2023-5

KERC
Issue Report

EU 5G 네트워크 사이버보안 툴박스 동향

회원국별 EU 툴박스 이행 및 중국 대응 현황

KERC
Korea-EU Research Centre

ISSUE REPORT
2023-5

EU 5G 네트워크 사이버보안 툴박스 동향

회원국별 EU 툴박스 이행 및 중국 대응 현황

[발행일] 2023.09.19.
[발행처] 한-EU 연구협력센터
Rue de la science 14A
1040 브뤼셀, 벨기에
http://www.k-erc.eu
+32 (0)2 880 39 05
[발행인] 조 우 현 센터장
[담당자] 송 예 일 연구원
[저 자] 송 예 일 연구원

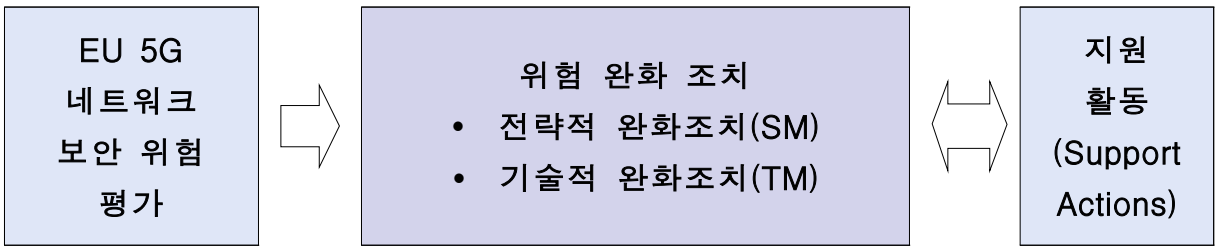
Content

1 EU 5G 보안 툴박스 개요

□ 개요

ㅇ 5G 네트워크 보완 관련 EU의 조정된 접근방식을 위한 종합적 조치

- 툴박스는 5G 네트워크 사이버보안 관련 위험 평가 보고서('19.10)에서 식별된 주요 보안 위험을 효과적으로 완화하고 안전한 5G 네트워크가 유럽 전역에 배포될 수 있도록 다양한 보안 조치를 제시함
- 이를 통해 툴박스는 EU 전역에서 적절한 수준의 5G 네트워크 사이버 보안을 보장할 강력하고 객관적인 보안 조치 프레임워크를 만드는 것을 목표로 함



□ 정책 경과

ㅇ EU 5G 보안 툴박스는 '19년 3월 집행위원회의 권고에서 제안됨

- NIS Cooperation Group은 동 권고에 따라 5G 네트워크 사이버보안 관련 위험 평가를 시행('19.07)하였으며, 이에 따라 식별된 위험 영역에 대한 완화 조치 툴박스를 개발하여 발표함('20.01)

> NIS Cooperation Group[1] (NIS: Network and Information Systems)
> - 27개 EU 회원국, 집행위원회 및 ENISA(유럽사이버보안청) 대표로 이루어진 그룹

- 이후 5G 보안 툴박스 이행에 대한 회원국의 진행 경과를 평가하는 보고서가 '20년 7월 1차 발간되었으며, '23년 6월 2번째 보고서가 발간됨

1) https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

<EU 5G 보안 툴박스 정책 주요 경과>

'19.03	• 집행위원회, 5G 네트워크 사이버보안에 관한 집행위원회 권고 발표
'19.10	• NIS Cooperation Group, 5G 네트워크 사이버보안 관련 위험 평가 보고서 발간 • 유럽사이버보안청(ENISA), 5G 네트워크 위험성 관련 보고서 발간('19.11)
'20.01	• NIS Cooperation Group, 5G 네트워크 사이버보안 - 위험 완화 조치 EU 툴박스 발간
'20.07	• NIS Cooperation Group, EU 5G 사이버보안 툴박스 이행에 관한 회원국의 진행 경과 보고서 발간
'20.10	• EU 이사회 결론, EU 및 회원국에 '5G 사이버보안 툴박스 활용 최대화' 및 '핵심 자산에 대한 고위험 공급자 관련 규제 적용' 촉구
'20.12	• 집행위원회, 5G 사이버보안 권고의 파급력(Impacts)에 관한 보고서 발간
'22.01	• 유럽회계감사원(ECA), 5G 툴박스 관련 특별 보고서 발간
'22.12	• EU 이사회 권고, EU 회원국에 5G 툴박스 이행 촉구
'23.06	• NIS Cooperation Group, EU 툴박스 이행에 관한 회원국의 진행 경과 보고서 제2권 발간 • 집행위원회, 5G 보안 툴박스 이행에 관한 커뮤니케이션 발간

□ 정책 내용

○ EU 위험 평가 결과

- EU의 조정된 5G 네트워크 보안 위험 평가는 5개의 위험 시나리오로 그룹화된 9개의 주요 위험을 식별함

위험 시나리오	주요 위험 가능성
보안 조치 부족	• (R1) 네트워크의 잘못된 구성 • (R2) 액세스 제어 부족
5G 공급망	• (R3) 낮은 제품 품질 • (R4) 개별 네트워크 내 단일 공급자에 대한 의존성 또는 전국적 다양성 부족
주요 위협 행위자의 작업 방식	• (R5) 5G 공급망을 통한 국가의 간섭 • (R6) 범죄조직의 5G 네트워크 악용 및 최종사용자 타겟팅
5G 네트워크 및 기타 핵심 시스템 간의 상호의존성	• (R7) 중요 인프라 또는 서비스의 심각한 중단 • (R8) 전기 공급 또는 기타 지원 시스템의 중단으로 인한 네트워크 대규모 장애
최종사용자 기기 관련	• (R9) 사물인터넷, 핸드폰, 스마트 장치 악용

○ EU 5G 보안 툴박스 핵심 조치

EU 회원국	집행위원회
EU 회원국은 위험을 완화할 수 있는 권한을 갖고 있어야 하며, 관련된 조치를 취해야 함 • **모바일 네트워크 사업자에 대한 보안 요건 강화** • **공급업체의 위험 프로필 평가** – 주요 자산 관련 배제 등 고위험 공급업체에 대한 제한사항 적용 등 • **각 사업자가 단일 공급업체에 대한 의존을 피하고, 고위험 공급업체에 대한 의존을 피하기 위한 적절한 다중 공급업체 전략을 갖고 있는지 확인**	집행위원회는 EU 회원국과 함께 다음과 같은 조치를 취해야 함 • **특정 업체에 대한 장기적 의존을 피하기 위해 다양하고 지속 가능한 5G 공급망 유지:** ☞ 기존 EU 도구 및 수단 활용 ☞ 관련 EU 프로그램 및 자금을 사용하여 5G(혹은 그 이상) 기술 관련 EU 역량 강화 • **특정 보안 목표 및 관련 EU 차원의 인증 체계 개발을 위해 표준화 관련 회원국 간의 조정 촉진**

- 툴박스는 3가지 유형의 완화 조치를 제시함

전략적 조치	규제 당국의 권한 증가, 비기술적 취약성과 관련된 위험 해결, 공급업체의 위험 프로필 평가, 지속가능하고 다양한 5G 공급업체의 개발 지원 이니셔티브 촉진 등
기술적 조치	엄격한 액세스 제어, 안전한 네트워크 관리·운영·모니터링, 5G 네트워크 구성 요소·프로세스에 대한 인증 사용 등
지원 조치	5G 표준, 테스트 및 감사 기능 강화, 조정 능력 개선, EU 자금 지원 5G 프로젝트 내 사이버보안 위험 요소 고려를 위한 조치 등

○ 전략적 위험 완화 조치(Strategic Measures, SM)

- 툴박스는 다음 8개의 전략적 조치를 제시함

규제 권한 강화	
SM01	규제 당국의 역할 강화
SM02	사업자에 대한 감사 수행 및 정보 요구
제3 공급업체	
SM03	공급업체의 위험 프로필 평가 및 고위험 공급업체 규제
SM04	관리 서비스 제공자(MSP) 및 장비 공급업체의 3차 지원(Third line support) 사용 통제
공급업체 다양화	
SM05	적절한 멀티벤더(multi-vendor) 전략을 통해 개별 모바일 네트워크 사업자(MNO)를 위한 공급업체의 다양성 보장
SM06	국가 차원의 회복탄력성 강화
5G 공급 및 가치 사슬의 다양화 및 지속가능성	
SM07	EU 내 주요 자산 식별 및 다양하고 지속가능한 5G 생태계 육성
SM08	미래 네트워크 기술에서 다양성과 EU 역량 유지 및 구축

- (SM01) 국가 당국이 다음을 수행할 수 있는 규제 권한을 갖추도록 보장

• 신호/관리 영역 보안과 관련하여 사업자에게 강화된 의무 부과 • 다음 사항을 고려하여 5G 네트워크 장비의 공급, 배포 및 운영을 위해 위험 기반 접근방식에 따라 특정 요구사항이나 조건을 제한, 금지 또는 부과하기 위한 사전 권한을 사용 – 5G 네트워크의 중요하고 민감한 부분의 보안 – 장비 자체 또는 환경의 보안 – 5G 공급망에서 제3국의 간섭 위험 – 개별 MNO 또는 전국적으로 단일 공급업체에 크게 의존할 위험 – 국가 안보에 대한 위험

- (SM02) EECC 제41조[2]에 따라 권한을 행사할 때 관할 당국이 다음을 수행하도록 보장

• 필요한 경우 심층적인 기술 수준(5G 네트워크의 중요 구성 요소나 민감한 부분)에서 모바일 네트워크 사업자(MNO)를 감사하거나 감사하도록 요구 • 사업자에게 5G 장비 조달 및 제3 공급업체 참여 계획에 대한 자세한 최신 정보를 제공하도록 요구 • 사업자에게 기본 기술네트워크 보안 조치가 이행되는 방법에 대한 설명을 문서화하고 유지하도록 요구

- (SM03) EU 통합 위험 평가에서 식별된 위험 요소를 고려하여 명확한 기준이 있는 프레임워크를 확립하고, 국가 관할 당국 및 MNO를 위해 국가별 정보(예: 국가 보안 서비스의 위협 평가 등)를 추가하여 다음을 수행하도록 보장

• 국가 수준 또는 EU 수준에서 모든 관련 공급업체의 위험 프로필에 대한 엄격한 평가 수행 • 위험 프로필 평가를 기반으로 EU 통합 위험 평가 보고서에서 중요하거나 민감한 것으로 정의된 주요 자산(핵심 네트워크 기능, 네트워크 관리 및 조정 기능, 액세스 네트워크 기능 등)에 대해 위험을 효과적으로 완화하기 위해 필요한 제외를 포함하여 제한 사항을 적용 • 정기적인 공급망 감사 및 위험 평가, 강력한 위험 관리 또는 위험 프로필을 기반으로 한 공급업체에 대한 특정 요구사항 적용 등 MNO가 잠재적 잔여 위험을 관리하기 위한 적절한 제어 및 프로세스를 갖추고 있는지 확인

2) EECC 제41조는 관할 당국이 전자통신 네트워크 및 서비스 공급업체에게 네트워크 및 서비스의 보안을 평가하는 데 필요한 정보(보안 정책 포함)를 제공하도록 요청할 수 있도록 하고, 이를 권한을 갖춘 독립 기관이나 관할 기관의 보안 감사에 제출하도록 보장할 것을 회원국에 요구함

- **(SM04)** MNO가 MSP(관리형서비스제공업체)에 특정 기능을 아웃소싱할 수 있는 활동 유형과 조건을 제한하는 법률/규제 프레임워크 확립

• 특히 보안, 네트워크 운영 기능 등 5G 네트워크의 민감한 부분과 SM03에 따라 MSP가 고위험 공급업체로 간주되는 부분에 제한 적용 • MSP에 아웃소싱된 기능의 경우 MSP가 해당 기능을 수행하기 위해 제공하는 액세스에 대해 강화된 보안 조항 적용

- **(SM05)** 각 모바일 네트워크 사업자(MNO)가 5G 네트워크의 다양한 부분에 대한 기술적 제약과 상호운용성 요구사항을 고려하여 적절한 다중 공급업체 전략을 갖추도록 보장

• 단일 공급업체(또는 유사한 위험 프로필을 가진 공급업체)에 대한 주요 의존의 방지 및 제한 • SM03에 따라 위험도가 높은 것으로 간주되는 공급업체에 대한 의존 방지

- **(SM06)** 개별 회원국의 지리·인구 변화를 고려하여 하나의 사업자 또는 공급업체에 사고가 발생할 경우 회복력을 보장할 수 있도록 국가 차원에서 공급업체의 적절한 균형이 있도록 보장
- **(SM07)** EU의 외국인직접투자(FDI) 심사 메커니즘을 기반으로 5G 가치사슬 전반에 걸쳐 FDI 투자 모니터링 개선

• 이는 5G 가치사슬에 대한 외국인 투자가 하나 이상의 EU 회원국 보안이나 공공 질서에 위협을 가할 수 있는지 여부를 더 잘 탐지하기 위함 • 구매자/회사의 위험 프로필과 같은 요소를 고려하여 투자를 평가할 수 있도록 FDI 규정의 범위에는 중요 인프라, 공공 보안, 정보에 대한 접근 및 통제, 사이버보안 등이 잘 포함됨

- **(SM08)** 유럽 기술 기업을 위한 최적의 조건 조성 및 핵심 기술 분야의 혁신 촉진을 통해 다양하고 지속가능하며 안전한 유럽 5G 생태계를 촉진하는 정책 개발

• 6G SNS 등 제도화된 유러피안 파트너십을 개발하여 통신 가치 사슬 전반에 걸쳐 EU 내 공급업체의 다양성과 충분한 지식 및 공급 역량 보장 • 와해적이고 야심찬 연구혁신의 지원을 통한 EU 역량 개발(특히, 호라이즌 유럽(HE), 디지털유럽프로그램(DEP), EU 연결 프로그램(CEF)등 활용) • EU 전역의 지식, 전문 지식, 재정 지원 및 경제 주체 등 통합

○ 기술적 위험 완화 조치(Technical Measures, TM)

- 툴박스는 다음 11개의 기술적 조치를 제시함

네트워크 보안 - 기본 조치	
TM01	기본 보안 요구 사항의 적용 보장(보안 네트워크 설계 및 아키텍처)
TM02	기존 5G 표준의 보안 조치 구현 보장 및 평가
네트워크 보안 - 5G 특정 조치	
TM03	엄격한 액세스 제어 보장
TM04	가상화된 네트워크 기능의 보안 강화
TM05	안전한 5G 네트워크 관리, 운영 및 모니터링 보장
TM06	물리적 보안 강화
TM07	소프트웨어 무결성, 업데이트 및 패치 관리 강화
공급업체의 프로세스 및 장비 관련 요구사항	
TM08	강력한 조달 조건을 통해 공급업체 프로세스의 보안 표준 향상
TM09	5G 네트워크 구성 요소, 고객 장비·공급업체 프로세스에 EU 인증 사용
TM10	기타 비5G 관련 ICT 제품 및 서비스에 EU 인증 사용(연결 장치, 클라우드 서비스 등)
TM11	회복탄력성 및 연속성 계획 강화

- **(TM01)** MNO가 기존 보안 모범 사례 및 권장사항을 이행하도록 보장

• 제품 개발, 구성, 일상적인 네트워크 관리, 사고 관리, 보안 업데이트 (예를 들어, MNO에 위험 평가 계획을 부과하고 검토) 등 5G 네트워크에 국한되지 않는 기존 보안 모범 사례 및 권장 사항 이행 보장 • MNO가 운영 정보를 포함하여 보안 정책에 대한 최신 정보를 유지하고 주요 네트워크 및 정보 시스템에 대한 변경 및 사고 관리 절차와 연결되도록 보장

- **(TM02)** 모바일 네트워크 사업자(MNO)와 그 공급업체가 관련 5G 기술 표준(예: 3GPP)의 기존 보안 조치를 이행하도록 보장

• 또한, 이러한 표준이 MNO를 위한 최소 보안 기준으로 사용되도록 보장하고, 보안과 관련된 이러한 표준의 선택적 부분도 적절하게 이행되도록 보장

- **(TM03)** MNO가 다음을 보장하기 위해 적절하고 유연하며 검증 가능한 기술적 조치를 이행하도록 보장

• 엄격한 네트워크 액세스 제어 적용 • 최소 권한 원칙의 적용을 통한 네트워크 내 다양한 권한 최소화 • 직무분리 원칙 적용 • 이러한 규칙이 항상 유효하고 네트워크와 함께 발전하도록 보장하는 절차 마련

- **(TM04)** MNO가 네트워크 기능 가상화에 대한 보안 모범 사례를 따르도록 보장

• 한편, 네트워크 기능이 매우 중요하거나 매우 민감한 정보를 처리하는 경우 가상화가 적절하지 않을 수 있으며, 이러한 설정에서는 물리적 분리가 필요할 수도 있다는 점에 유의할 것

- **(TM05)** MNO가 국가 또는 EU 내부에서 자체 네트워크운영센터(NOC) 또는 보안운영센터(SOC)를 운영하도록 보장

• NOC와 SOC는 보안 네트워크 관리 및 운영을 위한 조치를 이행하고 모니터링하는 데 있어 MNO 인프라의 핵심 구성요소로임 • NOC와 SOC는 5G 네트워크의 최소한 모든 중요 구성 요소와 민감한 부분에 대해 명확한 가시성을 제공하고 효과적인 모니터링을 구현하여 이상 현상을 감지하고 위협을 식별하고 방지해야함

- 또한, MNO가 통신 네트워크 또는 서비스 구성요소에 대한 무단 변경을 방지하기 위해 관리 트래픽을 적절하게 보호하도록 보장
- **(TM06)** MNO가 위험 기반 접근방식을 취하여 5G 네트워크의 중요 구성요소와 민감한 부분에 대한 물리적 보호를 강화하도록 보장

  - 물리적 접근 통제를 강화할 때는 보안 심사를 받고 교육을 받고 자격을 갖춘 제한된 수의 직원에게만 접근 권한을 부여하는 것이 중요
  - 제3자, 계약자, 공급업체/벤더 직원, 통합업체의 액세스는 제한되고 모니터링 되어야 함

- **(TM07)** MNO가 5G 네트워크에서 소프트웨어 업데이트를 수행하고 보안 패치를 적용할 때 적절한 도구와 프로세스를 효과적으로 사용하도록 보장

  - 이는 변경 사항과 패치 상태를 안정적으로 식별하고 추적하는 소프트웨어 무결성을 보장하기 위함

- **(TM08)** MNO가 조달 프로세스에서 장비 공급업체에게 특정 보안 표준을 요구하도록 보장

  - 예: 특정 보안 개선 및 품질 수준 입증, 장비 수명 전반에 걸친 보안 유지 관리 및 제품 개발 프로세스에 내장된 보안 등

- **(TM11)** MNO가 탄력성과 연속성 계획을 강화하도록 보장

  - MNO는 재해가 발생하여 네트워크의 지속적인 운영에 영향을 미치는 경우 적절한 계획을 마련하고 필요에 따라 중요한 의존성을 매핑하고 완화해야 함
  - MNO는 공급업체 내에 유사한 조치를 요청해야 하며, 충분한 수준의 장기적 회복력을 입증하는 공급업체만 이용해야 함

○ 지원 조치(A set of targeted supporting actions)

- 더하여 툴박스는 전략적·기술적 조치의 효과를 향상하도록 지원하는 10개의 지원 조치를 제시함

네트워크 보안	
SA01	네트워크 보안에 대한 지침 및 모범 사례 검토 또는 개발
SA02	국가 및 EU 수준에서 테스트 및 감사 기능 강화
표준화	
SA03	5G 표준화 지원 및 형성
SA04	기존 5G 표준의 보안 조치 구현에 대한 지침 개발
SA05	특정 EU 차원의 인증 체계를 통해 표준 기술 및 조직 보안 조치의 적용 보장
서드파티(Third party) 공급업체	
SA06	전략적 조치, 특히 공급업체의 위험 프로필을 평가하기 위한 국가 프레임워크의 이행에 대한 모범 사례 교환
회복탄력성 및 연속성	
SA07	사고 대응 및 위기 관리의 조정 개선
SA08	5G 네트워크와 기타 중요 서비스 간의 상호 의존성 감사 수행
협력 및 조정	
SA09	협력, 조정 및 정보 공유 메커니즘 강화
공적 조달	
SA10	공적 자금으로 지원되는 5G 보급 프로젝트가 사이버보안 위험을 고려하도록 보장

2 EU 5G 툴박스 이행 현황

※ 해당 장은 EU 5G 툴박스 이행 진행 현황 관련 '20년 7월 발간된 1차 보고서와 '23년 6월 발간된 2차 보고서의 내용 중 주요사항 발췌

□ EU 회원국의 전략적 조치(SM) 이행 현황

ㅇ (SM01) 규제 당국의 권한 및 역할 강화

	1차 보고서('20.07)
이행완료	6
진행중	14
계획됨	6
조치안됨	-
총계	26개국

2차 보고서('23.06)
23
1
3
27개국

- 상당수 회원국이 5G 네트워크 장비의 공급·배치·운용을 제한하거나 금지할 수 있는 법적 근거를 마련하기 위한 세부 계획을 도입하거나 전달하였음

※ 반면 이전까지는 사후 권한과 통제권만 가졌으며, 사업자에 의한 장비 및 서비스 조달을 규제할 권한이 없었음(1차 보고서 기준)

- 일부 회원국은 사전 승인 또는 알림 메커니즘을 도입했거나 고려하고 있으며, 이를 통해 사업자는 규제 당국에 5G 장비를 배치하기 전에 승인을 받거나 계획을 신고해야 함

※ 몇몇 회원국은 장비가 국가 안보에 위협이 되는 것으로 의심되는 경우 장비 제거를 명령할 수 있는 권한을 당국에 부여하는 조치를 제안했거나 고려하고 있음

<국가별 이행 예시(출처:1차 보고서)>

에스토니아	• 에스토니아 의회는 전자통신법 개정안을 승인하여 정부가 국가안보를 보장하기 위해 통신사업자에게 통신망에 사용되는 하드웨어와 소프트웨어에 대한 정보를 제공할 의무를 부과하고 통신망 하드웨어와 소프트웨어의 사용 허가를 신청할 수 있는 권한을 부여함
프랑스	• '19년 8월 1일자 법률 N 2019-810은 5G 장비의 공급·배치·운영에 대한 요구사항이나 조건을 제한·금지·부과하는 데 필요한 권한을 당국에 제공함 • 이는 5G(및 6G와 같은 미래기술) 네트워크에 민감한 장비를 출시하고 운영하기 전에 총리의 승인을 받도록 의무화 함
스웨덴	• 스웨덴은 전자통신법 개정을 통해 '무선송신기 사용'허가는 '무선 이용이 국가안보에 지장이 없다고 판단되는 경우에' 한해 승인할 수 있다는 조건을 추가하였으며, 5G 주파수에 대한 스펙트럼 경매에는 주파수 입찰을 신청하려는 행위자에게 특정 조건을 부과함

ㅇ (SM02) 사업자에 대한 감사 수행 및 정보 요구

	1차 보고서('20.07)		2차 보고서('23.06)
이행완료	7	→	18
진행중	11		8
계획됨	6		
조치안됨	2		1
총계	26개국		27개국

※ 동 전략적 조치는 보안 감사를 수행하기 위해 기존 권한의 사용을 늘리는 것을 목표로 하는 한편, 모바일 네트워크 사업자(MNO)의 부과된 보안 의무를 모니터링할 수 있도록 규제 기관이 올바른 정보를 갖도록 보장함

※ 따라서 이는 SM01에 따른 중요한 결과이며, 다른 툴박스 조치의 효과적인 이행, 모니터링 및 집행을 보장하는 데 필요함

- '23년 1월, 25개 회원국이 집행위에 EECC*로의 완전한 전환을 통보하는 등 대부분의 회원국은 EECC 전환을 통해 SM02를 이행함

* 유럽전자통신코드(EECC)는 '18년 12월 발효된 새로운 EU 통신 규칙 세트로, EU 회원국은 '20년 말까지 해당 EU 지침을 국내법으로 전환해야 했음

- 16개 회원국은 감사에 대한 규제 프레임워크를 강화했다고 보고했으며, 18개 회원국은 정기적으로 감사를 수행하고 있으며, 평균 감사 주기는 4개월에서 2년으로 다양하게 나타남

- 10개 회원국은 5G 장비 소싱 및 서드파티 공급업체 참여 관련 MNO 계획에 대한 정보를 요구하며, 일부 회원국에서는 이 정보를 관할 당국에 제출해야 하는 MNO의 위험 분석 또는 다양화 전략 보고서의 일부로 제공하거나 SM01에 언급된 승인 프로세스의 일부로 제공해야 함

<국가별 이행 예시(출처:1차 보고서)>

오스트리아	• 통신네트워크보안규정(TNSR)에 따라 5G 네트워크를 운영하는 MNO는 정보 보안을 준수해야 하고, 특정 3GPP 표준 및 추가 요구 사항에 따라 정보보안관리시스템(ISMS)을 유지해야 하며, 5G 네트워크 기능과 공급업체를 2년에 한 번씩 NRA에 보고해야 함

ㅇ (SM03) 공급업체의 위험 프로필 평가 및 고위험 공급업체 규제

2차 보고서 ('23.06)	위험 프로필 평가를 위한 법적 프레임워크	고위험 공급업체 규제
이행완료	21	10
진행중	3	3
계획됨		
조치안됨	3	14
총계	27개국	

① 국가 당국의 규제 권한

- 5개 회원국은 MNO가 5G 장비를 배치할 수 있도록 관할 당국에 승인을 요청해야 하는 사전 승인 시스템/메커니즘을 가지고 있으며, 이 메커니즘은 공급망 위험과 관련된 다른 전략적 조치를 가능하게 함
- 4개 회원국은 정치적 수준에서 고위험 공급업체에 대한 의사 결정을 위한 기반을 마련하고 조언하기 위해 자문 기구를 설립하였거나 설립할 것이라고 보고하였음
- **21개 회원국**이 공급업체의 위험 프로필을 평가하기 위한 기준 목록을 가지고 있거나 개발 중이라고 보고하였으며, 대부분의 경우 이러한 기준은 공개되어 있고, EU 툴박스에서 권장하는 기준을 기반으로 함
- 17개 회원국은 5G 장비 배치를 금지할 수 있는 사전 접근 방식을 시행했거나 시행할 예정이며, 19개 회원국은 고위험 공급업체가 이미 설치한 장비를 제거하도록 명령할 수 있다고 밝힘

※ 제한 범위는 일반적으로 주요 자산 목록을 통해 국가 법률에서 정의되며, 이 범위가 법률에 정의되어 있는 17개 회원국에서는 이 목록에 'EU 공동 위험 평가'에서 중요하고 매우 민감한 것으로 정의된 자산을 포함했거나 포함할 계획

- 이러한 규제의 적용과 관련하여 12개 회원국에서 채택되었거나 제안된 법적 프레임워크는 전환 기간을 지정하여 MNO가 고위험 공급업체의 장비를 교체할 시간을 허용하고 있음

② 고위험 공급업체 규제

- EU 10개 회원국*은 위에서 언급한 권한을 사용하여 5G 네트워크에 고위험으로 간주되는 공급업체를 제한하거나 제외하도록 MNO에 의무를 부과함

* 10개 회원국이 정확히 어디인지는 언급되지 않고 있으나, 동 자료 제3장의 각국의 현황에서 유추 가능

※ 몇몇 회원국은 고위험 공급업체 또는 부품의 사용을 제한하거나 배제하는 조치를 취하였으며, 한 회원국은 화웨이와 ZTE를 5G 네트워크에서 제외하기로 공개 결정을 내림

- 3개 회원국은 현재 국내법 이행을 위해 노력하고 있음

<국가별 이행 예시(출처:1차 보고서)>

이탈리아	• 골든파워법(Golden Power Law)에 따라 정부는 MNO가 5G 배치를 위해 이러한 장비 또는 서비스를 EU 외 공급업체로부터 조달하여 사용할 때 관련된 신고를 받게 되어있음
네덜란드	• '19년 11월 통신의 안전 및 무결성에 관한 법령은 신뢰할 수 없는 공급업체가 다음 기준에 따라 지정될 것이라고 규정함 *(1) 제품서비스를 제공하는 당사자가 해당 국가의 정부와 협력하도록 의무화하는 법률이 있는 국가에 속하였거나 통제하에 있는가?* *(2) 제품서비스를 제공하는 당사자가 네덜란드의 국익에 영향을 미칠 수 있을 정도로 관계가 긴장될 수 있는 국가에 속하였는가?*

ㅇ (SM04) 관리 서비스 제공자(MSP) 및 장비 공급업체의 서드라인 지원(Third line support) 사용 통제

	1차 보고서('20.07)		2차 보고서('23.06)
이행완료	5	→	12
진행중	12		6
계획됨	6		
조치안됨	3		9
총계	26개국		27개국

- 대부분의 경우 SM03 이행을 위해 수립된 고위험 공급업체에 대해 동일한 절차와 규제가 SM04에도 적용되고 있음
- 4개 회원국은 5G 서비스 관리를 위한 현지화 요구사항 또는 제3국에서 아웃소싱할 때 특정 요구사항이 있다고 보고함

<국가별 이행 예시(출처:1차 보고서)>

키프로스	• 규제 프레임워크에 따라 MNO는 물리적 인프라와 가상 인프라 모두에 대해 관리 서비스 공급자에게 특정 기능을 아웃소싱할 수 있는 활동 유형 및 조건에 대한 제한을 도입해야 함 • 여기에는 5G 네트워크의 일부 요소, 아웃소싱 및 MSP 원격 액세스와 관련된 향상된 보안 조항, 서드라인 지원과 관련된 엄격한 액세스 제어 등이 포함됨
핀란드	• MNO는 긴급상황에서 핵심 시스템과 해당 지침, 유지 관리 및 통제가 지체없이 핀란드로 반환될 수 있도록 보장해야 함 • Traficom은 또한 네트워크 관리와 관련된 규정을 발행할 권한이 있음
프랑스	• 승인을 받기위해 MNO는 운영 양식에 관한 정보를 제공해야 하며, 이는 호스팅 서비스에서 발생할 가능성이 있는 작업과 운영, 관리, 유지 보수 등과 관련된 계약자 목록을 포함해야 함
아일랜드	• 준비 중인 통신보안요구사항(TSR)에는 MSP 또는 공급업체의 서드라인 지원 사용이 네트워크의 전체 보안에 악영향을 미치지 않도록 보장하는 요구사항이 포함되어 있음 • TSR은 사업자가 타사 액세스와 관련된 위험으로부터 네트워크를 보호하기 위해 이행해야하는 여러 기술 및 조직 통제를 정의함

ㅇ (SM05) 적절한 멀티벤더(multi-vendor) 전략을 통해 개별 모바일 네트워크 사업자(MNO)를 위한 공급업체의 다양성 보장

	1차 보고서('20.07)		2차 보고서('23.06)
이행완료	2	→	9
진행중	12		2
계획됨	3		
조치안됨	7		16
총계	24개국*		27개국

* 2개국은 응답하지 않음

- 9개 회원국이 SM05를 이행했다고 보고하였으며, 해당 국가에서 관할 당국은 5G MNO의 멀티 벤더 전략에 대한 정보를 요청하거나 MNO가 다양한 전략을 제출하도록 요구할 수 있음

※ 이 중 2개의 회원국은 네트워크의 서로 다른 부분에 최소 일정 수의 공급업체를 갖도록 요구함

- 몇몇 회원국은 시장이나 국가의 규모가 작거나 각 국가에서 규제되는 다국적 사업자의 상호의존성이 있어 SM05를 이행하는 데 어려움을 겪고 있다고 보고하였음

<국가별 이행 예시(출처:1차 보고서)>

키프로스	• 규제 프레임워크는 MNO가 위험 기반 접근 방식을 사용하여 적절한 다중 공급업체 전략을 개발하고 채택하기 위한 지침을 포함함
이탈리아	• 골든파워법이 적용되는 핵심 구성 요소와 관련된 계약에서 MNO는 다양화 프로젝트를 만들어야 함

ㅇ (SM06) 국가 차원의 회복탄력성 강화

	1차 보고서('20.07)
이행완료	1
진행중	7
계획됨	8
조치안됨	7
총계	23개국

2차 보고서('23.06)
3
6
18
27개국

- 조치가 안 되었다고 답한 회원국 중 5개 회원국은 국가 종속성 위험이 존재하지 않기 때문에* 조치 또는 이행 계획이 없다고 응답함

* 예) 이미 국가 수준에서 공급업체의 적절한 균형이 갖추어 있는 경우에 해당

- 그러나 이 경우 일부 회원국은 향후 동향을 모니터링하고 다양성 감소 위험이 있는 경우 조치를 취할 수 있다고 언급함
- 또한, SM05와 유사하게 몇몇 회원국은 자국 시장의 규모가 작기 때문에 SM06을 이행하기 어렵다고 답하였음

<국가별 이행 예시(출처:1차 보고서)>

스페인	• 국가 차원의 다양화 목표는 국가 5G 전략에서 고려될 예정
크로아티아	• 공급업체의 적절한 균형을 통해 국가 차원에서 회복탄력성을 확보하는 조치를 관련 법률에 포함하는 방안을 검토하고 있음

ㅇ (SM07) 외국인 직접 투자(FDI) 스크리닝

- FDI 심사를 위한 EU 프레임워크는 '20년 10월 완전히 운영되기 시작
- 집행위원회와 회원국은 규정의 완전한 적용을 위해 필요한 운영 요건을 마련하기 위해 노력하였음

• 회원국은 기존 국가 투자 심사 메커니즘을 집행위원회에 통지 • 정보 및 분석의 교환을 위해 각 회원국과 집행위 내에 공식 연락망 구축 • 회원국과 집행위가 FDI 문제에 신속하게 대응하고 의견을 제시할 수 있도록 관련 절차 개발

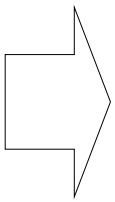
- '21년 말 25개 회원국은 국가 FDI 심사 메커니즘을 이미 갖추었거나, 새롭게 채택하였거나, 기존 메커니즘을 수정하였거나, 이를 갖추기 위한 자문 또는 입법 프로세스를 시작한 것으로 나타남

□ EU 회원국의 기술적 조치(TM) 이행 현황

※ 툴박스의 기술적 조치는 모바일네트워크사업자(MNO)에 대한 보안 요구사항을 강화하는 것과 관련됨

ㅇ (TM01) 기본 보안 요구사항의 적용 보장

	1차 보고서('20.07)
이행완료	8
진행중	15
계획됨	2
이행안됨	1
총계	26개국



2차 보고서('23.06)
23
2 (일부 이행)
2
27개국

- 대부분의 회원국에서 해당 조치는 주로 EU 프레임워크 지침[3] 13a조를 기반으로 현행 의무에 따라 통신 부문에 대한 일반 보안 요구사항의 일부로 이미 구현됨

※ 경우에 따라 국가사이버보안법 또는 MNO에 적용되는 기타 유사한 입법 문서에 정의된 특정 의무를 기반으로 하기도 함

※ 법적 구속력이 있는 조치 외에도 일부 회원국에서는 MNO가 시행해야 할 지침이나 권장사항을 제공함

- 동시에 많은 회원국에서는 기존 기본 요구사항의 개선 및 추가 보안 강화의 중요성을 인식하고 있으며, 현재 12개국이 개선 중이거나 개선할 계획이 있다고 밝힘

※ 이들은 주로 유럽전자통신코드(EECC)의 전치 범위나 사이버보안을 위한 기타 특정 법적 수단 개발의 일환으로 이에 대한 작업을 진행 중

- 또한, 여러 회원국에서 MNO는 자발적으로 ISO/IEC 27001 인증을 채택했거나 채택하는 과정에 있음

※ ISO/IEC27001은 정보보안관리시스템(ISMS)이 충족해야 할 요구사항을 정의하는 표준

- 회원국이 권장하는 일부 기술과 모범 사례는 다음과 같음:

- 메인 코어에서 시험 네트워크를 분리
- 백홀 보호 시스템에 대한 테스트를 포함하여 독립적이고 신뢰할 수 있는 제3자에 의한 정기적인 보안 테스트 및 취약성 평가
- 5G-Ensure 프로젝트에서 발표한 회사의 보안 기능과 관련된 권장사항에 따라 5G 시스템을 설계 및 관리

3) Regulatory framework for electronic communications

ㅇ (TM02) 기존 5G 표준의 보안 조치 이행

	1차 보고서('20.07)		2차 보고서('23.06)
이행완료	3	→	8
진행중	9		5
계획됨	10		
조치안됨	3		13
총계	25개국		26개국

※ 1차 및 2차 조사에서 1개국이 응답하지 않아 25개국 및 26개국의 이행 현황만 분석됨

- 일부 회원국에서는 정기적인 감사를 수행하거나 3GPP[4]를 포함한 특정 표준 및 기술 사양 준수 선언문을 요구함

※ 5개 회원국은 대부분의 경우 3GPP 기술 사양에 중점을 두고 해당 조치를 위한 국가적 조치를 도입하거나 확장할 계획

- 다른 회원국에서는 정의된 표준 및 사양의 준수를 명시적으로 의무화하지는 않으나, 기술 감독 활동에서 이러한 표준을 참조한다고 보고함

※ 이들은 3GPP, ETSI[5] 기술 사양 및 기타 표준을 참조하여 MNO에 지침을 제공

<국가별 이행 예시(출처:1차 보고서)>

오스트리아	• 통신네트워크보안규정(TNSR)에 따라 5G 네트워크를 운영하는 MNO는 필수 3GPP 보안 표준을 준수해야 함

4) 3GPP(3rd Generation Partnership Project) : 모바일통신 관련 단체들 간의 공동 연구 프로젝트로 전 세계적으로 적용 가능한 모바일통신 시스템의 표준화를 추진

5) 유럽전기통신표준협회(European Telecommunications Standards Institute) : 정보통신기술(ICT) 분야의 ES(ETSI Standard) 표준 제정을 촉진하고 조정하는 유럽의 독립된 비영리 기관

○ (TM03) 엄격한 액세스 제어 보장

	1차 보고서('20.07)		2차 보고서('23.06)
이행완료	7	→	19
진행중	14		4
계획됨	4		
조치안됨	1		2
총계	26개국		25개국

- 많은 회원국은 액세스 모니터링 및 사전 배경 조사에 대한 조항을 포함하여 해당 기술적 조치를 다루는 상세한 조치를 취하고 있음

※ 한편, 일부 회원국은 위험 기반 접근 제한을 적용하도록 하는 일반적 법적 의무를 부과함

- 몇몇 회원국은 제3자의 원격 액세스를 최소화하거나 방지하는 조치를 시행하고 있음
- 일부 회원국에서는 해당 기술적 조치가 5G 경매 이전에 요구되는 승인 과정에서 관련 특정 요구사항을 포함함으로써 해결되고, 일부 회원국에서는 해당 조치가 관련 중요 인프라 보안 프레임워크의 일부로 구현됨
- 회원국이 권장하는 특정 기술과 모범 사례는 다음과 같음:

- 운영 및 유지 관리에 대한 원격 지원 불허
- 중요한 경우에만 모니터링 하에 원격 액세스 허용
- 정기적인 액세스 제어 검토
- 관리 애플리케이션에 대한 액세스 제어(예: 중앙 집중식 권한 부여, 인증 및 액세스, 권한 있는 액세스 관리 등)
- MNO 직원과 제3자에 대한 원격 액세스 제어 및 모니터링

<국가별 이행 예시(출처:1차 보고서)>

아일랜드	• 통신보안요구사항(TSR)에는 네트워크 설계 및 액세스 제어에 대한 사업자의 세부 요구사항이 포함됨 • 이에는 네트워크 분할, 액세스 제어 및 권한 부여, 다중 요소 인증(MFA), 최소 권한 원칙 및 업무 분리에 관한 규칙이 포함됨 • TSR은 또한 사업자가 비정상적인 활동을 감지하기 위해 액세스에 대한 적절한 로깅 및 모니터링을 구현하도록 보장

○ (TM04) 가상화된 네트워크 기능의 보안 강화

	1차 보고서('20.07)		2차 보고서('23.06)
이행완료	1	→	8
진행중	9		5
계획됨	9		
조치안됨	6		14
총계	25개국		27개국

- 몇몇 회원국에서는 관련 ETSI 사양을 기반으로 네트워크기능가상화(NFV) 관련 제어를 준수하도록 요구하고 있으나, 다른 많은 회원국의 경우 네트워크 분리 및 패치 관리와 같은 기술적으로 중립적인 기존 조치를 통해 해당 조치를 이행하고 있음
- ENISA는 해당 조치 이행을 검토하고 강화하기 위한 맥락에서 '22년 2월 '5G NFV보안 - 도전과제 및 모범 사례'라는 제목의 보고서를 발간하였으며, 해당 내용은 5G 네트워크 및 서비스와 관련된 보안 제어를 통합하는 리포지토리인 'ENISA 5G 보안 제어 매트릭스'에 통합됨
- 1차 보고서에 따르면 해당 조치를 이행하기 위해 회원국들은 다음과 같은 계획을 수행할 예정

- 가상 네트워크를 포괄하는 요구사항 강화
- 독립적인 전문가나 EU 실무 그룹에 의한 정기적 테스트
- 위험 관리 프로세스 개선 및 가상화에 대한 위험 기반 접근방식 채택
- 승인 과정에서 관련 요구사항 포함
- NFV 확보를 위한 최신 기술 규정
- 위험 관리 개선 및 가상화에 대한 위험 기반 접근방식 채택을 위한 민간 부문과의 협력

<국가별 이행 예시(출처:1차 보고서)>

오스트리아	• 통신네트워크보안규정(TNSR)은 5G 네트워크를 운영하는 MNO가 ENISA의 문서인 '가상화의 보안 측면(2017)'에 명시된 권장사항을 준수하도록 명시함

ㅇ (TM05) 안전한 5G 네트워크 관리, 운영 및 모니터링 보장

	1차 보고서('20.07)		2차 보고서('23.06)
이행완료	4	→	11
진행중	12		7
계획됨	6		
조치안됨	3		8
총계	25개국		26개국

- EU 툴박스는 MNO가 국가 및 EU 내부에서 자체 네트워크운영센터(NOC)나 보안운영센터(SOC)를 운영하도록 보장할 것을 요구함
- 대부분의 회원국에는 NOC/SOC 배치에 대한 명시적인 법조문이 없어, MNO는 네트워크 관리 작업이 수행되는 국가의 법적/정치적 상황을 고려하는 등 위험 평가를 기반으로 NOC/SOC 배치를 결정해야 함
- 해당 조치의 시행을 위해 회원국은 다음을 고려하고 있음:

- MNO가 네트워크 운영에 있어 높은 수준의 자율성을 달성하도록 요청
- 위협 탐지 및 사고 대응을 향한 문화적 전환 장려
- MNO에 위협 관련 정보 제공
- 신뢰할 수 있는 구성 요소와 신뢰할 수 없는 구성 요소 간의 인터페이스 정의 및 이를 모니터링하는 데 사용할 수 있는 솔루션 식별

<국가별 이행 예시(출처:1차 보고서)>

이탈리아	• 해당 기술적 조치를 다루기 위한 기본 요구사항은 경제개발부 법령 '전자통신 네트워크의 보안 및 무결성 조치 및 중대한 사고 알림' 제4조에 포함되어 있음 • Golden Power의 적용에 따라, MNO는 NOC를 아웃소싱할 수 없으며, 네트워크 운영에 있어 높은 수준의 자율성을 달성해야 함

ㅇ (TM06) 물리적 보안 강화

	1차 보고서('20.07)		2차 보고서('23.06)
이행완료	7	→	17
진행중	12		6
계획됨	4		
조치안됨	2		4
총계	25개국		27개국

- 많은 회원국의 경우 MNO가 물리적 시설 액세스에 대한 자체 보안 정책을 갖고 있는 것이 일반적이며, 때로 관련 보안 사항에 대한 MNO의 의무는 중요인프라보안프레임워크의 일부로 구현됨

※ 많은 MNO는 업무연속성계획(BCP) 및 재해복구계획(DRP)뿐만 아니라 위험 평가에 모든 물리적 구성 요소를 포함함

- 또한, 많은 경우 기지국 및 데이터실과 같은 자산 보호를 위해 CCTV, 경보, 경비 및 펜스 등 표준 물리적 제어 장치가 배치되어 있음
- 한편, 다중액세스엣지컴퓨팅(MEC)과 관련된 위험 등 5G 네트워크 기술과 관련된 새로운 위험을 해결하기 위해 이러한 조치를 업데이트 할 필요가 있음

※ 많은 회원국에서는 주로 5G와 관련된 새로운 위험을 적절하게 완화하기 위한 목적으로 기존 물리적 보안 지침을 개정하고 강화하고 있음

※ 8개 회원국은 해당 기술적 조치에 대한 업데이트를 진행하였거나, 관련 추가 개선을 고려하고 있음

<국가별 이행 예시(출처:1차 보고서)>

오스트리아	• 통신네트워크보안규정(TNSR)에 따르면 5G 네트워크를 운영하는 MNO는 다중액세스엣지컴퓨팅 및 기지국과 관련하여 중요한 네트워크 구성 요소와 민감한 부분의 물리적 보안을 명시적으로 보장해야 함

○ (TM07) 소프트웨어 무결성, 업데이트 및 패치 관리 강화

	1차 보고서('20.07)		2차 보고서('23.06)
이행완료	3		19
진행중	15		5
계획됨	6		
조치안됨	1		3
총계	25개국		27개국

- 다수의 회원국에는 자발적으로 시행되거나 MNO에 부과된 소프트웨어 무결성, 업데이트 및 패치 관리를 위한 기존 패치 정책이나 프로세스가 마련되어 있음

※ 이들은 변경 제어, 테스트, 백업 및 복구가 통합된 패치 관리, 매입 절차, 보안 요구사항의 식별 및 보장, 악성 코드로부터의 보호를 다루는 보다 자세한 대비책을 갖추고 있었음

- 일부 회원국은 위험 기반 소프트웨어 무결성, 업데이트 및 패치 관리를 보장하는 더 높은 수준의 보안 목표를 가지고 있었음
- 6개 회원국은 EECC의 보안 조치에 대한 ENISA 지침 및 그에 수반되는 보완 문서(5G Supplement)를 참고하여 해당 기술적 조치를 이행하거나 개선하겠다는 의사를 밝힘
- 해당 조치의 시행을 위해 회원국은 다음을 고려하고 있음:

• MNO 패치 프로세스의 빈도 및 범위에 관한 요구사항 지정 • 자동 소프트웨어 업데이트 제어 및 제한 • 랩 환경에서 패치를 테스트하고 배포 전에 제어된 설정에서 장치가 업데이트 되는지 확인

<국가별 이행 예시(출처:1차 보고서)>

네덜란드	• 기술적 및 조직적 보안 요구사항은 통신법의 일부로 보조 법률에서 규정함 • 의무는 무엇보다도 액세스 제어, 보안 패치 및 사고 감지, 네트워크 세분화 및 타사 소프트웨어 보안 등과 관련됨

○ (TM08) 강력한 조달 조건을 통해 공급업체 프로세스의 보안 표준 향상

	1차 보고서('20.07)		2차 보고서('23.06)
이행완료	5	→	13
진행중	6		6
계획됨	7		
조치안됨	6		8
총계	25개국		27개국

- 일부 회원국은 자국 법률 내에서 더 넓은 범위의 보안 목표에 의존하고 있는 것으로 보이는 한편, 다른 회원국은 더 자세한 요구사항을 갖고 해당 기술적 조치에 대해 정기적인 감사를 수행하고 있음
- 일부 회원국은 현재 ENISA의 '안전한 ICT 서비스제품 조달을 위한 기본 보안 요구사항'을 포함하여 국제 모범 사례를 기반으로 이러한 요구사항을 도입하는 것을 고려하고 있으며, 일부 회원국은 무선 장비 지침과 같은 관련 법률에서 EU 조치를 따르고 있음

※ 한 회원국에서는 ENISA의 필수 기본 보안 요구사항 문서에 설명된 요구사항을 준수하도록 조치함

<국가별 이행 예시(출처:1차 보고서)>

아일랜드	• 통신보안요구사항(TSR)에는 공급자의 제품 수명주기 및 보안 관리 평가를 포함하여 사업자가 테스트 및 평가 프로세스의 일부로 보안 요구사항을 포함해야 한다는 요건이 포함됨 • TSR은 또한 사업자에게 공급업체와의 계약 협정의 일부로 제품 수명주기 및 보안 관리와 관련된 조항을 포함하도록 요구함

○ (TM11) 회복탄력성 및 연속성 강화

	1차 보고서('20.07)		2차 보고서('23.06)
이행완료	9	→	18
진행중	8		6
계획됨	6		
조치안됨	0		3
총계	24개국		27개국

- 대부분의 회원국은 MNO의 네트워크 및 서비스를 대상으로 하는 비즈니스 연속성 조치에 대한 조항을 가지고 있으나, 이러한 조치가 선택된 공급업체 내에서 연속성을 요구하도록 확장된 보고 사례는 상대적으로 적음

※ TM11은 MNO가 공급업체 내에서 유사한 조치를 요청해야 하며, 충분한 수준의 장기적 회복력을 입증하는 공급업체만 이용하도록 요구함

- 일부 회원국은 탐지, 대응, 에스컬레이션, 보고와 같은 결함 관리 절차뿐만 아니라 서비스 가용성 및 공급 연속성, 비상 계획 및 재해 복구 계획을 포함한 비즈니스 연속성 관리를 포함한 구체적인 조항을 제시함
- 또한 일부 회원국에서는 MNO가 연속성 정책을 구현할 때 EECC의 보안 조치에 대한 ENISA 지침과 그에 수반되는 5G 보완 자료를 최대한 고려할 것을 요구함

<국가별 이행 예시(출처:1차 보고서)>

벨기에	• 보안조치를 포함하여 위험 평가가 NRA에 보고됨 • 5G를 포함하는 중요 인프라의 맥락에서 NRA는 사업자의 정기적인 연속성 훈련 실행을 모니터링하고 있음 • NRA는 부문별 통신 위기 계획을 유지하고 정기적인 훈련을 조직함

□ 지원 조치(SA) 이행 현황

ㅇ 지식 교류 및 역량 구축

- **(SA06)** 회원국들은 5G 사이버보안 관련 NIS 작업반을 통해 EU 툴박스 이행의 모범 사례 및 관련 정보를 정기적으로 교류함으로써 EU 차원의 조정 및 접근방식을 지원하였음
- **(SA01)(SA04)(SA09)** ENISA는 통신 보안 규제 당국을 위한 사이버보안 조치 관련 여러 가이드라인을 제공하였으며, 대부분의 회원국들은 다양한 수준에서 활용하였음

※ 일부 경우에는 ENISA 가이드라인이 국가 연성법이나 사업자의 보안 요구 사항 또는 감사 지침에 대한 법적 문서의 기초로 직접 사용됨

- ENISA는 또한, 5G 보안의 다양한 측면에 관한 여러 보고서를 작성하여 EU 툴박스 조치 중 일부를 구현하는 데 있어 국가 당국을 지원하였음

• 5G 네트워크에 대한 업데이트된 위협 환경 • 5G 사양의 보안 제어 보고서 • 네트워크 기능 가상화 보안 보고서 • 5G 사이버보안 표준 분석

※ ENISA는 또한 다양한 보안 제어를 5G 보안 제어 매트릭스를 통해 하나의 동적 온라인 리포지터리로 통합함

ㅇ 공급망 회복탄력성

- **(Open RAN 사이버보안)** 회원국은 집행위와 ENISA의 지원을 받아 '22년 5월 Open RAN 사이버보안 관련 보고서를 발간함
- **(유럽 통신 인프라 및 네트워크의 사이버보안 및 회복력 위험 평가)** EU의 사이버보안 역량 강화를 위한 EU 통신부 장관들의 요청('22.03)에 따라 회원국(NIS 그룹)은 집행위, ENISA 및 BEREC과 함께 관련 위험 평가를 진행하고 있음
- **(EU 조정 beyond 5G 위험 평가)** NIS2 지침은 NIS 그룹이 집행위 및 ENISA와 협력하여 5G 네트워크에 대해 수행된 위험 평가를 중요한 공급망에 대해 수행할 수 있는 가능성을 제공함

※ NIS2 지침에 따라 특정 ICT 서비스, 시스템 또는 제품에 대한 이러한 조정된 공급망 위험 평가를 보완하기 위해 EU 이사회는 NIS그룹이 집행위 및 ENISA와 협력하여 중요한 ICT 공급망 위험을 줄이기 위한 조치 툴박스를 개발하도록 요청함('22.10)

※ 이들은 또한 EU의 사이버 태세에 관한 EU 이사회 결론('22.5)에 요청된 바에 따라 관련 민간 및 군 기관, 구축된 네트워크와 협력하여 현재 통신 및 일부 에너지 부문에 대한 위험 평가를 수행하고 있으며, 위험 시나리오를 개발할 예정

- **(네트워크 기술 분야 EU 역량 강화 투자)** '21년 11월 설립된 스마트 네트워크서비스 공동사업단(SNS JU)운 '27년까지 9억 유로의 EU 예산 및 동일한 금액의 민간 투자를 통해 5G/6G에 대한 연구혁신을 지원함

- **(안전한 5G 보급을 위한 EU 펀딩)** 집행위는 글로벌 게이트웨이와 같은 국제 이니셔티브를 통해 파트너 국가에서 5G를 포함한 연결성을 확보하기 위해 노력하고 있음

※ 또한, 집행위는 EU 툴박스에 따른 사이버보안 요구사항을 HE, DEP, CEF 등 관련 작업프로그램에 도입함

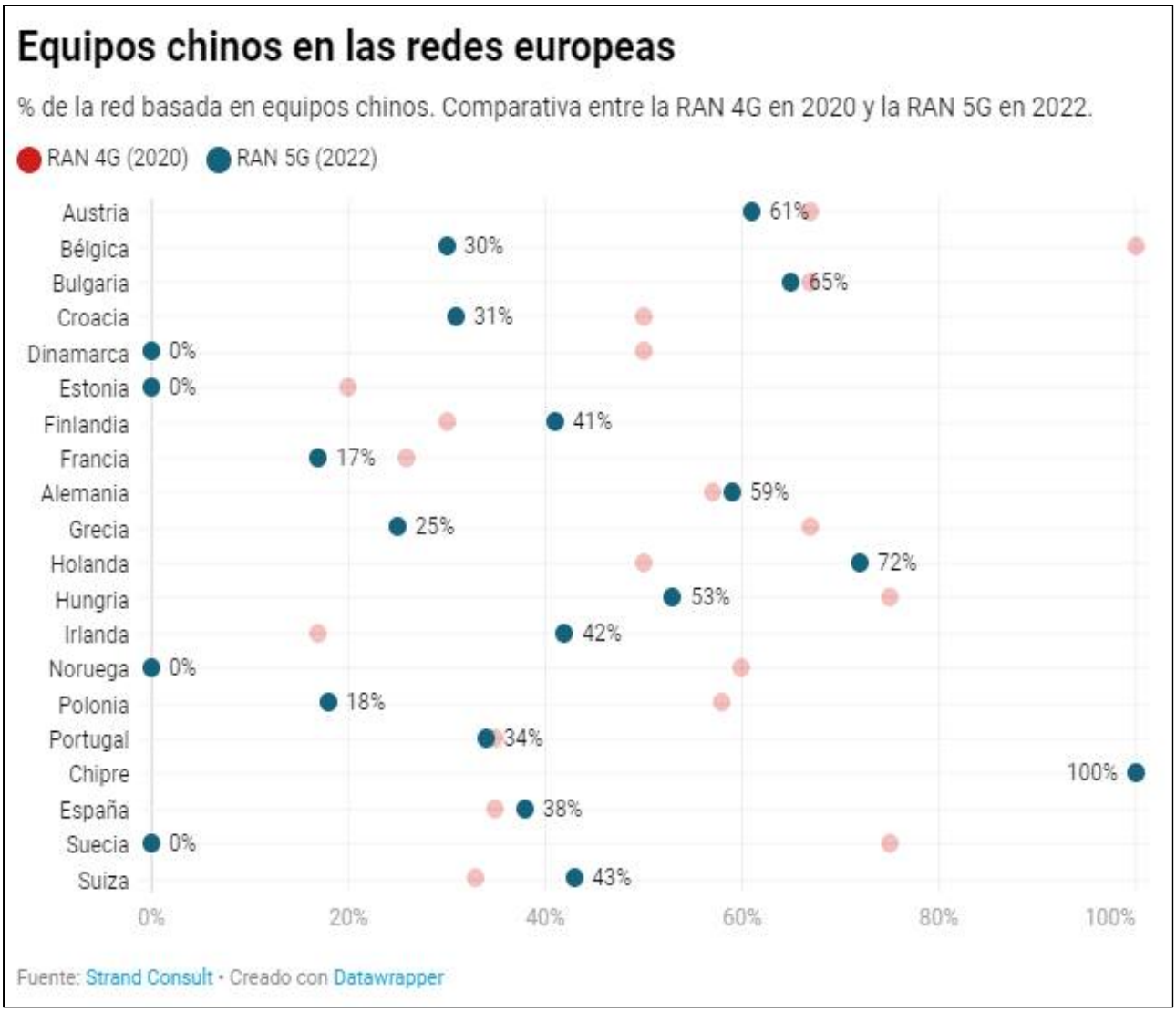
※ 더하여, 집행위는 유럽투자은행(EIB)를 포함한 국제 금융 기관과 협력하여 EU 펀딩 프로젝트에 EU 툴박스 등 EU 정책이 반영되도록 촉진하고 있음

3 5G 사이버보안 관련 EU 회원국의 중국 대응 현황

□ EU 5G 네트워크 내 중국 장비 사용 현황

○ 한 보고서에 따르면 유럽 5G 네트워크의 60%는 화웨이 및 ZTE 장비를 사용하고 있는 것으로 나타남('22.12)

<유럽 5G 네트워크 내 중국 장비 사용 비율(원자료: 덴마크 Strand Consult)(표출처: 스페인 언론 El Confidencial)>



- 키프로스의 경우 5G 인프라에서 100% 중국 장비를 사용하고 있으며, 그 뒤를 이어 루마니아(79%), 네덜란드(72%), 불가리아(62%), 오스트리아(61%) 순으로 많은 중국 장비를 가지고 있는 것으로 나타남

※ 다음 국가들은 국내 5G 네트워크에서 고위험 공급업체(특히, 중국)를 제외하는 등의 조치를 취하는 등 EU 툴박스를 성실히 이행하고 있음 (벨기에, 체코, 덴마크, 프랑스, 독일, 아일랜드, 네덜란드, 폴란드, 포르투갈, 루마니아, 스페인, 스웨덴)

□ 벨기에

ㅇ 벨기에는 '22년 2월 5G 모바일 서비스 제공을 위한 추가 보안 조치를 도입하기 위해 전자통신에 관한 다양한 조항을 개정하는 법률을 채택함

- 해당 법에는 MNO*와 MVNO**에 대한 정의가 포함되어 있으며, MNO는 5G 네트워크의 일부를 사용하기 전에 총리, 통신부 장관, 국방부 장관, 법무부 장관, 내무부 장관, 외교부 장관의 공동 승인을 받아야 함

* Mobile Network Operator(MNO): 모바일 전자통신 서비스를 제공하고 자체 네트워크와 이를 운영하는 데 필요한 모든 요소를 갖춘 사업자

** Mobile Virtual Network Operator(MVNO): MNO가 아니더라도, 즉 자체 네트워크 없이 동일한 서비스를 제공하는 사업자

- 또한, 해당 법은 공급업체의 위험 프로필을 평가하는 기준을 명시함

ㅇ 벨기에 정부, 고위험 5G 장비 공급업체 사용에 대한 제한 적용 예정… 중국 공급업체 사용 실질적으로 제한할 것으로 예상(20.06)

- 벨기에 국가안보위원회는 5G 네트워크의 핵심 및 백본(backbone) 부분 관련 고위험 공급업체 사용 전면 금지 및 무선 액세스(radio access) 관련 이러한 공급업체에 대한 상한선(35%) 도입 등 제한을 부과하기로 결정
- 또한, 국가안보위원회는 이러한 벤더의 사용이 제한되는 민감한 지역을 정의할 것이라고 밝힘

※ 중국 장비에 대한 의존은 NATO 본부와 EU 기관을 보유하고 있는 벨기에에 있어 정치적으로 까다로운 문제임

□ 체코

ㅇ 체코의 정책은 EU의 중국 정책, 특히 사이버보안 부문에서 한 선상에 있으며 체코 정부는 국제적으로도 선제적 조치를 취하였음

- 체코는 '19년 5월 제1회 프라하 5G 보안 컨퍼런스를 주최하였으며, 이에 5G 인프라를 계획·구축·시작·운영할 때 고려해야 하는 기술적·비기술적 위험에 대한 일련의 권장사항을 제공하는 '프라하 제안' 문서를 발표함

※ 프라하 제안은 5G 보안에 대한 국가의 접근방식을 다루는 첫 번째 관련 문서였으며, 프라하 제안에 대한 언급은 G7 디지털 및 기술 장관 선언을 포함하여 '19년부터 '21년까지 채택된 여러 양자 협정 및 국제 이니셔티브에서 찾아볼 수 있음

- 또한, 체코는 프라하 제안과 EU 5G 툴박스를 기반으로 미국과 5G 보안에 관한 공동 성명을 발표하였음('20.05)

- 이어 체코는 EU 5G 툴박스의 준비 과정에 상당 부분 참여하였으며, 후에 국립사이버정보보안청(NUKIB)은 산업통상부, 외무부 등과 체코 내 5G 네트워크 공급자의 신뢰도 평가를 위한 권고를 발간하였음('22.02)

□ 덴마크

ㅇ 덴마크 국방부는 국가 안보를 위해 덴마크의 동맹국에 속하지 않은 5G 기술 공급업체를 제외하겠다고 밝힘(20.06)

- 이처럼 덴마크는 5G 보안 툴박스와 같이 간접적으로 중국을 대상으로 하는 EU 이니셔티브를 지지해오고 있음

※ '19년도 덴마크 최대 단일 통신사인 TDC는 자사의 5G 네트워크로 화웨이 대신 에릭슨을 선택한 바 있으며, 이들은 상업적 결정이었다고 밝히는 동시에 화웨이와 정보 보안에 대한 우려 역시 잘 인지하고 있다고 밝히기도 함

- 덴마크는 '21년 5월 미래의 외국인 투자가 국가 안보에 위협이 되지 않도록 심사할 수 있도록 하는 법안을 통과시켰으며, 이 새로운 법안은 부분적으로 덴마크의 5G 네트워크 구축 관련 중국 화웨이의 입찰에 대한 보안 우려에 따라 개발됨

□ 프랑스

ㅇ 프랑스는 5G 보안 툴박스와 같은 EU의 중국 대응 관련 이니셔티브에 매우 적극적으로 나서고 있음

- 프랑스 사이버보안 기관 ANSSI는 '20년 7월 프랑스 5G 통신 네트워크

구축에서 화웨이 장비 사용을 전면 금지하지는 않을 것이라 밝혔으나, 5G 통신회사에 화웨이 사용을 자제할 것을 촉구함

- 프랑스 정부는 화웨이 5G 장비를 '28년까지 단계적으로 퇴출하기 위해 화웨이 5G 장비를 사용한 통신사의 사업 면허 기간에 패널티를 주는 방식으로 화웨이 퇴출을 추진하였음('20.07)

ㅇ **'21년 2월 프랑스는 5G 네트워크 관련 화웨이 반대법을 승인하여 고위험 공급업체로부터 이미 설치된 5G 장비를 제거하도록 조치함**

※ 한편 화웨이는 프랑스에 최대 규모 5G 공장 건설 계획을 발표('21.03)하고, 주프랑스 중국 대사관은 프랑스에 5G 네트워크에서 화웨이를 퇴출하지 말 것을 촉구하는 등 프랑스에 대응하였음

※ 또한, 프랑스 통신사들은 정부에 화웨이 장비 강제 철거에 대한 배상을 요구하고 있음('23.04)

□ 독일

ㅇ **독일은 '21년 4월 IT 보안법 2.0을 채택하여 신뢰할 수 없는 공급자로부터의 조달을 거부할 수 있게 되는 등 화웨이 장비 배제와 관련하여 EU와 같은 입장을 취함**

※ 한편, 독일에 있어 중국은 매우 중요한 수출 시장이자 무역 파트너로, 독일은 5G와 관련하여 중국을 배제하지 않기 위해 경계해 왔음

- 법은 그 자체로 화웨이를 직접 선별하지 않으나, 권위주의 국가의 통제를 받는 기업은 해당 법에 따라 신뢰할 수 없는 기업으로 간주됨
- IT 보안법 2.0은 모바일 네트워크의 사이버보안 부문에서 독일의 공공질서 또는 보안을 보호하기 위해 핵심 구성요소의 사용을 금지하는 규정을 포함하며, 네트워크 사업자는 동 법에 따라 특정 높은 수준의 보안 요구사항을 충족하고 핵심 구성요소의 인증을 받아야 함

※ 무엇보다 해당 법은 5G 모바일 네트워크에서의 정보 보안을 보장함

- 독일은 '23년 7월 중국 전략을 채택하였으며, 해당 전략은 핵심 인프라 보호와 관련하여 공공 5G 모바일 네트워크 부문에서 이미 특정 법률이 이행되고 있음을 언급함

□ 아일랜드

ㅇ **아일랜드 정부는 차세대 전자 통신 네트워크를 보호할 프레임워크로 EU 5G 보안 툴박스를 승인함('21.11)**

- 정부는 5G 네트워크 등 전자통신 보안 강화 방안에 합의하였으며, 동 이니셔티브의 일환으로 정부는 전자통신보안조치(ECSM)의 협의를 진행함
- ECSM은 공개 전자 통신 네트워크 및 공개적으로 사용 가능한 전자통신 서비스 공급자가 이행해야 하는 상세한 기술적·조직적 조치를 통해 국가 내 전자통신 인프라를 보호하는 것을 목표로 함
- 정부는 또한 전자통신 네트워크 장비 공급자의 위험 프로필을 평가하고 필요한 경우 특정 공급업체를 고위험으로 지정할 수 있도록 하는 기본 법안을 도입할 계획이라고 발표함

※ 해당 법안은 전자통신 네트워크의 특정 부분을 주요 자산으로 지정하고 고위험 공급업체가 해당 부문에서 사용되지 않도록 하는 특정 권한을 제공함

□ 네덜란드

ㅇ **네덜란드는 '19년 12월 통신 네트워크의 무결성 및 보안에 관한 법령(Bvit)을 발표함**

- 일반행정명령(AMvB)은 공급업체를 제외하기 위한 법적 근거를 만들며 정부는 Bvit을 사용하여 제외할 회사를 지정하는 장관급 규정을 만들 예정

※ 해당 법령에 따라 네덜란드에서 제공되는 통신 네트워크 또는 서비스를 오용하거나 훼손할 의도가 있거나 그러한 의도를 가진 당사자와 긴밀한 관계가 있거나 영향을 받는 것으로 알려지거나 의심되는 공급업체는 제외될 수 있음

ㅇ **'20년 10월, 통신 부문에 대한 새로운 투자 통제 체제를 도입하는 '통신 사업의 바람직하지 않은 영향력에 관한 새로운 법률'이 발효됨**

- 새로운 조항에는 국가 안보 위협으로 간주될 수 있는 행위의 목록이 포함되어 있음
- 동 법안에 따른 투자 통제 제도는 한 당사자가 통신 사업에서 직간접적으로 상당한 영향력을 얻게 되었을 때 적용되며, 이 경우 당사자는 네덜란드 당국에 통보해야 함

※ 한편 회사 간의 공정한 경쟁을 감독하는 네덜란드 규제 기관인 ACM은 '20년도 주파수 경쟁 이후 단일 사업자가 사용할 수 있는 최대 주파수를 40%로 제한함

ㅇ **'21년 외교부 연구에서 여러 정부 지도자와 전문가는 디지털 인프라 보안 및 스파이 활동 위험 등을 이유로 화웨이의 5G 네트워크 출시에 대해 경고함**

- 이에 따라 네덜란드의 3대 통신사인 KPN, T-Mobile, Vodafone은 그들의 핵심 네트워크에서 화웨이 5G 장비 사용을 중단하기로 결정함

※ 그러나 화웨이는 여전히 소위 엣지 네트워크용 안테나와 같은 장비를 공급 중

ㅇ **'21년 10월 Bvit를 기반으로 한 통신보안 및 무결성 규정이 발효됨**

- 동 규정은 모바일 네트워크 사업자가 취해야 하는 보안 조치에 대한 규칙을 포함하며, 약 19개의 조직적·기술적 보안 조치가 규정에 언급됨

□ 폴란드

ㅇ **폴란드는 여전히 사이버보안법 개정 작업을 진행중이나, 중국 5G 사업자의 폴란드 시장 진출은 사실상 이미 금지된 것으로 보임[6]**

- 5G 표준은 폴란드의 핵심 인프라로 간주되며, 폴란드는 보안상의 이유로 선택된 회사를 제외할 권리를 행사하고 있음
- '23년 1월 17일자 개정안 초안은 국가 사이버보안에 높은 위험이 있다고 판단되는 하드웨어 및 소프트웨어 공급업체를 공공 조달 절차에서 제외할 수 있는 조항이 포함되어 있음
- 또한, 개정안을 통해 사이버보안 위원단은 직권으로 관련 하드웨어 및 소프트웨어 공급업체의 위험을 평가할 수 있음

※ 고위험 공급업체의 경우 국가 사이버보안 시스템 기관은 해당 공급업체의 장비, 소프트웨어 및 서비스를 사용할 수 없으며 이미 사용 중인 모든 장비는 발표 후 5년 이내에 제거해야 함

□ 포르투갈

ㅇ **포르투갈 경매 규정에 따르면 RUF 보유자는 EU 5G 보안 툴박스 등을 고려하여 국가 또는 유럽 수준의 보안 규칙을 따르도록 함**

6) https://cms.law/en/int/expert-guides/cms-expert-guide-to-5g-regulation-and-law/poland

- 관련 규칙을 따르지 않을 경우 ANACOM(국가통신당국)은 전자통신법에 따라 전체 또는 일부 주파수 사용 권한을 박탈할 수 있음

※ 정부는 공식 성명을 발표하지 않았으나 NOS, Altice Protugal 및 Vodafone은 이미 새로운 핵심 5G 네트워크에서 화웨이 기술을 사용할 계획이 없다고 밝힘

□ 루마니아

○ 루마니아는 중국에 대한 공식적인 전략 없이 중국 정부를 공개적으로 비판하지 않는 동시에 5G 네트워크에서 중국을 제외하고 있음

- 루마니아는 5G 네트워크에서 '신뢰할 수 없는 벤더'를 제외하고, 중국 국영 기업의 접근을 제한하고, 엄격한 외국인 투자 심사 메커니즘을 만드는 등 비공식 전략으로 중국에 대응하고 있음

○ '21년 6월 루마니아는 5G 생산자가 정부로부터 사전 승인을 받도록 하는 5G 법을 통과시킴

- '20년 11월 루마니아 전 총리는 5G 분야에서 중국과 협력하지 않을 것을 공식적으로 밝힌 바 있으며, 현재까지 승인된 중국 기업은 없음
- 새로운 법률에 따라 통신 회사는 국익 통신 인프라와 5G 네트워크에 기술·장비·소프트웨어를 제공하기 위해 국가 최고 국방 위원회(CSAT)의 허가를 받아야 함

※ 이 법안의 채택은 '19년 8월 루마니아와 미국이 서명한 양해각서에 따르며, 루마니아는 화웨이를 표적으로 한 MoU에 서명한 첫 국가임

○ '19년 8월 루마니아와 미국은 5G 네트워크 공급업체에 대한 투명성 기준을 수립하기 위한 양해각서를 체결한 바 있음

- '19년 9월 EU 주재 미국 대사는 루마니아가 5G 네트워크에서 중국 기술을 사용하지 않는 것을 반겼으며, '22년 5월 미국 공화당 상원의원 포트만은 루마니아가 통신 네트워크에 중국 기업을 참여시키지 않은 데 만족감을 표하였음

□ 스페인

ㅇ **스페인이 '22년 3월 채택한 5G 사이버보안 법은 EU 보안 툴박스를 직접적으로 언급하며 툴박스에 제시된 조치를 취함으로써 EU의 주권 및 자율성과 5G 기술의 보안을 보장하고 있음을 명시함**

- 해당 법률에 따라 중국 공급업체는 고위험 제공자로 분류될 수 있으나, 해당 법의 이행은 정부 차원에서 지연되고 있는 것으로 나타남

※ 스페인 보안 기관은 일부 화웨이 장비의 제품 보안 인증을 승인하여 사용하고 있음

※ Telefonica는 핵심 5G 네트워크를 위해 화웨이와 협력해왔으나 앞으로는 에릭슨과 노키아 등에 의존할 것이라고 발표함

□ 스웨덴

ㅇ **스웨덴 우편통신위원회(PTS)는 '20년 10월 보안 위험을 이유로 5G 네트워크에서 화웨이와 ZTE 장비를 제외하기로 결정함**

- '22년 6월 판결에서 스웨덴 행정법원은 이러한 PTS의 결정을 지지함
- 스웨덴 전자통신법('22.06)에 따라 PTS는 무선송신기 라이선스와 관련된 문제에 대해 스웨덴보안청 및 스웨덴 군대와 협의해야 함

□ 영국

ㅇ **영국은 '20년 7월 국가사이버보안센터(NCSC)의 조언에 따라 '27년 말까지 5G 네트워크에서 화웨이 제품을 완전히 제거할 것임을 발표함**

- 영국은 '20년 11월 5G 네트워크 내 고위험 공급업체 장비의 완전한 제거를 위한 로드맵을 발표하였으며, 이에 따라 영국은 '20년 12월 31일부터 새로운 5G 화웨이 장비 구매를 전면 금지하였음

※ 한편 이는 '21년 5월 미국의 화웨이 제재에 따른 것임

- 같은 날, 영국은 로드맵과 함께 5G 공급망 다양화 전략을 발표함

※ 아래 국가들은 고위험 공급업체(특히, 중국)에 대한 별다른 조치를 취하고 있지 않은 것으로 보임

□ 오스트리아

ㅇ **오스트리아 통신 네트워크 보안 규정은 5G 네트워크 보안 요구사항을 포함하여 네트워크 보안에 대한 일반 조항을 다룸**

- 해당 법안은 총 가입자가 10만 명 이상인 네트워크 사업자를 대상으로 할 뿐 중국과 관련된 특정 규정은 없음

ㅇ **한편, 오스트리아 통신사업자들은 중국산 통신장비 사용에 신중한 모습을 보임**

- 주요 언론의 조사에 따르면 주요 네트워크 사업자 중 단 한 곳(Magenta Telekom)만이 화웨이 장비를 사용하고 있음

□ 그리스

ㅇ **그리스는 일반적으로 서방 동맹국들과 의견을 같이하고 있으나, 중국과도 좋은 관계를 유지하려고 하는 경향이 있음**

- 한편 그리스는 (시장 전문가에 따르면 화웨이 장비가 경쟁사보다 약 30%나 저렴함에도 불구하고) '20년 6월 화웨이 대신 에릭슨을 5G 공급자로 선택하였음

□ 헝가리

ㅇ **미국의 초청에도 불구하고 헝가리는 국제 클린 이니셔티브에 참여하는 것을 거부하였으며, '21년 10월에 헝가리 정부는 5G 관련 화웨이와 장기 협력 계약을 체결함**

- 해당 계약은 화웨이가 혁신과 지식 이전을 통해 디지털 교육의 발전을 지원하기 위해 헝가리 교육 기관과 계속 긴밀히 협력할 것이라고 명시
- 화웨이는 스마트 캠퍼스 솔루션을 테스트 및 출시하고 교육 기관에서 WiFi 시스템 및 광대역 네트워킹을 지속적으로 개발하여 국내 고등 교육을 지원할 것임

※ 원격 교육을 개선하기 위한 5G 네트워크 솔루션, 스마트 협업 및 가상 데스크톱 솔루션이 포함됨

□ 불가리아

ㅇ **통신규제위원회는 사이버보안 및 네트워크 보안에 관한 특별 규칙을 도입, 공급자에게 위험 평가 및 관련 목록 작성 등 의무를 부과함**

- 해당 법은 중국을 명시적으로 언급하지 않으나, 불가리아는 중국 기술 회사로부터 5G 네트워크를 보호하는 것을 목표로 하는 US Clean Network 이니셔티브에 서명한 바 있음

□ 룩셈부르크

ㅇ **중국 기술에 대한 공식적인 규제나 정치적 입장이 없으나, 사업자는 네트워크가 안전한지 확인해야 함**

- 4G RAN을 위해 화웨이 장비에 100% 의존했던 Proximus와 Orange Luxembourg는 이제 5G 네트워크에서 핀란드 Nokia를 선택하는 등, 3대 이동통신사는 더 이상 중국 공급업체를 신뢰하지 않는 것으로 보임

□ 스위스

ㅇ **스위스의 기존 법적 프레임워크에 따르면 정부는 네트워크 사업자가 중국 공급업체로부터 장비를 취득하는 것을 금지할 수 없음**

- 스위스는 5G 네트워크와 관련하여 외국 기술 제공업체에 의존해야 하는 상황이며, 정부는 관련 보안 문제를 심각하게 받아들이고 있음에도, 이러한 법적 제약으로 인해 별다른 조치를 취하기 어려운 상황

ㅇ **'23년 1월 연방 의회는 모바일 네트워크 관련 통신서비스조례(OTS)를 개정하여 국제적으로 정의된 추가 보안 요구사항을 도입함**

- 개정된 OTS에 따르면 사업자는 사업연속성관리계획서, 보안사고관리 계획서 등 정보보안 관리 체계를 개발 및 이행하고 지속적으로 검토해야 함
- 네트워크 및 보안 운영 센터는 스위스 또는 법적으로 적절한 데이터 보호를 보장하는 국가에서만 운영될 수 있음

4 결론 및 시사점

□ 결론

① 5G 네트워크는 EU 내부시장 및 사회경제적 기능 운영에 필수적인 서비스 기반을 제공하는 중요 인프라임

- 따라서 5G 네트워크의 사이버보안과 탄력성을 보장하는 것은 필수임

② 이에 따라 EU는 5G 네트워크의 주요 사이버보안 위험을 완화할 수 있는 조치를 제시하는 EU 5G 보안 툴박스를 제시함

- 툴박스는 국가 및 EU 수준의 우선순위 완화 계획 설정을 위한 지침을 제공

③ '23년 6월 발간된 두 번째 툴박스 이행 보고서에 따르면 대부분의 EU 회원국은 툴박스 조치에 따라 보안을 강화했거나 그 과정 중에 있음

- 그러나 27개 회원국 가운데 10개 회원국만이 고위험 공급업체에 의무를 부과하거나 5G 네트워크 제한 및 배제 조치를 취하고 있으며, 다수의 회원국의 이러한 기업에 대한 의존은 여전히 지속되고 있음

④ 집행위는 아직 툴박스를 이행하지 않고 있는 회원국들이 툴박스에서 권고하는 조치를 채택하여 규명된 고위험 업체에 대해 신속히 대응할 것을 촉구함

- 특히, 집행위는 화웨이 및 ZTE 등 고위험 공급업체를 사용하는 모바일 네트워크에 큰 규모 조직들의 통신이 노출되지 않도록 조치할 예정

> 집행위는 해당 공급업체 장비에 의존하는 새로운 연결 서비스를 조달하지 않도록 관련 보안 조치를 취하고, 회원국 및 통신 사업자와 협력하여 기존 집행위의 모든 네트워크 서비스에서도 고위험 공급업체의 장비 사용을 점진적으로 제한할 예정

⑤ 집행위는 이러한 결정을 모든 EU 펀딩 프로그램 및 조치에도 적용할 계획

- 예를 들어, 집행위는 EU가 고위험으로 분류한 화웨이를 Horizon Europe 프로그램에서 제외하기 위해 HE 규칙을 변경할 것임을 밝힘('23.08)[7]

7) 집행위, Horizon Europe에서 화웨이 배제 계획(8.18)
https://k-erc.eu/%ec%a7%91%ed%96%89%ec%9c%84-horizon-europe%ec%97%90%ec%84%9c-%ed%99%9

□ 시사점

ㅇ EU 툴박스 조치에는 화웨이, ZTE 등 중국 벤더들의 5G 장비 도입을 제한하는 조치도 포함되어 있어 우리나라와 관련이 높음

- 우리나라와 EU 간의 5G를 포함한 디지털 분야의 협력이 확대됨에 따라 EU의 관련 정책 조치를 파악하고 향후 전망을 분석할 필요 있음

> **ㅇ 전략적 조치와 관련하여 EU 이사회는 EU 조정 위험 평가에서 중요하고 민감한 것으로 정의된 주요 자산에 대해 고위험 공급업체에 관련 제한을 적용하는 것이 특히 중요하다고 강조**
>
> - 이 단계에서 24개 회원국은 국가 당국에 이러한 평가를 수행하고 제한 사항을 발생할 수 있는 권한을 부여하는 입법 조치를 채택했거나 준비 중임
> - 또한 10개 회원국은 이러한 제한을 부과했으며, 3개 회원국은 현재 관련 국내법 시행을 위해 노력하고 있는 등 앞으로도 EU 내 관련 조치가 확대될 것으로 전망
>
> **ㅇ 기술적 조치에 따른 통신사업자에 대한 요구사항 및 감독은 NIS2 지침의 이행을 통해 더욱 강화될 것**
>
> - 또한, 사이버탄력성법(CRA)은 하드웨어 및 소프트웨어 제품이 더 나은 보안 기준에 따라 개발되도록 요구하는 등 관련 보안 조치가 더욱 강화될 것으로 예상됨

ㅇ EU 회원국이 중국 기업을 배제함에 따라 생기는 빈자리에 우리나라 기업의 진출 기회를 더욱 적극적으로 모색할 필요 있음

- 일부 회원국에서는 중국 기업을 배제함에 따라 삼성전자 등과 같은 우리나라 공급업체와 공급 계약을 체결하는 등 민주주의 협력 국가의 5G 장비 공급업체로 관심을 돌리고 있음[8)]
- 특히, 이와 관련하여 한-EU 디지털 파트너십, 호라이즌 유럽 준회원국 가입 등 최근 강화되고 있는 한-EU 협력 관계를 적극적으로 활용하도록 장려됨

4%ec%9b%a8%ec%9d%b4-%eb%b0%b0%ec%a0%9c-%ea%b3%84%ed%9a%8d-18/

8) https://brussels-school.be/sites/default/files/5G%20in%20Europe%20and%20South%20Korea.pdf

<참고자료>

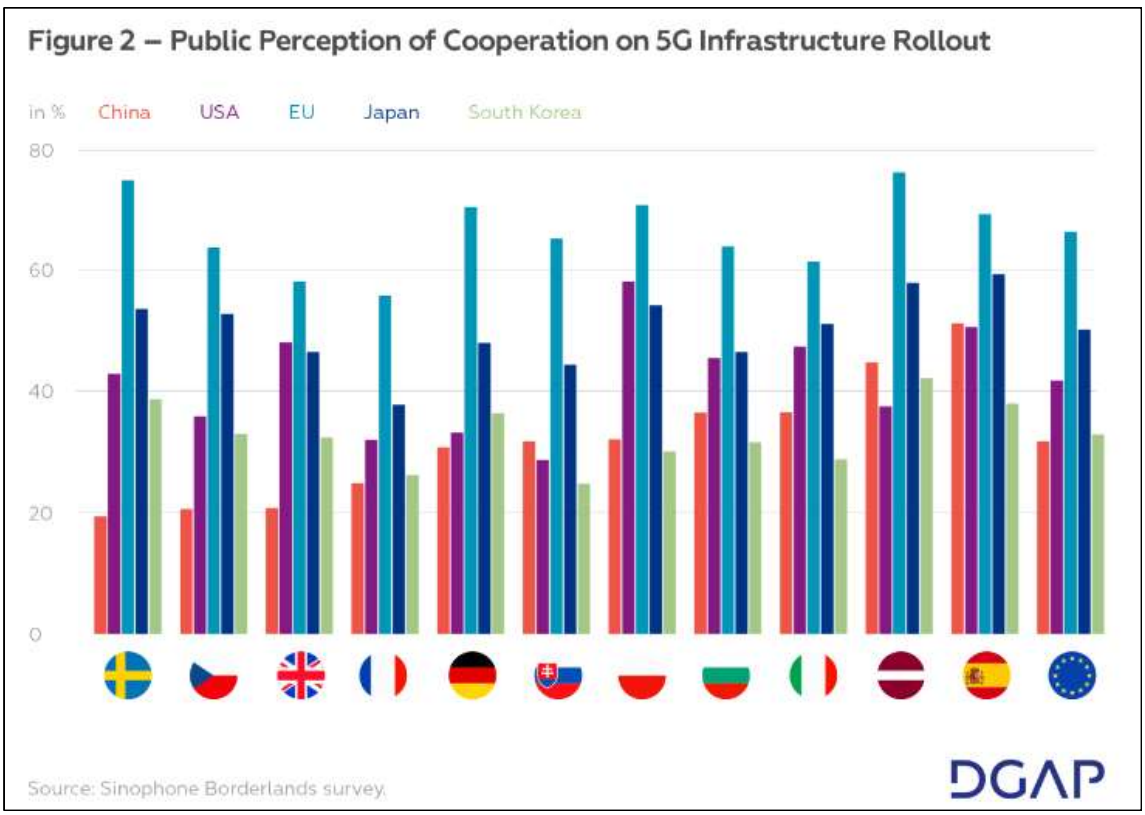
ㅇ **NMS Market Research가 '20년도 9월~10월 유럽 11개국에서 시행한 설문조사에 따르면 유럽인의 약 66%는 유럽 내 5G 협력을 지지하며, 50% 이하는 일본, 미국, 한국과의 제휴를 지지함**[9)]

- 중국 공급업체와의 협력에 대한 지지는 평균 31.8%로 스웨덴의 19.4%에서 스페인의 51.2%까지 다양하게 나타남

스웨덴	19.4%	폴란드	32.1%
체코	20.6%	헝가리	36.5%
영국	20.8%	이탈리아	36.6%
프랑스	24.9%	라트비아	44.8%
독일	30.8%	스페인	51.2%
슬로바키아	31.8%	평균	30.8%

※ 동 여론 조사에는 각 국가당 1,500명씩 총 16,500명이 응답함

- 우리나라(연두색 막대)는 대부분의 경우 중국(빨간색)보다는 좋은 평을 받았으나, 미국(보라색)과 일본(남색)에는 뒤처지는 것으로 나타남



9) https://ceias.eu/evaluating-public-support-for-chinese-vendors-in-europes-5g-infrastructure/