안보기술연구센터 개소식 환영사

(2020. 1. 29. 수. 문지캠퍼스 학부동 대회의실)

여러분 대단히 반갑습니다.

오늘 '안보기술연구센터'의 개소를 축하하기 위해 이 자리에 참석하신 여러분께 충심으로 감사드립니다.

'안보기술연구센터'는 국가안보를 위한 우리 대학의 역할을 새롭게 정립하는 이정표가 될 것이기에 오늘 행사는 매우 의미가 크다고 생각합니다.

그동안 '안보기술연구센터'의 개소를 위해 각별한 관심과 지원을 아끼지 않으신 '미래기술융합센터'의 과학본부장님 및 관계자 여러분에게 이 자리를 빌려 특별한 감사의 말씀을 드립니다.

한편, '안보기술연구센터' 설립을 위해 그동안 헌신적인 리더십을 발휘한 방효충 안보융합연구원장과 김창익 초대 안보기술연구센터장 이하 교직원들에게도 감사드립니다.

인류사회에는 지금 4차 산업혁명의 파고가 쓰나미처럼 몰려오고 있으며, 초연결(Hyperconnectivity)과 초지능(Superintelligence) 및 초융합(Meta-Convergence)의 4차 산업혁명 메가트랜드에 의해 인류는 상상을 초월한 기하급수적인 변화를 경험하며 새로운 문명의 혜택을 누릴 것입니다.

지구촌은 모바일과 IoT 디바이스로 초연결화 되면서 광속도로 정보를 교환하는 문명의 혜택을 누리게 되었지만, 이러한 기술적 진보를 악용한 사이버 범죄(Cyber Crime) 역시 증가하며 21세기 인류의 새로운 위협이 되고 있습니다.

2019년 현재 전 세계 인구의 53.6%인 41억 명이 인터넷을 사용하고 있습니다. IoT 디바이스는 2019년 기준 약 83억 개가 사용되고 있지만 기하급수적인 증가로 인해 2025년에는 약 220억 개가 사용될 것이라는 전망이 있습니다.

하지만, 문명의 이기(利器)인 인터넷과 IoT 디바이스는 사이버 공격의 접촉점(Contact Point)으로 악용될 수도 있기 때문에 인터넷과 모바일 및 IoT 기기 사용의 확대는 사이버 범죄의 기하급수적 부작용을 함께 내포하고 있습니다.

이러한 우려는 이미 현실화되고 있습니다. 전문가들에 의하면 현재까지 전 세계적으로 약 4천만 건의 사이버 범죄가 발생했으며 4초마다 한 번씩 새로운 사이버 범죄가 발생한다고 합니다.

사이버 공격의 범위는 전력 시스템, 은행, 항공, 도로 교통망, 군 컨트롤 시스템, 병원 등 전방위적으로 확대되고 있으며 이에 따른 경제적 손실 규모는 2018년 1조 5천억 달러 수준에서 매년 증가해 10년 후인 2030년에는 90조 달러의 천문학적 수치를 기록할 것으로 예상됩니다.

지난주 저는 스위스 다보스에서 개최된 세계경제포럼(World Economic Forum, WEF) 제50회 연차총회에 참석했습니다. WEF는 지구온난화에 따르는 기후·환경 변화와 더불어 사이버 테러를 올해 총회의 양대 핵심 아젠다 중 하나로 선정했습니다.

이에 따라 세션별 토론 시간에서 뿐만 아니라 제가 회원대학의 총장 자격으로 공식초청을 받아 참석한 WEF의 '글로벌대학 리더스포럼(Global University Leaders Forum, GULF)'에서도 사이버 테러 관련 논의가 비중 있게 다루어졌습니다.

과학적 분석과 데이터에 기반을 둔 심도 있는 논의가 이어졌으며, 앞서 소개해 드린 사이버 범죄 관련 최신 통계와 전망치는 WEF 연차총회에서 활용했던 토의자료 중 일부를 발췌한 것입니다.

이러한 상황에서 인공지능, IoT 등 4차 산업혁명 핵심기술의 발전을 기반으로 21세기 디지털 유토피아(Digital Utopia) 세상을 꿈꾸는 인류는 지능적 사이버 공격을 비롯한 신기술의 악용으로 인해 대혼란의 디스토피아(Chaotic Dystopia) 세상을 경험하게 될 수도 있습니다.

사이버 테러를 포함해 4차 산업혁명 시대 새롭게 부상하는 안보 위협에 대처하기 위해 각국은 안보기술 분야의 연구개발 투자를 확대하고 있습니다.

미국은 국가안보를 연방정부 연구개발의 5대 중점 분야 중 하나로 지정하고 사이버 공격, 테러 등 안보 위협 요인으로부터 국가적 피해를 최소화하기 위한 연구개발 활동에 예산을 집중적으로 투입하고 있습니다.

우리 정부도 기민한 대처를 하고 있습니다. 작년 9월에는 '국가 사이버안보 기본계획'을 발표하고 사이버 공격 대응 역량 고도화를 위한 관련 연구개발 예산 확대 등의 계획을 제시했습니다.

이러한 국내외 변화를 직시하며 새로운 안보 위협에 대처하기 위한 노력의 일환으로 '안보기술연구센터'를 설립한 것은 매우 시의적절한 결정입니다. 특히, KAIST에 센터를 설치한 것은 탁월한 판단임을 확신합니다.

1971년 설립 이래 KAIST는 국가가 필요로 하는 과학기술 인재양성과 연구개발 수행이라는 '임무 중심 대학 (Mission-oriented University)'의 역할을 성실히 수행하며 국가 산업화와 정보화 및 과학기술 선진화를 이끌어 왔습니다.

KAIST는 지난 반세기 동안 박사 13,300여 명을 포함해 65,000여 명의 고급과학기술 인재를 배출했으며, 이들은 산업계와 학계 등 각 분야에서 중추적인 역할을 담당하고 있습니다.

4차 산업혁명 태동기를 맞이해 KAIST는 새로운 시대적·국가적 미션인 '4차 산업혁명 선도대학'의 사명을 위한 세 가지 측면의 혁신을 추구하고 있습니다.

첫째, 교육과 연구혁신을 통해 4차 산업혁명 시대가 필요로 하는 인재를 양성하고 인공지능 등 4차 산업혁명 핵심기술 연구를 확대하고 있습니다.

둘째, 기술사업화 혁신을 바탕으로 과학기술 연구 성과를 기술사업화와 창업으로 연계하는 '기업가형 대학'을 지향하고 있습니다.

셋째, 미래전략 혁신을 기반으로 국가혁신을 위한 미래비전과 전략 및 과학기술정책의 수립을 지원할 싱크탱크의 역할을 강화하고 있습니다.

이러한 혁신의 노력과 함께 국가안보 분야의 연구와 인력양성이 KAIST가 추구해야 할 새로운 사명 중 하나라는 인식하에 총장으로 취임한 직후부터 저는 다양한 관련 사업을 추진해오고 있습니다. 'KAIST 안보융합연구원'을 설립했고 '융합보안대학원'을 유치했으며 '미래국방 인공지능 특화연구센터'를 개소했고 드디어 오늘 '안보기술연구센터'를 설립하게 되었습니다.

'안보기술연구센터'를 통해서 국가안보를 위한 첨단과학기술 연구가 활발히 이루어지고, 이를 기반으로 센터가 안보기술 분야에서 'Global first-mover, 글로벌 선도자'로 도약하기를 총장으로서 기대하고 있습니다.

이를 위해 본 센터에 참여하는 연구자들에게 세 가지를 특별히 당부하고자 합니다.

첫째, 세계 최고(Best)이거나 최초(First)이거나 유일한(Only) 소위 B·F·O 연구를 추구해야 합니다. 4차 산업혁명 시대는 승자독식(Winner takes all.)의 시대로서 1~2등의 기술만이 살아남으며 안보 기술 분야에서는 이러한 경향이 더욱 뚜렷하기 때문입니다.

둘째, 협업연구를 확대해야 합니다. 우리보다 연구 인력과 자원의 측면에서 우위를 점하고 있는 선진국과의 경쟁을 위해서는 자체적인 협력 뿐 만 아니라 외부 연구자 및 연구기관들과의 협업연구를 적극 추진해야 하며 필요시에는 국제협력연구의 수행까지 모색해야 합니다.

셋째, 기술사업화를 추구해야 합니다. 개발된 기술이 스핀오프(Spin-off)를 통해 유니콘(Unicorn) 기업 육성으로 이어지도록 노력한다면 우리나라의 혁신성장 및 안보 기술 분야 글로벌 시장 선점에 기여할 수 있을 것입니다.

아무쪼록 B·F·O 연구, 협업연구, 기술사업화를 통해 '안보기술연구센터'가 가까운 장래에 안보기술 분야에서 세계를 선도하는 연구기관으로 자리매김하기를 기원하며 대학 차원에서도 센터의 활동을 적극 지원하겠습니다.

마지막으로 '안보기술연구센터'의 관계자 모든 분에게 부탁을 드립니다. 우리가 개발하는 안보기술은 분쟁 일으키거나 공격이 아닌 방어를 위한 것이어야 하며, 국민과 인류의 번영과 행복을 위한 것임을 늘 명심하기 바랍니다.

다시 한 번 '안보기술연구센터'의 개소를 축하드리며, 센터의 성공적인 출발을 함께 준비해 주신 여러분의 노고에 감사드립니다.

2020. 1. 29.

KAIST 총장 **신 성 철**