів до забезпечення безпеки таких інфраструктур. На це наголошує *Володимир Горбулін*: «Очевидно, що Росія цілком свідомо використовує атаки проти критичної інфраструктури, зокрема енергетичної, як для досягнення своїх цілей у політичній та економічній сферах, так і зниження воєнно-економічного потенціалу держави в найкоротший термін» [13].

Висновки і перспективи подальших досліджень. Нині захист критичної інфраструктури є частиною безпекової політики провідних країн світу в сфері національної безпеки, він є врегульованим в нормативно-правовому полі, інституційно забезпечений в структурі державних органів і служб сектору безпеки і оборони таких країн. Такий масивний емпіричний матеріал відкриває можливості для осмислення захисту критичної інфраструктури як політологічної концепції в теорії національної безпеки.

На нашу думку, концепція захисту критичної інфраструктури є «способом розуміння» низки перетворень

в системах забезпечення національної безпеки, що відбулися в провідних країнах світу, і в першу чергу в США (формування внутрішньої безпеки), на початку цього століття.

«Керівну ідею» даної концепції можна сформулювати так: в системі забезпечення національної безпеки необхідно зосереджувати основну увагу на «критичних» об'єктах, перерозподіляти ресурси та посилювати вимоги до їх захисту, задіювати всіх стейкхолдерів (особливо власників/операторів об'єктів інфраструктури та суспільство). Водночас потрібно підкреслити, що референтним об'єктом безпеки, який захищається, є не самі системи, мережі, об'єкти критичної інфраструктури, а послуги та товари, які є життєво необхідними для функціонування суспільства, економіки та держави.

Концепція є конструктивною, тобто дозволяє визначати конкретні варіанти побудови правової та інституційної основ системи забезпечення національної безпеки. Отже, імплементуючи захист критичної інфраструктури в систему забезпечення національної безпеки, держава фокусує вимоги до безпеки певної групи ключових об'єктів, що надають життєво необхідні послуги та товари для суспільства, національної економіки та системи державного управління.

Нами також визначено «проблемне поле» даної концепції. В нього входять питання операціоналізації національних інтересів, знаходження балансу інтересів (держава-суспільство-бізнес), формування політичних рішень (в т.ч. лобювання інтересів еліт), сек'юритизації (політизації) загроз тощо. Оскільки захист критичної інфраструктури значним чином впливає на управління станом національної безпеки, саме через нього можна операціоналізувати питання захисту національних інтересів. Тобто побудувати зв'язок між конкретними заходами (діями) щодо критичної інфраструктури та досить «розмитим» поняттям національні інтереси.

Список використаних джерел

1. Contemporary Security Studies. 3rd ed. / Edt. Collins A. – Oxford, 2013. – 479 p.
2. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні: аналіт. доп. / Д. С. Бірюков, С. І. Кондратов. – К.: НІСД, 2012. – 102 с.
3. Концепція захисту критичної інфраструктури: зб. міжнар. наук.-практ. конф. (7–8 листопада 2013 р., Київ – Вишгород). – К.: НІСД, 2014. – 147 с.
4. Lewis T. G. Critical infrastructure protection in homeland security: defending a networked nation. – Willey and Sons, 2006. – 486 p.
5. Business and Security: Public-Private Sector Relationships in a New Security Environment / Edt. A. Bailes, I. Frommelt. – Oxford University Press, 2004. – 328 p.
6. Философский энциклопедический словарь. – М.: Сов. энциклопедия. Гл. ред.: Л. Ф. Ильичев и др., 1983.
7. Lazari A. European Critical Infrastructure Protection. – Springer, 2014. – 154 p.
8. Rothschild E. What is Security? // Daedalus. – 1995. – 124 (3). – P.53–98.
9. SWD (2013) 318 final: On a new approach to the European Programme for Critical Infrastructure Protection [Електронний ресурс]. – Режим доступу: <http://ec.europa.eu/>
10. Protection of critical infrastructures and critical societal functions in Norway [Електронний ресурс] // Report NOU 2006:6 submitted to the Ministry of Justice and Police on 05.04.2006. – Режим доступу: <http://www.regjeringen.no/>
11. Brassett J., Vaughan-Williams N., Security and the performative politics of resilience: Critical infrastructure protection and humanitarian emergency preparedness // Security Dialogue. – 2015. – 46 (1). – P.32–50.

12. De Bruijne M., Van Eeten M. Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment // J. of Contingencies and Crisis Management. – 2007. – 15 (1). – P.18–29.

13. Горбулін В. П. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу // Стратегічні пріоритети. – 2014. – №4 (33). – С.5–11.

14. Рыбка С. В., Кільчицький А. В., Післегін О. М. Кіберпростір, управління інфраструктурою, кібербезпека // Страт. панорама. – 2015. – №1. – С.126–134.

15. Comprehensive Approach as «Sine Qua Non» for Critical Infrastructure Protection / Edt. Čaleta D., Radović V. – IOS Press, 2015. – P.308.

16. Aradau C. Security That Matters: Critical Infrastructure and Objects of Protection // Security Dialogue. – 2010. – 41 (5). – P.491–514.

References

1. Contemporary Security Studies. 3rd ed. / Edt. Collins A. – Oxford, 2013. – 479 p.

2. Zahyst krytychnoyi infrastruktury: problemy ta perspektyvy vprovadzhennya v Ukraini: analit. dop. / D. S. Biriukov, S. I. Kondratov. – K.: NISD, 2012. – 102 s.

3. Koncepcija zahystu krytychnoyi infrastruktury: zb. mizhnar. nauk.–prakt. konf. (7–8 lystopada 2013 r., Kyiv – Vyshhorod). – K.: NISD, 2014. – 147 s.

4. Lewis T. G. Critical infrastructure protection in homeland security: defending a networked nation. – Willey and Sons, 2006. – 486 p.

5. Business and Security: Public–Private Sector Relationships in a New Security Environment / Edt. A. Bailes, I. Frommelt. – Oxford University Press, 2004. – 328 p.

6. Filosofskij jenciklopedicheskij slovar'. – M.: Sov. jenciklopedija. Gl. red.: L. F. Il'ich'ov i dr., 1983.

7. Lazari A. European Critical Infrastructure Protection. – Springer, 2014. – 154 p.

8. Rothschild E. What is Security? // Daedalus. – 1995. – 124 (3). – P.53–98.

9. SWD (2013) 318 final: On a new approach to the European Programme for Critical Infrastructure Protection [Elektronnyj resurs]. – Rezhym dostupu: <http://ec.europa.eu/>

10. Protection of critical infrastructures and critical societal functions in Norway [Elektronnyj resurs] // Report NOU 2006:6 submitted to the Ministry of Justice and Police on 05.04.2006. – Rezhym dostupu: <http://www.regjeringen.no/>

11. Brassett J., Vaughan–Williams N., Security and the performative politics of resilience: Critical infrastructure protection and humanitarian emergency preparedness // Security Dialogue. – 2015. – 46 (1). – P.32–50.

12. De Bruijne M., Van Eeten M. Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment // J. of Contingencies and Crisis Management. – 2007. – 15 (1). – P.18–29.

13. Horbulin V. P. «Гібридна війна» як klyuchovoy instrument rosijs'koyi heostrategiyi revanshu // Stratehichni priorytety. – 2014. – №4 (33). – С.5–11.

14. Rybka S. V., Kilchyckyj A. V., Pislehin O. M. Kiberprostir, upravlinnya infrastrukturoyu, kiberbezpeka // Strateh. panorama. – 2015. – №1. – С.126–134.

15. Comprehensive Approach as «Sine Qua Non» for Critical Infrastructure Protection / Edt. Čaleta D., Radović V. – IOS Press, 2015. – P.308.

16. Aradau C. Security That Matters: Critical Infrastructure and Objects of Protection // Security Dialogue. – 2010. – 41 (5). – P.491–514.

Biriukov D. S., cand. tech. sciences, head of sector, National Institute for Strategic Studies (Ukraine, Kyiv), dmytro.biriukov@niss.gov.ua

Conceptualisation of the critical infrastructure protection within contemporary security studies

This paper discusses the formation of the political science concept of critical infrastructure protection as a way for understanding, explanation and investigation of transformations in the national security system of modern states. The object for which this concept is «a way of understanding» was defined, and the «guiding idea» of this concept was formulated. Within the field of application of this concept there are issues of the operationalization of national interests, balance of interests in the «state–society–business» triangle, politicization (securitization) of security threats.

Keywords: national security, critical infrastructure, concept in political science, applied political research.

Бирюков Д. С., кандидат технических наук, заведующий сектором, Национальный институт стратегических исследований (Украина, Киев), dmytro.biriukov@niss.gov.ua

Концептуализация защиты критической инфраструктуры в современных исследованиях по вопросам безопасности

Рассматривается вопрос о формировании политологической концепции защиты критической инфраструктуры как способа понимания, объяснения и исследования процессов преобразований в системах обеспечения национальной безопасности современных государств. Определены предмет, для которого данная концепция «способом понимания», сформулирована ее «руководящая идея». В прикладном поле концепции разрабатываются вопросы операционализации национальных интересов, установления баланса интересов в треугольнике «государство–общество–бизнес», политизации (секьюритизации) проблем безопасности и др.

Ключевые слова: национальная безопасность, критическая инфраструктура, политологическая концепция, прикладные политологические исследования.

УДК 323.1:321.01:316.322(091)

Горло Н. В.,
кандидат історичних наук, доцент, доцент кафедри
політології, Запорізький національний університет
(Україна, Запоріжжя), ngm1@rambler.ru

Підходи до типології іредентизму

Мета дослідження полягає у критичному аналізі підходів, запропонованих зарубіжними науковцями для типології іредентизму, та у формуванні нових критеріїв типології. Виокремлення якісних характеристик різноманітних проявів іредентизму дозволяє провести теоретичну типологію, результатом якої є формування ідеальних типів (моделей) іредентизму. Їх розробка сприяє кращому пізнанню явища, адже специфічні риси кожного конкретного прояву іредентизму виступають більш яскраво саме на фоні особливостей всього типу.

Автором запропоновані критерії типології: характер відносин між суб'єктами іредентизму; характер дій, який приписується іншими політичними акторами суб'єктам іредентизму; зміст іредентистських вимог. На основі цих критеріїв виділено такі типи іредентизму: однобічний і взаємний; сепаратистський і експансіоністський; етнотериторіальний і територіальний.

Ключові слова: іредентизм, типологія, типи іредентизму, споріднена держава, іредента.

З огляду на масштаби світової історії іредентизм є відносно молодим політичним явищем, яке виникло у другій половині XIX століття в Італії. Але з того часу він неодмінно здійснює потужний вплив на міжнародні відносини, виконуючи дестабілізуючу роль на світовій політичній арені. Географія іредентизму розширилася, тому що нині різноманітні його прояви спостерігаються у різних кутках світу.

Іредентизм породжений модерною епохою, як, власне, і самі нації та національні держави. Його виникнення обумовлене орієнтацією національних урядів на приведення у відповідність державних кордонів до ареалів розселення етнонаціональних груп, які, як вважається, мають відноситися до однієї нації. Іредентизм – це політичний курс, суб'єктами якого можуть бути держави, політичні партії чи суспільно–політичні рухи, які закликають приєднати до складу однієї держави суміжні території сусідніх держав разом з населенням, яке споріднене за низкою етнокультурних ознак, серед яких культура, мова чи релігія. Проте таке досить універсальне визначення іредентизму у той же час є надто загальним, тому що претендує на всеохоплюючу характеристику цілком відмінних проявів іредентизму. Погляд на історію засвідчує відмінності між італійським іредентизмом, об'єднавчим рухом курдського народу чи експансіоністським іредентизмом Німеччини стосовно Судетської області або Російської Федерації стосовно