

중국의 은밀한 對美 전쟁

미국을 약화시키기 위한 전복전략과 무제한 전쟁 방법

- STEP 1

도덕적 가치 파괴
- STEP 2

사회 불안 형성
- STEP 3

갈등 유발
- STEP 4

개입

<https://kr.theepochtimes.com>

STEP 1

도덕적 가치 파괴

STEP 2

사회 불안 형성

STEP 3

갈등 유발

STEP 4

개입

THE
EPOCH
TIMES

문화 선전전 (MEMETIC WARFARE)

문화 개념을 도입하고, 궁극적으로 문화에 영향을 미치기 위해 대상 집단에 사상을 주입하고 전파한다.

문화전 (CULTURE WARFARE)

해외 유명 영화에 막대한 자본을 투자하고, 거대 시장을 미끼 삼아 할리우드 영화계에 영향력을 확대했다. 이는 할리우드 영화가 중국을 지배할 것이고, 중국 선전을 촉진시킬 수 있게 하였다.

정계 침투 (POLITICAL INFILTRATION)

중국은 경제 단체나 싱크탱크 등에 침투해 정치적 영향력을 행사한다. 중국에서 사업하는 미국 기업에도 정치적 영향력을 행사해 미국 대선 후보 또는 후보 선출에까지 영향력을 행사한다.

외교전 (DIPLOMATIC WARFARE)

상대국을 압박하거나 행동을 비난하는 방식으로 정보 활동이 전개된다. 특히 최근에는 코로나19 초기 대응 비판에 맞서 '늑대전사' 외교 전술을 구사함으로써 강도 높은 공세를 이어오고 있다.

해외통제 (OVERSEAS GOVERNANCE)

중국은 국무원교무관공실과 같은 기관을 통해 해외 중국 공동체를 감독하거나 통제하고 있다.

통신전 (TELECOMMUNICATIONS WARFARE)

최대 통신장비업체인 화웨이(華為)를 통해 전 세계 5세대(5G) 이동통신망 통제를 꾀한다. 화웨이 장비는 스파이 활동이나 통신망 교란 등에 사용될 수 있다.

무역전 (TRADE WARFARE)

중국 정부는 불공정한 무역 관행과 중국의 요구에 따르지 않는 국가에 관세를 부과하고 시장 접근을 제한하는 등 상인주의적 국내 정책을 통해 자유롭고 공정한 세계 무역 질서를 저해해왔다.

사이버전 (CYBERWARFARE)

중공군 및 정보기관과 연계된 중국 해커들은 무역기밀과 개인정보를 탈취하기 위해 미국 기업들과 정부 기관을 대상으로 대규모 사이버 공격을 감행한다.

제재전 (SANCTION WARFARE)

타국의 주요 산업을 공격하거나 자국의 이익에 영향을 미치는 조직에 대해 선 제재를 가한다.

대리전 (PROXY WARFARE)

다른 나라의 군대를 조종하고 군비를 제공해 비공개적으로 전쟁에 개입한다.

게릴라전 (GUERRILLA WARFARE)

적을 교란시키기 위해 전문화된 전투 부대를 이용한다. 여기에는 암살, 자원 파괴, 보급선 차단 등이 포함된다.

독살전 (POISONING WARFARE)

독극물을 사용해 목표로 하는 사람들을 살해하거나 약화시킨다. 이는 구소련 시절 공산당의 전술과 동일한다. 마러 전쟁 당시 구소련은 상수도에 독극물을 주입하라는 지시를 내린 바 있다.

생화학전 (BIOCHEMICAL WARFARE)

화학 무기와 생물학 작용제를 사용하여 질병과 혼란을 야기하고, 인구를 관리한다.

휴면 첩보전 (SLEEPER AGENTS)

활동하지 않는 첩보망을 활성화하여 테러나 비밀 작전을 시작한다.

언론전 (MEDIA WARFARE)

중공은 공공 정보를 조작하고, 인식을 전환시키기 위해 공격 플랫폼을 활용했다. 일례로 2019년 홍콩 민주화 시위와 중공 바이러스(코로나19)에 대한 허위정보 유포 및 선전선동을 위해 미국의 글로벌 소셜미디어 업체 페이스북과 트위터에 봇(bot-소프트웨어 형태의 AI 로봇) 네트워크를 배치시켰다.

밀수전 (SMUGGLING WARFARE)

조직화된 범죄 조직이나 인도주의 단체를 밀수 등 반입 통로로 활용하고 추가 전복 작전에 사용한다.

금융전 (FINANCIAL WARFARE)

통화 조작, 은행 통제, 위조 외화 유통 등이 일반적이다. 트럼프 행정부가 중국산 제품에 추가 관세 부과 방침을 밝히자 2019년 8월 중국 정부는 위안화 가치를 떨어뜨려 환율을 조작했다.

정보전 (INTELLIGENCE WARFARE)

중국은 타겟이 어떻게 작동하는지 알아보기 위해 광범위한 정보망을 유지하고 있다.

반대파 통제 (CONTROLLED OPPOSITION)

상대방의 이익을 지지하는 것처럼 보이는 단체를 만들거나 활동을 하고, 갈등 상황이 생길 때 이를 이용한다.

원자전 (ATOMIC WARFARE)

컨테이너 선적, 여행가방 폭탄 또는 대리국으로부터 전략 물품을 파괴하기 위해 선제 핵 공격을 감행한다.

전자기 펄스 (ELECTROMAGNETIC PULSE)

해무기로부터 발생하는 전자기 펄스를 사용해 전력망과 대다수의 전자 제품을 파괴한다.

전자전 (ELECTRONIC WARFARE)

통신망을 가로채고 명령 및 제어 시스템을 교란하기 위해 전자기파 스펙트럼을 공격한다.

우주전 (SPACE WARFARE)

전략 위성을 파괴하여 목표로 하는 국가와 군의 의존하는 중요한 시스템을 무력화시킨다.

심리전 (PSYCHOLOGICAL WARFARE)

사람들의 사고방식을 바꾸고 특정 메시지에 대한 감정을 유발하는 데 초점을 맞추고 있다. 중공은 정권을 향한 비판을 중국인을 향한 비난으로 인식하도록 만들어 애국적인 반응을 촉진시킨다.

허위정보 (DISINFORMATION)

허위 사건과 보도를 만들어 신뢰할 수 있는 해외 매체를 통해 확산시켰다. 중국이 코로나19 발병 사례를 축소 보고하고 있다는 증거가 많았지만, 사방 언론과 기관들이 중국 당국의 발병 수치를 계속해서 보도하는 것이 그 예다.

오보전 (MISINFORMATION)

대중의 토론과 분석을 혼란하게 만들기 위한 목적으로 명백한 허위 정보를 유포한다. 중국 외교관들은 코로나19 사태 책임론에서 벗어나기 위해 미군이 중국 우한에 바이러스를 유입했다는 근거 없는 음모론을 퍼뜨렸다.

교육전 (EDUCATION WARFARE)

중공 정부로부터 자금을 지원받는 교육기관인 공자학원은 공산주의 이념을 선전하고, 중국이 민간이라고 여기는 문제에 대한 검열을 실시해 학교 내 언론 및 표현의 자유를 억압한다. 미국 대학 캠퍼스 내 80여개, 초·중고 내 500여개 공자학원이 설립됐다.



인프라전 (INFRASTRUCTURE WARFARE)

중국은 자국 중심 경제벨트인 '일대일로'(一帶一路)를 통해 유럽과 아프리카, 아시아를 비롯한 참여국들에게 항만, 철도, 도로 등의 대규모 디지털 인프라 투자를 할으로써 국제 정치·경제에 대한 영향력을 확대해 나간다.

스파이전 (SPY WARFARE)

베이징은 간첩을 이용해 정치적 전복, 정보 수집, 경제적 이익 취득, 영향력 확대 등을 수행한다.

미인계와 협박 (HONEYTRAPS AND BLACKMAIL)

정치인과 기업인 등 영향력 있는 인사들을 유혹하여 협박에 사용할 수 있는 상황을 만든다.

환경전 (ENVIRONMENTAL WARFARE)

환경 문제를 이용해 자원 공급을 차단하거나 조작한다. 세계 최대 탄소 배출국인 중국은 파리 기후협약에 서명했음에도 자국 내 석탄화력발전 용량을 늘리는 한편 개발도상국에 수백개의 석탄발전소를 건설 및 투자하고 있다.

강압 및 협박 전술 (STRONG-ARM AND INTIMIDATION TACTICS)

영향력 있는 평론가 또는 반체제 인사를 위협하고 살해하기 위해 조직적인 범죄 조직 및 불량배를 동원한다.



위조상품전 (COUNTERFEIT WARFARE)

중국은 최대 위조품 수출국이다. 미국 세관 국경보호국(CBP)은 2019년 10억달러 규모의 중국산 악동 물품을 압수했는데, 이는 압수된 물품 전체 가운데 절반을 차지했다.