민주사회를 위한 변호사모임, 민주주의법학연구회, 인권운동사랑방, 진보네트워크센터, 참여연대, 천주교인권위원회

수 신 각 언론사 사회부

발 신 **민주사회를 위한 변호사모임, 민주주의법학연구회, 인권운동사랑방, 진보네트워크센터, 참여연대, 천주교인권위원회**

(담당 : 진보네트워크센터 오병일 02-774-4551, 참여연대 이은미 02-723-5302)

제 목 [보도자료] 6개 시민단체, 국정원의 '사이버 보안' 권한 강화한 「국가 사이버안보 기본법」 제정(안) 반대 의견서 제출

날 짜 2016. 10. 10. (의견서 포함 총 12 쪽)

보 도 자 료

6개 시민단체, 국가정보원의 '사이버 보안' 권한 강화한 「국가 사이버안보 기본법」 제정(안) 반대 의견서 제출

1. 민주사회를 위한 변호사모임, 민주주의법학연구회, 인권운동사랑방, 진보네트워크센터, 참여연대, 천주교인권위원회는 오늘(10/10) 지난 9월 1일 국가정보원(이하 국정원)이 입법예고 한「국가 사이버안보 기본법」 제정(안)에 대한 반대 의견서를 국정원에 제출했다.

2. 이들 단체는「국가 사이버안보 기본법」은 기존에 의원입법으로 발의되었던 사이버테러방지 관련 법안이 정부입법으로 재추진 된 것으로 기존 사이버테러방지법과 마찬가지로, '안보'를 명분으로 '사이버 보안'에 관한 국정원의 권한을 민간으로 확대하는 것이라고 밝혔다. 이들은 국정원의 권한을 국가 안보를 넘어 민간 영역의 일상적인 사이버보안까지 확장하는 것은 국정원의 기본 직무 범위를 벗어날 뿐만 아니라 민간에 대한 국가 감시의 우려를 초래할 수 있다고 지적했다. 또한 사이버보안 위협은 천재지변, 인재, 정보유출 등 다양한 요인에 의해 발생할 수 있으나 사이버공격에 대한 보안만을 언급하고 있어 기본법이라고 하기에는 개념도 협소하고, 타 법령과의 관계도 모호하다고 지적했다

3. 입법예고 된 「국가 사이버안보 기본법」 제정(안)은 국정원이 국가사이버

안보 실무위원회를 공동 운영하고 사이버안보 기본계획을 수립, 시행하도록 함으로써 컨트롤타워로서 핵심적인 역할을 하고, ‘국가안보를 위협하는 사이버공격’에 대한 사고조사까지 진행할 수 있다. 이들 단체는 비밀정보기관인 국정원이 침해사고 조사를 명분으로 공공기관 및 민간업체의 정보통신망에 접근 할 수 있다며, 국정원에 대한 사법부나 입법부의 감독 체제가 효과적으로 작동하지 않는 현실에서 국정원에 민간 영역을 포괄하는 사이버 보안에 대한 실질적 권한을 부여하는 것은 국정원의 사이버 사찰 의혹을 부추길 것이라고 지적했다.

4. 또한 이들 단체는 대통령 훈령에 불과한 ‘국가사이버안전관리규정’에 따라 국정원이 현재 공공 영역의 정보통신망에 대한 사이버 보안을 책임지고 있는 것도 문제라고 지적하고, 사이버보안와 관련한 국정원의 기존 권한도 다른 기관으로 이양해야 한다고 주장했다. 이들은 공공이든 민간이든 각 기관/업체가 자신이 관리하고 있는 정보통신망에 대한 사이버보안을 책임지되, 국가정보통신망의 사이버보안에 대한 조율과 지원이 필요하다면, 비밀정보기관이 아니라 투명하게 감독을 받을 수 있는 별도의 정부부처에서 담당하는 것이 적절하다고 밝혔다.

5. 이들은「국가 사이버안보 기본법」제정 반대 의견을 국회 정보위원회 소속 의원들에게도 전달 할 예정이다. 끝.

▣ 별첨1. 의견서

국가 사이버안보 기본법 제정(안)에 대한 의견서

1. 국내 사이버 보안 체제의 문제점

(1) 국내 사이버 보안 체제

현재 국내에는 민간 영역의 사이버 보안을 규율하는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률', 국가기반시설의 사이버 보안을 위한 '정보통신기반보호법', 공공 영역의 사이버 보안을 규율하는 '국가사이버안전관리규정'에 따라 사이버 보안을 위한 대응 체제가 갖추어져 있음.

	관할 영역	관할 부처
정보통신망법	민간 정보통신망 일반	미래창조과학부
정보통신기반보호법	민간 기반시설	미래창조과학부
	공공 기반시설	국가정보원
국가사이버안전관리규정	공공 정보통신망	국가정보원

(2) 국내 사이버 보안의 가장 큰 문제점 - 국가정보원

국가정보원은 '국가사이버안전관리규정'에 근거하여, 국가 및 공공기관망에 대한 관리 권한과 함께, '국가사이버안전센터'를 통해 '민·관·군 사이버위협 합동대응팀'을 이끌고 있음. 또한, 정보보호시스템에 대한 인증(IT보안인증사무국), 암호 인증 등의 업무를 수행하면서, 국내 보안 업계에도 막강한 영향력을 행사하고 있음. 한편, '정보통신기반보호법'에서도 국가정보원에 주요정보통신기반시설 지정권고, 보호대책 이행여부 확인, 보호계획의 수립, 침해사고 등의 지원 권한을 부여하고 있음.

이는 사이버보안(Cyber Security)의 특성에 대한 이해 없이 국가 안보

(National Security) 관점으로 접근한 것에 기인함. 사이버 공간은 그 특성상 국경의 구분이나 민간/공공의 경계가 모호한 공간이며, 주요 정보통신망 인프라는 주로 민간에 의해 운용되고 있음. 국가 안보에 영향을 미치는 사이버 위협이 있을 수 있으나, 대다수 사이버 위협은 그 규모나 목적의 측면에서 국가 안보와는 무관함. 또한 사이버 보안에는 정보통신망의 안정성과 무결성의 유지뿐만 아니라, 개인 기기의 데이터와 개인정보의 보호 역시 포함됨. 암호 역시 과거의 군사적 의미에서 벗어나 이미 온라인 상의 이용자 보호를 위해서도 필수적인 수단이 되고 있음.

사이버 보안의 이러한 특성을 고려할 때 비밀정보기관인 국가정보원이 사이버보안와 관련된 광범한 권한을 갖는 것은 적절하지 않음.

- 이는 국가정보원법 제3조에서 규정하고 있는 국정원의 기본 직무 범위를 벗어난 것임.
- 국정원에 대한 사법부나 입법부의 감독 체제가 효과적으로 작동하지 않는 현실에서, 국정원에 민간 영역을 포괄하는 사이버 보안에 대한 실질적 권한을 부여하는 것은 국정원의 사이버 사찰 의혹을 부추길 뿐임.

주요 선진국들은 정부 주도의 사이버 보안 정책보다는 민, 관 협력적인 거버넌스 모델을 추구하고 있음. 비밀정보기관인 국가정보원이 사이버 보안 거버넌스에서 중추적인 역할을 할 경우, 원활한 민, 관 협력 거버너스가 이루어질 수 있을지 의문임. 국가정보원도 인정했다시피, 국가정보원은 2012년부터 이탈리아 업체인 해킹팀이 개발한 해킹 도구인 RCS를 이용해온 바 있음. 그 목적이 무엇이든 간에 RCS는 악성코드를 이용하여 기기의 보안을 해제하거나 소프트웨어의 취약점을 이용하는 방식으로, 이용자의 정보 인권뿐만 아니라 사이버 보안에 해를 끼치는 도구임. 이를 운용했던 국정원이 사이버 보안을 위한 핵심적인 역할을 담당한다는 것은 어불성설임.

어떠한 국가도 비밀정보기관이 국가 사이버 보안의 컨트롤타워를 담당하도록 하고 있지 않음. 예를 들어, 미국의 경우 백악관 하에 사이버 보안국(Cybersecurity Directorate)과 사이버보안조정관(Cybersecurity

Coordinator)을 두어 컨트롤타워 역할을 하고 있고, 국방부, 국무부, 국토안보부, 법무부, 상무부 등 각 부처가 관련 업무를 수행하고 있음. 예컨대, 국방과 관련된 사이버보안 이슈의 경우는 국방부가, 사이버 범죄에 관련 있다면 법무부(및 FBI)가 관장하며, 상무부의 국립표준기술원(NIST)에서 보안 기술 표준과 관련한 업무를 맡고 있음.
현행 국가 사이버보안 체제는 마치 CIA 혹은 NSA가 미국 사이버안보 정책의 실무 총괄 역할을 하는 것이나 마찬가지임.

2. 국가 사이버안보 기본법(안)의 문제점

(1) 법 제정의 필요성 없음

법 제정 필요성으로 "북한의 사이버 공격이 크게 증가하고 있으나", "공공. 민간 부문이 제각각 분리, 독립적으로 대응하고 있어 광범위한 사이버공격 위협에 효율적인 대처가 불가"하다고 함.

그러나 지금까지 정부는 수차례 사이버 안보 종합대책을 세웠으며, 그에 따라 효율적인 대처를 해 왔다고 자랑한 바 있음. 기존 정부 발표와 달리, 민관을 포함한 사이버 보안 체제에 문제가 있었다면, 지금까지 법률 미비로 발생한 문제가 무엇이었는지에 대한 구체적인 분석이 필요함.

2014.11.17 미래창조과학부 보도자료 '「국가 사이버안보 종합대책」으로 사이버 안심국가 초석 다져'

우선,「국가 사이버안보 종합대책」을 통해 범국가 차원의 사이버 위기 대응을 위한 대응 체계를 정립하였다.

○ 이를 위해 청와대를 컨트롤타워로 민(미래부).관(국정원).군(국방부) 등 분야별 책임기관 체제를 확립하여, 관계기관 간 사이버위협 정보 공유를 강화하고, 사이버공격

발생시 유기적인 협력이 가능한 확고한 대응체계를 구축하였다.

○ 특히,「사이버위협 정보분석공유시스템*(C-TAS)」을 본격 가동('14.8월) 하여, 주요 통신사 및 포털, 백신업체, 보안업체 등과 사이버위협 정보의 공유연계를 강화하고, 사이버 위협정보 분석시간을 단축 (6시간→30분)하는 등 대응 시스템을 고도화 하였다.

"민간 부문은 사이버공격 예방 및 대응을 위한 법률 미흡으로 사이버공격 징후를 실시간 탐지, 차단하거나 신속한 사고 대응에 한계" 가 있다고 하나, 이는 사실이 아님. '정보통신망 이용촉진 및 정보보호에 관한 법률', '' 정보통신기반보호법' 등 다수의 법률에서 이미 민간 영역의 사이버 보안을 규율하고 있음.

기존 법률을 통해 이미 수행되고 있음에도 불구하고, 법률안에서 중복 규정한 부분도 있음. 예를 들어, 법률안 제18조 연구개발은 이미 국가보안기술연구소를 통해 국정원이 하고 있으며, '정보보호산업의 진흥에 관한 법률'에 따라 미래창조과학부도 수행하고 있음. 제19조 산업육성, 제20조 인력양성과 관련해서는, 이미 같은 목적으로 2015년에 '정보보호산업의 진흥에 관한 법률'을 제정한 바 있음. 제21조 국제협력도 굳이 동 법안이 없더라도 이미 여러 법률에 규정되어 있고, 해당 정부 부처에서 이미 하고 있는 내용임.

민간 부문의 보안과 관련하여 오히려 경직되고 중복적인 규제 문제가 제기되고, 기존 법제의 개념 정의조차 통일되어 있지 않은 상황에서, 또 하나의 새로운 법률을 제정하는 것은 오히려 중복으로 인한 비효율과 혼란을 가중시킬 것임. 기존 법적 체제에 대한 종합적인 검토와 평가에 기반하여, 기존 법률의 재개정을 포함하여 국내 사이버 보안을 위한 체계적인 법제 정비가 필요함.

⑵ 사이버 '안보'를 명분으로 국정원의 '사이버 보안' 권한 강화

‘추진 경과’에 나타나 있듯이, 이 법률안은 기존에 발의되었던 사이버테러 방지 관련 법률안이 재추진된 것임. 기존 사이버테러방지법과 마찬가지로, 이 법률안도 ‘안보’를 명분으로 ‘사이버 보안’에 관한 국정원의 권한을 민간으로 확대하려는 것임. 그러나 ‘사이버 보안’은 ‘국가 안보’보다 훨씬 넓은 개념이며, 그 특성도 다름.

실제로 ‘사이버공격’의 개념에서부터, 2장 국가 사이버안보 수행체계와 3장 국가 사이버안보 활동 등 사이버보안 일반에 대한 대응 체계와 활동을 포괄하고 있음. 이는 법률안에서 사이버보안 컨트롤타워의 실질적 역할을 맡고 있는 국가정보원의 권한을 국가 안보를 넘어 민간 영역의 일상적인 사이버 보안까지 확장하는 것으로, 국가정보원의 기본 직무 범위를 벗어날 뿐만 아니라 민간에 대한 국가 감시의 우려를 초래할 수 있음.

반면, 법률안은 사이버보안에 대한 기본법이라고 하기에는 개념도 협소하고, 타 법령과의 관계도 모호함. 사이버보안에 대한 위협은 비단 사이버공격에 의해서만 발생하는 것은 아니며, 지진 등 천재지변, 화재 등 인재, 내부자에 의한 중요 정보의 유출 등 다양한 요인에 의해서 발생할 수 있으나, 법률안은 사이버공격으로 인한 보안만을 언급하고 있음. 또한, 사이버보안은 ‘국가의 안전과 이익’ 뿐만 아니라 이용자(국민)의 기기와 정보의 보안을 포괄하는 개념이지만, 이 법률안에서는 제외되어 있음.

해외 입법사례로 들고 있는 미국의 〈사이버안보법〉 (이는 〈사이버안보법〉이 아니라, ‘사이버보안정보공유법안’임. Cybersecurity Information Sharing Act of 2015), 일본의 〈사이버시큐리티기본법〉, 독일의 〈IT-보안법〉 역시 ‘사이버테러 방지 관련 법률’이 아니라 각 국의 ‘사이버보안’ 일반과 관련된 법률로서, 이번 법률안과는 별로 관계가 없음.

(3) 국정원의 민간 사찰과 감시 확대

법률안에서 국가정보원은 사이버보안과 관련한 컨트롤타워로서 핵심적인 역

할을 맡고 있음.

법안에서 국가정보원의 역할
- 지원기관에 사실상 국정원 영향 하에 있는 국가보안기술연구소 포함 (제2조 7호) - 국가사이버안보 실무위원회 공동 운영 (제5조 3항) - 사이버안보 기본계획 수립 · 시행 권한 (제7조 1항) - 사이버안보 실태 평가 권한 (제8조) - 국가 차원의 일원화된 신고 및 조사 체계 운영 (제12조 1항) - '국가 안보를 위협하는 사이버 공격'의 신고 접수 (제12조 2항) - '국가안보를 위협하는 사이버공격'에 대한 사고조사 (제12조 4항) - 사이버위기대책본부의 구성 관여 (제15조 2항)

국가사이버안보위원회 위원장은 국가안보실장이 맡는다고 하지만, 법률안은 국정원이 국가사이버안보실무위원회를 공동 운영하고 사이버안보 기본계획을 수립, 시행하도록 함으로써 컨트롤타워로서의 실질적인 역할을 하도록 하고 있음. 비밀정보기관이 한 국가의 사이버보안 컨트롤타워 역할을 하는 것은 적절하지 않으며, 국제적인 흐름에도 부합하지 않음.

국가사이버안보위원회는 책임기관 및 지원기관에게 사이버 보안 관련하여 '필요한 자료' 제출을 요청할 권한이 있으며, 실무위원회를 맡고 있는 국가정보원은 이 자료에 접근 가능할 것임. 국가정보원은 공공기관들(구체적인 대상은 시행령에 위임)에 대한 실태 평가를 할 수 있어, 시행령이 어떻게 제정되느냐에 따라 행정기관뿐만 아니라, 법원, 국회, 헌법재판소, 선관위 등의 사이버 보안 관련 정보와 시설에 접근할 수 있음. 비밀정보기관인 국가정보원이 국회, 법원 등의 사이버보안을 관할하는 것은 헌법기관의 독립성을 침해할 우려가 있음.

국가정보원은 공공기관 및 민간업체의 사이버 침해 사고 신고를 접수 받고 사고조사를 통해 개입할 수 있음. '국가 안보를 위협하는 사이버 공격'으로 제한한다고 하지만, '국가 안보를 위협하는 사이버 공격'의 정의를 보면, 주

요 책임기관의 정보통신망에 대한 일상적인 침해 사고에도 자의적으로 개입할 수 있는 여지를 열어놓고 있음.

제2조(정의) 3. “국가안보를 위협하는 사이버공격”이란 다음 각 목에 해당하는 행위를 말한다. 가. 대한민국의 통치권이 사실상 미치지 아니하는 한반도 내의 집단이 자행하는 사이버공격 나. 전자정부와 국가기반시설 등 국가적으로 중요한 사이버공간을 교란, 마비, 파괴하는 사이버공격 다. 국가 기밀이나 핵심 산업기술 등 국가적으로 중요한 정보를 절취, 훼손하는 사이버 공격

제2조(정의) 3호 (가)의 경우 북한을 지칭하는 것인데, 사고 조사를 통해 공격자를 밝히기 전까지 특정한 사이버 침해사고가 북한의 공격임을 어떻게 알 수 있는지 의문임. 또한, (나)와 (다)의 경우에는 책임기관으로 지정되어 있는 국가 및 공공기관, 주요 정보통신기반사업자 (나 항) 그리고 국가 핵심기술을 보유한 기업체나 연구기관, 방위산업체 및 전문연구기관 (다 항) 등의 정보통신망에 대한 사이버 공격이 모두 ‘국가 안보를 위협하는 사이버 공격’으로 자의적으로 규정될 수 있어서, 사실상 이 법률안이 책임기관으로 규정하고 있는 공공기관 및 민간업체의 정보통신망에 침해사고 조사를 명분으로 접근할 수 있음.

침해사고 조사는 일종의 수사와 유사한 과정으로 볼 수 있는데, 비밀정보기관인 국정원이 침해사고 조사를 명분으로 책임기관의 정보통신망에 관여할 수 있다면 기관이나 민간업체의 민감한 정보에 접근할 가능성이 있으며, 이를 통한 기관과 업체에 대한 감시나 통제를 하게 될 우려가 있음.

19대 국회에 발의되었던 사이버테러 관련 법안과 달리, 법률안은 포털 등 인터넷서비스 사업자들을 명시적으로 포함하고 있지는 않지만, 국가사이버안보위원회가 의결을 통해 ‘책임기관’을 지정할 수 있도록 하고 있어, 포털,

언론 등으로 법률안의 규율 대상이 확대될 가능성이 존재함.

법률안은 사고가 발생할 경우 상급 책임기관 혹은 국가정보원에 신고하도록 하고, 상급 책임기관 혹은 국가정보원이 사고 조사를 하도록 하고 있음. 그러나 크고 작은 수준의 사이버 보안 사고는 무수히 발생함을 고려할 때, 이와 같이 일률적으로 규정하는 것은 침해에 대한 대응이나 사고 조사의 효율성도 저해할 우려가 있으며, 책임 소재도 모호해질 수 있음.

국가사이버안전관리규정은 국가정보원이 '국가사이버안전센터'를 운영하도록 하고 있으며, 국가사이버안전센터는 국가사이버안전정책수립, 사이버위협 관련 정보의 수집 · 분석 · 전파, 국가정보통신망의 안전성 확인 등의 역할을 수행하도록 하고 있음. 또한, 국가사이버안전센터에 '민 · 관 · 군 합동대응반'을 설치할 수 있도록 하고 있음. 한편, 19대 국회에 발의되었던 사이버테러 관련 법안(예를 들어, 서상기 의원 발의 '국가 사이버테러 방지 등에 관한 법률안(2016. 2. 22.))은 국가사이버안전센터를 법률로 규정하고 그 권한을 민간으로 확대하며, 민 · 관 · 군 합동대응팀 설치, 운영을 규정하고 있음. 그러나 법률안에서는 국가사이버안전센터 및 민 · 관 · 군합동대응팀 설치에 대한 규정이 없는데, 테러방지법에서 시행령을 통해 테러정보통합센터, 대테러합동조사팀, 지역 테러대책협의회, 공항·항만 테러대책협의회 등 각종 테러 관련 전담조직을 구성하고 또 관계기관들을 주도하도록 한 것과 마찬가지로, 국가 사이버안보 기본법 역시 시행령을 통해 국가정보원에 사이버 보안에 대한 막강한 권한을 부여할 것이 우려됨.

3. 20대 국회에 제안하는 국내 사이버 보안 체제 개선 방안

(1) 사이버 보안을 위한 원칙 확립

유엔 및 유럽연합 등 세계 각 국은 사이버 보안을 위한 원칙으로 개방적인 인터넷의 보존, 프라이버시와 인권 존중, 공공과 민간의 협력 등을 강조하고

있음. 국내 사이버 보안 체제도 이와 같은 원칙에 기반하여 수립될 필요가 있음.

비밀정보기관인 국정원이 사이버 보안과 관련한 컨트롤 타워의 역할을 수행할 경우, 인권 보호를 위한 사회적 감독이 이루어지기 힘들며, 민간과의 원활한 협력도 불가능함.

⑵ 국정원의 사이버 보안 권한 이양과 국정원 개혁

국가정보원이 사이버보안 업무를 맡는 것에 대한 근본적인 우려는 국정원에 대한 불신에 기반하고 있음. 이는 단지 과거 국정원의 민간인 사찰과 정치 개입의 역사 때문이 아니라, 여전히 국정원에 대한 사회적인 (사법부 및 입법부의) 감독체제가 부재하기 때문임. RCS 사태와 관련해서도, 국정원이 RCS를 사용해왔음을 인정했음에도 불구하고, 실제 어떠한 목적으로 어떻게 사용해왔는지 국회가 검증하는데 실패함으로써 이러한 감독 체제가 부재하다는 것을 보여주었음. 따라서 국가정보원의 구조개혁과 사회적 감독체제를 마련하는 것이 국정원이 신뢰를 회복할 수 있는 방도임.

대통령 훈령에 불과한 ‘국가사이버안전관리규정’에 따라 국가정보원이 공공영역의 정보통신망에 대한 사이버 보안을 책임지고 있는 것은 큰 문제임. 국가 정보통신망의 사이버보안에 대한 책임, 정보보호시스템에 대한 인증, 암호 인증 등 사이버보안와 관련한 기존 국정원의 권한도 다른 기관으로 이양되어야 함. 공공이든 민간이든 각 기관/업체가 자신이 관리하고 있는 정보통신망에 대한 사이버보안을 책임지되, 국가정보통신망의 사이버보안에 대한 조율과 지원이 필요하다면, 비밀정보기관이 아니라 투명하게 감독을 받을 수 있는 별도의 정부부처에서 담당하는 것이 적절함.

⑶ 국내 사이버보안 관련 법제에 대한 종합적인 평가

국가 차원의 사이버보안과 관련한 기본법 제정을 논의하기 이전에, 기존 사

이버보안 체제에 대한 종합적인 평가에 기반하여, 사이버 보안을 위한 기본 원칙과 국가적 기본 체계에 대한 사회적 합의가 먼저 도출되어야 하며, '사이버보안' 관련 개념부터 기존 법률들도 일관성 있게 개편할 필요가 있음.

서로 다른 법률에서 개념 정의의 혼란

정보통신기반보호법은 '전자적 침해행위'를 "정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위"로 규정하고 있으나, 국가사이버안전규정 및 법률안은 '사이버공격'이라고 하고 있음. 정보통신망법은 '전자적 침해행위'나 '사이버공격'에 대한 정의규정 없이, 전자적 침해행위로 발생한 사태를 '침해사고'로 정의하고 있음.

국가사이버안전관리규정은 '사이버안전'을 "사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태"로 정의하고 있으나, 법률안은 '사이버안보'라는 용어를 사용하고 있고, "사이버공격과 사이버공격으로 인한 사이버위기로부터 사이버공간을 보호함으로써 국가의 안전과 이익을 수호하는 활동"으로 규정하고 있음.

사이버 보안은 네트워크 및 정보의 보안, 사이버 범죄, 국가 안보, 개인의 보안과 인권 등의 이슈와 상호 중첩되어 있으며, 따라서 사이버 보안과 관련된 국가적 기본 체계는 기존에 이를 담당했던 제반 정부 부처 및 민간과의 협력과 조정을 어떻게 할 것인지에 대한 정비가 필요함.