-조지훈: 안녕하세요? 저희 3시 15분부터 시작하기로 한 사이버보안과 민주적 거버넌스 관련한 트랙을 시작하도록 하겠습니다. 머인사드리겠습니다. 저는 오늘 토론에 사회를 맡게 된 민주사회를 위한 변호사모임의 조지훈 변호사라고 합니다. 반갑습니다. 한 분씩 돌아가면서 자기소개 간단히 하고 토론에 바로 들어가도록 하겠습니다.
-오병일: 저는 진보네트워크센터라는 정보인권단체고요. 대표를 맡고 있는 오병일이라고 합니다. 반갑습니다.
-권석철: 안녕하십니까? 저는 보안솔루션 제품을 개발을 하고 있는 권석철 대표입니다. 만나서 반갑습니다.
-김승주: 저는 고려대학교 김승주 교수입니다. 반갑습니다.
-신용우: 저는 국회입법조사처의 신용우 조사관이라고 합니다. 반갑습니다.
-조지훈: 저희가 오늘 주로 나눌 것은 사회적 보안 거버넌스, 어떻게 보면 시민의 눈으로 그다음에 기본권이 침해되지 않는 사이버 보안 정책이나 구조, 체계 이런 것을 어떻게 설계하고 지금의 구조에서 어떻게 바꿔나가야 하는지 이런 측면에 대해서 고민을 많이 하고 열린 토론을 진행하려 합니다.
그래서 따로 발제를 준비하거나 하지 않고 바로 여기에 계시는 패널분들의 의견 그리고 그것에 대한 다른 패널분들의 의견들을 쭉 서로 이야기를 하고 나중에는 질의응답을 하는 순간으로 진행하도록 하겠습니다.
먼저 첫 토론, 질문이라고 할까요? 제가 먼저 말씀을 드리자면 지금 국내 사이버 보안 체제에 대해서는 많은, 관에서도 정부에서도 민간은 더욱 그렇고요. 그리고 시민사회단체나 이런 쪽에서도 문제가 있고 이 문제를 어떻게 바꿔야 할 것이냐를 문제의식을 항상 가지고 있는데요. 현행, 사이버 보안 체제 관련해서 문제점이 무엇이고 어떤 문제점이 가장 중요하고 이것을 고쳐야 되는지에 대해서 패널분들의 의견을 조금 듣도록 하겠습니다. 먼저 말씀해 주실 분이 혹시 계시나요?
먼저...
-오병일: 사실 이 사물인터넷 환경이 도래하면서 여러 가지 보안 위협도 증가하고 있고 또 우리나라 같은 경우에는 북한과 여전히 적대적

관계에 있다보니까 해킹 사고가 났다고 하면 '북한에서 했나보다' 이런 얘기도 많이 나오잖아요? 사이버 보안 관련해서 언론 기사들도 많이 나고 있는데 다른 차원에서 크게 제가 생각하는, 사이버 보안 문제점 세 가지를 이야기하고 싶습니다.
첫 번째는 국내 사이버 보안 체계에 대해서 사람들에게 잘 알려져 있지 않은 것 같습니다. 그런데 아시는지 모르겠지만 국내 사이버 보안의 총괄 초정 책임은 여전히 국가적으로 갖고 있는데 정보 기관이지요. 특히 공공정보통신망으로 우리나라 사이버 보안에 정책적인 차원, 총괄조정 역할을 맡고 있고 실무적인 차원에서도 상당히 다양한 역할들을 하고 있습니다.
그런데 과연정보기관이 국내사이버보안에 어떤 전반적인 책임을 맡고 있는 것이 적절하냐는... 어떻게 우리나라에서 상당히 많이 오래 전부터 문민화가 진행됐지만 가장 뒤떨어진게 사이버 보안이. 사실 보안이라는 부분도 열어놓고 토론하고, 어떻게 하면 잘 할 수 있는지 이야기해야 하는데 되게 은밀하고 국가안보와 관련된 무서운 것 같은 느낌이 드는데 그런 이유중에 하나가 국가정보원이 이런 역할들을 담당해 왔고 비공개적인 방식으로 지금까지 사이버 보안 정책이 수립이 되었기 때문이 아닐까 해서 그렇게 되고 있고요.
두 번째는 세계 각국이 한 국가의 어떤 사이버 보안의 전반적인 방향성을 정하는 그런 사이버 보안 전략이라는 것들을 세우고 있습니다. 2010년을 전후해서 인 것 같은데유럽에서도 사이버 보안와 관련된 지침 같은 것도 나오고 각국의 사이버 보안 전략을 세우려고 하고 있고요.
우리나라에서는 지금까지 여러 가지 디도스 사고라든가 해킹 사고가 터질 때마다 종합대책이라는 것은 발표됐습니다. 그런데 우리나라의 사이버 보안 전략이 없었느냐하면 없었거든요. 우리나라의 사이버 보안 전략, 그러니까 사이버 보안 정책이 가지는 가치는 뭐냐, 어떤 원칙에 의해서 이루어지느냐, 어떤 거버넌스에 의해서 이루어지느냐하는 전략이 있어야 하는데 사이버 보안 전략이 나온 게 사실 올해가 처음입니다. 올해 정부에서 처음으로 한국의 사이버 보안 전략을 냈는데 아직까지는 상당히 간단한 수준입니다.

이런 전략이 있어야 실제적인 역할을 맡는 것은 여러 정부부처가 맡고 그럴 수 있지만 하나의 비전을 보여주는 한 국가의 전략, 또 우리나라의 가장 시급한 과정 이런 전략들도 업데이트 될 수 있겠지요. 이런 것도 논의될 수 있을 텐데 이런 게 만들어진지가 올해 처음이라는 것. 이런 부분들이 현재까지 우리나라 사이버 보안 체제에 문제가 아니었나 생각하고요.
마지막으로 제가 생각하는 세 번째는 사실 일반 사람들은 사이버 보안에 대해서는 큰 인식이 없는 것 같아요. 그렇죠? 주로 실제 어떤 네트워크나 서버를 운영하고 있는 기업이나 정부기관이나 그러한 인식을 갖고 거기한테 이야기를 하고 있지만 개인 차원에서 사이버 보안이라고 한다면 나와는 동떨어진 이야기라고 생각을 하고 있지요.
그런데 우리 모두 컴퓨터, 휴대폰을 다 가지고 있는 세상에 살고 있지요. 집에서 아이오티 기기가 들어와 있고. 사실 사이버 보안이라는 게 궁극적으로 개인의 사이버 보안이기도 하다고 생각을 합니다.
그리고 개인의 사이버 보안을 위협하는 것은 그 위협하는 주체는 굉장히 다양할 수 있습니다. 예를 들면 해커일 수도 있고, 범죄자일 수도 있고. 그런 것은 어떤 기업에 의해서 내 권리가 침해될 수도 있고 국가기관, 정부에 의해서도 내 사이버 보안이 위협받을 수 있습니다.
사실 개인 차원에서는 정부가 세우는 사이버 보안 전략이나 계획과는 또다른 차원의 사이버 보안에 대한 관점이 존재한다고 생각을 하거든요.
그래서 사실은 2013년도죠? 그때 미국에 대량감청, 인터넷 대량감청이 일어났을 때 세계 각국에서는 저희와 같은 시민단체 활동가들이 인권활동가들이 이런 교육을 어떻게 할 것인지 했어요. 그런데 모든 시민이 그러한 대상이 될 수 있고 이런 일반 시민들의 보안 교육이나 보안에 대한 관점을 어떻게 수립할 것인지 이런 부분들에 대한 고민이 필요한데 그것은 저희의 역할이, 어떻게 보면 저희와 같은 선생님 사회 역할이기도 하겠지만 그런 운동이 한국에서 부족하지 않나 생각합니다. 여기까지 말씀드리겠습니다.
-조지훈: 예, 진보네트워크 오병일 대표님께서 3가지 정도 중요한 점을 가지고 시작하셨는데요. 국가정보의 권한, 사이버 관련한 부재, 일반시

민들의 어떤 인식 이 3가지를 말씀하셨습니다. 관련해서 저는 사이버 보안하고 사이버 안보하고 약간 규범적으로는 딱 정리가 되어있지 않은 사항. 어떻게 됐든 간에 그래서 좀... 우리나라는 분단이라는 특수한 상황이 원인이기도 하지만 이 사이버 안보가 들어가면 모든 것이 해결되는 방향으로, 국정원이 모든 일을 할 수 있는 권한이 주어지는 방향으로 가는 것이 문제의 원인이라고 생각을 하는데요.
이 사이버 보안이나 안보 이 관계에 대해서도 다음 패널분들께서 이야기하실 때 생각이나 견해를 밝혀주시기 바랍니다.
다음은 활동을 하고 계시는 권석철 대표님께 먼저 여쭙겠습니다.
-권석철: 예, 지금 말씀하신 것처럼 사실 사회보안에 대해서는 우리 국가정보원이 그 부분에 대해서 알고 있고 그것에 대해서 문제점이 많은 것은 사실 입니다, 어떻게 보면.
그런데 저는 기업체고 사업체로써 바라보는 시각으로 말씀드리겠습니다.
사실 해킹을 막을 수가 없다보니까 우리는 여태까지 해킹을 막을 수 있다는 전제 하에서 보안제품을 만들고, 그것을 막을 수 있다는 생각을 갖고 있지만 사실은 현재 어느 국가도 해킹을 완벽하게 막을 수 없는 상태입니다. 아까 북한이라고 말씀하셨지만 북한이 했는지, 안 했는지 이런 것을 알 수 없는 상황까지 일어나고 있습니다. 몇 가지 정보를 보면 어느 국가에서 어떻게 했다는 것을 알 수 있지만 또다른 것을 보면 그 아이피는 어떻게 됐는지 알 수가 없다는 것이지요.
저는 이렇게 생각해 봤습니다. 제가 이 주제를 받고 나서 가장 먼저 떠오르는 것은 바로 자동차 블랙박스인데요. 이것이 있기 전까지는 오프라인 상황에서 블랙박스가 없을 때 시시비비를 가리는 언성이 높아지거나 목소리 큰 사람이 이기는 그런 시대가 있었습니다. 하지만 그것이 나오고 나서 시시비비가 한방에 해결됐지요.
지금 일어나는 것들이 모으고 그 데이터가 전화, 기록 이런 것은 생각한다면 나에 대한 ~ 프라이버시가 침해될 수 있다는 것입니다.
이렇게 문제가 되고 있는데요. 정보가 과거 정권이라든가 국가에서 볼 때는 예전에는 정보를 장악하는 것이 사실 국가가 통제하는 기반이 되었습니다. 그리고 그것을 오프라인에서 됐었지요. 그런데 지금은 모든

게 컴퓨터라든가 이런 것을 통해서 인터넷이라는 것을 통해서 하고 있기 때문에 각 국가끼리 정보를 수집하는 데에 굉장히 많은 노력을 하고 있고 그러다 보니까 거기에 역효과가 일어나지 않나 생각을 하고 있습니다. 이 문제는 사이버 보안와 사이버 안보라는 부분에 있어서 국가가 어디까지 접근할 수 있는지 그런 부분에 대해서 조금 더 허락되거나 아니면 그 부분에 대해서 조금 더 오픈되어있는 내용까지 허락을 한다, 예를 들어서 당신에 대한 접근을 해 봐서 이 부분을 확인하고 싶다는 이러한 열린 형태의 접근이 된다면 그 보다.은 일반인한테는 큰 문제가 되지 않을 것이라고 보고 있습니다. 예.
-조지훈: 직접 회사를 운영하시면서 고민이 드는 측면들을 말씀해 주셨고요.
그러면 학계에 계시는 김승주 교수님께서 의견을 말씀해 주시기 바랍니다.
-김승주: 일단 아까 얘기를 꺼내셨으니 소개부터 하자면 일단 우리가 인포메이션 시큐리티라고 하는 정보보호는, 정확한 정의가 있습니다. 정보보호는 컴퓨터 속에 들어가 있는 디지털 데이터를 보호하는 게 정보보호고 사이버 연동되어있는 것을 다 보호할 때 사이버 시크릿이라고 합니다. 예를 들어서 카톡으로 초등학생들이 왕따하지요? 사이버 불링.
이것을 정보보호의 범주 중에 들어가지않습니다. 컴퓨터 속의 데이터를 보호하는 게 아니어서. 그런데 사이버 보안 범죄 안에 들어갑니다. 예를 들어서 가짜뉴스를 퍼뜨려서 선한 영향을 미쳤다면 범죄에 들어가지않지만 여론죄를 펴서 사람의 심기를 공격했기 때문에 사이버 시크릿트 범죄가 되는 것입니다. 이게 사이버 디펜스로 들어가면 보통 조직이나 회사 이런 것을 지킬 때는 보안팀이 있어서 지키잖아요. 그런데 나라 전체를 지키려고 하면 군인이라는 한정된 조직에서 나를 지켜야 합니다.
그래서 사이버 시큐리티의 전략적 개념이 들어가야 하고 그래서 사이버는 디펜스라고 이야기합니다. 우리나라정책적 대부분을 보면 사이버 보안이라는 용어를 쓰지만 대부분의 정책은 인포메이션 씨큐리티 안에 갇혀있지요. 그래서 외국에서 보는 스콥스는 분명히 다릅니다.

그리고 사실은 사이버 안보라고 이야기를 하시는데 그 우리나라에서 사실 이야기하고 있는 것 중에 하나가 사이버 안보에 관련것은 거의 없습니다. 홈페이지 다운되고 인터넷 뭐 반나절 먹통됐다고 해서 그게 국가 안보의 안위에 영향을 미쳐서 대통령에게 보고 받아야할 안건이냐는 거죠. 아니라는 거죠. 미국에서 이야기하는 것은 무기 체제 자체가 해킹당해서 그럴 수도 있기 때문에 그런 것이고. 아니면 사이버 상에서의 선거에 영향을 미칠 수 있기 때문에 이게 이정도 가야 사이버 안보가 되면서 탄도미사일에게 보고가 가는 것입니다.
그런데 우리나라는 그런 것을 해야 됨에도 불구하고 여러 가지 언론에 미치는 것도 있고, 아니면 기술력이 미흡하다든가 여러 가지 이유로 그정도까지는 이야기가 나오지 않고 있는 것입니다.
그래서 잘 보신다면 신문에 무슨 사이버 테러가 일어났다 이런 거 보면 인터넷 마비거든요. 그게 과연 테러냐? 비행기가 떨어지기 직전까지 간다든가 선거결과가 뒤집힌다든가 이런 게 테러라고 이야기할 수 있고 용어적인 것은 대충 이렇습니다.
그리고 정보기관, 뭐 정확히는 지금 우리나라에서 보안 총괄하는 것은 명문화되어있습니다. 그것이 국가안보실입니다. 감사기관을 하는 것인데 이슈가 되었지요.
그런데 다른 나라들은 어떠냐? 다른 나라들을 보면 정보기관들이 굉장히 많은 것들을 간사를 한다든가 총괄기관이라든가 하고 있습니다. 왜냐하면 기술력, 정보력의 차이 때문인데요. 문제는 뭐냐면 우리나라정부부처에서 어떤 것을 총괄, 그러니까 저는 기술력이나 정보력을 많이 가진 기관이 뭘 하든 총괄하든 그것을 비난할 수 없다고 봅니다.
그런데 일하는 범위가 명확해질 필요는 있거든요. 예를 들면 우리나라 보통 미국의 엘에스에이가 국가공공영역을 총괄한다 이렇게 이야기하거든요. 그런데 미국에서 이것은 국가공공영역 총괄이 아닌 국가기밀에 해당하는 자료들에 대해서 보호한다든가 이럴 때 엘에스에이가 관여를 합니다.
그런데 우리나라는 인터넷을 도입하면서 보안정책을 이렇게 영역, 도메인 중심의 갖고 왔습니다. 신문 같은 것을 보시면 우리나라는 인터넷을 금융 그다음에 정부, 공공, 민간 이렇게 나누지요. 금융 영역은 금

감원이나 금융위 이런 쪽에서 하고 민간은 과학기술 이쪽으로 담당합니다.
그러면 일리가 있는 것 같은데 인터넷이라는 공간이 그렇게 영역이 나누어지지 않습니다. 어디까지가 민간, 어디까지 정부라고 선이 그어지지 않는다는 것이지요. 그래서 인터넷 상에서는 사실은 데이터의 중요도를 기준으로 해서 나누는 게 맞습니다.
그게 우리가 그냥 생각하는 중요 데이터냐, 아니면 국가기밀 데이터냐, 아니면 군 안보와 관련한 데이터냐 이런 식으로 데이터의 중요도에 따라서 나누고 그 데이터 중요도에 따라서 관할부처를 지정해 주는 것이 맞습니다. 예를 들어서 기밀 정보헤해당하는 것은 여기가 하고 뭐 이런 식으로 나눠줘야 사실은 깔끔한 정책이 가능하고 그다음에 중복적인 일이 생기지 않습니다.
예를 들면 우리나라에서 어떤 회사가 금융기관에 물건을 납품했습니다. 그런데 똑같은 제품을 정부부처에 납품하려고 하다는면 다른 보안성을 중요 심사를 받아야합니다. 똑같은 짓을 반복하는 것이지요. 그런데 미국 같은 경우에는 정부부처에 납품되는 제품이라할지라도 그것이 기밀자료가 아닌 일반자료에 적용되는 장비라면 추가 적인 보안성 심사를 받을 필요가 없습니다. 그런데 이게 만약에 군 자료가,
중요한 것이라면 심사를 받아야합니다.
그래서 저는 정보기관이 또는 국가의 어떤 기술력이나 정보를 갖고 있는 기관이 간사나 아니면 ~ 만든 것이 타당하다고 생각합니다. 하지만 다 싸잡아서 무차별적으로 관리한다고 하는 것은 문제가 있다고 보고요.
그것을 이야기하려면 데이터 중요도에 따라서 조금은 디테일한 정책을 가져가는 것이 조금은 중복되는 어떠한 업무도 없애고, 대중들이 납득할만한 정책을 펼 수 있지 않나 생각을 하고 있습니다.
-조지훈: 개념, 정보보호와 사이버 보안, 사이버 안보 이런 얘기부터 그다음에 우리나라의 문제점, 분야별로 되어있는 문제점은 관할하고 있다는 이런 의견까지 말씀을 하셨습니다.
교수님 의견을 들으면 명쾌하게 정의가 되는데요. 우리나라의 가장 큰 문제는 입법에서 이러한 규정, 이러한 어떤 학계에서 어느 정도 연구

가 되고 정리된 내용들이 입법이 되면서 전혀 다른, 각 국가 개별 부처, 사이버 보안 관련해서는 국정원인데요. 국정원의 권한 확대나 이런 여러 가지 것이 복합되면서 조금 얽히는 게 문제가 됩니다. 지금 정부 안으로 국회에 제출되어있는 국가 사이버 안보법이 있습니다. 지금까지 국가 사이버 안보법 법률이 우리나라에는 없습니다. 보안업무 처리 규정을, 국정원이 총괄적으로 할 수 있게 되어있는 문제가 있는데 지금 정부에서 입법, 정부 안으로 입법한 국가사이버안보법안에서 사이버 안보를 이렇게 규정합니다. 사이버 공간의 기능을 정상적으로 유지하거나 정보의 안정성을 유지하여 국민의 이익을 보호하는 것. 다 들어가는 거고 다 할 수 있다는 거죠, 이 개념 규정으로 본다면
그래서 국가입법조사처에서 이야기를 해 주시면 좋겠습니다.
-신용우: 사이버 안보 관련해서 말씀하신 정부안이 있고 2차적인 게 있고. 국정원이 중심이 되고 위원회 형태에서 국정원, 말씀하신 간사 역할을 하고 국가사이버안보센터를 설치했다고 했고 정부안에서는 한 발 물러서서 국정원에 주지 않겠다는 그런 식으로 되어있는 것으로 이야기하고 있습니다.
그래서 기본계획 같은 것들은 국정원이 만들고, 그러니까 소위 이제 어떤 기본법이 만들어지고 기본계획, 신행계획이 나오면 주무부서종합적으로 관리를 하는데 국정원이 하겠다고 사실상 명문화하는 상황입니다. 2016년에 발의되고 여러 가지 사정으로 논의는 전혀 되지 않고 20대 국회에서는 임기 만료로 폐기될 것으로 보입니다. 지금부터 논의를 해서 21대 국회 초반에 사실은 이렇게 왕성하게 활동하는 시기에 재점화될 것 같고 이 논의가 지금부터 이어나가면 좋을 것 같고요.
그러니까 아까 교수님께서 말씀을 하셨지만 전체적인 체계는 이미, 매년 나오는 것도 있고 이번에 나오는 사이버안보전략에서도 전체 컨트롤타워는 청와대 국가안보실이 하고 공공기관, 군 이런 식으로 해서 공공기관은 국정원, 민간은 ○○, ○○는 군 이런 식으로 역할이 나누어 져 있고요.
언뜻 적절하게 분산이 된 것처럼 보이기는 하지만 지금 재기되는 것은 청와대가 결국 뭔가를 할 수 있느냐, 내가 정말로 그 역할을 하면 국정원이든 어디든 정보를 받아서, 자체적으로 어떤 내용을 이해하고 그

다음에 어느 정도 파악을 해서 조율할 수 있는 실질적인 능력을 갖기 위해서는 조직이 필요하다. 그러면 청와대에 어떤 큰 조직을 두기 어렵다고 한다면 별도의 기관을 둘 때 그것을 국정원, 국정원이 그 역할을 맡는지 여부에 대해서는 논란이 있고 그것을 만약에 문제가 있다고 한다면 일각에서 제의된 사이버안전청 이런 식으로 두자는 문제가 제기되어서 여기에서 옳다, 아니다 이런 것을 말씀드리기 어렵지만 거버넌스 형태에 대해서는 펼쳐놓고 장단점을 논의할 시기가 되었다고 생각합니다.
해외에서도 여러 가지가 존재하는데 대체적으로 컨트롤타워를 두고서 2010년 초반에 테러가 많이 발생하면서 유럽 각국 중심에서 사이버안보를 강화하는 추세가 되어있고 정보기관이 아니더라도 특정기관에 힘을 실어서 컨트롤타워을 주관하는 형태로 보입니다.
그리고 아까 말씀을 주셨지만 국가 사이버 안전 규정이라고 해서 정부 안에서만 하는 것이기 때문에 훈련으로도 가능하다고 하지만 전체 컨트롤, 말씀하신 대로 구분하기가 어려운 상황에서 조차 적인 컨트롤타워는 필요하고 법률에서 규정을 해서 전체, 또 이게 정부만이 아니고 국회 사법 이런 영역도 정부에서 관리가 안 되는 영역이 있어서 필요하다.
법률에는 의미가 없지만 어떤 의미 냐면 정부 안에서만 하는 게 아닌 위원회 형태로 해서 의사결정을 조금 더 민주적으로 할 수 있고 그리고 국회든 어떤 외부에서는 견제가 가능하다는 그런 점들이 장점이라는 생각이 듭니다.
20대 국회에 계류를 중이기는 하지만 법적인 체계를 갖추는 게 필요하다고 생각하고 가까운 일본은 2015년에 사이버 시큐리티라고 제정을 했습니다.
그런 법적인 체계를 정비할 필요가 있다고 생각이 들고 한 가지 말씀드리면 사이버 보안 관련한 용어에 대해서도 논란이 많은데그래서 일본은 사이버 시큐리티로 해 놓은 게 아닐지 추측되고요. 영어로는 그렇지요.
제가 이해하기로는 국가차원의 재점에서는 사이버를 안보, 기업이나 개인 차원에서는 사이버 보안 이렇게 하는 경향이 있는 것 같고 김승

주 교수님 말씀처럼 정보보호라는 형태로 해서 협의되는 상황입니다. 새로운 법에서 사이버 안보가 되어있는데 ~ 거부감을 줄일 수 있다고 생각하는데 논의가 필요하고요.
그리고 법 이야기를 드렸는데 우리나라는 정보통신기반보호법이 있습니다. 그래서 이게 어떤 금융권이라든가, 통신 이런 것이 포함되고 몇 백 개 정도의 기관, 시설을 정해서 주요 시설로 지정하고 별도 관리를 하게 되어있습니다. 일단 국정원이 같이 참여하고 두 부처가 같이 참여하는 것으로 되어있고요.
아까 김승주 교수님 말씀처럼 사이버 안보, 안전, 보안에서 단순히 일률적으로 관리하기가 어렵다면 그런 식으로 정보통신기반보호법이 확장을 해서 우선적으로 관리되어야 할 부분을 법으로 규율하고 그 외의 것들에 대해서 차등을 두어서 관리의 정도를 레벨화시키는 것도 필요할 것 같습니다.
그리고 사실은 각국에서 이 보안, 사이버 보안을 강화하는 데에 있어서 민간과 공공의 정보교류를 중요하게 생각하고 있습니다. 신속하게 해킹을 파악해서 차단하는 게 중요하기 때문에 미국 같은 경우에는 2015년도에 사이버 안보법이 묶어서 그렇게 부르는데 연관정부간의 정보공유를 강화했고 다만 여기에서 개인피씨 정보 식별화라든지, 원칙적으로 명시를 했기 때문에 사이버 보안적인 부분만 프라이버시 부분을 균형을 도모했다고 이야기를 하고 있는데 저희가 이 법을 계속 만들어갈 때도 이런 부분에 있어서 충분히 개인정보, 프라이버시가 보호되는지, 그것을 이의제기할 수 있는 그런 게 보장되는지 그런 것을 볼 필요가 있는 것 같습니다. 여기까지 마치겠습니다.
-오병일: 그를 정의에 대한 이야기가 나왔는데요. 학술적인 의미에서의 정의는 김승주 교수님 말씀과 동일하고요. 몇분들은 말씀하시지만 명확히 제가 말씀드리고 싶은 것은 학술적인 정의, 그런데 실제로 우리나라 법에서 말씀드레는 것은 김 교수님 말씀처럼 전반적인 내용을 다루고 있다기 보다는 외부적인 공격 내용 중심으로 하고 있어요. 정보보안을 위협하는 것은 꼭 해킹은 아니잖아요. 내부자의 어떤 악의 뭐 이런 것에서 정보보안의 문제가 발생할 수도 있고 여기에서 정전, 지진 이런 천재지변에 의해서도 보안이 발생할 수 있는.

정보보안이든 사이버 보안이든 공격에 의한, 외부적 공격에 의한 방어만을 의미 하는 게 아닌데 우리나라는 그쪽에 너무 포커스를 맞춘다는 것 하나하고.
사이버 보안은 넓은 영역인데 정보보안도 연관이 되어 있고 어떤 측면에서는 개인정보 보호라는 측면에서 연관이 있고요. 그리고 사이버 보안와 사이버 안보를 말씀하셨는데 저는 사이버, 사실 사이버 보안와 사이버 안보를 그 선을 그을 수 없다고 생각합니다.
사이버 안보가 따로 있다고 생각하지 않는데 일부 사이버 보안 사고가 안보적인 문제로 이어질 수 있지요. 예를 들면 꼭 테러가 아니더라도 국가기간 시설에 여러 가지 보안사고가 났다, 이런 것은 경제에 큰 충격을 줄 수도 있고 그러한 맥락에서 안보적인 문제까지 발생을 할 수도 있는데 이 문제가 뭐냐면 사이버 안보라는, 사실 사이버 안보법에서는 사이버 보안와 관련한 내용이 포함되어있는데 그것을 사이버 안보라고 하는 순간 안보라는 관점에서 이 문제를 바라보게 되는 것이지요.
사이버 안보라는 말을 쓸지 사이버 보안이라는 말을 쓸 것인지 아니면 사이버 안전이라는 말을 쓸것인지. 국가규정에서 사이버 안전이라고 하거든요. 실제이런 법에서의 정의에 들어가도 어떤 데는 치매사고, 어떤 덴사이버 이렇게 해서 개념정의가 필요하다는 것이고요.
국가안보실이 컨트롤타워역할을 하고 있다고 들었는데요. 그런데 문제는 법적 근거가 없어요, 국가에 대해서는. 국가사이버안전관리규정에서는 사이버 정책에 총괄적으로 한다는. 그리고 국가 사이버 안보법, 국정원이 관리하는 법인데 여기에서 사이버 국가안보실를 컨트롤타워로 두고 있고요. 저는 국가안보실에서 일하시는 분들, 국가정보원실에 파견되는 부분들이 있어요. 실무적인 부분에 대해서 기본적인 방향성 이런 것을 합니다. 그리고 위원회에서는 어느 정도 도장을 찍는, 물론 정치적 결정은 중요하기는 하지요. 그런 것을 무시하는 게 아닌데 일상적인 것을 국정원이 하는 게 바람직한지에 대한 부분을 말씀드린 거였고요.
하나 제가 정정하고 싶은 게 국가사이버보안센터에서 국가사이버안보법에는 그 내용이 없습니다. 그런데 이게 후퇴한 게 아닌 사실은 뺐다

고 생각을 합니다. 논쟁이 될까 봐 일부러 뺀 것이다, 하지만 법의 근거 없이 여전히 그 기구는 있고 그 법에 따른 법에는 없지만 둘 것이라고 생각합니다.
-조지훈: 개념부터 국정원의 역할 그다음에 하나의 발의된 법률명 문제까지 말씀을 하셨습니다. 시민사회단체입장이기도 하고 법률가 단체입장이기도 한데 주로 보는 것이 통제입니다. 국가권력기관에 대한 민주적 통제 이게 얼마나 되느냐에 따라서 그 민주주의 사회가 어느 정도 성숙하냐, 실질적인 민주주의가 구축되어있느냐 이것이 논의될 수 있는데요.
저희는 국가정보원이, 그러니까 정보기관이 역할을 하는 게 문제가 아닌 정보기관은 비밀 기관이 본성이거든요. 국가의 비밀기관으로써의 정보기관에 유치해서 많은 권한을 행사하다보니까 실제로 국회통제가 거의 안 됩니다. 국회정보위원회에서 오면 실제국정원 관련 서류, 보통 다른 부처는 예결산서 이런 것을 자료를 입수해서 분석하고 이야기할 수 있습니다. 그런데 국정원은 일단 기밀이라는 이유만으로 국가안보 기밀이라는 이유로 국회의원도 국정원이나 국회에 있는 이상한 방, 그러니까 방에 들어가서 그냥 보고만 옵니다. 메모할 수도 없어요. 그래서 저는 국정원이 이렇게 통제를 할 수 없는 구조에 있기 때문에 국정원이 사이버 안보나 영역에서 과도한 역할을 하는 게 우리 사회에서 너무 심각한, 민주주의 측면에서도 투명성에서도 심각하다는 문제의식을 가지고 있습니다.
혹시 관련해서 국정원 역할 관련해서 의견이 있으시면 말씀해주시면 감사하겠습니다.
-권석철: 1-2년 정도 된 것 같은데사이버 안보 기본법인가요? 정부에서 제안한 그 내용에 대해서 새 정부에서 이야기가 나온 것 같고요. 그것에 대해서 검토를 한 적이 있었는데 이야기가 나온 게 법 이전에 이미 국가정보원이 모든 것을 맡아 해왔어서 아무런 어떤 그런 게 없었어요.
그런데 국가정보원에서 민간사찰 이런 문제가 나오면서 커졌죠. 이런 게 암암리에 일어났을 때 이런 것은 민간에 또다른 피해가 올 수 있다. 그리고 우리를 왜 감청해야 하는지 부분이 커지면서 기본법 자체

가 추진하는 데에 어려움이 있었습니다.
그런데 사실 어느 나라도 국가기관이 많은 것들을 통제한다기 보다는 정보를 수집하고 그런 것들을 하는 것은 많은 국가가 사이버 시큐리티를 하고 있지요. 저는 깊게 들어가 보겠습니다.
과연국가정보원이 이미 그전에도 국방부, 민간업체들을 불러서 같이 협의체를 구성하고 그 협의체를 구성한 정보들을 공유했느냐? 사실 그동안 못했을 거거든요. 그러니까 데이터를 모집해서 수집하면 어떻게 쓰이는지 이런 공표는 거의 안 합니다.
사실 해킹 사고가 나면 그 민간업체 역할이 큽니다. 그 정보를 가지고 분석된 자료를 수집하게 되지요. 그러면 그 각 부처마다 배부가 되거나 이래야 하는데 가공된 정보만 밑으로 내려온다는 거죠. 다시 말씀드리면 어디가 어디를 해킹해서 북한이 해킹을 했다고 민간에서 찾아서 올려주면 그것이 가공이 되어서 북한이 한 거다! 이렇게 끝납니다.
그러니까 밑에서는 통제, 어떤 자료를 전달하는 역할만 하는 것이고 그 정보가 앞으로 어떻게 쓰이고 어떻게 쓰이는지 논의 자체가 없습니다. 그러다 보니까 사실은 기관들도 비협조적이고 통제를 하기 위한 어떠한 정보 활용도만 늘어날 뿐 많은 기관들, 다시 말하면 민간이라든가 금융이라든가 국가기관, 각 부처마다 갖고 있는 센터들 이런 정보가 같이 공유가 되면서 자신들이 원하고 있는 정보들로 다시 재구성이 되거나 만들어져서, 가공이 되어서 사용되어야 하는데 현재 그렇지 못하다는 것이지요.
그것이 가장 큰 문제고 두 번째 문제가 뭐냐면 일본에 일어난 홍콩인데요. 홍콩 문제도 아실 것입니다. 원인은 그거잖습니까? 결국에는 본국으로 범죄자를 송환할 수 있다는. 그런데 내가 범죄자가 아니어도 본국에서 언제든지 송환할 수 있는 위협에 대해서 두려움이 있다보니까 시위에 나오는 것이지요. 지금 그 당시안보기본법인지 그것을 보면 해킹사고가 나면 어떤 정보도 국가가 볼 수 있다는 되어있다는 것이지요. 해킹사고가 나거나 어떤 상황일 때 요구하면 그 밑에 장, 기관, 통신 이런 곳에서 무조건 그 자요를 제공하게 되어있습니다. 그러다 보니까 그 제공된 자료에 의해서 그때 만약에 다른 의도를 가지고 그것을 활용하게 된다면 감청이라든가 이런 자료로 활용될 수 있다는 게

그런 내용이 있다보니 민간사회에서 굉장히 걱정을 하는 게 아닌값 싶습니다.
오늘도, 어제도 굉장히 많은 정보들이 나오고 있습니다. 실제로 악성코드가 나오는 것은 북한에서 나오는 게 많고 고려대학교도 마찬가지겠지만 저희의도 그런 정보를 수집하고 있습니다. 그런데 북한에 대한 사이버 위협이라든가 그런 것에 대해서 정상회담 이런 분위기때문인지 이런 이야기들 자체가 터부시 되어있습니다. 말하기도 힘들고 외교적인 문제가 될 수도 있어서 사이버 문제를 하고 있는 입장에서 뻔히 알고 있고, 확인해야 되는 입장에서 못하고 있다는 게 많다는 거죠.
그런데 그런 것들에 대해서 현재 국가의 역할이 사실 많이 부족합니다. 이번에 ㅇㅇ이 들어왔습니다. 별거 아닌 것 같지만 굉장히 위험한 거거든요. 한쪽에서는 준비를 하고 또 한쪽에서는 그것에 대해서 남북한 화해 분위기로 가야 되는데 한쪽에서는 여러 가지 여론이라든가 밀리고 있습니다.
마지막으로 말씀을 드리자면 안보와 사이버 보안과의 차이는 사실 없다고 봅니다. 다만 모아지는 이 데이터, 국가가 이것을 활용할 때 이 활용을 잘못한다면 안 되니까 그것에 대한 감시제도 그런 것들을 통해서 그 부분에 대해서 조정을 한다면 이런 문제들은 오히려 투명해지지 않을까 싶습니다.
-김승주: 계속 이야기할까요?
앞부분에 이야기했듯이 분명히 사이버 시큐리티 영역에서 정보기관이 담당해야 할 부분은 분명히 있습니다. 그것을 부인할 수는 없고요. 왜냐하면 그만한 인력과 기술력을 갖고 있기 때문에 그렇습니다. 정보도 가지고 있고요. 미국 엘에스에이에서도 담당하는 영역이 있습니다. 여러 가지를 했다가 ㅇㅇ에 의해서 프리즘 프로젝트가 폭로되어서 과도하게 정보를 수집한다는 논란이 있었지요. 엘에으에이를 폐지시킨다고 되는 게 아닌 엔에스에이가 할 수 있는 이야기를 했지 폐지 이야기를 하지 않았습니다. 저는 정보기관이 할 일은 있다고 생각하고 그런데 우리나라의 문제는 사이버 안보라는 용어가 명확하게 정의되어있지 않다는 데에 문제가 있습니다.
그것의 중심적인 요인이 뭐냐면 우리가 보통 안보다 뭐다라고 한다면

지킬 자신이 무엇인지, 내가 뭘 지키는지 이런 게 이루어져서 안보에 관한 거다, 아니다 할 수 있거든요.
예를 들면 국가정보원 법이 있습니다. 국가정보원 법에 관련해서 직무라고 해서 각호의 직무를 수행한다고 되어있습니다. 그래서 1항을 보면 대정부정보, 방첩, 대테러 및 국제범죄조직 관련한 정보의 수집 작성, 배포 이게 1항이고 2항은 국가기밀에 속하는 문서, 자재, 시설 및 지역에 대한 보안업무. 구체적이지요. 그런데 이게 사이버로 넘어오면 이정도 디테일한 용어정의가 없습니다. 왜 그러지 못하냐 하면 이런 게 되려면 보통 해킹이라고 하는 것은 기본적으로 데이터를 훔쳐가는 거잖아요? 이 데이터에 대한 분류가 있어야 됩니다. 그래서 전자 데이터 중에 이것은 국가에 어떤 큰 영향을 미칠 수 있는 기밀 데이터에 해당되고 이것은 어느 정도 되고 분류가 되어야 하거든요.
그런데 우리나라는 전자데이터에 대한 분류체계가 없습니다. 그래서 사이버 안보를 구체적으로 정의할 수 없지요. 그래서 애매모호하게 하다보니까 여러 시민단체에서는 이렇게 확대해석이 가능하다고 이런 문제가 생기고 그러면서 국정원은 빼버립시다 이렇게 이야기가 가버리거든요.
저는 그것은 너무 과도 한 것 같고, 분명히 정보기관이 할 역할은 있는데 어떻게 명확하게 규정해야 하는지 이게 본질이라고 보고요. 그것을 명확하게 정해줄 수 있는 방법에 대해서 논의해야 한다고 생각합니다.
그리고 아까 정보공유문제가 잠깐 나온 것 같은데우리가 여러 가지 법들을 보면 물론 사이버 공간에서 그런 게 있습니다. 민간 컴퓨터가 정부시설을 공격하는 데에 악용되기도 하고 역으로 악용되기도 하거든요.
땅덩어리라는 게 명확하게 구분되지 않는 것도 있습니다. 그러다 보니까 사이버 쪽만 나오면 지키는 쪽에서 넓게 해석하고 싶고 대상이 되는 쪽은 좁게 해석하고 싶고 그래서 나온 것중에 하나가 정보 공유라는 것입니다. 민간에서 발생할 수 있는 해킹 위협정보, 공공기관에서 발생할 수 있는 해킹 위협정보를 공유합시다 이런 것인데요. 다른 나라에서도 이렇게 합니다. 왜냐하면 인터넷에서는 경계가 존재하지 회

의기 때문에.
그런데 많은 분들의 위에가 국가정보원은 정보를 수집하는 데에 목적이 있는데 그들이 가지고 있는 정보를 민간에도 공유할지. 기술적으로는 공유합니다. 예를 들어서 북한 관련, 해킹 관련해서 저희 학생들이 이 해킹 보아에서는 탑이 있는데 거기에서 두어번 발표를 했었는데 어떤 정보는 저희가 얻어낸 것이 있고 한데 저것은 정보를 공유하지 않는다고 보면 잘못된 것 같고 그 정보가 공유되는 양이 동등한지 그 부분은 따져볼 필요가 있습니다. 50만큼 줬으면 상대방도 50만큼 받아야 하지요.
그런데 정부, 민간기관이라는 것은 힘의 균형이 우리의 진 조직이 아니어서 나는 70 줬는데 상대방이 20을 줄 수도 있지요. 그래서 미국은 어떻게 하냐면 정부영역에 공유하는 총괄센터가 있고 민간영역에 서로 공유하는 총괄센터가 있고 그러면 대등한 힘을 갖습니다. 그러면 둘이 정보를 공유합니다. 힘의 균형을 맞춰를 주는 것이지요.
그래서 저는 정보공유를 안 하니까 하면 안 된다기 보다는 힘의 균형을 맞춰야 한다는 쪽으로 가야 발전적인 논의를 할 수 있지 않을까 싶습니다.
-신용우: 앞에서 좋은 말씀을 주셔서 제가 많이 첨언드릴 것은 아니겠지만 말씀하신대로 국정원의 역할에 대해서 우려와 순기능에 대한 두 가지 측면이 있는데 국정원의 전체를 담당하기 보다는 어떤 일원으로서, 그 영역을 명확하게 직무를 명시한 다음에 그 영역에서 한다고 한다면 그 공존이 가능하지 않을까 생각하고요.
그다음에 미국에 말씀드린 사례가 나왔었지만 행정부 견제 ㅇㅇ가 포함되어있습니다. 말씀하신는 대로 정보위원회에서 실질적으로 그게 이루어지냐는 논란이 있지만 법에 어떠한 정보공유의 범위, 절차를 명시한다면 밀실식으로 이렇게 넘어가지 않을 수 있는 어떠한 기회가 제공되지 않을까 싶습니다.
그리고 마이크 든 김에 말씀을 드리면 아까 말씀을 해 주신 외부의 위협뿐만 아니라내부자 소행, 정전 이런 것도 고려하는 사이버 안보 체계, 개념정의가 필요하다고 하셨는데 거기에 대한 문제제기가 있어왔고 사실 화웨이, 이게 전국적으로 내부에 백도어를 심어서 정보를 빼

내는 게 아니냐는 우려가 있던 상황에서 법상에서 결국에는 그런 행위까지 잡아낼 수 있는지. 그러니까 모호한 부분으로 보이거든요. 그런 부분도 이루어져야 할 것이라고 생각합니다. 감사합니다.
-오병일: 제 생각에는 접점을 찾아갈 수도 있을 것 같은데요. 사실 아까 제가 국정원 비판을 했었지만 국정원, 정보위반은 사이버 보안과 관련해서 개입하면 안 된다, 손을 떼야 한다 이렇게 말씀드리는 게 아닙니다.
어떻게 보면 국정원, 정보기관의 역할은 군 정보기관도 있고 국정원만 있는 게 아닙니다. 경찰 관련해서도 있고. 그래서 이 역할을 명확하게 구분하고 그 역할에 맞는 그 역할을 하면 됩니다, 투명하게 하면 되고. 그런데 디테일하게 들어가면 그 역할이 뭐냐는 그렇게 될 수도 있겠지요.
그리고 사이버 보안은 폭넓다고 말씀드렸지만 해외에서도 어떻게 보면 비슷한 유사영역이 많습니다.
예를 들어서 국방영역의 사이버 보안, 사이버 전까지 포함한 그러면 사이버 사령부 같은 게 있습니다. 그렇죠?
그리고 사이버 범죄와 관련한 것은 법무부나 경찰 이런 곳에서 담당합니다, 그렇지요? 그리고 사이버 보안이 단순히 국내적 문제가 아닌 국제적 문제이기 때문에 국제적 협력 관련해서는 외교부가 담당합니다. 어느 나라나, 국가 기반시설을 지정하고 그 시설의 보호를 되게 중요하게 생각한다, 물론 모든 영역에서 사이버 보안은 중요하지만 국가시설은 별도로 목록을 만들고 보호기준도 만들고 표준도 만들고 감독도 하고 이런 역할을 하는데 미국은 국토안보부 이런 식으로 우리나라로 치면 행정안전부 같은 역할을 하거든요.
우리나라 전자정부의 ○○ 행정안전부죠. 통신보호법에 따르면 민간은 ○○ 공공영역의 기반시설은 국정원이 맡고 있거든요. 저는 정보기관이 해야 할 역할이 있다고 생각하는데 이게 과도 하게 정보기관이 맡고 있다는 거에 문제의식을 니낍니다.
공공영역의 기본적인 사이버 보안은 행정안전부든 일반적인, 그러니까 사실 일반행정부는 국회의 감독을 맡지 않습니까? 국회의 감독을 받을 수 있는 일반적인 행정기관이 일상적인 차원에서의 사이버 보안에 대

한 업무를 맡고 국가 사이버 보안 센터가 여러 가지 사고가 발생했을 때 긴급하게 지원한다든가 이런 역할들도 현재 키사도 그런 역할을 하지만 공공영역에서 기관이 필요하다면 그런 역할들도 굳이 국정원에서 하의 기관이 아닌 별도의 행정기관에서 그러한 역할들도 맡을 수 있지 않느냐는.
그리고 국가 기밀 같은 경우에는 기밀의 분류는 당연히필요하지요. 우리나라도 기밀분류를 하고 있지 않습니까? 그런데 그것도 사실 그 분류에 따라서 각 기밀을 관리하고 하는 각 행정부처, 공공기관의 역할이고 그 기준을 만드는 것은 별도의 행정기관에서 할 수 있다고 생각을 하거든요.
외국 같은 경우에는 인포메이션 어슈얼언스라고 말하기도 하는데 그런 게 필요하다는 것이지요.
저는 정보기관의 역할이 말그대로 정보기관의 역할이라고 생각합니다. 특히 우리나라 같은 경우에는 국가정보원의 것도 논의되는데 현재는 국내 수집까지 하고 있습니다. 국가정보원이 해외수집전문기관으로 전문화된다는 전제 하에 해외 정부에 사이버 위협 정부도 있지 않겠습니까? 그런 정보들을 갖고 필요한만큼 국내에 각 해당 기관에 공유하고 하는 그런 역할들을 국정원이 할 수 있다고 생각은 해요. 그러기 위해서는 아까 말씀드린 것처럼 일단 국정원이 개혁되어야 하고 두 번째는 해외정보기관으로써 사이버 보안와 관련된 역할이 무엇이냐는 그런 게 정리가 잘 되었으면 좋겠다는 것입니다.
전반적인 사이버 보안 전략의 하나로 갈 필요가 있지 않느냐는 생각을 합니다.
-권석철: 저도 공감을 합니다. 공감하고 그 부분에 대해서 정확히 말씀을 드리고 싶었습니다.
사실 김 교수님 말씀처럼 우리나라에서 이 일화를 말씀드리자면 국정원에서 이 법에 대해서 우리가 양보를 하고 이 부분에 대해서 그러면 우리가 이것을 다른 부처가 하거나 다른 부서가 맡으면 좋겠다고 의견을 낸 적이 있었습니다. 그런데 ○○○에서도 전부 다 부정을 하셨었어요. 그만큼 그동안에 쉽지 않았던 정부에 대해서 그 부분을 맞출 수 있는 자신감이 있었지요. 그동안 국가정보원이 그만큼의 노하우 그런

것을 갖고 있습니다. 만약에 국정원이 이것을 탁 놓으면 다른 부서도 어떻게 할 수 있는 게 만만치 않다는 게 현실입니다.
정보를 모니터링하고 그런 정보를 수집하고 그런데 방어를 하는 팀이거든요, 어떻게 보면. 각 정보를 민간이라든가 공공기관에 어떤 사고가, 사이버 사고가 났을 때 대응을 한단 말입니다. 문제는 어떤 사고가 나면 그 사건에 대해서 사실로 밝히는 것보다는 숨기는 것도 많다는 거예요. 그것이 뭐냐면 우리나라는 이 사고가 났을 때 이 부분에 대한 책임추궁이 심합니다. 국가가 어떤 역할을 맡아서 그런 역할을 하고 있는데 그것이 뚫렸다? 그러면 그 부분에 대해서 인정하고 대응해야 되는데 일단 현재 어떤 상황이냐면 아무 일이 없는 것처럼 이야기를 하는 거예요. 그런 부분들이 민간에서는 답답해 하는 부분들이 많이 있습니다. 그러니까 정확한 정보, 정확한 분석을 통해서 이것은 책임추궁에 대한 문제는 나중에 하더라도 이 문제는 문제를 막을 수 없으니 진실을 밝히는 게 중요한데 그런 것이지요.
여러 가지 사건들, 우리가 이야기하는 가벼운 사건들 아니면 다운 됐다든지 그냥 사고난 것처럼 보이지만 사이버에 대한 문제들도 분명히 있단 말입니다. 그런 부분에 대해서 사이버 전문가들의 의견에 대해서 그동안 좀 방관하거나 등한시 했던 것 같습니다.
저희는 그래서 국가정보원이 어떤 역할을 해야 하고 그 많은 정보 중에서 국가정보원이 원하는 정보가 있을 테니 국정원이 원하는 정보만 그 안에서 취득을 하고 나머지 정보들을 가지고 다른 기관들, 원하는 정보들로 취득하는 공유센터에 대해서 국정원이 아닌 다른 기관들이 맡아서 투명한 공간, 투명하게 그 부분에서 협력관계를 가져간다면 이런 문제들은 조금 더 가벼워지지 않을까, 그렇게 보고 있습니다.
-김승주: 계속 돌아가면서 이야기하네요. (웃음)
-조지훈: 순서가 그렇게 되네요.
-김승주: 일단 아까 그 말씀을 해 주셨잖아요? 권 대표님께서 다른 부처에게 주고 싶어 하는데 실력이 없더라, 저는 백 퍼센트 동감합니다. 실제로 맡으라고 해도 안 하려고 합니다. 왜냐하면 그동안 굉장히 타 기관에 의존을 해 왔고 그렇기 때문에.
아까 국가안보실 이야기가 나왔지만 국가안보실은 컨트롤타워입니다.

컨트롤타워고 국가안보실에 이 사이버를 담당하는 수장은 국정원에서 오신 분이 아니고 과기부에서 오신 분입니다. 다른 분들도 여러 부처에서 왔고요.
그런데 진짜 국가안보실을 제대로 된 컨트롤타워로 만들고 싶다면 실행력을 줘야 되거든요. 실제로 어떤 것을 움직일 수 있는 힘을 줘야 합니다. 그러니까 국가정보실이 있는데 거기에 아무것도 없다면, 하다못해서 어떤 정보를 듣거나 뭘 들을 때도 기관이 지원해줘야 한다고 하면 컨트롤타워될 수 없지요. 거꾸로 이런 컨트롤타워인데 다른 기관들 눈치를 보니까.
그래서 미국 같은 경우에는 그런 국가안보실 같은 컨트롤타워에다가 예산집행권을 줍니다. 예산 배분권한을 주는 거지요. 그래서 국가안보실이 있다고 되는 게 아닌 이것을 컨트롤타워로 만들려면 거기에서 정하는 힘을 어떻게 줄 수 있을지를 논의해야 하고요.
그다음에 공공기관뿐만 아니라 일반기업이 사고가 나면 다 쉬쉬합니다. 그게 왜 그러냐면 우리나라문화 자체가 잘못돼서 그런 게 있습니다.
우리는 어떤 기업에서 사고가 나고 사고가 나면 아이씨 ㅇㅇㅇ 이러거든요.
그런데 예를 들어서 우리나라주요 공공기관에 하루에 들어오는 해킹 시도 건수가 135만 건이 조금 넘습니다. 이게 하루 들어오는 평균 기준이 이렇거든아버지? 135만 회 해킹 건수를 어떻게 다 막습니까? 그렇죠?
특히 4차 산업혁명 시대에 오고 인터넷과 연결되고 그렇다면 2020년이 되면 전세계 인구의 50%가 인터넷을 쓰고 인터넷과 연결된 것은 402억개가 넘어간다고 합니다. 엄청난데 이것을 다 막는 게 불가능합니다. 그래서 외국에서 패러다임을 바꿔야 한다고 이야기하고 프리베이션, 막는다고 해서 얼마나 빨리 원상태로 복원하는지, 패러다임을 바꾸고 있는 것입니다. 그래서 물론 혼내야죠. 그런데 그것은 우리가 기존에 뻔히 알고 있던 공격법인데 그것을 못 막으면 그것은 나무라야 합니다. 그런데 듣도 보도 못한 공격을 가지고 뚫이면 나무랄 수 없습니다. 그런데 우리나라는 뚫리면 나무라는 문화가 있어서 보안팀은 숨기고

싶은 것입니다. 그리고 보안팀은 3d 업종이 되어가고 있고요.
복원, 리커버리를 빨리 하는 게 최대관심사인데 그 복원력이 얼마나 빠른가가 잘못인데 무조건 막는다는 게 관심사가 아닙니다. 정보공유도 ㅇㅇ 하는 거여서 그렇지 막는 시각도 복원 개념으로 바꿔야 우리가 뚫렸고, 이런 게 생겼다는 것을 사람들이 자발적으로 이야기할 수 있는 것입니다.
왜? 이렇게 자발적으로 이야기할 수 있어야 다른 기관이 빨리 듣고 나도 방어태세를 갖추거든요. 그렇게 이야기하는 사람들에게 칭찬을 해줘야지 그게 안 된다고 해서 왜 이야기 안 했냐고 탓하면 문제가 있는 것 같고요.
그다음에 우리가 사실은 우리가 갖고 있는 특정 권한을 어떻게 해서 각자 세분화시켜서 각자 기관에 권한을 주겠다고 할 때는 반드시 뒤따라야 하는 게 뭐냐면 만약에 너희들이 막을 수 있는 것을 못 악으면 책임을 어떻게 질거냐는 조항이 들어 가야 합니다. 민간기업은 잘못하면 사장이 잘리고 그러는데 공공기관에서는 그렇게 했다는 것을 들어보신 적이 없잖아요? 권한과 책임을 같이 주었을 때 훨씬 더 명확한 업무분장도 가능해지고 여러 가지 일이 생기거든요.
예를 들어서 권한, 책임을 같이 주는데 내가 많은 것들을 다 커버하고 싶을까요? 할 수 있는 것을 하고 싶을까요? 그래서 권한, 책임을 들이해서 논의했으면 좋겠다는 생각을 하고 있습니다.
-조지훈: 예, 다양한 말씀을 하셨는데요. 잠깐 쉬어가는 질문을 하나 드리면 아까 신용우 입법조사관님이 최근에 ㅇㅇㅇ 발의된 것은 폐기가 될 것으로 전망하셨는데 전망에 근거가 있으신지, 저희는 전혀 그런 생각을 하지 않고 있는데요.
-신용우: 약간 법 재개정 절차가 도깨비 같은, 아 예측이 불가능한 부분이 있어서 지지부진 하다가도 갑작스럽게 되는 경우도 있어서 사실 이것을 단언적으로 말하기에는 어려운데요.
엄밀히 이야기하면 전정부에서 발의했어서 현정부에서 어떻게 할지는 명확히 의견을 내지 않고 그 사이에 안보전략이 나온 상황이어서 이것이 급속도로 논의가 되고 합의가 되기는 어렵다고 개인적인 판단을 합니다. 공식적인 판단은 아닌 것이고요.

그리고 또 마이크 든 김에 몇 가지 말씀드리면 김 교수님께서 공공 쪽에 사이버 안보를 행정안전부가 담당하는 게 바람직 할 것이라는. 공공분야에서 행안부가 중요한 역할을 하고 주요 정보토. 신시설 기반에서도 많은 영역이 행안부 소관 시설이 지정되어있습니다. 그래서 그 시설에 대한 관리권한은 소관부처에 있기 때문에 사실 1차적인 금년, 책임은 행안부에 있는 것으로 보이는데요. 큰 컨트롤타워그것은 국정원이 하냐 마냐의 문제고 ㅇㅇ법에 국정원이 있는데 이것은 다시 검토를 필요가 있는 것 같고요.
그리고 교수님이 말씀하신 것처럼 컨트롤타워의 필요성이 필요하고 권한, 책임이 같이 들어가야 한다. 그래서 아까 말씀드린 것중에 하나가 여기에는 저도 국가안보실이 됐든 별도 기관이든 어떤 조직과 예산을 갖추는 게, 정부는 조직과 예산이니까가
예를 들어서 부다페스트 협약이라고 해서 미국, 일본 사이버 조약이라고 하지만 이런 나라들이 참여하고 있는 협약이 있고요. 결국에는 국제범죄에 대해서 사이버 범죄를 공유하자는 것이고 우리나라는 가입되어있지 않습니다.
이게 외교부가 국제협약, 외교부가 담당하고 있는데 이게 걸림돌 중에 하나는 통신비밀보호법 개정과도 연결이 있습니다. 이 법은 과기총부에서 담당을 합니다. 컨트롤타워라고 하는데 여러 부처의 의견을 듣고 의사결정을 해야 되는데 이 이야기만 듣고 결정할 수 있을지, 자체적으로 정보를 수집하고 판단할 수 있는 그런 조직이 필요하지 않는지, 그런 것들에 의해서 고민해 보면 어떤 형태로든지 어떤 컨트롤타워는 필요하다는 말씀을 드리고자 합니다.
-조지훈: 예, 지금까지 조금 모호하지는, 의견이 약간 다르지만 합치된 부분은 사이버 보안 전체를 담당하는 컨트롤타워고 필요하고 그 컨트롤타워에는 집행력, 실행력이 담보되는 조직이 있어야 한다는 취지에 대해서는 다들 공감하시는 것 같습니다.
그리고 어떤 정보공유의 투명성이나 권한과 책임에 대한 권한 분산, 개념의 명확화 이런 측면들은 일체적으로 동의가 되는 내용들인 것 같습니다.
기본적으로 국정원 이야기가 조금 나왔었는데 사이버 보안 측면뿐만

아니라 국정원이 가지고 있는 권한, 전체적인 권한이 지금 수사권이 있고 기획조정권이 있고 하거든요.
그렇기 때문에 이 여러 가지 권한을 다 포괄하고 있는데 여기에 사이버까지 다 하겠다고 하니 문제가 더 심각해지는 것 같습니다.
예를 들면 수사권과 지금 사이버, 실제로 법률상 근거는 없지만 사이버 보안 전반을 공공 영역에서 전반을 국정원이 책임지고 있는데 예를 들면 이런 것입니다.
국가보안법 위반 사건에서 ㅇ을 하는데 국정원이 수사를 하면서 ㅇㅇ 감청을 합니다. 설비가 다 있어서.
그런데 사무실에 감청을 다는데 그 사무실에는 피협의자뿐만 아니라민간인분들도 되게 많이 가거든요. 그런데 국정원에 들어가있는 그 감정기계는 그 피협의자는 상관없이 그 모든 정보가 그 기기에 들어가게 됩니다. 그 이후의 처분에 대해서는 밖에서 알 수 없는 거예요.
이런, 어떻게 보면 다른 권한까지 포함하는 조직이기 때문에 더 개혁에 목소리가 있는 것 같고 예산집행도 국정원이 배정할 수 있는 권한이 있습니다. 정부에서 관련해서 총괄하는 것인데요. 그렇기 때문에 이 사이버 부분까지 계속 맡겨야 하냐는 부분이 있는 것 같고.
아직 구체적인 안이나 이런 게 나온 게 없지만 기본적으로 행안부, 일반적인 사이버 보안과 관련한 업무는 진짜로 국가적 위기나남북관계나 해외 이런 안보 정보 이외에 사이버 보안 관련해서는 행안부에서 담당하는 게 맞는 게 아니냐는, 가장 간단하게 표현하자는 그런 논의들이 이어가고 있습니다.
그러면 저희가 패널들 논의를 거의 이 정도로 마무리를 하고요. 플로어에서 말씀하시는 게 있다면 저희 패널들끼리만 토론을 했는데 다른 분하고도 토론자리에 참여하셔서 진행을 하셨으면 좋겠습니다.
혹시 의견이나 말씀하고 싶은 게 있으신 분 계세요?
-전북대학교 교수입니다.
저는 패널분들이 다 같이 5분이 하시는 말씀이 공통적인 게 2가지가 있다고 생각됩니다.
하나는 ㅇㅇ, 또 하나는 사이버 안보관련해서 민간 협력 거버넌스를 어떻게 만들것인지 그런 부분에 대해서 조금 더 구체적인 아이디어가

있으면 듣고 싶습니다.
예를 들어서 정부의 스탠드 설립 같은 경우에 패널에서도 말씀해주셨지만 2010년 인데, 2010년도 정도부터 시작이 되어서 2015년도 되면 얼라이언스, 따라 하기 시작하는데요. 말할 것도 없고요. 그중에 저희가 배울 만한 것이 있다면 센터를 만들 때에 그런 아까 말씀하신 안보척도 관련한 것에 대해서 어떤 관련된 기관에서 ㅇㅇ받고 민간인들도 참여시켜주고 어떻게 보면 멀티 그런 것을 반영한 센터를 만들기 시작하더라고요.
그런데 그것이 가능할 것인지 질문을 드리고 싶고요. 아무래도 우리나라 같은 경우에는 안보 그런 것에 민감하다고 생각을 해서요.
또 하나는 사이버 안보에서 거버넌스 생태계를 어떻게 조성할지 구체적인 아이디어가 있으면 듣고 싶은데예를 들어서 아까도 말씀드렸다시피 외교부 그다음에 국정원 같은 경우에는 안보에 민감하지 않습니까? 그러니까 자신들의 정보를 취하는데 민감하고 꺼려하는 기관이 있는데 이들을 포함한 민간인들도 참여하는 어떻게 보면 사이버 안보 이게 매일 ㅇㅇㅇ강조를 많이 하는데 어떻게 그런 거버넌스 민간협력 거버넌스 생태계를 만들어나갈 수 있을지 말씀해 주시면 좋을 것 같습니다.
-권석철: 제가 해 보겠습니다. 사실 어떻게 보면 말씀하신 부분처럼 저희는 기관이 법에도 이야기가 나온 ㅇㅇ가 나오는데 독립된 기관이었으면 좋겠다는 개인적인 의견을 드리고 싶습니다.
왜냐하면 사이버안전청이라는 것을 가지고 실행력을 가지고 대통령이, 그러니까 안보실이 아닌 대통령이 직접 컨트롤타워가 되어서 그 밑에 안전청을 두고 그 아래에 민간, 방어 이런 부분은 방어에 대한 어떠한 정보를 수집할 수 있는 것들을 다 그 부처쪽 형태로 붙이고 가공해서 국가 관련한 자료는 국가정보원이 수집해서 나머지에 대한 부분은 고민을 해서 그 정보들이 해킹 공격이라는 것이 뭐 군은 군이 공격, 민은 민이 공격하는 그런 게 아니지요. 군을 민간이 공격할 수도 있고. 그런데 군은 접근을 못하게 되는 그런 문제점들이 많이 있습니다. 그리고 어떤 특정정보에 보면 이런 군의 문제가 아니니까 군은 오지 말라는 그렇게 되는 것들이 현재 일어나고 있거든요.
그런 것을 같이 판단할 수 있는 정보가 필요하다고 생각을 하고 영국

그다음에 두 번째 그 부분이 가장 큰 것입니다. 미국이라든가 이런 곳에서 남북한 정보수집에 대한 그런 것들이 서로 정보공유가 많이 되느냐, 그렇지 않습니다. 대한민국이 해킹대응능력이 약한 것을 알아서 많은 정보를 주지 않습니다. 국가기밀, 국가의 중요한 정보들이 많이 나가지 않습니다. 특히 외교부에서 일어났던 미국대통령, 대한민국 대통령이 통화한 내용이 유출됐다는 사실은 엄청난 사건 입니다. 그래서 그렇게 보면 굉장히 위험한데 중국의 어떤 화웨이 장비까지 쓴다고 하니까 민감하고 발끈할 수 밖에 없는 것이지요. 그러한 정보들이 각 국마다 정보를 공유하는 자체는 분명한 것은 필요합니다.
필요한데, 과연 그것이 비밀정보까지 공유될 것인지 그 부분은 의문점이 많이 있습니다. 그러한 것들은 조금 더, 아무리 우방이라고 하더라도 각자 수집한 정보들은 각각 굉장히 중요하기 때문에 정보를 공유하는 게 힘들지 않을지 이렇게 보고 있습니다. 제 개인적인 의견이라고 말씀드리고 싶습니다.
-오병일: 저는 두 가지 측면에서 말씀을 드리고 싶습니다.
하나는 사실은 정부의 마인드. 뭐라고 해야 할까요? 이 행사, 한국인터넷거버넌스포럼 프로그램 위원회에 위원장이기도 한데 이게 표방을 하잖아요? 이런 행사를 몇년동안 하지만 전체 영역에서 이런 방식이 아직까지는 일반적이지는 않습니다. 물론 많은 위원회들이 있지요. 위원회들이 있는데 그래서 대부분 정부가 위원들을 알아서 선임합니다. 자신의 마음에 드는. 다양하게 선임한다고는 하는데 자발적인 참여에 기반을 해서 관심있는 사람이 참여하는 구조는 아닙니다.
한 가지를 에피소드를 말씀드리면 사이버 보안와 관련한 기구는 없지요. 그런데 러시아, 중국, 이런 쪽은 다르기는 한데 서방쪽에서는 영국이 시작했던 사이버 스페이스 컨퍼런스 이런 게 런던에서 시작해서 13년인지 14년인지 한국에서 열렸었어요. 그런데 저도 관심이 있어서 참가신청을 했는데 참가가 안 된다는 거예요.
그래서 막 졸라서 여러 번 전화를 해서 간신히 참여 허가를 받았습니다.그다음에 네덜란드에서 개최를 했었는데 네덜란드 정부는 엔지오들을 110명을 불렀습니다. 국제적으로 그렇게 붙렀고 트레이닝 하기 위한 별도의 프로그램을 엔지니어들이 ㅇㅇ하게 끔 했고

이런 전반적인 정책에 접근을 하는 방식의 그러한 차이라는 생각이 들거든요. 그래서 일단은 사이버 보안 문제만은 아니지만, 특히 인터넷과 관련해서 민간이 많이 주도 하는 부분이 많지 않습니까? 그런 민간의 참여라든가 기업, 정책결정 어느 정도 정책결정을 주는 그러한 방식의 인식의 변화가 필요할 것 같고요.
그것을 사이버 보안 거버넌스에서 도입을 한다면 하다 못해 자문위원회라든가 민간협력을 같이 할 수 있는 그런 자문기구의 이름은 학계라든가 기술계도, 업계도 참여를 해야 되겠지만 시민사회에 어떤 참여도 하는, 저는 저희가 업계만큼 기술적 전문성이 있다거나 그럴 수 있다고 생각하지는 않습니다.
다만, 업계나 일반학계에서, 그러니까 학계와 다른 또다른 관점에서 여러 가지 의견들, 견해를 제시할 수 있거든요. 그런 다양한 민간의 참여를 보장할 수 있는 그러한 틀을 아예 공식적인 거버넌스 체계 내에 포함을 하면 좋겠다는 그런 생각을 가지고 있습니다.
-조지훈: 원래 저희 패널 자체 토론회에서도 논의를 해야 될 주제를 잘 질문해 주셔서 우리 김승주 교수님께 방향, 상에 대해서 답변을 부탁드립니다.
-학계의 역할에 대해서 조금 더 강조를 해 주시면, 특히 학계에 어떤 역할을 기대할 수 있을지 말씀해 주시면 더 좋을 것 같습니다.
-김승주: 저는 그렇게 정책을 맞이하는 사람이 아니어서 자세한 것은 저희들이 한계가 있을 것 같고요. 다만, 민간에서 어떻게 할 것인지, 그러니까 예전에도 그랬고 우리 뭐 국가사이버안전센터든 어디든 가면 산하기관, 민간기관들이 파견을 합니다. 한두명씩 가서 이렇게 같이 있는데요. 어떤 정보가 있으니까 공유하고, 빨리 빨리 대응을 위해서 그렇게 합니다. 그런 형태는 갖추어 져 있다는 것입니다. 국내 안에서요. 그런데 문제가 뭐냐면 아가 말씀드렸듯이 형태의 문제가 아닌 그 힘의 균형을 어떻게 맞춰 줄 것이냐는 그런 게 훨씬 더 큰. 우리가 논의를 하면 조직체계를 만들어야 한다조직체계를 만들어야 한다그렇게 이야기하는데 거의 다 있습니다. 그런데 힘의 밸런스가 맞지 않아서 거든요. 제가 아까 컨트롤타워, 컨트롤타워 우리 다 있습니다. 실행력이나 권한이 없어서 그런 것이지 실질적인. 그러니까 우리 뭐라고 하면 체

계를 만든다고 하면 그것은 있다고 보시면 됩니다. 그것을 어떻게 제대로 굴러가게 만들어줄 것인지를 논의하는 것이 지금 단계에서는 더 우리에게 시급하다고 보고 있고요.
그다음에 사실 국내에서 민간협력, 민간이 협력한다 이것보다도 허위사태를 보시면 아시겠지만 글로벌적인 게 더 중요합니다. 글로벌한 것을 할 필요가 있는데 이런 사이버 보안이나 이런 데에서 정보를 공유하는 데에 있어서 미국을 중심으로 이야기하면 미국은 정확히 정보공동체라는 게 있습니다. 우리가 소위 미국, 영국, 캐나다, 뉴질랜드, ㅇ이 5개의 나라를 이야기합니다. 우리나라는 이 안에 들어가 있지 않고 당연히정보공유하지 않습니다. 왜냐하면 정보공유체에 들어가 있지 않으니까. 우리는 우방이지만 상황에 따라서 해킹 대상이 될 수 있는 나라로 분류되어있습니다. 미국 기준에서 보았을 때요.
일본에서는 외국에서 보면 이 역할에 들어가기 위해서 정말 많은 노력을 합니다. 외국에 가면 그 나라들 주변에서 알짱알짱 있고 컨택을 하려고 노력을 합니다. 그리고 올초에 나오는 실제일본 사이버 보안와 관련한 전체 보고서를 보더라도 앞에 기술적인 내용들이 쭉 있고 뒷부분에는 "우리는 미국과 ~" 이런 식으로 나라 이름을 딱 명시해서 우리는 어느 나라와 이러한 정보공유를 위해서 노력한다고 명확하게 되어있거든요.
그런데 우리는 이게 없는 것입니다. 국제적인 협력강조 이 정도 들어가 있고 그러면 어느 나라를 가냐고 하면 그때그때 달라지거든요. 지정학적 일 때문에 그럴 수도 있겠으나 그렇게 애매모호하게 해 놓으면 일단 사람이 계속 바뀝니다. 지속적인 것을 맺을 수 없거든요. 우리나라도 지금은 민관, 협력뿐만 아니라글로벌 협력도 중요한데 그럴 때 어떤 전략을 가지고 어디부터 컨택해서 할지 명확하게 할 필요가 있습니다. 그때그때 포인트가 바뀌는 게 아니고요.
민간협력 관련해서는 체계보다는 어떻게 보면 그것을 힘의 밸런스를 맞춰줄 것인지, 실제로 돌아갈것인지에 초점을 맞추면 좋겠고 글로벌 협력관련해서는 우리나라가 정확히 어떤 나라를 타겟으로 해서 할 것인지를 명확히 뽑았으면 좋겠고요. 그다음에 전체적으로 우리나라의 전체관련부 체계를 보는 데에 있어서는 제가 사이버 안보에 명확한 정

의 그런 것을 통해서 책임, 권한을 명확히 했으면 좋겠다고 했는데 그렇게 따지면 우리나라조직체계가, 우리 영역이 이렇게 이렇게 나누어져 있습니다. 이게 동등하게 있지요.
그런데 외국을 잘 보면 삼각형 체제로 되어있습니다. 어떤 지병이 돌면 1차 보건소, 그 다음에 2차, 국가 질병관리본부가 나오고 삼각형 구조입니다. 이렇게 정보의 중요도, 대상이 정해지면 그것들이 얼마나 국가에 중요한지 정해지고 삼각형 체계가 나오기 시작합니다. 그렇게 역할에 맡게끔 합니다. 우리나라 한국인터넷진흥원, 1차 보건소 역할을 합니다. 기본적인 것은 여기에서 하고 넘어가서 중대질병이 되면 2차 기관이 나오고 동작을 해야 되는 거거든요.
물론, 우리가 질병을 하다보면 1차 보고서로 충분할줄 알았는데 생각보다 중증이네, 할 수도 있습니다. 우리가 인터넷을 하다보면, 이게 물론 어떤 데이터는 국가기밀, 직접 적으로 위협이 되는 해킹 공격들 이렇게 식별되는 게 있고 어떤 것은 민간을 공격하는 줄 알았는데 국가기밀로 연계되는 것도 있습니다. 보통 이런 이야기가 나올 때는 사이버 공격은 대테러냐 명확하게 나눌 수 없어서 애매모호한 정일내릴 수 밖에 없다는 것이 제 논리거든요.
물론 그럴 수 있습니다. 물론 그럴 수 있지만 그렇게 애매모호해서 영역을 침범하는 것을 가급적 최소화시켜야 힘의 균형이 맞는 거버넌스 체계가 된다고 보거든요.
그래서 저는 우리나라조직체계도 그런 전체적인 대응체계를 우리나라 보건소 같은 그런 구조를 따라 가려고 노력하면 조금은 나아지지 않을까 그런 생각이 있습니다.
-권석철: 추가로 하나만 더 말씀드리겠습니다. 김승주 교수님 말씀처럼 힘의 균형에 대해서 크게 공감합니다. 사실 힘의 균형을 하려다 보니까 그동안 저는 군의 사령부 ○○ 일을 해왔다보니까 사건이 터지고 그런 일들이 있었고 그것을 보면서 가장 큰 문제점을 찾게 됐습니다.
그것을 말씀드리겠습니다. 힘의 균형이라는 것은 돈입니다. 그러니까 돈을 누가 주느냐, 누가 갖고 있느냐죠. 우리는 국가가 민간기업 같은 경우에는 주주가 있습니다. 기업이 뭘 하려고 해도 주주가, 대주주가 그렇게 하면 안 된다고 하면 못합니다. 그러다 보니까 민간기업도 마

찬가지로 돈을 갖고 있거나 대주주의 힘이 셉니다. 그런데 국가쪽으로 와보겠습니다. 와보면 여러 가지 사건 들이 터지는데 국가안보가 끼어 있는 사건을 말씀드려보면 국가정보원은 정보 ㅇ을 갖고 있고 각 부처에 예산을 분배합니다.
그 부서에서는 예산을 받기 위해서 국가정보 관련해서 관계를 갖게 되지요. 그렇게 갖게 되면 갑과 을이 굉장히 명확해 집니다. 물론, 하고 싶지 않더라도 해야 되는 상황도 있고요. 그 예산을 못 따면 기관므로써의 활동이 어렵습니다. 금액은 잘 모릅니다. 하지만 그런 관계속에서 국가정보원이 그런 역할을 많이 해왔다는 것이지요.
이것은 굉장히 큰 문제라고 볼 수 있어요. 그래서 힘의 균형이라는 것은 경찰, 검찰 수사 이런 것처럼 갖고 있는 것을 놓는 게 어려울 수 있습니다. 그런데 여러 가지 체제를 만들었는데 활용이 안 되는 경우는 그 힘의 균형에 의해서 정의를 못하는 거죠. 그러면 힘의 형이 무엇일까 하면 예산인거거든요. 그 예산에 대한 이야기를 조금 더 해서 예를 들어서 a라는 이야기를 해서 예산을 받고 다른 데에서는 예산을 받을 필요가 없지요. 국방부도 마찬가지고 정보산업 이런 데도 마찬가지고 국가정보원이 관여하면 안 되는 것이지요. 그렇게 되면 독립성이 유지됩니다. 그런데 유지가 되지 않는 것은 예산에 대한 문제가 아닐까, 그것을 우연히 알게 됐는데 심각한 것으로 받아들이고 있습니다.
-조지훈: 지금 질문에 대해서 조금 의견들을 주셨는데요. 힘의 균형, 그리고 글로벌까지 연계 제안을 주셨습니다. 구체적으로의 예산, 현실에서 힘이 나타나는 예산권 말씀을 주셨는데 그 시간은 거의 다 됐고요. 오늘 혹시 마지막으로 뭐 질문을 꼭 하고 싶으신 분이 계시면 마지막질문을 받고 마무리를 하려고 합니다. 혹시 질문이 있으신가요? 특별히 없으시면 오늘 저희 주제가 사이버 보안과 민주 거버넌스 관련한 거잖아요? 저희 논의의 시작이 신용우 조사관님 말씀처럼 21대 국회에서 새로운 법률을 개정할 때쯤 ㅇㅇ 됐으면 좋겠고 마지막으로 입법조사관님부터 마지막발언을 듣고 마치도록 하겠습니다.
-신용우: 오늘 되게 많은 논의가 있었고 사실은 어떤 서면으로, 글로 보통 접하다가 되게 생생하게 여러 전문가 분들, 패널분들 말씀을 듣고 나니까 좀 명확해 지는 부분도 있고 쟁점이 무엇인지, 앞으로 관련

되는 부분들도 생기는 것 같습니다.
결국에는 두 가지 가치가, 대립되는 것 같습니다. 어떤 정보보호, 사실은 사이버분리공간이 결합되는 이 공간에서 정보보호에 대한 게 강호되는 한편에 이 인터넷 사이버 공간에서의 프라이버시를 이런 문제는 물리적인 공간보다 더 심각해 지니까 프라이버시 이 부분에 대해서 섬세한 어떠한 정책과 법적인 기반이 필요할 것 같고요.
그 어느 한편에 가지는 정책을 할 수 있도록 노력하겠습니다. 감사합니다.
-김승주: 재미있는 자리에 불러주셔서 감사드리고요. 어쨌든 많이 배웠습니다. 제가 학교에 있으니까 논문을 쓰거나 학생들을 가르칠 때 제일 제가 신경을 많이 쓰는 게 정의. 정의가 흔들리면 나머지가 전부 다 흔들리거든요. 외국에서는 에스시아이 논문 이야기하는데 외국은 학계에서 용어의 정의를 명확히 내리는 논문을 정확히 많이 씁니다. 인포메이션 뭐 이런 게 뭔지 여태까지 나와있는 문헌과 법자료, 기술문서를 자 분석해서 용어정의를 내리거든요. 그런 자료가 굉장히 많습니다.
용어정의가 튼튼해야 나머지가 쉽거든요. 그런데 우리는 용어정의에 공을 들이지 않고 국 자료갖다가 짜집기하고 해서 나머지가 다 안 되는 것입니다.
저는 학교에 있는 입장으로써 프로그램을 짜고 수식있는 것만 하는 게 아니고 용어정의를 명확히 하는 것도 학계에서 큰 기여가 될 수 있어서 용어 정의에서도 힘을 쓰고 예산배분에서도 용어정의를 열심히 해서 할 수 있는 그런 프로젝트도 많이 나왔으면 좋겠습니다.
-권석철: 오늘 이야기를 조금 저도 어떻게 많이 했는데 국가도 양보하고 민간도 양보하는 그런 관계가 되었으면 좋겠습니다. 조금씩 양보하면 정보에 대한 두려움과 그것이 잘 사용할 수 있다는 형태로 된다면 인터넷, 거버넌스 자체가 민주적으로 갈 수 있지 않을까 생각합니다. 감사합니다.
-오병일: 저는 양보하려고 한 것보다는 이 인터넷 거버넌스 포럼을 하려고 한 게 어떻게 보면 도와주고 싶은 거예요. 여기에 계신 분들이 다 국가정책에 참여하고 싶고 그러면 일정책임을 질 수 밖에 없거든

요. 조금 더 건설적으로 나갈 수 있도록 그렇게 하고 싶은 것이고요. 미국에서는 90년대인가요? 암호전쟁 이런 게있었는데 국가가 일종의 암호의 백도어를 설치했어서 여러 가지의 범죄수사라든가 정보수집 목적으로 하려고 했을 때 시민사회단체가 많이 반대했어요. 시민사회뿐만 아니라 엔지니어들, 기술자들이 같이 결합을 해서 반대를 했었거든요. 그런데 사실 국내에서는 시민사회단체들도 사이버를 보안문제에 관심을 가진지 사실 오래 되지 않았고 사실 이런 토론 자체가 별로 없었다는 생각이 듭니다. 어떻게 보면 한정된 케뮤니티 내에서만 토론이 되어왔지 않았냐, 사실 발제가 없었음에도 불구하고 할 이야기가 되게 많잖아요? 이런 이야기들이 제한된 시간이었지만 앞으로도 잘 되었으면 하는 바람입니다. 감사합니다.

-조지훈: 저도 발제가 없어서 시간은 이렇게 1시간 넘고 그래서 시간을 이걸 어떻게 사회를 보나 했는데 막상 말씀을 들어보니까 시간이 너무 짧네요. 시간이 너무 짧고 저는 개인적으로는 실제현업에 계신분, 함께 계시는 분, 입법에 계시는 분들 이야기를, 구체적인 경험들과 좀 전해들으니까 제가 몰랐던 부분들도 많이 알게 되고... 이런 논의가 실제로 앞으로 계속 더 심화시키고 확산시켜가면서 우리 사이버 보안 21세기, 어떻게 보면 가장 큰 화두가 될 텐데 사이버 보안에 대한 민주적인 어떤 컨퍼런스를 어떻게 구축하고 확산시킬 것인지 하는 고민을 전문가 분들, 여러분들과 해야 하지 싶습니다. 자리를 해 주셔서 감사하고요. 거버넌스 토론 부분을 마치겠습니다. 고맙습니다.