보도자료

담당	사이버안보비서관실

대한민국 대통령실

다시 대한민국! 새로운 국민의 나라

배포 : 2024년 2월 1일(목)

국가안보실, 윤석열 정부의 '국가사이버안보전략' 수립

- 자유·인권·법치의 가치를 바탕으로 「글로벌 중추국가」 지향 -

국가안보실은 오늘(2/1, 목) 국정원, 외교부, 국방부, 과기정통부 및 경찰청 등과 합동으로 마련한 윤석열 정부의 '국가사이버안보전략'을 발표했습니다. 이는 국가 차원의 사이버 전략 방향을 제시하는 사이버안보 분야 최상위 지침서로, 변화된 안보 환경과 국정 기조를 담아 수립됐습니다.

윤석열정부의 국가사이버안보전략은 수립 배경, 비전과 목표, 전략과제, 이행 방안의 총 4개 장으로 구성되어 있으며 △자유민주주의 가치 수호 △글로벌 중추국가 실현 △법치와 규범 기반 질서 수호 등 정부의 외교안보 분야 국정 철학 구현 방안을 담고 있습니다.

특히, 국가사이버안보전략의 비전을 '사이버공간에서 자유·인권·법치의 가치를 수호하면서 국제적 역할과 책임을 다하는 글로벌 중추국가'로 설정함으로써, 2023년 6월 발표한 윤석열 정부 국가안보전략서의 방향성과 맥을 같이하고 있습니다.

이를 실현하기 위해 국가의 핵심 가치와 국민의 이익을 함께 중시하고, 모든 이해관계자 간 긴밀한 협력을 바탕으로 위협에 공동 대응하며, 국제규범을 기반으로 적법하게 업무를 수행한다는 원칙을 담고 있습니다.

또한 △공세적 사이버 방어 및 대응 △글로벌 리더십 확장 △건실한 사이버 복원력이라는 사이버안보 전략 3대 목표를 제시했고, 이를 추진하기 위한 5대 전략과제를 실행해 나갈 것입니다.

* 5대 전략과제 : ① 공세적 사이버 방어 활동 강화 ② 글로벌 공조체계 구축 ③ 국가 핵심 인프라 사이버 복원력 강화 ④ 新기술 경쟁 우위 확보 ⑤ 업무 수행 기반 강화

국가사이버안보전략서는 정부 각 부처가 소관 계획과 시행 계획을 수립·추진하는 가운데 그 이행상황을 주기적으로 점검하도록 기술하고 있습니다.

국가사이버안보전략서에 담긴 내용의 주요 특징은 다음과 같습니다.

첫째, 북한의 사이버 위협을 중점 기술합니다. 우리 기반시설에 대한 사이버 위협은 물론, 핵과 미사일 개발 자금을 확보하기 위한 가상자산 탈취, 허위정보 유포 등 북한의 사이버 위협에 대처하기 위한 정책과 대응 방안을 제시합니다.

둘째, 기존의 방어 중심 대응에서 벗어나 사이버 위협을 선제적으로 식별하고 대응하는 공세적이고 포괄적인 접근과 이를 위한 대응역량 강화방안이 포함되어 있습니다.

셋째, 글로벌 사이버 협력의 중요성을 강조했습니다. 그간 정부는 한미동맹의 범주를 사이버 공간으로 확장한 데 이어, 캠프 데이비드 협력체계를 통해 한미일 3국 간 사이버 공조를 강화했으며, 영국과도 사이버 파트너십을 체결했습니다. 정부는 핵심 협력국들과 강력한 사이버 파트너십을 구축하는 가운데, 인·태 지역 및 NATO 회원국들과의 사이버안보 협력을 강화해 나갈 것입니다.

넷째, 최근 행정 전산망 장애로 국민들이 큰 불편을 겪었던 사례를 교훈 삼아, 신속한 대응체계를 마련하는 데 주력하고자 합니다. 아울러 정보보호 기업의 혁신을 지원하고 이를 위한 투자를 확충하면서 사이버 인프라의 국제 경쟁력을 확보해 나갈 계획입니다.

정부는 사이버안보 전략 수립을 계기로 국가 사이버안보 역량을 한층 강화함으로써 국민을 더욱 안전하게 보호하는 데 최선의 노력을 다할 것입니다.

국가안보실은 '국가사이버안보전략' 책자(국문, 영문)를 배포하여 윤석열 정부의 국가사이버안보 전략을 국내외에 널리 알려 나갈 계획입니다.

붙임: 국가사이버안보전략 요지 1부. <끝>

보도자료

담당	사이버안보비서관실

국가사이버안보전략 요지

수립 배경

o 사이버안보의 중요성이 부각됨에 따라 각국은 사이버안보 수준을 향상시키기 위해 국가 차원의 전략을 수립, 우리도 안보환경 변화에 맞는 새로운 전략의 구상이 필요

o 정부는 우리나라를 겨냥하는 다양한 사이버 위협 앞에서, 국가 핵심 기능을 안정적으로 운영하고 국민을 안전하게 보호하기 위한 새로운 전략 구상이 필요하다고 판단

비전과 목표

< 비 전 >

사이버공간에서 자유·인권·법치의 가치를 수호하며
국제사회에 역할과 책임을 다하는 글로벌 중추국가

1. 공세적 사이버 방어 및 대응 : 방어 위주의 기존 전략만으로는 고도화하는 사이버위협 대응에 한계가 있으므로 공격징후를 사전에 포착하고 이에 대한 선제적인 대응을 취하여 위협을 제거·완화

2. 글로벌 리더십 확장 : 사이버공간에서 가치를 공유하는 국가들과 연대하여 다양한 사이버 위협에 맞서며 UN·NATO 등 국제무대에서 사이버안보 문제를 보다 적극적으로 주도하는 등 우리나라의 국제 영향력 확대

3. 건실한 사이버 복원력 확보 : 사이버공격 발생시 정부의 역량을 신속하게 집중하여 복구하고, 포괄적인 보안 역량을 지속적으로 강화시켜 우리 사이버 공간을 든든하게 보호

전략과제

1. 공세적 사이버 방어활동 강화 : 국가안보·국익을 위협하는 악의적 사이버활동에 대한 억지력을 확보하고, 위협 행위자의 사이버 공격에 대한 선제적 방어역량 강화

* 사이버공격의 주체를 규명하기 위한 역량 강화, 공격 근원지 대상 탐지·분석을 통한 위협 사전포착, 사이버공간에서 국론 분열과 사회·경제적 혼란을 유발하는 영향력 공작 대응, 랜섬웨어 유포 및 가상자산 해킹 등 사이버위협 대응 역량 강화

2. 글로벌 공조체계 구축 : 국제사회와의 적극적인 협력을 통해 사이버 위협 대응의 실효성을 제고하고, 글로벌 중추국가로서 안전하고 평화로운 사이버 공간 구축에 기여

* 주요국과 사이버안보 협력 강화를 통한 국제 사이버 협력 네트워크 확충, UN·NATO 등의 국제사회 논의 주도, 국제표준·규범·통상협정 등에서 우리의 영향력 강화, 국내외 민간기업과 위협정보·정책·기술 교류 확대, 개발도상국을 대상으로 글로벌 역량강화 지원 확대 등

3. 국가 핵심인프라 사이버 복원력 강화 : 국가 핵심인프라와 중요 시스템의 사이버 복원력을 강화하여, 모든 기업과 국민에게 편리하고 안전한 서비스를 제공

* 정보시스템 장애 대비를 위한 신속한 대응체계 수립, 기반시설 관리시스템의 최소 보안 요구사항 수립 및 위협탐지체계 구축, 제로 트러스트 보안전략 구현을 위한 기반작업 및 단계별 추진계획 수립·시행, ICT 공급망 보안을 위한 제도·지침을 개정하고 관련 인력 육성 등

4. 新기술 경쟁우위 확보 : 국가 사이버안보 역량의 기반인 핵심 기술을 적극적으로 육성하고 안전하게 보호함으로써 국제 경쟁력 및 기술 주도권을 확보

* 사이버안보 핵심기술 식별 및 전략산업화 추진, AI·양자기술 등 新기술 연구개발 지원 확대, 신기술 적용 정보보호제품 규제개선 등 혁신 촉진을 통한 경쟁력 확보, 新기술 보안관리 프레임워크 마련, 양자대응 암호체계 구축 및 국제암호표준 개발에 적극 참여 등

5. 업무 수행기반 강화 : 개인, 기업, 정부의 역할과 책임을 유기적으로 연결하여 조화를 이루고 제도화하는 범국가 차원의 사이버안보 체계 확립

* 국가안보실 산하에 국가사이버안보위원회를 설치하여 정책 사항을 조정하고, 정부·기업의 핵심 역량을 결집하기 위한 통합대응조직 설치, 사이버안보 업무 관련 제도와 기반 개선, 사이버안보 위기에 관한 지침·매뉴얼 제·개정, 정보공유체계 정비를 포함한 민관 협력 활성화 등

이행방안

o 정부는 국가사이버안보전략을 매 5년마다 개정하고, 전략의 비전·목표를 달성하기 위한 기본계획과 시행계획을 수립하여 이를 효과적으로 추진.