

2 미국 FBI, 첫 공개 사이버 전략으로 선제 대응체계 전환

➔ FBI, 사후 수사·기소에서 공격 생태계의 상시적 약화로 대응 목표 확대

- FBI, 범죄·국가안보 위협을 포괄하는 첫 공개 사이버 전략 발표
 - 미 연방수사국(FBI)은 사이버범죄와 국가안보 위협에 대응하기 위한 첫 공개 사이버 전략을 발표, 본부·지부·해외 인력을 포괄하는 사이버수사국 전체의 임무·우선순위 제시 ('26.9.9.)
 - 기존 사이버 전략이 기밀로 운용되거나 중국·러시아·범죄조직 등 개별 위협 단위로 마련된 것과 달리, 조직 전체의 임무와 우선순위를 외부에 공개한 최초의 전략이라는 점에서 차별화
 - 이번 전략 공개는 정부·산업계·국제 파트너에게 FBI와의 협력 방식을 제시하는 동시에 공격자에게는 지속적인 추적·차단 의지를 전달하며, 문서 공개 자체가 사이버 대응을 위한 정책적 수단으로 기능
- 국경·관할의 한계와 공격의 고속·대규모화가 전략 전환의 핵심 배경
 - FBI는 공격자가 국경 밖에서 인프라·도구를 빠르게 재구축하는 반면 수사·체포는 관할과 절차의 제약으로 지연되는 대응 속도의 구조적 격차를 이번 전략 수립의 직접적 배경으로 제시
 - 범죄조직은 개발자·중개자·서비스 제공자가 역할을 분담하는 구조로 진화해, 개별 행위자를 제거해도 공격 능력이 유지되는 복원력을 확보
 - 여기에 AI가 침투 시간을 줄이고 공격 진입 장벽을 낮춰 공격의 생성·확산 주기가 더 짧아지면서, 사후 수사·기소 중심 체계로는 대응 속도를 맞추기 어렵다는 판단이 새 전략의 출발점
- 트럼프 행정부의 국가사이버전략, 기관별 실행체계 구체화 단계 진입
 - 이번 전략은 '26년 3월 트럼프 행정부가 발표한 국가 차원의 사이버 대응 기조(President Trump's Cyber Strategy for America)를 FBI의 임무와 권한에 맞춰 구체화하는 과정의 일환
 - CISA·NSA·CIA 등도 국가전략에 맞춰 기관별 실행전략을 별도로 수립 중이며 일부는 비공개로 운용될 예정으로, 미국은 단일 국가전략을 기관별 임무체제로 구체화하는 단계에 진입
 - FBI 전략은 ▲공격 생태계의 상시적 무력화 ▲정부·민간·국제 파트너와의 공동작전 ▲AI·전문인력 기반의 내부 역량 강화라는 세 축으로 구체화

➔ FBI 사이버 전략의 3대 핵심축: 상시적 무력화·외부 협력·내부 역량 강화

1. 사후 수사·기소에서 공격 능력의 상시적 차단·약화로 대응 목표 전환

- 사후 체포 중심 대응에서 ‘공격 생태계의 상시적 무력화’로 작전 목표 전환
 - FBI는 사이버 위협을 ▲공격자·조직 ▲인프라 ▲자금 ▲공격 도구 네 요소가 결합된 생태계로 규정, 해당 요소를 함께 겨냥해 하나의 경로가 막혀도 다른 경로로 압박이 이어지도록 설계
 - 체포·기소가 가능한 경우 기존 사법절차를 우선하되, 즉각적인 집행이 어려운 경우에도 인프라 차단·자금 압수·도구 해체로 작전 지속성, 조직 확장성, 재공격 능력을 각각 약화
 - 체포 여부뿐 아니라 작전능력을 얼마나 약화했는지를 성과로 평가하고, 장기간 준비하는 대형작전 대신 기회가 생길 때마다 압박을 이어가 공격자가 이익보다 큰 비용을 부담하도록 설계
- 작전 단계별 최적 주체 투입으로 관할·권한 제약 최소화
 - 생태계 4요소를 동시에 압박하려면 여러 국가에 분산된 인프라·자금에 접근해야 하나 FBI 단독으로는 한계가 있어, 작전 단계별로 주도 주체를 달리하는 원칙도 함께 제시
 - FBI는 각 작전 단계에서 가장 적합한 권한·접근 경로·역량을 보유한 기관이 해당 국면을 주도하는 ‘최적 주체(Best Athlete)’ 원칙을 적용해 작전 주체를 유연하게 배치
 - FBI가 모든 단계를 직접 주도하지 않고 국내외 정부기관·민간 파트너의 강점을 단계별로 결합해, 관할·권한 한계로 인한 지연을 줄이고 여러 관할에 걸친 압박을 연속적으로 이어갈 수 있는 효과

2. 외부 정보 공유 원칙 전환과 민관·동맹 공동 작전 체계 확대

- 수사상 정보 보호보다 피해 차단을 우선하는 신속 정보 공유 체계로 전환
 - 단계별 최적 주체와의 공동작전은 외부와의 신속한 정보 공유를 전제로 하는 만큼, 정보 보류에 따른 수사상 이익보다 조기 공유를 통한 피해 차단 효과를 우선하도록 판단 기준을 변경
 - 레더먼 부국장은 이를 FBI 내부의 ‘문화적 전환’으로 설명, 정보 공유를 기본값으로 두고 미공유 시 근거 제시를 요구하는 방향으로 운영 원칙을 바꿔 수사 성과보다 피해 차단에 우선순위를 부여



- 자동화된 침해지표 공유체계로 위협 탐지부터 민간 통보까지의 소요 시간을 일→시간→분 단위로 단축하겠다는 목표도 제시해, 공유 원칙의 변화를 측정 가능한 지표로 구체화
- 피해기업 신고 유도과 초기 대응 지원체계 강화
 - 민관 협력의 실효성은 피해기업의 조기 신고에 달려 있으나, 최근 기업의 신고 기피가 이어지며 신속한 정보 공유의 출발점 자체가 악화되는 문제 부상
 - 기업 입장에서는 신고에 따른 지원 효과보다 침해 사실의 규제기관 노출과 후속 책임에 대한 부담을 크게 인식하여 법률 자문으로 신고가 지연되는 등, 추가 공격 여지를 키우는 사례도 발생
 - 이에 FBI는 피해기업을 조사 대상이 아닌 보호·지원 협력 주체로 규정하고, 제공 정보의 규제기관 비공유 입장과 피해자금 동결·회수 등 대응수단을 제시해 초기 대응 파트너로서 신뢰를 강화
- 민간·동맹을 정보 공유 상대에서 실제 작전 파트너로 확대
 - 앞서 구축한 신뢰 기반 위에 '26년 8월 트럼프 대통령 각서가 검증된 미국 기업의 해외 작전 참여 제도를 마련하면서, 민간기업이 공격 징후 데이터·인프라 접근권을 결합하는 '작전 파트너'로 격상
 - 다만 민간이 독자적으로 표적을 선정·공격하는 구조는 아니며, 연방정부가 작전 통제권을 유지한 채 기술·실행 역량만 선택적으로 결합해 역할과 책임의 경계를 설정
 - 20개국 이상에 배치된 사이버 주재관을 통해 각국의 정보·법적 권한·현지 접근성을 연결, 민간·동맹의 역할을 정보 제공에서 실제 작전 수행으로 확대

3. AI·전문인력·기술 고도화를 통해 작전 속도와 규모를 동시에 확대

- AI 기반 대규모 수사 분석 자동화 및 능동적 위협 대응 확대
 - 전략의 마지막 축은 앞서 제시한 상시적 무력화와 공동작전 체계를 뒷받침할 FBI 내부 처리역량의 확장에 초점, AI를 수사·분석·대응의 속도와 규모를 높이는 핵심 수단으로 제시
 - AI 활용은 ▲7개 수사·분석 업무의 자동화와 판단 지원 고도화, ▲위협 행위자 탐지·유도·기만 등 대응 과업의 자율 수행을 위한 에이전틱 AI 도입의 두 축으로 확대해 속도와 대응 범위 제고
 - 다만 최종 판단과 책임은 인간 검토 및 기존 법집행 체계에 남겨두는 통제된 원칙을 적용하고, 시민 자유·정확성·작전 보안을 위한 안전장치를 갖춰 CISA·민간 기업과 협력해 도입할 계획

- AI 도입을 현장 작전 역량으로 연결하는 인력·기술 기반 정비
 - AI 도입과 함께 수사 판단과 기술 전문성을 결합한 인력 확보를 내부 역량의 핵심 기반으로 설정, 특수요원·정보분석관·데이터과학자·악성코드 및 가상자산 전문가 등 사이버 특화 직군 채용 확대
 - 사이버교육훈련부서(CETU)를 중심으로 기술교육·자격 과정·모의훈련을 확대해 새로운 기술을 도입하는 데 그치지 않고 현장 수사·작전으로 전환할 수 있는 내부 전문성을 축적
 - 기술 기반도 최대 8,800만 달러 규모의 기관용 AI 하드웨어 조달과 증거 수집·작전 시스템의 양자 내성 전환으로 정비해, 인력·기술 양면에서 새 전략을 뒷받침하는 내부 기반을 마련하는 단계

출처 : Politico 외(2026.9.)

<https://subscriber.politicopro.com/article/2026/09/fbi-cybersecurity-strategy-promises-urgency-in-disruptions-01068735>

<https://www.politico.com/news/2026/03/06/white-house-trump-cyber-strategy-00817698>

<https://www.nextgov.com/cybersecurity/2026/09/new-fbi-cyber-strategy-seeks-faster-action-against-hackers-larger-industry-role/415869/>

<https://www.fbi.gov/file-repository/fbi-cyber-strategy-2026.pdf/view>

<https://www.ic3.gov/Outreach/PrivateSectorEngagement>

<https://therecord.media/fbi-releases-first-public-cybersecurity-strategy>

<https://www.cybersecuritydive.com/news/fbi-cybersecurity-strategy-disruptions-information-sharing/829913/>