사이버 안보

1. 사이버공간의 특성

1) 활용의 편리성 **2) 정보확산의 신속성** **3) 대상의 광범위성**
4) 통신의 쌍 방향성 5) 경비의 저렴성 6) 정보의 축적성
7) 정보의 보안유지성 **8) 정보보 안의 취약성**
9) 정보원(情報源)의 익명성(anonymity)

2. 사이버안보의 개념

1) 전자데이터의 범죄적 사용 또는 비인가 사용으로부터 보호 받는 상태 또는 이를 달성하기 위한 조치(영국 옥스포드 사전)
2) **가용성, 무결성, 인증, 기밀성, 그리고 부인방지 보장을 위한 정보를 내장하고 있는 컴퓨터, 전자통신시스템, 전자통신서비스, 유선통신 및 전자통신 등을 손상으로부터 예방, 보호 및 복원**(미국의 국가안보 대통령령)
3) 의도적이거나 의도하지 않은 위협에 저항하고 대응 하고 복구할 수 있는 사이버공간의 속성(Karl Fredrick Rausche & Valery Yaschenko)
4) **사이버공간 내에서 여러 가지 전자적 침해수단을 활용하는 것은 물론, 사이버공간 자체를 범죄의 수단으로 삼아 특정 국가의 안보를 위협 또는 위태롭게 하거나 국익을 손상시키는 모든 활동을 망라해 이에 대한 대응**

3. 사이버안보 vs. 전통적 안보 위협 비교

주요 비교 대상	사이버 안보 위협	전통적 안보 위협
안보위협의 핵심수단	정보와 사이버 무기	군사력(무기)
안보위협의 대내외 대응연계성	위협에 대한 대내외 대응의 느슨한 연계성	위협에 대한 대내외 오대응의 높은 연계성
안보위협의 예방활동의 통합성 수준	수평적 협력 체계 필요	중앙집중식 예방 체계 필요
통합방위의 핵심수단	정보와 기술(전문성)	
통합방위의 주체	대내 안보 조직(정보기관)	
통합방위의 민관 관계	바퀴형 일원화 통합 조직	

4. 한국의 사이버안보 기본계획 : 2019년 9월

1) **비전** : 자유롭고 안전한 사이버공간을 구현하여 국가 안보와 경제발전을 뒷받침하고 국제 평화에 기여

2) 목표

o 국가 주요기능의 안정적 수행 : 어떠한 사이버위협에도 지속적 운영이 가능하도록 국가 핵심 인프라의 생존성과 복원력 강화

o 사이버공격에 빈틈없는 대응 : 사이버위협을 억지하고 조기 탐지·차단하며 신속하고 능동적인 사고대응 역량 확보

o 튼튼한 사이버안보 기반 구축 : 사이버보안 기술·인력·산업이 경쟁력을 갖출 수 있는 공정하고 자율적인 생태계 조성

3) 기본원칙

o 국민 기본권과 사이버안보의 조화 : 프라이버시 등 국민의 기본권 보장과 사이버공간 보호 활동을 균형 있게 추진

o 법치주의 기반 안보활동 전개 : 정부의 사이버안보 정책과 활동은 관련 국내법과 국제법·규범을 준수하여 투명하게 추진

o 참여와 협력의 수행체계 구축 : 개인, 기업, 정부가 사이버안보 활동에 함께 참여하여 협력하며 국제사회와도 긴밀히 공조

4) 전략 과제

o 국가 핵심 인프라 안전성 제고
- 국가 정보통신망 보안 강화
- 주요 기반시설 보안환경 개선
- 차세대 보안 인프라 개발

o 사이버공격 대응역량 고도화
- 사이버공격 억지력 확보
- 대규모 공격 대비태세 강화
- 포괄적·능동적 수단 강구
- 사이버범죄 대응역량 제고

o 신뢰와 협력 기반 거버넌스 정립
- 민·관·군 협력 체계 활성화
- 범국가 정보공유체계 구축 및 활성화
- 사이버안보 법적기반 강화

o 사이버보안 산업 성장기반 구축
- 사이버보안 투자 확대
- 보안 인력·기술 경쟁력 강화
- 보안기업 성장환경 조성
- 공정경쟁 원칙 확립

o 사이버보안 문화 정착
- 사이버보안 인식 제고 및 실천 강화

- 기본권과 사이버안보의 균형

o 사이버안보 국제협력 선도

- 양·다자간 협력체계 내실화
- 국제협력 리더십 확보