유·무인복합체계를 위한 지능적 다계층 은닉 위장 기술 동향

Technological Trends of Intelligent Multi-Layered Concealment and Camouflage for Manned-Unmanned Teaming

홍강운 (K.W. Hong, gwhong@etri.re.kr) 국방ICT융합연구실 책임연구원
김태엽 (T.Y. Kim, youby@etri.re.kr) 플렉시블전자소자연구실 책임연구원
임진혁 (J.H. Yim, jhyim@etri.re.kr) 국방ICT융합연구실 선임연구원
유윤식 (Y.S. Yoo, ys5315@etri.re.kr) 국방ICT융합연구실 책임연구원
정부금 (B.G. Jung, bgjung@etri.re.kr) 국방ICT융합연구실 책임연구원
이종국 (J.K. Lee, raphael@etri.re.kr) 국방ICT융합연구실 책임연구원/실장
박혜숙 (H.S. Park, parkhs@etri.re.kr) 국방안전융합연구본부 책임연구원/본부장

ABSTRACT

As shown in the recent war in Ukraine, asymmetric approaches such as drones, cyber warfare, satellite communications, AI, and big data can undermine the superiority of conventional force. Consequently, multi-layered concealment and camouflage systems covering wireless communications, networks, physical devices, and cyber counterattacks have become decisive in modern warfare. In particular, the ability to hide assets, counter eavesdropping and detection, thwart jamming and hacking, and even launch counterattacks is now essential. In this paper, we examine recent advances in wireless, network, and physical concealment, along with cyber counterattacks, focusing on the modern drone- and satellite-driven battlefield environment. We also explore strategies such as intelligent service platforms, edge AI, on-device AI, and standardization to enhance autonomy in unmanned systems and enable efficient mass production for future battlefields, where manned–unmanned teaming is expected. Ultimately, concealment/camouflage and asymmetric capabilities will be crucial in future military operations. When combined with the intelligence and production efficiency technologies of manned–unmanned teaming, they enable reduced casualties, enhanced efficiency, and flexible force deployment.

KEYWORDS 생산효율화, 위장, 유·무인복합체계, 은닉, 지능화

* DOI: https://doi.org/10.22648/ETRI.2025.J.400304
* 이 연구는 2022년 정부(방위사업청)의 재원으로 국방과학연구소의 지원을 받아 수행된 미래도전국방기술 연구개발사업임[No. 915064201].

Ⅰ. 서론

2022년 러시아-우크라이나 전쟁의 발발 초기에는 군사력을 앞세운 러시아의 일방적 우위가 전망되었다. 과거 미국 중심의 연합군은 이라크 전쟁에서 GPS · 레이저를 통한 정밀유도무기, 현대화된 전술 전략 항공기를 앞세운 항공우세, 인공위성 등 고성능 정찰 및 정보자산을 운용한 네트워크 중심전, 정찰감시를 위한 무인기 운용, 미사일과 레이더망을 무력화시킨 전자전, 헬기 · 전차 · 항공 협동 운용을 통한 기동전이라는 첨단 군사기술을 활용하여 이라크 정규군을 제압하여 단기간에 승기를 잡을 수 있었다[1]. 따라서, 러시아와 우크라이나는 군병력, 항공전력, 재래식 무기 및 첨단 무기 면에서 군사전력 차이를 보여 이라크 전쟁에서와 같은 결과를 예상할 수 있었다. 하지만, 군사전력 규모와 기술수준에서 열세인 입장에서 상대의 우위를 무력화하고 억제하기 위해 정면승부나 상대의 강점을 피하고 약점을 노리는 비전통적이고 비대칭적인 수단인 드론, 사이버전 등의 비대칭전력이 적극 활용되어 강대국에 저항할 수 있었다.

우크라이나 전쟁에서는 더 이상 전차와 포탄이 중요한 전통적 군사전력이나 압도적 전력 우위의 현대화된 군사전력이 전쟁승리의 핵심이 아니다. 대신에 드론, 사이버전, 저궤도 위성 및 민간 위성통신, AI · 빅데이터의 활용이 그 역할을 대신한다. 소형 상업용 드론부터 정찰 · 공격용 군사 드론, 자폭 드론까지 폭넓게 활용되고, 드론이 포병 지휘, 표적 지정, 적 전차 · 장비 파괴 등 드론을 대규모로 다양하게 사용함으로써 전투에서 결정적 역할을 수행한다. 전면 침공 전에 기간망과 위성 및 광역통신망을 무력화시키고 전력과 원자력 등 핵심인프라를 교란시키며 정보를 탈취하기 위한 사이버전을 적극적으로 전개한다. 파괴된 군사지휘통신체계를 복구하고 위성사진을 통해 전장 정보를 획득하기 위해 저궤도 위성 및 민간 위성통신을 활용한다. AI · 빅데이터는 피아식별, 포병 사격좌표 산출, 병력 · 장비 추적 등에 활용된다[2].

상기와 같이 전쟁에서 드론, 위성 등을 통한 탐지 · 표적화가 매우 활발한 환경으로 변화함에 따라 은닉 및 위장 기술이 전쟁의 성패를 좌우할 정도로 중요해졌다. 드론의 위협을 무력화하거나 방어하기 위해 GPS 교란이나 가짜 신호를 송출하여 비행경로를 왜곡하거나 목표에 도달하지 못하도록 하고, 전파 방해 신호를 발생시켜 드론의 통신 채널을 방해함으로써 원격 조정을 무력화하거나 공격을 저지한다. 차량 · 장비를 위한 위장망을 주변 지형 · 식생과 유사한 색상 · 패턴으로 구성하거나 열영상 탐지를 막기 위해 열 신호를 흡수 · 분산 · 차단하는 소재로 제작하여 항공 · 드론 시각 탐지를 어렵게 한다. 교란된 드론을 회수하거나 자폭 드론을 적진으로 되돌려 보내는 방식으로 역공격을 시도하기도 한다.

본고에서는 전장의 환경 변화에 대응하기 위한 군 자원 은닉 및 위장의 필요성과 그 동향에 대하여 고찰하고, 유 · 무인복합체계를 위한 적의 탐지, 공격을 감내하는 지능적 다계층 은닉 위장 기술 개발에 대해 소개하며, 유 · 무인전투체계가 보편화될 미래의 전장환경에 대응하기 위한 유 · 무인복합체계의 지능화, 자동화, 생산효율화 기술에 대해 간략하게 소개한다.

Ⅱ. 군 자원 은닉 및 위장의 필요성

미래전은 네트워크, 데이터, 지능 중심으로 빠르게 전개되며, 국방 정보통신 인프라에 상용 무선 네트워크와 IoT 활용이 필요하지만, 신뢰성 있는 상용 솔루션이 부족해 기술 개발이 요구된다. 무선 자원은 공유되어 재밍에 취약하고, 네트워크는 신뢰성

향상을 위해 피아식별과 경로 최적화가 필요하다. 또한, 장치의 물리적 위장과 공격에 대한 방어만으로는 한계가 있어, 역공격 기술 및 정보통신 기술과 물리 기술의 융합이 요구된다.

미래 전투체계인 아미타이거 4.0, 유 · 무인복합체계, 드론봇전투체계에서는 상용 통신 기술의 군사적 활용성을 강화하기 위해 적의 탐지 · 공격을 감내하는 지능적 다계층 은닉 · 위장 기술 연구가 필요하다. 무선통신, 네트워크, 사이버 분야에서 자원을 은닉 · 위장하여 적의 공격을 막고, 역공격을 지원하는 시나리오 기반 분석을 통해 연구개발의 효율성 향상이 요구된다.

미래 전투체계에서 스텔스 기동 및 네트워크화가 중요해짐에 따라 국방부, 합참, 육군 아미타이거 4.0 등이 해당 기술의 주요 수요자로 예상된다. 군은 높은 보안성과 효율적인 지능형 다계층 은닉 · 위장 기술에 대한 수요가 증가할 것으로 예상된다.

기존 국방 연구와 달리, 다중경로 및 Multi-RAT 환경에서 다계층 은닉기능을 유지하면서 우군 통신망의 신뢰성 확보와 역공격 기술이 필요하다. 이는 기술 패러다임 전환, 차별적, 혁신적, 도전적 연구를 요구한다.

Ⅲ. 군 자원 은닉 및 위장 기술 동향

군 자원 은닉 및 위장 기술과 관련 프로젝트/프로그램은 표 1과 같이 기술별로 구분하여 제시한다.

1. 무선통신 자원은닉 기술

무선통신 자원은닉 기술은 적의 감청 · 탐지 · 재밍 공격으로부터 아군 통신을 보호하고, 아군 무선통신 신호가 노출되지 않도록 하여 작전의 은밀성과 생존성을 확보하기 위한 기술이다.

확산 스펙트럼 기법은 통신신호를 원래 대역폭보다 넓은 대역에 퍼뜨려서 전송하는 방식이다. 정해진 주파수 대역 내에서 주파수를 옮겨 다니며 전송함으로써 적이 특정 주파수를 재밍하더라도 전체

표 1 은닉·위장 기술과 관련 프로젝트/프로그램

은닉·위장 기술		관련 프로그램/프로젝트
무선통신 [3-6]	• 확산 스펙트럼 기법 • 신호 방사 패턴 은닉·집중화 빔포밍 • 주파수를 실시간 변경하는 인지 무선 • 초저전력·위장 신호 전송 • 암호화·위장 프로토콜 적용 • 메시 네트워크 분산화	• DARPA의 SC2·SHARE·SSPARC·ART, DoD의 JTRS, OCCAR의 ESSOR, AFC의 Project Convergence, NATO의 FMN • 영국 국방부의 MORPHEUS·LETacCIS • 5G/6G MILTECH 융합 연구 • Drone Swarm 통신 연구
네트워크 [7-9]	• 동적 네트워크 주소 할당 • SDN 기반 이동 표적 방어 • 다계층 암호화 및 토폴로지 위장 • 분산·메시 네트워크의 다중경로 라우팅 • 사이버 기만·가상 세그먼트 기술	• DARPA의 Plan X·CINDER·CADETS, DoD의 제로트러스트, NATO의 FMN • 영국 국방부의 MORPHEUS, OCCAR의 ESSOR • 이스라엘, 싱가포르 등의 특수전·사이버 부문 연구 • Google의 BeyondCorp
물리장치 [10-16]	• 가시광선, 적외선, 레이더 다중 스펙트럼 • 전자기파 차폐 • 열 신호 감쇄 • 환경 동화형 위장 기술	• ETRI의 전기변색 위장 • 서울대의 다중스펙트럼 위장 피부, 연세대의 투명 메타물질 • 중국 하얼빈대학교 금속-유기 골격체 기반 소재 • 러시아의 Chameleon, 중국의 Chimera, EDA의 ASCALS
사이버 역공격	• 해킹백(Hacking-Back) • 사이버 기만 역공격 • AI/ML 기반 자동화 역공격 • 전자전·사이버 융합 역공격	• DARPA의 Plan X·HACCS·Cyber Grand Challenge, NSA TAO • NATO의 CCDCOE, 영국의 NCF, 프랑스의 COMCYBER • 이스라엘의 Unit 8200, CyberGym, CyberSpark

통신을 마비시키기 어렵게 하는 주파수 도약과 원 신호에 스프레딩 코드를 곱해 대역폭을 넓게 확산한 후 전송하고 수신 측에서는 동일 스프레딩 코드를 이용해야 함으로써 적의 신호 포착과 복원을 어렵게 하는 직접 확산 방식이 있다.

빔포밍 기술은 다중 안테나 배열을 이용해 특정 방향으로 신호 이득을 집중시킨다. 디지털 신호 처리 기법을 통해 특정 방향으로 전파가 강하고, 다른 방향에는 약하도록 빔 패턴을 조정하여 무선 신호가 원하는 수신기 쪽으로만 강하게 전달되어, 적 레이더나 탐지 장비가 있는 방향으로의 신호 유출을 최소화하여 신호 포착과 추적이 어렵고 재밍 공격에 대한 내성이 강하다.

지능형 주파수 선택과 인지 무선 기술은 무선환경을 실시간으로 파악하여 사용 가능한 주파수를 동적으로 탐색 · 선택하고 적의 재밍이나 감청 시도를 회피한다. 단말과 기지국이 스펙트럼 잡음과 신호 간섭을 지속적으로 모니터링하고, 적이 특정 주파수를 재밍하거나 감청을 시도할 경우 혼잡이 덜한 다른 주파수 대역으로 전환하고, 출력 세기, 변조 방식 등을 동적으로 조정하여 탐지 · 감청 난이도를 높일 수 있다.

초저전력 통신 및 숨김 전송 기법은 매우 낮은 전력으로 통신 신호를 전송하여 잡음 수준에 묻히도록 함으로써 적 레이더 · 수신기에 포착되지 않게 한다. 신호 대 잡음비가 극단적으로 낮은 조건에서 통신이 가능하도록 하고, 전송 속도와 범위가 제한된 특수환경에서의 군사작전에 활용할 수 있다.

주파수 · 위치 위장 방법은 정상적인 군 통신 신호처럼 보이지 않도록 상용 통신 또는 레이더 펄스 등 다른 형태로 위장하거나 전송 위치를 숨긴다. 군용 통신이 LTE, WiFi 등 일반 민간신호처럼 보이도록 변조 · 암호화하고 송신 지점을 의도적으로 분산 · 지연 · 변조함으로써 군 통신을 선별 · 재밍하거나 신호 발신지 파악을 어렵게 한다.

암호화와 위장 기술은 통신 신호 자체를 강력하게 암호화하여 내용을 판독하기 어렵게 하고, 패킷 헤더나 프로토콜 형태도 숨김 · 변조한다. AES, 공개키 암호 등의 고강도 암호화 기법을 사용하고, 패킷 구조나 헤더 정보를 위장하여 아군의 신호가 포착되더라도 유효 정보를 추출하기 어렵거나 파형 분석에 많은 시간과 자원이 소요되도록 한다.

그 외에도, 다수 노드가 상호 연결되어 다중경로로 데이터를 전달하도록 네트워크를 구성할 수 있다. 단일 노드나 기지국에 의존하지 않고 여러 경로를 통해 통신이 가능하도록 분산구조로 구성하고, 특정 노드나 경로가 재밍 · 파괴되더라도 네트워크 전체가 마비되지 않고 우회할 수 있도록 하여 트래픽 패턴을 추적하기 어렵게 할 수 있다.

2. 네트워크 자원은닉 기술

네트워크 자원은닉 기술은 네트워크의 물리 · 논리 자원(라우팅 경로, IP 주소, 노드 위치, 트래픽 패턴 등)을 적에게 노출하지 않거나 최소화하여 탐지 · 식별 회피, 공격 표적화 차단, 네트워크의 운용 보장, 보안성을 강화하기 위한 기술이다.

동적 네트워크 주소 할당 기법은 고정된 IP나 MAC 주소를 사용하지 않고, 주기적으로 변경하거나 여러 가상 주소를 번갈아 사용하여 네트워크 스캐닝과 IP 추적을 어렵게 한다. 소프트웨어 정의 라디오나 소프트웨어 정의 네트워크 환경에서 중앙 제어 노드가 일정 주기로 IP · 포트 · MAC 주소를 변경하고, 데이터가 전송되는 세션 구간에 임시 주소를 부여 후 세션 종료 후 폐기함으로써 적의 특정 노드에 대한 장기간 추적 · 감청, 대규모 포트 스캔이 필요하도록 하여 공격 지점에 대한 탐색, 트래픽 분석을 통한 패턴 식별 등을 어렵게 하여 재밍 · 전

자전 공격 시도를 약화시킬 수 있다.

소프트웨어 정의 네트워크 기반 이동 표적 방어는 네트워크 구성 · 포트 · 라우팅 경로 등을 지속적으로 변경하여 적의 공격 표적화 과정을 무력화한다. 방화벽 · IDS/IPS · AI 모델 등이 네트워크 이상 징후를 감지하고, SDN 컨트롤러가 해당 구간의 라우팅 경로, 가상 네트워크 세그먼트, 주소 블록 등을 할당하며, 아군 노드들을 인증/키 교환 등을 통해 변동 사항을 즉시 공유, 통신 세션이 단절되지 않도록 세션 유지함으로써 적의 네트워크 특성 파악을 어렵게 하고 전장 환경에서의 고신뢰 통신을 운영할 수 있도록 한다.

다계층 암호화 및 토폴로지 위장은 네트워크 계층부터 응용 계층까지 다계층 암호화를 적용하고, 라우팅/헤더 정보 등을 별도의 오버레이 계층으로 추상화해 숨긴다. 실제 IP 헤더라우팅 정보 위에 암호화된 헤더를 추가하고, 각 중간 노드는 자신에게 해당하는 암호 계층만을 해독하여 전체 경로를 알 수 없도록 하며, 적이 패킷을 캡처해도 프로토콜, 송신지와 수신지를 식별하기 어렵게 하여 전장 · 특수작전 환경에서 지휘소, 무인기, 지상군 노드 등의 정확한 물리 위치나 트래픽 관계가 노출되지 않도록 보호할 수 있다.

분산 · 메시 네트워크의 다중경로 라우팅은 네트워크 노드가 다수 존재하여 트래픽을 여러 경로로 나누어 전송함으로써 특정 경로에 대한 공격 · 재밍 시도를 무력화한다. OLSR, AODV, DSR 등 군용 라우팅 프로토콜을 통해 패킷마다 가능한 복수의 경로를 동적으로 선택하고, 중요한 정보를 여러 조각으로 나누어 다른 경로로 전송하며, 특정 노드 · 링크가 파괴되면 주변 노드가 자동으로 다른 경로를 통해 연결을 유지하는 경로 자가 치유를 통해 재밍, 물리적 파괴 상황에서도 고생존성 네트워크를 확보하고 네트워크 토폴로지에 대한 은닉성을 강화할 수 있다.

사이버 기만 · 가상 세그먼트 기술은 네트워크 내에 허위 세그먼트나 허니넷을 구축하여 적의 네트워크 침투 시 허위 시스템 · 허위 트래픽을 접하도록 유도한다. 실제 운영망과 기만용 망을 물리 · 논리적으로 구분하고, 적이 스캐닝 · 침투하면 우선 접근할 만한 유인용 자료를 제공하며, 아군 주요 서버나 지휘 노드는 공개되지 않는 별도 주소 · 경로로 통신하는 동시에 허위 세그먼트에 들어온 공격자 활동을 추적, 정보를 수집 또는 역공격하는 능동형 방어를 가능하게 한다.

3. 물리장치의 위장/스텔스 기술

물리장치의 위장/스텔스 기술은 물리장치나 개체를 주변 환경과 비슷하게 만들어 적으로부터 탐지를 회피하기 위한 차세대 위장 기술이다. 대표적으로 가시광선, 적외선, 레이더 대역을 포함한 다중 스펙트럼, 전자기파 차폐, 열 신호 감쇄, 환경 동화형 위장 등의 기술이 있다.

서울대학교 연구팀은 두족류의 위장과 같이 가시광선과 적외선 영역에서 동시에 작동하는 다중 스펙트럼 위장 피부를 개발하였다. 이는 금속 필러를 포함한 열전소재 엘라스토머를 이용하여 기존 대비 8.8배 높은 열전도도를 제공하며, 특정 적외선 파장에서 위장 효과를 극대화한다.

연세대학교 연구팀은 투명 메타물질을 개발하여 가시광선 및 적외선 영역에서 동시에 위장 효과를 구현하였다. 이 기술은 석영 기판 위에 ITO, Si_3N_4, Au/Ti로 구성된 다층 구조를 적용하여, 가시광선 영역에서 0.44의 투과율을 보이며 적외선 영역에서는 35μm 대역에서 64%, 814μm 대역에서 75%의 신호 감소 효과를 제공한다.

한국기계연구원은 12개의 그래핀 층을 PET 기판

위에 적용한 전기제어형 위장 기술을 개발하여 가시광선 차광률을 72%까지 조절하고, 적외선 방사율도 0.91에서 0.64로 변환한다.

한국전자통신연구원은 전기변색 기술을 활용한 위장 시스템을 개발하여 G4L 전극을 사용하여 전기변색 소자의 응답속도를 500ms 단위로 단축시키고, 낮은 작동전압(±2.5V)에서도 우수한 광학적 대비와 에너지 효율성을 제공한다.

러시아는 전기변색 유리를 기반으로 하여 전류 흐름에 따라 색상과 투명도를 조절하는 Chameleon 위장 기술을 개발하여 NATO 드론의 95%에 대한 은폐 효과를 제공한다. 중국은 가시광선 및 적외선 영역에서 동시에 작동하고 다양한 기상 조건에서 적용 가능한 Chimera 메타물질 기반 위장 기술을 구현하였다.

전자파 스텔스 기술 관련해서, 중국 하얼빈 공업대학 연구팀은 금속-유기 골격체 기반 고성능 광대역 전자파 흡수 소재를 기반으로 1.5mm 두께에서 -37.63dB, 4.0mm 두께에서 -50.7dB의 우수한 전자파 흡수 성능을 보이는 고성능 광대역 전자파 흡수 소재를 개발하여 다공성 구조와 금속 이온의 도입을 통해 전자파 감쇠 성능을 극대화한다.

유럽 방위청은 가시광선, 적외선, 레이더 대역에서의 탐지 회피를 위한 ASCALS 프로젝트를 추진 중이다.

미래 전장에서의 위장 및 스텔스 기술은 기존의 패시브 방식에서 능동적으로 환경에 적응하는 방식으로 발전하고 있으며, AI 기반 분석 및 메타물질을 활용한 위장 기술이 핵심 요소가 될 것으로 보인다.

Ⅳ. 지능적 다계층 은닉 위장 기술

상용통신기술은 항재밍 기능이 없어 군사적 활용이 어려우며, 재밍 · 도청에 취약하다. 무선통신 자원은 정적으로 할당되어 보안성과 주파수 효율이 낮고, 네트워크는 기존 구조와 장비의 취약성으로 보안성 제공이 어렵다. 또한, 물리적 장치는 적의 탐지에 쉽게 노출될 수 있으며, 사이버 전자전 대응은 수동적이다. 이를 해결하기 위해 은닉 위장 기술이 발전하고 있다.

지능적이고 다계층의 은닉 위장 기술을 통해 아군의 정보통신 자원과 장치를 적에게 보이지 않도록 하거나 노출을 최소화할 수 있다. 무선통신 자원을 은닉하여 재밍과 도청을 방지하고, 네트워크 자원을 숨겨 보안을 강화한다. 또한, 물리적 장치들은 적의 시각, 센서, 전자파 탐지에 대비해 위장되며, 사이버 전자전에서는 악의적 공격을 사전에 탐지해 대응하거나 역공격을 통해 능동적으로 방어할 수 있다.

1. 무선통신 자원의 지능적 은닉 기술

무선통신 자원의 지능적 은닉 기술은 무선자원을 대상으로 하는 재밍 공격을 회피하거나 인지하여 지능적으로 대응하는 기술이다. 기존 무선통신에서는 주파수, 코드 등이 고정되어 정보 노출 시 재밍 · 도청에 취약하고 단일 경로를 활용함으로써 적의 재밍 공격에 취약하며, 주파수 변환 시 단일 인터페이스 내에서 이루어지는 문제가 예상된다. 지능적 은닉 기술을 통해, 2계층 이상의 다계층 주파수와 인터페이스를 이용하여 인공지능 기반 광대역 주파수 동적 변환을 통해 보안 능력을 향상시키고 자원 할당 정보를 분산 전송함으로써 정보탈취를 불가능하게 하며, 다중채널 기반 분산 전송하여 무선통신 자원 정보에 대한 안전성을 확보할 수 있다.

무선통신 자원의 지능적 은닉 기술은 인공지능 기반 광대역 주파수 동적 변환, 지능적 무선자원 할당정보 은닉, 다중채널 기반 분산 데이터 전송 기술

로 구성된다. 인공지능 기반 광대역 주파수 동적 변환 기술은 인공지능 기반으로 무선 자원의 재밍 공격을 예측하고 지능적 무선할당 정보 은닉과 다중 채널 기반 분산 데이터 전송을 위해 재밍상태정보를 제공한다. 지능적 무선자원 할당정보 은닉 기술은 다자간 계산 기법을 바탕으로 비밀 정보를 조각내어 분산 저장하고 이를 복원하는 기능을 제공한다. 다중채널 기반 분산 데이터전송 기술은 할당받은 채널들을 동시에 활용하여 데이터를 전송하는 기능을 제공하고, 다중채널을 통해 수신된 데이터를 병합하는 기능을 제공한다. 이 기술은 SDR과 이상탐지 기반 재밍탐지, 다자간 계산 기반 비밀공유 및 복원, MPTCP 기반 데이터 전송 기능으로 구체화된다.

2. 지능적 블랙 네트워크 기술

피아식별을 통한 지능적 블랙 네트워크 기술은 전술 네트워크를 블랙 네트워크로 은닉하여 적의 해킹 공격으로부터 보호하는 기술이다. 기존 네트워크에서는 목적지 IP 기반의 정적 공개 라우팅 경로를 사용하고, 채널 폭주 시에는 성능이 저하되며, 정적 · 수동적 · 개별적으로 네트워크를 운용하는 것이 일반적이다. 지능적 블랙 네트워크 기술을 통해 피아식별을 통한 정보 기반의 최적 경로를 제공하고, 실시간 모니터링 및 최적화로 채널 성능을 보장하며, 연합 정책에 따른 동적 연결성 관리 및 보호가 가능하다.

피아식별을 통한 지능적 블랙 네트워크 기술은 임무 단위의 동적 트러스트 네트워크, 인공지능 기반 네트워크 위협 활동 탐지, 정책 기반 네트워크 제어 시스템 자동화 기술로 구성된다. 임무 단위의 동적 트러스트 네트워크 기술은 군 정보통신망의 인입점에 위치하여 사용자/단말 인증 후 서비스 접속 제어를 통제하고, 군 단말에 앱 형태로 탑재되어 액세스 단위의 사전 인증을 요청하는 기능을 제공한다. 인공지능 기반 네트워크 위협 활동 탐지 기술은 네트워크 위협 탐지, 인공지능 기반의 위협 판별, 위협 정보를 알림 등 군 정보통신망의 네트워크 위협을 인공지능으로 탐지 기능을 제공한다. 정책 기반 네트워크 제어 시스템 자동화 기술은 네트워크 리소스 관리 제어, 네트워크 리소스 상태 모니터링, 단말과 서비스의 접속 제어 등 군 정보통신망의 네트워크 엔티티들에 대한 관리, 제어 및 관제 기능을 제공한다. 이 기술은 제로 트러스트 네트워크 구조, SDP 기반 정책 제어 기능, 이상탐지와 분류 결합 기반 네트워크 위협 탐지 기능으로 구체화된다.

3. 지능형 광대역 스텔스/위장 기술

지능형 광대역 스텔스/위장 기술은 아군의 물리적 자산에 대한 광대역 가시광선/적외선 가변위장 및 전자파 스텔스 기술이다. 기존 물리적 장치에 대한 위장 분야에서는 다양한 종류의 이동형 무선 네트워크 장비를 적으로부터 보호하기 어렵고, 현재 사용되는 스텔스 기술은 협대역 고정형으로 제한적이고, 최근 안티드론 시스템은 급속히 기술 발전이 이루어지고 있으며, 스텔스/위장 기술은 전투기 및 전차 중심으로 개발되고 있어 정보통신장비/자산이 공간상에 노출되는 문제가 있다. 지능형 광대역 스텔스/위장 기술을 통해 투명 물질 기반의 다중 스펙트럼 가변 All-in-One 통합 스텔스/위장 플랫폼을 구현하고, AI 기반으로 환경변화 적응형 디지털 위장패턴을 형성하고, 근거리 및 장거리 무선 통신 모드에서 다양한 적의 탐지센서로부터 장비를 보호하며, 이동형 무선 통신장비를 위한 경량화 및 소형화된 정보통신 장비 보호가 가능하다.

지능형 광대역 스텔스/위장 기술은 가시광선 반

사율 제어를 통한 가시광선 감시로부터의 위장 기능, 적외선 방사율 제어 변색 물질 적용 적외선 감시로부터의 위장 기능, 메타물질을 이용한 X-band 흡수 산란을 통한 레이더 감시로부터의 위장 기능, 주변 환경에 은닉 가능한 적외선 및 가시광선 위장 패턴 형성 및 전달을 통해 위장을 구현할 수 있는 패턴 데이터 제공 기능으로 구성된다.

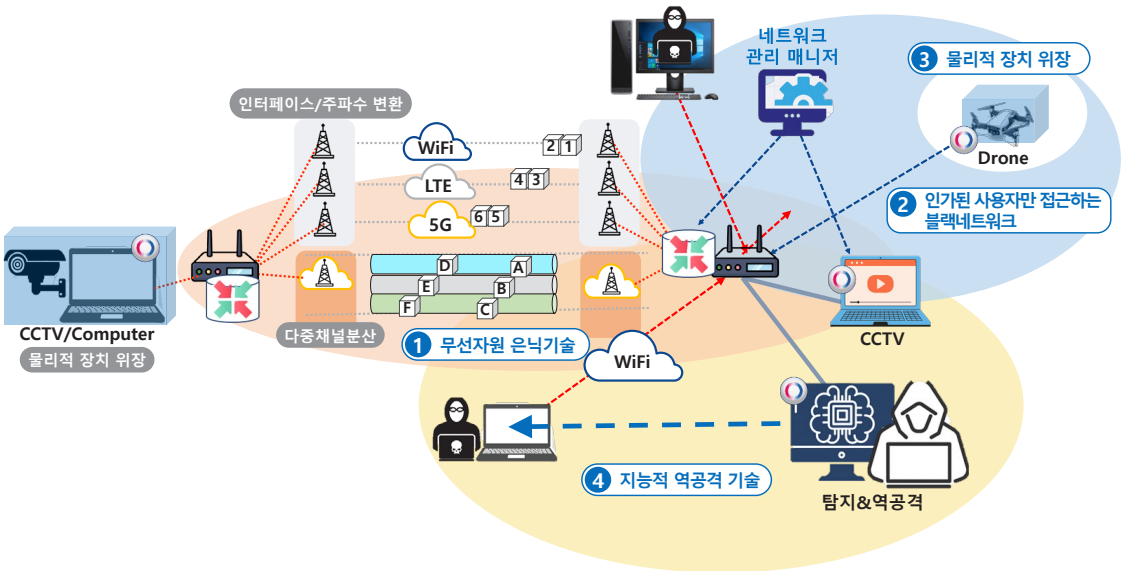
4. 악의적 노드 지능형 역공격 기술

악의적 노드 지능형 역공격 기술은 무선자원을 대상으로 하는 재밍 공격을 회피하거나 인지하여 지능적으로 대응하는 기술이다. 기존 사이버전에서는 아날로그 신호 위주의 분석으로 공격 맥락 파악 및 능동적 대응, 한정된 공격 데이터로 유사공격/신유형 공격의 대응이 어렵고, 공격 혹은 방어의 단일 연구 위주로 아군 방어와 동시에 역공격을 수행하는 연구가 제한되어 있으며, 단조로운 공격 방식 및 패턴, 단일 경로 활용으로 공격 실패 확률이 높은 문제점이 있다. 지능형 역공격 기술을 통해 공격 상황을 정밀 파악하고, 풍부한 사이버 공격 데이터 확보 및 대응력을 향상시키며 아군 전술망 신뢰성 유지 및 적군의 취약 요소 맞춤형 역공격이 가능하다.

악의적 노드 지능형 역공격 기술은 3D 위치, 프로토콜, 공격 패킷 특성 등 복합 정보를 이용한 악의적 노드 위치 및 공격패턴 탐지 기능, GAN 기반 공격/대응패턴 생성 기능, 그리고 TCP/IP 4계층 및 우군/적군 네트워크 토폴로지 기반의 복합 역공격 기능으로 구성된다.

5. 개념검증을 위한 테스트베드

프로토타입 기반 개념검증은 테스트베드에서의 기술시연을 통해 가능하다. 시연은 악의적 노드가 해킹을 시도할 수 있는 환경에서 위장된 CCTV가 설치된 서버로부터 관제 서버로 영상을 전송하



출처 게티이미지뱅크, 무단 전재 및 재배포 금지

그림 1 적의 탐지·공격을 감내하는 지능적 다계층 은닉 위장 기술 개념검증을 위한 테스트베드

는 시나리오(그림 1)를 통해 진행된다[17]. 지능적 은닉 위장 기술을 이용하여, 인터페이스 및 주파수를 변환하면서 다중채널을 통해 영상데이터를 전송한다. 지능적 블랙 네트워크 기술을 이용하여, 악의적 노드의 해킹 시도는 제로 트러스트 네트워크 기술에 의해 인가된 사용자만 접근 가능하고 인가되지 않은 사용자가 접근 시 알람 등을 발생시킨다. 지능적 역공격 기술을 이용하여, 서버에 대한 사이버 공격으로부터 공격을 시도한 컴퓨터의 위치로 역공격한다. 지능형 광대역 스텔스/위장 기술을 이용하여, CCTV와 드론을 물리적으로 위장시켜 보이지 않게 한다.

Ⅴ. MUM-T 지능화·생산효율화 기술

유 · 무인전투체계가 보편화될 미래의 전장환경에 대비하기 위해 유 · 무인복합체계를 지능화시키고 효율적으로 생산하는 데 필요한 기술을 소개한다.

1. 유·무인복합체계 지능화 기술

유 · 무인복합체계 지능화 기술은 인공지능, 머신러닝, 자율주행, 센서 융합 등의 기술을 통합해 상황을 스스로 인식하고 임무를 자율적으로 수행하여, 단순 정보수집 기능을 넘어 고도화된 의사결정을 지원하는 역할을 수행할 수 있도록 하는 기술이다. 이를 통해 전장, 핵 · 화생방 오염지역 등의 위험지대에 인간 대신 투입되어 인명 위험을 최소화하고, 사람의 개입 없이도 서로 협업하고, 복잡한 임무를 신속 · 정확하게 처리하여 작전 효율을 극대화하고, 인공지능 기반으로 임무 계획 · 경로 최적화 · 표적 식별 등을 통해 오작동이나 오인식을 줄여 정밀성 · 신뢰성을 향상시키며, 전장에서 예측 불가 상황이 발생하더라도 스스로 재계획 · 대응함으로써 다양한 환경에 적응할 수 있다.

유 · 무인복합체계의 지능화에 필요한 요소기술 중 지능형 서비스 플랫폼, 엣지AI 및 온디바이스AI에 대한 기술 동향을 살펴본다.

가. 국방 지능형 서비스 플랫폼

유 · 무인복합체계는 지능형 서비스 플랫폼과의 연계를 통해 실시간 빅데이터 · AI분석, 다수 무인체계의 협업 및 통합 운용 등이 가능하다. 유 · 무인복합체계는 탑재가 어려운 딥러닝 · 영상분석 등 고부가 연산을 지능형 서비스 플랫폼에서 대신 처리함으로써 분석결과에 따른 임무 재설정 · 위협 판단 등을 빠르게 수행할 수 있고, 다수의 유 · 무인복합체계가 동시에 임무를 수행 시에도 개별시스템에 대한 위치 · 상태 · 임무 진행도를 지능형 서비스 플랫폼에서 통합 관리함으로써 협업 등의 집단지능을 구현할 수 있다.

국방 분야의 주요 선진국인 미국을 중심으로 AI 기술을 접목하여 전장의 데이터의 실시간 분석 및 처리가 가능한 국방 SW 플랫폼이 개발되고 있다. 팔란티어는 미 육군의 1억 7,800만 달러 규모의 TITAN 지상국 시스템을 개발하고('24.03), 적의 위치와 화력, 아군 규모 등 전장에서의 수많은 데이터를 분석하여 무인체계를 언제, 어떤 방식과 규모로 전장에 투입할 것인지 제안할 수 있다. 안두릴은 자사의 국방 데이터를 팔란티어의 AI 학습에 활용하는 것에 대해 양사가 파트너십을 체결하고('24.12), 전장에서 생성되는 차량, 로봇, 무기 등 데이터를 수집해 팔란티어의 보안 플랫폼으로 전송하며, 이 플랫폼은 최고 수준의 기밀 정보를 포함한 AI 훈련 · 개발에 필요한 데이터를 처리할 수 있다. 안트로픽은 미 국방기관에 클로드 AI 모델 제공 계획을 발표하고('24.11), 국방기관이 방대한 양의 복잡한 데

이터를 신속히 처리하고 분석할 수 있도록 지원할 수 있다. 스케일AI는 군대가 고수준의 AI를 통해 기존 방어 체계를 강화할 수 있는 기술을 개발 중에 있고('24.12), 미국의 국가 및 국방 분야의 임무에 맞게 조정되어, 국방부의 지침을 준수하면서 적의 행동을 시뮬레이션하고 작전을 계획할 수 있다. BAE 시스템즈는 고정밀 탐지 및 데이터 분석 시스템인 HADES를 개발하고('24.03), HADES는 강화학습, 의사결정 트리, 멀티 모달 데이터 분석 등 딥러닝 기반의 알고리즘에 의해 구동되며, 공중, 지상, 해상에 배치된 다양한 센서로부터 데이터를 수집하고 이를 실시간으로 처리해 고정밀 경고 및 탐지 기능을 제공할 수 있다[18-20].

나. 엣지AI 및 온디바이스AI

유 · 무인복합체계는 엣지AI 및 온디바이스AI 활용을 통해 고도화된 자율 운용이 가능하다. 유 · 무인복합체계는 클라우드나 중앙 서버에 전적으로 의존하지 않고도 현장에서 인공지능 연산과 의사결정을 수행할 수 있어야 하고, 이는 전장이나 재난현장처럼 통신이 제한적이거나, 실시간 대응이 필요한 상황에서 중요하다. 따라서, 클라우드 환경이 아닌 보안성이 강화된 유 · 무인복합체에서 로컬 데이터를 수집하고 데이터 생성, 의사결정 등의 프로세스를 밀리초 단위 내로 처리할 수 있어야 한다.

유 · 무인복합체계의 경우 다양한 전장 환경에서 데이터 분석의 처리 속도 및 보안이 매우 중요하고, 각국에서는 빠른 데이터 분석과 국방 분야의 민감한 정보를 보호하기 위해서 유 · 무인복합체계에 온디바이스AI 기술을 적극 적용하는 중이다. 퀄컴은 온디바이스AI 지원을 위한 AIMET을 오픈소스로 제공 중이고('24.09), AIMET은 AI 모델의 양자화 및 압축 기술을 지원하여, 디바이스 내 AI 모델 최적화를 통해 유 · 무인복합체의 AI 모델 경량화와 효율성을 향상시킨다. 탈레스는 AI를 탑재한 장거리 식별광학시스템타겟팅을 공개했고('24.11), 정밀 타격과 전술 정찰을 동시 수행할 수 있는 다목적 전자광학 표적 포드로서 2024년 이후로 프랑스 공군과 우주군의 라팔 전투기에 실전 적용될 것으로 예상된다. AVIC는 AI 기반의 자율 무인기 개발에 주력 중이며, 온디바이스AI를 활용하여 자율 비행과 실시간 임무 수행이 가능한 무인기를 개발 중이다('22.05). NORINCO는 AI 통합 지상 무인 차량을 개발하고('24.01), 온디바이스AI를 탑재한 지상 무인 차량을 통해, 자율주행과 목표물 탐지 및 추적 기능을 구현 중이다('24.01). CASC는 AI 기반의 자율 드론 군집 기술을 개발하고('23.07), 온디바이스AI를 활용하여 다수의 드론이 자율적으로 협력하여 임무를 수행하는 군집 기술을 개발 중이다('23.07). 인텔리빅스는 AI가 적군의 동태를 24시간 모니터링하면서 시각언어모델을 통해 영상 데이터를 텍스트로 변환해 실시간 보고서를 작성할 수 있다[21-23].

2. 유·무인복합체계 생산효율화 기술

유 · 무인복합체계 생산효율화 기술은 유 · 무인복합체계를 빠르고 저렴하게 대량생산하면서도 품질 · 성능을 유지 또는 향상시키기 위한 개발 단계부터 생산 공정과 운용 · 정비 효율을 극대화하는 기술이다. 이를 통해, 대규모 유 · 무인복합체계 소요에 대비해 단가를 낮추고 납기 · 공급량을 안정적으로 확보하여 비용을 절감하고, 급변하는 전장 상황에 맞춰 다양한 유 · 무인복합체계를 신속히 개발 · 생산하여 생산 속도 및 유연성을 확보하고, 부품 · 모듈의 규격화 · 호환성을 높여 정비 · 업그레이드를 용이하게 함으로써 품질 보증 및 표준화를 추진하며 정비 · 성능 개량 등 라이프사이클 관리 차원에서 효율성을 극대화하여 지속적으로 운용성

표 2 주요 개방형 국방표준 아키텍처

표준명	목적	특징	적용분야
MOSA	국방 시스템의 유연성, 상호운용성, 확장성 확보를 통해 효과적 전투력 유지 및 비용 절감	모듈화 설계, 개방형 인터페이스, 시스템 업그레이드 용이성	전투 시스템, 전술 통합, 방위산업 통합 시스템
SOSA	센서 및 정보 시스템 간 상호운용성 강화로 신속한 정보 수집 및 분석 지원	표준화된 센서 인터페이스, 통합 데이터 처리, 모듈화	감시, 정찰, 전투 정보 수집
FACE	항공 전자 시스템 소프트웨어의 재사용성과 통합성 극대화를 통해 임무 수행 효율 증대	서비스 지향 아키텍처, 모듈식 소프트웨어, 표준화된 인터페이스	전투기 및 항공 임베디드 시스템, 항공 전자 시스템
NGVA	차세대 군용 차량의 모듈화 및 업그레이드 용이성 제공으로 전투력 유지 및 향상	모듈식 설계, 개방형 인터페이스, 기술 통합 및 개선 용이성	군용 차량, 육상 전투체계, 이동체 통합 시스템
STANAG	NATO 국가 간 군사 장비 및 통신 시스템의 상호운용성 확보로 공동 작전 효율성 증대	국제 합의 기반 표준, 정기적 업데이트, 표준화된 기술 요구사항	NATO 작전, 통신 및 정보 교환 시스템, 군사 장비
AGVRA	고급 군용 차량 시스템의 통합 및 모듈화를 통해 신속한 전투 변화에 대응	고급 통합 기술, 모듈식 설계, 신속 재구성 및 높은 신뢰성 제공	군용 차량, 전자전/제어 시스템, 미래 전투 차량

출처 참고자료 활용하여 저자 작성[24,25].

을 확보할 수 있다. 유 · 무인복합체계의 생산효율화에 필요한 요소기술 중 표준화에 대한 기술 동향을 살펴본다.

가. 표준화

유 · 무인복합체계는 혁신적인 전투역량을 빠르고 대규모로 제공하기 위한 Replicator Initiative 개념과 유 · 무인복합체계의 재활용과 소모성을 고려하는 미래전의 Layered Effects 전투력 개념 적용을 통한 군 전력 강화를 위해 표준화를 통한 생산성을 향상시켜야 한다.

개방형 아키텍처(표 2) 채용에 대한 국제적인 추세에 맞춰 국방부는 AI기반 유 · 무인복합전투체계의 조속한 구축을 위해 2024년부터 '국방무인체계 계열화 · 모듈화(K-MOSA)' 정책을 본격적으로 추진 발표했다.

Ⅵ. 결론

우크라이나 전쟁을 통해 확인된 것처럼, 전통적 재래식 병력과 무기체계의 단순 우위만으로는 승리를 담보하기 어려워지고 있다. 오히려 드론 · 사이버전 · 인공위성 통신, AI · 빅데이터 등 신기술을 접목한 비대칭전력이 전장의 양상을 근본적으로 변화시킬 수 있다. 이에 따라 은닉 · 위장 기술의 중요성은 비약적으로 부각되고 있으며, 무선통신 · 네트워크 · 물리장치 · 사이버 역공격 등에 걸친 다계층 은닉과 능동형 방어능력이 필수 역량으로 떠오르고 있다.

정보통신망의 지능적 다계층 은닉 위장 기술은 상용 통신 기술을 국방에 활용하기 위해 무선통신과 네트워크 자원의 은닉, 장치의 위장을 목표로 하고 있다. 이 기술은 적의 접근, 해킹, 재밍을 최소화하고 미래 전투체계에서 상용 통신 기술의 국방 활용성을 강화하는 융합 기술의 잠재력을 제시한다. 또한, 경제적 측면뿐만 아니라 무기 체계 연구 개발, 전력 증강, 국내 과학기술 및 산업 발전에도 기여할 것으로 예상된다. 구체적으로, 국방 무선망의 보안성 향상, 주파수 고갈 문제 해결, 동적 자원할당을 통한 강건한 무선 인프라 제공, 접근 불가능한 블랙 네트워크 개발, 국방 임무 수행을 위한 보안 네트워크 기술 개발이 포함된다. 이 외에도, 변화하는 환경에 적응하는 물리적 장치 위장, 군사시설의 시각적 은폐, 사이버 전자전 상황 제공, 인공지능 기반 데이

터 패턴 분석을 통한 신형 공격 대비, 공격 지점 및 패턴 탐지 및 역공격 가능성 등 다양한 응용이 기대된다.

미래 전장환경에서는 유 · 무인복합체계가 보편화되고, 이러한 전력들이 지능형 서비스 플랫폼과 연계됨으로써 전장 정보를 신속하게 수집 · 분석 · 공유하게 될 것으로 예상된다. 이때, 엣지AI · 온디바이스AI를 통해 현장에서 자율 의사결정이 가능해지고, 대규모 유 · 무인복합체계를 빠르고 저렴하게 대량생산할 수 있는 생산효율화 기술이 함께 발전해야 한다. 또한, MOSA와 같은 표준화된 아키텍처를 국내 맞춤형으로 적용해 군사장비 · 부품 간 상호 운용성과 확장성을 확보함으로써 전력의 신속 조달과 지속 운용을 동시에 달성할 수 있다.

결과적으로, 은닉 · 위장 기술은 미래 국방의 유 · 무인복합체계에 있어서 핵심축을 이룰 것으로 전망된다. 이와 동시에 전장 정보환경과 비대칭전 양상에 대응하기 위해선, 유 · 무인복합체계 지능화 · 생산효율화 기술을 보완함으로써 고도화된 전력 구조와 군사작전 개념이 은닉 · 위장 · 표준화 · 지능화를 중심으로 재편되어야 하며, 이를 통해 인명피해 최소화, 작전효율 극대화, 유연한 전력운용이 가능해질 것으로 예상된다.

약어 정리

AFC	Army Futures Command
AGVRA	Autonomous Ground Vehicle Reference Architecture
AIMET	AI Model Efficiency Toolkit
AODV	Ad hoc On-demand Distance Vector
ART	Autonomous Radio Transceiver
ASCALS	Advanced Solutions for Camouflage of Land Systems
CSA	Cloud Security Alliance
DARPA	Defense Advanced Research Projects Agency
DoD	Department of Defense
DSR	Dynamic Source Routing
ESSOR	European Secure Software-defined Radio
FMN	Future Military Network
G4L	Graphene 4-layer
JTRS	Joint Tactical Radio System
LETacCIS	Land Environment Tactical Communications and Information Systems
MILTECH	Military Technology
MOSA	Modular Open Systems Approach
MPTCP	Multipath TCP
MUM-T	Manned-Unmanned Teaming
NGVA	NATO Generic Vehicle Architecture
OCCAR	Organisation for Joint Armaments Cooperation
OLSR	Optimized Link State Routing
SC2	Spectrum Collaboration Challenge
SDP	Software Defined Perimeter
SDR	Software Defined Radio
SHARE	Spectrum Holistic Adaptive Radio Environment
SOSA	Sensor Open Systems Architecture
SSPARC	Spectrum Sharing Protocol for Adaptive Radio Communications
STANAG	Standardization Agreement
TITAN	Tactical Intelligence Targeting Access Node

참고문헌

[1] 박휘락, "네트워크 중심전의 이해와 추진 현황," 국방정책연구, 제21권 제3호, 2005, pp. 155-182.

[2] 신치범, "비대칭성 창출 기반의 군사력 건설 관점에서 본 러시아 우크라이나 전쟁 - 1단계 작전(개전~D+40일)을 중심으로," 한국군사학논총, 제11권 제2호, 2022, pp. 105-127.

[3] G.M. Jacyna et al., "A high-level overview of fundamental limits studies for the DARPA SSPARC program," in Proc. IEEE Radar Conf., (Philadelphia, PA, USA), May. 2016, pp. 1-6.

[4] D.M. Cooper et al., “JTRS applications to DoD programs: technology and implementation,” in Proc. IEEE Mil. Commun. Conf., (Anaheim, CA, USA), vol. 2, Oct. 2002, pp. 1427–1432.

[5] K. Galvin et al., “Advancing Modelling and Simulation in NATO Federated Mission Networking,” in Proc. NATO Model. Simul. Symp., (Monterey, CA, USA), Oct. 2023.

[6] N. Brown, “The path towards NEC: France, Germany and the United Kingdom,” Technological Innovation and Defence: The Forza NEC Program in the Euro-Atlantic Framework, 2016, pp. 65–100.

[7] J.J. Dawkins et al., “Deployment and flight operations of a large scale UAS combat swarm: Results from DARPA service academies swarm challenge,” in Proc. Int. Conf. Unmanned Aircraft Syst (ICUAS), (Dallas, TX, USA), Jun. 2018, pp. 1271–1278.

[8] M.L. Gambo and A. Almulhem, “Zero Trust Architecture: A Systematic Literature Review,” IEEE Access, 2024.

[9] R. Ward and B. Beyer, “BeyondCorp, A New Approach toEnterprise Security,” ;login:, vol. 39, no. 6, 2014, pp. 6–11.

[10] J.W. Lee et al., “Thermally controlled, active imperceptible artificial skin in visible-to-infrared range,” Adv. Funct. Mater., vol. 30, no. 36, 2020.

[11] N.K. Lee et al., “Transparent Metamaterials for Multispectral Camouflage with Thermal Management,” Int. J. Heat Mass Transf., vol. 173, 2021.

[12] M.K. Lim et al., “Optically transparent and infrared tunable flexible camouflage device,” Nano Energy, vol. 131, 2024.

[13] J.Y. Kim et al., “Graphene Electrode Enabling Electrochromic Approaches for Daylight-Dimming Applications,” Sci. Rep., vol. 8, no. 3944, 2018.

[14] https://www.rbth.com/science-and-tech/334359-camouflage-russian-army

[15] https://www.eurasiantimes.com/invisible-to-radars-china-claims-developing-hybrid-camouflage-that-can-make-its-soldiers-undetectable/

[16] https://eda.europa.eu/news-and-events/news/2023/06/22/new-eda-project-to-identify-smart-and-adaptive-materials-to-enhance-camouflage-of-land-systems

[17] 홍강운 외, “적의 탐지·공격을 감내하는 네트워크 서비스를 위한 지능적 다계층 은닉 위장 기술,” 한국군사과학기술학회 추계학술대회, 2024, pp. 774–775.

[18] D.C. Youvan, “Tech Titans and the Surveillance State: Examining Support for Public Surveillance Among US Technology Leaders,” unpublished, Researchgate, 2024. doi: 10.13140/RG.2.2.29493.08164

[19] D.T. Caldwell, “Defense Innovation at an Inflection Point: The Rise of New Primes like Anduril and the Changing Military-Tech Ecosystem,” Open Access Cases, vol. 1, no. 4, 2024.

[20] L. Trabucco and M.M. Maas, “Technology Ties: The Rise and Roles of Military AI Strategic Partnerships,” SSRN, 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4629283

[21] https://github.com/quic/aimet

[22] https://www.aitimes.kr/news/articleView.html?idxno=33057

[23] https://kkmd.tistory.com/161

[24] 윤한의 외, “국제 표준 기반 방위 산업용 신호 처리 시스템 설계,” 한국정보기술학회논문지, 제22권 제10호, 2024, pp. 51–60.

[25] https://www.sealevel.com/advancing-defense-technology-mosa-sosa-and-face