발 간 등 록 번 호
12-1025000-000012-13

다시 대한민국!
새로운 국민의 나라

국가 사이버안보 전략

NATIONAL CYBERSECURITY STRATEGY

대한민국 대통령실 국가안보실

대한민국 대통령실 국가안보실

국가 사이버안보 전략

NATIONAL CYBERSECURITY STRATEGY

대한민국 대통령실 국가안보실

국 가 사 이 버 안 보 전 략

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

전 략 과 제

1	2	3	4	5
공세적 사이버 방어활동 강화	글로벌 사이버 공조체계 구축	국가 핵심인프라 사이버 복원력 강화	新기술 경쟁우위 확보	업무 수행기반 강화

"저와 바이든 대통령은 앞으로 한미동맹이 사이버, 우주 영역으로도 확장될 수 있도록 **한미 상호방위조약**을 **사이버**, **우주 공간**에 **적용**하기 위한 **논의**도 **개시**하기로 했습니다. 이번에 채택된 '**전략적 사이버안보 협력 프레임워크**'를 통해 **한미 양국**이 **사이버 위협**에 **공동 대응**하고 **정보공유**, **수집**, **분석**과 관련된 **협력**도 **심화**해 나가기로 했습니다."

윤석열 대통령 한미 공동기자회견 모두 발언(2023.4.27)

서문

사이버 공간은 디지털 기술의 무한한 잠재력을 바탕으로 진화와 확장을 거듭하고 있습니다. 우리는 사이버 공간이 제공하는 다양한 편익을 누리고 있지만, 동시에 디지털 수단들로부터 비롯된 여러 또 다른 위협에 노출되어 있습니다. 사이버 공간의 편익을 늘리면서도 불안과 혼란을 막을 수 있는 보편타당한 원칙과 규범이 필요합니다.

특히, 북한은 핵무기와 미사일 개발 자금을 마련하기 위해 가상자산 탈취를 비롯한 불법적 사이버 활동을 지속하고 있습니다. 또한, 세계 곳곳의 해킹 조직들은 고도화된 사이버 위협 수단으로 국가기밀과 첨단기술을 탈취하고 있습니다. 사이버 공간에서 무차별적으로 생산되고 확산되는 가짜뉴스와 허위정보들이 자유민주주의 질서를 흔들고 국가안보까지 위협하고 있습니다.

이번에 발간하는 〈국가사이버안보전략〉은 이처럼 증가하는 사이버 위협에 대응하는 우리 정부의 기본 전략을 담은 책자입니다. 지난해 6월 발간한 〈국가안보전략〉의 토대 위에, 우리 정부가 표방하는 사이버안보 전략을 상세하게 설명하고 있습니다.

이러한 전략을 토대로 우리 정부는 사이버안보 위협에 선제적으로 대처하고 사이버 역량과 복원력을 강화하여, 대한민국을 안전하게 지켜나갈 것입니다. 또한 자유, 인권, 법치의 규범과 가치를 공유하는 우방국들과 사이버안보 공조를 강화하면서 국제사회의 평화와 번영에 기여해 나갈 것입니다.

정부는 자유와 인권 등 국민의 기본권 보호를 최우선 목표로 두고, 국민과 함께 〈국가사이버안보전략〉을 충실히 실천해 나가겠습니다.

2024년 2월

대한민국 대통령

윤석열

I
BACKGROUND

II
VISION

III
STRATEGY

IV
PLAN

수립 배경 10

01 환경의 변화와 도전 13
02 평가와 필요성 14

비전과 목표 16

01 비전 16
02 목표 17
03 원칙 19

전략과제 20

01 공세적 사이버 방어활동 강화 20
02 글로벌 사이버 공조체계 구축 23
03 국가 핵심인프라 사이버 복원력 강화 26
04 新기술 경쟁우위 확보 28
05 업무 수행기반 강화 30

이행방안 34

I
수립 배경

사이버공간은 다양한 국가 · 비국가 행위자들이 상호 연결되어 지속적으로 영향을 미치는 역동적인 영역이다. 대한민국의 사이버공간은 다양한 정치 · 경제 · 사회 · 문화 활동을 영위하는 자유민주주의의 근간이며, 국민생활과 밀접한 정부시스템 등 핵심 인프라가 운용 · 관리되는 안보의 중심 영역이다.

최근에는 사이버공간에서 국제 및 국가배후 해킹조직 등 사이버위협 행위자(이하 위협행위자)들에 의한 첨단기술 유출, 가상자산 탈취와 함께 가짜뉴스 등 허위정보 유포를 통한 여론조작, 핵심인프라 무력화 등 악의적 사이버 활동들이 국가안보에 심각한 위협이 되고 있다. 또한, 랜섬웨어로 인해 정부기관은 물론 국가 핵심시설이 마비되는 사고가 세계 각국에서 끊임없이 발생하고 있으며, 의료기관 등을 겨냥한 랜섬웨어 공격은 국민의 생명까지 위협하는 실정이다.

특히, 북한은 전세계 군사 · 금융 · 통신 등 다양한 분야에 파괴적 영향을 미칠 수 있는 사이버공격 역량을 강화해오고 있으며, 불법 사이버 활동을 통해 국제사회 제재를 회피하면서 핵 · 미사일 개발에 필요한 자금을 충당하고 있다.

사이버안보는 북한 등 위협행위자들이 자행하는 국가안보와 국익에 반하는 사이버 활동을 확인 · 견제 · 차단하고, 그에 필요한 대응조치를 강구 · 이행함으로써 국가와 국민의 안전 그리고 국익을 보호하는 것을 말한다.

사이버안보의 중요성이 그 어느 때보다 높아짐에 따라 전세계적으로 사이버안보 수준을 향상시키기 위한 국가전략을 수립하고, 보다 효과적으로 이행하기 위한 법 · 제도 등의 개선에 노력하고 있으며, 우리나라도 이러한 시대적 흐름에 맞추어 2019년에 국가 사이버안보 전략을 발표한 바 있다.

그러나 국가 사이버안보 전략 발표 이후, 코로나19로 인한 글로벌 팬데믹 · 강대국 간 기술패권 경쟁 등 대내·외 사이버안보 환경이 급변하고 있는 데다 위협행위자들에 의한 사이버안보 위협이 지속적으로 증가하고 있다. 또한 국민들이 일상에서 이용하는 IT 서비스에 장애가 발생함으로써 국민을 불편케 하고 경제·사회적 혼란을 유발하기도 한다. 이에 따라 우리나라도 그에 맞는 새로운 국가 사이버안보 정책 방향을 재정립해야 할 것이다.

대한민국 정부는 이러한 사이버공간의 본질적 특성에 대한 이해를 바탕으로 전략적 범위를 확장하여 공세적 사이버 방어 역량을 확충하고, 국가들과의 협력을 심화하는 한편, 핵심적인 국가기능의 안정적인 운영과 국민 개개인을 보호하기 위한 새로운 전략의 구상이 필요하다고 판단한다.

특히, 한미 정상회담('23.4월) 계기, 「한미간 전략적 사이버안보 협력 프레임워크」가 체결되었으며, '한미 상호방위조약의 사이버공간 적용에 대한 논의를 추진'한다는 내용이 포함되는 성과를 도출하였다. 우리나라의 사이버안보 국제협력에서의 큰 전환점으로, 미국과의 협력수준 제고를 통한 안보역량 강화 및 국제사회에서의 공동 대응 등에 대한 비전을 제시할 필요성도 높아지게 되었다.

또한 한미일 정상회의('23.8월)에서는 3국 정상이 對北 사이버 공조 강화에 합의하고 이를 위한 실무그룹 신설을 발표하였으며, 영국과는 수교 140주년을 맞아 정상간 「전략적 사이버 파트너십」을 체결('23.11월)함으로써 정보공유, 연합훈련, 민간교류 활성화 등 양국간 협력을 한 차원 높은 수준으로 격상하기로 하였다.

이전 전략이 국내 정보보호 역량 제고와 주요 기반시설 보호 등 내면의 강화에 주안점을 두었던 것과는 다르게 새로운 전략은 사이버위협에 대한 공세적 방어 역량과 글로벌 리더십 확보를 위해 관련국들과의 긴밀한 협력관계를 강조한다. 또한, 국가 핵심 기능은 물론 국민의 디지털 일상을 보호하기 위해 범국가적인 역량을 투입하여 사이버 복원력을 제고하고 악의적 사이버 활동에 대하여 대응조치를 취하는 전략적 개념을 포함한다.

1. 환경의 변화와 도전

초연결 사회와 비대면 디지털 환경으로의 급속한 전환은 우리 일상을 ICT와 불가분의 관계로 변모시키면서 새로운 보안 취약점에 노출시켰다.

주요 기반시설과 정부 시스템도 ICT 발전과 고도화라는 시대적 흐름에 따라 사이버공간과 밀접하게 연결되면서 다양한 사이버위협에 직면하고 있다.

블록체인 기술이 적용된 가상자산이 안전자산으로 각광받고 있으나 불법 자금 세탁 등에 악용될 수 있으며 북한은 사이버 해킹을 통해 막대한 규모의 가상자산을 탈취하여 핵 · 미사일 개발에 전용(轉用)하고 있어 우리뿐만 아니라 국제사회에 큰 위협 요인이 되고 있다.

또한 가짜뉴스와 여론조작과 같은 새로운 위협이 자유민주주의의 도전요인으로 부상하고 있으며, 사이버범죄자들이 데이터를 암호화해 복구비용을 지불하도록 협박하는 랜섬웨어 공격도 증가하고 있다.

ICT 활용이 많아지면서 여러 국가와 업체를 거쳐 만들어진 ICT 제품이 국가 전 영역에서 사용됨에 따라 개발 · 배포 · 유지 · 관리와 같은 공급망 全 단계에서 부품 및 구성요소에 보안 취약점을 내재시킬 수 있는 공급망 보안위협 또한 증가할 것으로 보인다.

2. 평가와 필요성

우리나라는 2019년에 최초의 국가 사이버안보 전략을 수립 · 발표하며 6대 전략과제를 제시한 바 있다. 같은 해 9월, 정부는 6대 전략과제를 뒷받침하기 위한 국가 사이버안보 기본계획을 발표하고, 이를 통해 18개 중점과제, 100개 세부과제를 수립하여 단계적으로 추진하였다.

기존 전략은 국가 핵심인프라 안정성 제고, 사이버공격 대응역량 고도화, 사이버안보 거버넌스 정립 등 정부의 첫 번째 전략서로서의 이정표적 의미가 있었다.

사이버안보 전략은 국가안보전략에 명시된 국가안보관과 수호하고자 하는 국가 핵심가치를 반영해야 한다.

그러나 2019년 수립된 전략에는 우리나라의 가장 큰 실제적 위협인 북한의 사이버위협에 대한 직시(直視) 등 안보전략이 추구해야 할 근본적인 목표와 그에 부합하는 공세적 사이버 방어 등 안보 중심의 정책방향이 부족하였다. 또한, 랜섬웨어 및 하이브리드 위협의 대두 등 고도화되고 있는 사이버안보 환경 변화에 대응하기 위한 글로벌 리더십 노력 역시 미흡하였다.

또한, 기존 전략은 기본 · 실행계획 상의 세부과제들이 소관부처에서 이미 수행중이거나 해당기관의 정보보안 관련 임무 중심의 내용들로 구성되는 등 기존 정보화 추진 시기의 정보보호 수준을 벗어나지 못했다는 평가를 받기도 하였다.

사이버안보 환경변화에서 살펴볼 수 있듯이, 이제는 기존의 정보화 추진 시기

기술 중심의 정보보호 관점에서 사이버공간에서 발생하는 국가안보 이슈 전반을 다루는 '사이버안보' 관점으로 발전하여 전략을 수립할 필요성이 있다. 아울러 국가안보 전반을 총괄 · 조정할 수 있는 국가안보실의 역할과 위기관리 주관기관을 명문화하고, 이를 통해 각 실무 수행체계간 역할과 책임을 정의하는 국가 사이버안보 수행체계를 정립해야 한다.

Ⅱ 비전과 목표

1. 비전

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

- 사이버공간은 정치 · 경제 · 사회 · 문화활동이 자유롭게 이루어지는 자유민주주의의 근간이다.

- 자유민주주의를 우리나라의 핵심가치로 정립하고, 사이버공간에서도 국익과 자유민주주의 가치를 수호하여 국민의 기본권을 보호한다.

- 사이버안보 정책 · 제도 · 기술개발 등을 위한 국제사회의 노력에 적극적으로 참여하여 안전하고 신뢰할 수 있는 사이버공간을 구축하기 위한 책임있는 국가행동에 앞장선다.

- 이러한 전략적 비전은 ① 공세적 사이버 방어 및 대응 ② 글로벌 리더십 확장 ③ 건실한 사이버 복원력 확보라는 세 가지 핵심 목표의 달성을 통해 구체화 될 것이다.

2. 목표

① 공세적 사이버 방어 및 대응

- 북한을 위시한 위협행위자들이 자행하는 기밀 절취, 가짜뉴스 등 허위정보 유포, 가상자산 탈취와 같은 악의적 사이버활동에 효과적으로 대응하기 위해서는 방어 역량의 보강만으로는 한계가 있다.

- 사이버위협의 수행주체와 방법이 다양화 · 복잡화 · 정교화됨에 따라 기술적 차원의 완전한 예방 · 대응은 제한된다.

→ 이에, 북한 등 위협에 대한 공세적 대응으로 패러다임을 전환하여 우리나라 사이버안보 수준을 한 단계 향상시켜야 한다.

② 글로벌 리더십 확장

- 각 국가들과의 건전한 사이버 협력관계 형성은 사이버공간에서 자유·인권·법치의 가치를 수호하고, 사이버위협에 대한 효과적인 예방 · 대응조치를 취하기 위한 필수적인 요소이다.

→ 각국의 수준과 목표에 부합하는 맞춤형 협력을 통해 사이버위협 억지력을 강화하고 사이버공간에서의 책임있는 국가행동을 위한 관련 규범의 발전 등 국제협력 및 연대 수준을 제고해 나간다.

③ 건실한 사이버 복원력 확보

- 날로 지능화되고 있는 사이버공격은 피해의 파급력이 높은 에너지 · 교통 · 통신 등의 국가 기반시설 뿐만 아니라 우리 국민들의 일상과 연관된 필수 서비스를 겨냥할 것으로 예상된다.

- 외부에 의한 해킹 · 침해 등 사이버위협 뿐만 아니라 관리미흡 · 기술적 오류 등으로 인한 중요 전산망 장애 또한 국가의 기능 마비와 사회혼란을 초래할 수 있는 안보의 영역이다.

→ 범국가적 역량을 투입하여 국가 핵심 인프라부터 국민의 디지털 일상까지 보호할 수 있도록 상시 대비태세를 마련한다.

3. 원칙

- 상기 세가지 목표를 달성하는 과정에서 우리는 아래와 같은 원칙을 준수하여야 할 것이다.

첫째,
우리는 사이버안보 활동 수행에 있어
국가의 핵심가치와 국민의 경제적 이익을 균형있게 중시할 것이다.

둘째,
정부 · 산업계 · 학계 등 모든 이해관계자가 협력하여
사이버안보의 중요성을 인식하고 위협에 공동으로 대응할 것이다.

셋째,
사이버안보 활동으로 인한 프라이버시 침해 등 우려로부터
국민의 기본권을 보호하기 위해 규범에 기반하여
정당한 목적과 적법한 수단으로 업무를 수행할 것이다.

Ⅲ 전략과제

1. 공세적 사이버 방어활동 강화

국가안보 · 국익을 위협하는 악의적 사이버활동에 대한 억지력을 확보하고, 위협행위자의 사이버공격에 대한 선제적 방어역량 강화

가. 국가안보 위해(危害) 활동에 대한 공세적 대응 강화

1) 국가안보와 국익에 반하는 사이버공격의 주체를 규명하고, 책임 귀속에 필요한 법적 · 기술적 역량을 결집하여 국가적 대응 수준을 제고한다.

2) 가상자산 해킹, 랜섬웨어, 공급망 공격 등 치밀해지는 사이버위협에 대한 대응역량을 강화하기 위해 공격 근원지 식별, 다크웹 · 가상자산 추적 대응 시스템을 고도화한다.

3) 사이버공간에서 국가안보 위협에 대한 억지전략을 수립하고, 이행지침 마련 · 참여기관간 실행 공조와 주요국과의 합동 보안권고문 발표를 통해 실질적인 억지력을 확보한다.

4) 정보기관 · 軍은 공격 근원지를 능동적으로 탐지 · 분석하여 사전징후를 포착하고, 관련 정보를 유관부처와 신속 공유하고 예상되는 공격에 대비하는 등 공세적이고 선제적으로 대응한다.

5) 과학적 증거를 바탕으로 우리나라에 대한 사이버공격의 배후세력을 규명하고 악의적 행동에 상응하는 책임을 부과하도록 한다.

나. 위협정보 수집 · 분석 기반 강화

1) 해킹조직의 행적이 담긴 국내 · 외 디지털정보에 대한 정보수사기관 및 軍의 수집 · 분석을 위해 사법통제 등 법치주의 원칙에 충실한 국내 법 · 제도적 기반을 구축한다.

2) 국가안보를 위협하는 사이버공격을 선제적으로 차단할 수 있도록 침해행위 이전부터 첩보수집 및 정찰활동을 수행하여 위협행위자에 대한 정보수사기관 · 軍의 감시 · 추적을 강화한다.

3) 주요국 정보 · 보안기관 및 국내외 사이버 인텔리전스 기업 등 유관기관과 긴밀한 협력을 통해 사이버공격 예방 · 대응에 필요한 사이버 위협정보를 교류한다.

4) 인공지능 등 신기술을 적용한 국가 차원의 사이버위협 수집 · 분석시스템을 개발 · 운영하고, 위협 요인을 사전에 발굴 · 전파하여 피해를 차단한다.

5) 국가안보와 국익을 보호할 수 있도록 다양한 전략 · 전술을 수립하고, 전력 체계와 핵심기술을 고도화한다.

다. 사이버공간상 영향력 공작 대응

1) 사이버공간에서 국론 분열과 사회·경제적 혼란 등을 유발할 수 있는 북한 및 해외發 영향력 공작과 허위정보에 대해 모니터링을 수행하고 외교·기술적 대응수단을 개발한다.

2) 관계부처·기관 및 기업 간 협업을 강화하여 가짜뉴스·여론조작 등에 대응하기 위한 정책을 수립하고 미비한 법·제도를 개선한다.

3) 자유민주주의 수호와 건전한 여론조성을 위해 악의적인 영향력 공작의 위험성을 국민에게 제대로 알리고 경각심을 제고한다.

라. 사이버범죄에 대한 예방 · 대응역량 제고

1) 랜섬웨어 유포, 가상자산 탈취 등 진화하는 사이버범죄 대응 역량 강화를 위해 수사 전문성을 강화한다.

2) 사이버범죄에 악용되는 디지털플랫폼에 대한 국민적 보안의식을 제고하고 사이버범죄 피해에 대한 신속한 지원 체계를 강구한다.

3) 개인과 기업의 피해에 대한 디지털증거를 신속하게 수집 · 분석하고, 추가피해 방지를 위한 데이터 축적을 지원한다.

2. 글로벌 사이버 공조체계 구축

국제사회와의 적극적인 협력을 통해 사이버위협 대응의 실효성을 제고하고, 글로벌 중추국가로서 안전하고 평화로운 사이버공간 구축에 기여

가. 미국을 비롯한 다양한 국가와의 사이버안보 협력 공고화

1) 사이버공간의 자유와 개방성, 안전과 평화의 가치를 공유하는 국제사회와 사이버안보 협력을 강화한다.

2) 악의적 사이버활동에 대하여 구체적 · 객관적이고 신뢰할만한 증거와 정보를 바탕으로 국제사회와의 공동대응에 참여해나간다.

3) 한미간 「전략적 사이버안보 협력 프레임워크」를 기반으로 미국과의 사이버협력을 동맹에 걸맞는 수준으로 심화하여 글로벌 사이버안보 중추국가로 도약한다.

4) 한미일간 「캠프 데이비드 정신」을 바탕으로 북한의 가상자산 탈취, IT인력 송출 등 사이버상 불법행위와 각종 제재 회피수단을 차단하고, 글로벌 사이버 위협에 공동 대응하기 위해 3국간 사이버안보 협력을 강화한다.

5) 한영간 「전략적 사이버 파트너십」을 통하여 영국과 모든 영역의 사이버 위협에 공동 대응하고 이를 위한 사전 상호지원체계를 구축하는 등 양국간 사이버

협력을 확대·강화한다.

6) 호주, 캐나다, 인도 등 인·태 지역 내 주요 협력국 및 NATO 국가들과 사이버 정책 공조를 강화하고, 사이버위협 정보와 기술의 공유를 확대하면서, 국제 사이버 협력 네트워크를 확충해 나간다.

7) 불법적인 핵·미사일 개발자금 조달 등 北 사이버위협에 대한 국제사회의 경각심을 제고하고, 이를 차단·억지하기 위한 국제 공조를 주도한다.

8) 국가안보를 위협하는 사이버범죄 대응 강화를 위하여 다자간 사이버범죄 대응 공조협약 가입을 추진하고, 국제사회의 노력에 동참한다.

나. 국제 사이버규범 논의 및 신뢰구축조치 이행 활동에 적극 참여

1) UN · NATO 등의 사이버공간에 대한 국제법의 해석과 적용 등 국제사회 논의에 주도적으로 참여하여 규범에 기반한 사이버공간의 질서형성을 촉진한다.

2) 기존 국제법과 규범의 이행에 관한 국제사회의 논의에 동참하고, 초국경 사이버위협에 효과적으로 대응하기 위한 양 · 다자 협력을 강화한다.

3) 자국 정보통신시스템이 이용된 악의적 사이버활동에 대한 영토국의 책임이 국제법적 의무라는 입장을 재확인하고 공감대를 구축한다.

4) 악의적 사이버활동에 대한 국가안보적 위협 인식과 우리의 판단 및 대응에 관한 정책과 근거를 주기적으로 공개하여 우리 사이버안보 정책의 투명성과 신뢰를 제고한다.

5) 기존의 정부간 사이버안보 정책 협의를 우리의 국격과 위상에 걸맞게 다양한 국가로 확대하여 상호간 이해와 신뢰를 증진함으로써 글로벌 사이버안보 위협을 억지하고 긴장고조를 방지한다.

6) 新기술, 데이터 이전 등 다양한 사이버안보 관련 국제표준, 규범, 통상협정 등에 우리의 국익과 안보적 고려가 반영될 수 있도록 국제사회내 영향력을 강화한다.

다. 민간 · 국제기구들과 협력 및 글로벌 역량강화 지원 확대

1) 정부와 국내외 민간기업 및 국제기구 등과 사이버위협정보 · 보안기술 및 정책 교류를 확대하고, 민간 상호간 국제협력을 장려 · 지원한다.

2) 1.5트랙 정책 협의 등 국내외 정부 및 민간 전문가 간 논의의 장을 지속적으로 추진하여 다양한 이해관계자들이 참여하는 사이버안보 정책을 수립한다.

3) 세계 각국이 사이버위협에 대응하고 안전한 사이버공간 구축에 참여할 수 있는 역량을 갖출 수 있도록 개발도상국을 대상으로 한 역량강화 지원사업을 추진한다.

4) 기술적·물적 자원 중심의 지원에서 국가 전략 · 법제 · 정책의 수립 역량까지 지원범위를 종합적으로 확장하여 지속가능한 협력관계를 구축한다.

5) 국제기구 및 주요 공여국과의 역량강화 지원사업 조율을 통하여 글로벌 사이버안보 역량의 실질적 향상을 위한 효과적 자원 배분을 도모한다.

3. 국가 핵심인프라 사이버 복원력 강화

국가 핵심인프라와 중요 시스템의 사이버 복원력을 강화하여,
모든 기업과 국민에게 필수적인 서비스의 안전성 제공

가. 주요 정보시스템 보안 강화

1) 주요 기반시설 운영 시스템의 생애주기를 포괄하는 최소 보안 요구사항을 수립 · 강화하고 기술적 지원 확대를 통해 상시 대비태세를 마련한다.

2) 정보시스템 장애 대비를 위해 범정부 통합모니터링 및 복구 체계 구축, 시스템 운영 · 유지보수 제도 정비 등 신속한 대응체계를 수립한다.

3) 국가안보를 위협하는 고도화된 사이버공격을 방어하기 위해 기반시설 제어 시스템의 위협 탐지 체계를 확대 구축한다.

4) 사이버사고의 종류 및 피해 수준을 구분할 수 있는 기준을 구체화하고, 사고 수준별 대응을 효율화할 수 있도록 관련 제도를 개선한다.

5) 스마트그리드 등 IT 기술이 접목된 기반시설에 적합한 보안기술을 개발 · 적용하여, 주요 기반시설 운영의 안정성과 효율성을 제고한다.

나. 디지털플랫폼정부 구현에 대비한 보안관리체계 재정립

1) '제로 트러스트' 보안전략을 구현할 수 있도록 신원(ID) · 시스템 · 네트워크 및 데이터의 가시성을 확보하고 전략을 적용하기 위한 단계별 추진계획을 수립 · 시행한다.

2) 비밀 · 비공개 정보 · 공개 정보 등 보호 등급에 따른 보안관리를 명확히 하고, 모든 국민에게 디지털플랫폼을 안전하게 활용하는 방법을 제공한다.

3) 사물인터넷(IoT), 클라우드 등 디지털플랫폼의 도입 · 확산을 위해 디지털 플랫폼의 안전성을 확보하고 관련 보안인증제도를 개선한다.

다. 범국가적 차원의 ICT 공급망 보안정책 및 대응체계 확립

1) 정부 ICT 제품 및 부품의 조달과정에 대한 보안성을 확보할 수 있도록 기존 보안 관련 제도 · 지침을 개정하고 신뢰할 수 있는 공급업체를 지정 · 관리할 수 있는 방안을 마련한다.

2) 소프트웨어 개발 시 보안 취약점을 최소화할 수 있도록 소프트웨어에 대한 구성정보를 표준화하고 관리체계를 수립한다.

3) ICT 공급망 보안을 위한 교육 · 훈련, 지속적 관리 및 기술지원을 할 수 있는 역량과 환경을 구축한다.

4. 新기술 경쟁우위 확보

국가 사이버안보 역량의 기반이 되는 핵심기술을 적극적으로 육성하고
안전하게 보호함으로써 국제 경쟁력 및 기술주도권 확보

가. 기반 기술의 전략산업화

1) 정부와 産 · 學 · 硏이 합동으로 사이버안보에 기반이 되는 핵심기술을 식별하고, 전략산업화 추진을 위한 세부 정책을 상시 점검 · 개선한다.

2) AI · 양자기술 등 신기술이 촉발하는 새로운 안보위협에 대응하기 위해 관련 원천기술에 대한 연구개발 예산지원을 확대하고, 사이버안보 관련 기술 · 정책 연구개발 전문 조직을 설립 · 운영한다.

3) 신기술 적용 정보보호제품에 대한 규제개선 및 국제적 홍보와 관련 기업에 대한 투자를 통해 정보보호 기업의 혁신을 촉진하고, 국제 경쟁력을 확보한다.

나. 新기술에 대한 사이버위험 관리체계 확립

1) 신기술 부상이 수반하는 사이버안보 이슈에 신속하게 대응하고 관련 보안대책을 일관되게 수립할 수 있는 보안관리 프레임워크를 마련한다.

2) 민간기업과 공공 연구기관이 개발한 사이버안보 관련 신기술에 대한 교류 · 공유 · 이전을 확대하고, 기관 · 기업에 보안컨설팅 지원을 강화한다.

3) 양자컴퓨터를 활용한 정보의 유출 등으로부터 국가기밀을 보호하기 위한 양자대응 암호체계를 구축하고, 우리 암호화 솔루션의 보급 확대를 위해 국제암호표준 개발에 적극 참여한다.

5. 업무 수행기반 강화

개인, 기업, 정부의 역할과 책임을 유기적으로 연결하여
조화를 이루고 제도화하는 범국가 차원의 통합대응 체계 확립

가. 국가 사이버위협 대응체계 정립

1) 사이버안보가 국가안보와 직결된다는 점을 인식하여 「사이버안보법」을 제정함으로써 국가 차원의 대응체계를 정립하고, 실질적이고 구체적인 사이버안보 활동의 제도적 기반을 마련한다.

2) 국가안보실 산하에 '국가사이버안보위원회'를 두어 범국가적 사이버안보 정책 관련 사항을 조정하고, 정부 전체의 사이버안보 역량과 기능이 효과적으로 발휘되도록 여건을 조성한다.

3) 사이버공격 발생시 신속하게 정부·기업의 핵심역량을 결집하기 위해 통합대응 조직을 설치, 국가차원의 합동대응 역량을 강화한다.

4) 사이버 위기관리를 위해 국가정보원을 주관기관으로 설정하여 각급기관에 위협정보 공유, 경보발령 및 사고대응 등을 총괄토록 한다.

5) 관계부처·기관 및 기업 간 협업 강화를 위하여 범국가 차원의 사이버안보 협력 플랫폼과 허브를 구축한다.

나. 소관부처별 역할과 책임 정립

1) 개별 법령에 따른 직무범위를 기준으로 소관하는 분야별 사이버안보 업무가 제대로 수행될 수 있도록 제도와 기반을 개선한다.

2) 「국가위기관리기본지침」을 비롯한 사이버안보 위기에 관한 지침 및 매뉴얼을 제 · 개정하여 유관부처·기관들이 취할 조치들의 절차와 행동방침을 구체적으로 마련한다.

3) 각급기관이 수행하는 소관 분야별 사이버안보 활동에 대한 평가를 시행하고 후속 보완조치를 마련하는 체계를 수립한다.

다. 범국가적 사이버위기 대응을 위한 민간역량 활용 확대

1) 민간 이해당사자 간 협력을 활성화하고 민간 주체의 자율적 · 능동적 참여를 촉진하는 협력적 플랫폼을 구축한다.

2) 사이버사고에 대응하는 정부와 기업 간 정보공유체계를 정비하여 취약점 정보, 사이버위협징후 등 사이버안보 관련 정보를 신속하게 상호 공유하고 대처할 수 있도록 한다.

3) 유사시 국내 사이버안보 위협 및 국제적 위기대응 활동을 지원하는 다양한 분야의 민간 전문인력을 적극적으로 활용한다.

라. 전문인력 양성 및 유지

1) 사이버안보 특성화 교육 프로그램을 확대하고 최정예 인력양성 체계를 구축하며, 공공 · 민간 분야별로 적합한 사이버 전문인력이 공급될 수 있도록 맞춤형 인력양성 프로그램을 강화한다.

2) 민간과 공공이 함께 참여하는 국가적 차원의 연합 훈련을 추진하고, 국제적인 사이버방어 훈련을 개최하는 등 세계적 수준의 최첨단 교육훈련 기반을 마련한다.

3) 국가 · 공공기관 사이버안보 업무 및 정책 활동에 민간 사이버 전문인력을 활용하기 위해 혁신적 제도와 보상체계를 마련하여 단계적으로 이행한다.

4) 민간 사이버 전문인력의 軍 복무 및 전역 후 취업 · 창업을 연계하여 유관분야 업무기회를 확대하는 등 국내 사이버 전문인력을 지속적으로 관리한다.

5) 공급망 보안 · 하이브리드 위협 등 복합적인 위험 요소들에 대한 예측 · 평가 · 대응을 위해 전문인력을 양성하고 교육 · 연구개발 등에 투자하여 근본적인 복원력을 강화한다.

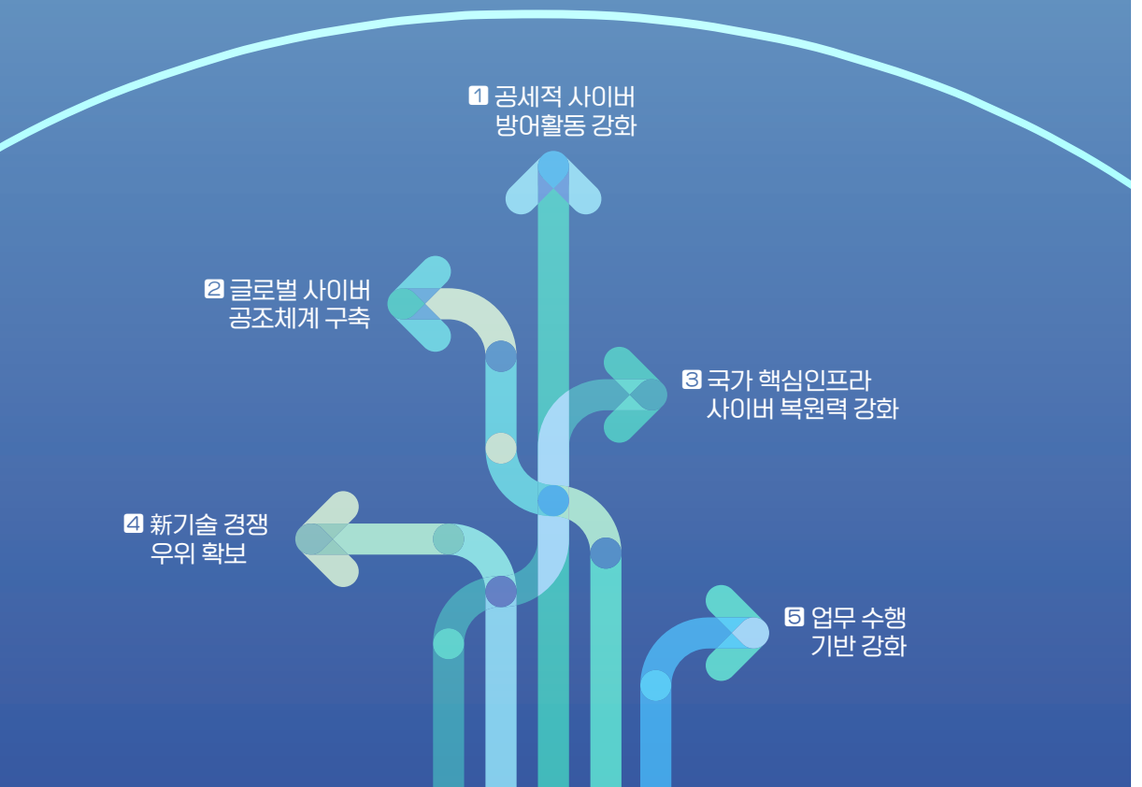
마. 대국민 인식 제고 및 실천 강화

1) 국민들이 사이버안보의 중요성과 안전수칙을 체득할 수 있도록 SNS · 대중매체 등을 활용한 국민 참여형 인식제고 캠페인을 활성화한다.

2) 국민들이 사이버안보 위협에 대한 중요성을 인식하고, 일상에서 사이버위협에 노출되지 않도록 맞춤형 인식제고 프로그램 및 콘텐츠를 개발 · 제공한다.

Ⅳ
이행방안

국가사이버안보전략은 매 5년마다 개정하는 것을 원칙으로 한다. 다만, 국가사이버안보에 중대한 영향을 미치는 대내·외적 환경변화에 따라 전략의 개정이 요구되는 경우, 국가사이버안보위원회의 심의 · 의결 등을 거쳐 개정할 수 있다.



정부는 국민, 기업, 국제사회와 협력하여 국가사이버안보전략의 비전과 목표를 달성할 수 있도록 책임을 다한다. 아울러 정부는 전략을 구체화하고 성실히 이행할 수 있도록 국가사이버안보기본계획과 국가사이버안보시행계획을 수립 · 추진한다.

정부는 전략 이행에 필요한 예산, 인력, 조직 등을 검토 · 개선하고 입법조치를 추진하며, 이를 각 부처별 중장기 업무계획에 적극적으로 반영할 수 있도록 노력한다.

아울러 각 부처는 전략목표를 달성할 수 있도록 사이버안보 관련 법규와 제도, 기본원칙을 준수해야 하며, 국가안보실은 전략과제의 이행여부 및 그에 따른 사이버안보 수준의 향상 정도를 정기적으로 점검한다.

국가 사이버안보 전략

NATIONAL CYBERSECURITY STRATEGY

발행일 2024년 2월

발행처 대통령실 국가안보실