



[기획연재] 미중 경쟁과 세계 정치 경제 질서의 변환 - 기술 편

사이버 안보와 미중 기술패권 경쟁: 그 진화의 복합지정학

김상배
서울대학교 교수

미중 기술패권 경쟁과 사이버 안보의 복합지정학

최근 미중갈등의 불꽃이 어느 한 영역에만 국한되지 않고 미중관계 전반으로 번져가는 양상을 보이고 있다. 그야말로 미중경쟁은 미래권력을 놓고 벌이는 패권경쟁을 방불케 한다. 이러한 면모를 단적으로 보여주는 사례가 선도부문(leading sector)인 '4차 산업혁명' 부문에서 벌어지는 양국의 기술 패권 경쟁이다. 역사적으로 해당 시기의 선도부문에서 벌어졌던 기술패권 경쟁의 향배는 패권국과 도전국의 승패를 가르고 국제질서의 구조를 변동시켰다. 오늘날 선도부문의 미중경쟁도 그러한 의미를 갖는다. 다만 이전의 경우와 다른 특징이 있다면, 지금의 경쟁은 사이버 공간을 매개로 한 네트워크 환경에서 진행되며, 이러한 과정에서 사이버 안보가 중요한 현안으로 불거졌다는 사실이다. 실제로 2010년대 초중반을 거치면서 사이버 안보는 명실상부한 국제정치학의 어젠다로 자리 잡았다.

이제 사이버 안보는 시스템 교란이나 지적재산의 탈취를 노리는 단순한 해킹의 문제를 넘어서 기술-산업-통상-데이터-정치군사-법제도-국제규범 등에 걸친 미래 패권경쟁의 복합적인 쟁점으로 진화하고 있다. 미시적 차원의 안전 문제일지라도 그 수량이 늘어나고, 여타 이슈들과 연계되면서, 거시적 차원의 지정학적 위기로 창발(創發)하는 신흥안보(emerging security) 현상의 전형적인 특징을 보이고 있다. 사이버 공격은 더 이상 해커들의 장난거리나 테러집단의 저항수단만은 아니다. 타국의 주요 기간시설에 대한 해킹의 이면에 국가 차원의 체계적 지원이 있음은 공공연한 비밀이 되었다. 국가안보를 이유로 사이버 안보에 위협이 되는 IT보안제품의 수출입 규제가 가해지며 데이터의 초국적 유통이 통제되기도 한다. 국제적으로도 사이버 안보는 동맹세력을 규합하는 명분이자 첨단 군비경쟁의 빌미가 된다.

사이버 안보 문제가 국가 간 갈등을 야기할 가능성이 커지면서, 전통 지정학의 시각을 원용하여 이 문제를 보려는 경향도 득세하고 있다. 실제로 사이버 공격의 문제는 전쟁 수행이라는 군사전략 차원에서 고려되고, 이를 지원하는 물적·인적 자원의 확보가 증시된다. 자국의 주요 기반시설을 노린 사이버 공격에 대해서는 맞공격을 가해서라도 억지하겠다는 행보가 힘을 얻고 있다. 그럼에도 사이버 안보의 세계정치는 과거의 현실에서 잉태된 전통 지정학의 시각을 그대로 적용하여 이해하기에는 너무나도 복잡한 양상으로 진화해 가고 있다. 이러한 문제의식을 바탕으로 이 글은 전통 지정학의 경계를 넘어서는 다양한 변수들을 포괄적으로 고려하는 새로운 시각으로 복합지정학(Complex Geopolitics)을 제안한다.

미중 사이버 안보 갈등의 진화: '중국 해커 위협론'에서 '중국산 IT보안제품 위협론'으로

길게 보면 사이버 안보를 둘러싼 미중갈등의 역사는 20여 년 전으로 거슬러 올라간다. 1999년 5월 미군이 유고 주재 중국 대사관을 오폭하여 당시 중국 해커들이 미국 내 사이트에 대해 보복 해킹을 가한 사건이 발생하였다. 2001년 4월 중국 전투기가 미군 정찰기와 충돌 후 중국 하이난에 추락하는 사고가 발생하자 중국 해커들이 사이버 공격을 감행하기도 했다. 당시 언론에서 '미중 사이버 전쟁'이라는 말이 처음으로 사용되기도 했다. 2003년 중국산으로 추정되는 웰치아 바이러스(Welchia virus)가 미국 정부 전산망을 공격하여 비자 발급업무가 일시 중단되는 일이 발생하고, 같은 해 미국 내 군사연구소와 미 항공우주국, 세계은행 등을 해킹한 '타이탄 레인 공격'은 미중 사이버 공방의 본격적인 신호탄이 됐다. 2009년에는 구글, 아도비, 시스코 등 30여개 미 IT기업들에 대한 중국 해커들의 대대적인 공격이 있었는데, 이는 '오로라 공격'으로 알려져 있다. 2011년의 '쉐이디 랫'(Shady RAT) 공격은 미국의 정부, 국제기구, 기업, 연구소 등 72개 기관에 대한 중국의 해킹 공격이었다.

미국의 주요 기반시설에 대한 중국 해커들의 공격은 2010년대로 넘어오면서 오바마 행정부로 하여금 군사적 방안까지 포함한 맞대응 카드를 꺼내들게 했다. 이른바 '중국 해커 위협론'은 2010년대 초중반 미중관계를 달구었던 뜨거운 현안 중의 하나였다. 2013년 미국의 정보보안업체인 맨디언트(Mandiant)의 보고서는, 1997년에 창설된 중국의 해커 부대인 61398부대가 미국의 기업과 공공기관을 해킹하여 지적재산을 탈취하고 있다고 폭로했으며, 이는 2014년 5월 미 법무부가 이들 61398 부대의 장교 5인을 기소하는 조치로 이어졌다. 이때에 즈음하여 오바마 행정부는 국가 기간시설에 대한 해킹을 국가안보 문제로 '안보화'(securitization)하고 때로는 미사일을 발사해서라도 대응하겠다는 '군사화'의 논리를 내세우며 사이버 안보를 국가 안보전략의 핵심 항목으로 격상시켰다. 급기야 사이버 안보 문제는 2013년 6월 미중 정상회담의 공식의제로 채택되는 상황에까지 이르렀다.

2017년 트럼프 행정부 출범 이후 미중 사이버 갈등은 좀 더 복잡한 양상으로 전개되었다. 예상과는 달리 미중 사이버 공방은 군사적 충돌로 비화되기보다는 오히려 산업과 통상 문제와 긴밀히 연계되는 양상을 보였다. 트럼프 행정부는 이른바 '중국산 IT보안제품 위협론'을 내세워 중국 기업들의 IT보안제품에 대한 규제를 강화했다. 특히 5G 이동통신 분야와 같은 4차 산업혁명 분야에서 기술경쟁력을 쌓고 있는 중국 기업들에 대한 미국의 견제가 가해졌다. 실제로 화웨이(华为), ZTE(中兴通讯), 차이나모바일(中国移动), DJI(大疆创新), 하이크비전(海康威视·Hikvision), 푸젠진화(福建晉華·JHICC) 등과 같은 중국 IT기업들이 미국 시장에 진출하는 과정에서 다양한 문제들이 빚미가 되어 발목이 잡혔다. 기술경쟁과 통상마찰의 외양을 한 이들 문제는 사이버 안보나 데이터 주권 등의 쟁점과 연계되면서 그 복잡성이 더해갔다. 국가안보의 함의가 큰 민군겸용기술(dual-use technology) 분야에서 벌어졌던, 과거 1990년대 미일 패권경쟁의 전례를 떠올리게 하는 양상이 벌어졌다.

화웨이 사태와 중국의 '5G 기술굴기'에 대한 미국의 견제

미중 사이버 안보 갈등의 가장 핵심적인 쟁점은 중국의 통신장비 업체인 화웨이를 둘러싼 논란이었다. 그전에도 미국 정부와 화웨이의 갈등은 없지 않았지만, 그것이 미중 양국의 기술패권 경쟁이라는 맥락에서 이해될 정도로 격화되기 시작한 것은, 2018년 2월 CIA, FBI, NSA 등 미국 정보기관들이 화웨이 제품을 사용하지 말라는 경고를 내리면서부터였다. 미국은 2018년 8월에는 <국방수권

법>을 통과시키며 미 공공기관 등에서 중국산 네트워크 장비의 사용을 금지했다. 2018년 12월에는 화웨이 창업자의 큰 딸인 명완저우(孟晚舟) 화웨이 최고재무책임자(CFO) 겸 부회장이 대이란 제재 위반 혐의로 체포되며 화웨이 장비 도입 문제를 둘러싼 미중 양국의 갈등은 클라이맥스에 다다랐다.

이른바 ‘화웨이 사태’로 불리는, 이러한 사이버 안보 논란의 과정에서 5G 이동통신 기술 분야에서 선두를 달리는 화웨이의 네트워크 장비가 표적이 되었다. 화웨이 장비가 이른바 백도어(backdoor)를 통해서 미국의 국가안보에 크게 영향을 미칠 수 있는 정보를 유출시킬 가능성이 있기 때문에 미국의 정부기관뿐만 아니라 민간 기업들도 이를 도입하지 말아야 한다는 것이었다. 4차 산업혁명 시대의 초연결 사회에서 화웨이 장비의 위험성은 단순한 기술의 문제가 아니라 국가안보의 문제라는 것이 강조되었다. 이러한 과정에서 화웨이 백도어가 실재하는 안보위협이라는 주장과 이는 단지 미국이 안보화의 과정을 통해서 구성해 낸 위협일 뿐이라는 주장이 팽팽히 맞섰다.

미국 정부가 주장하듯이 중국산 네트워크 장비의 도입은 보안위협이 될 수 있다. 특히 중국 정부의 지원을 받아 성장한 화웨이의 행보나 투명성이 부족한 기업문화와 성격을 보면 이러한 주장은 합리적 의심으로 인정될 수 있다. 그렇지만 정작 미국 정부가 보안위협의 객관적 증거를 제시하고 있는 것도 아니어서 문제의 복잡성이 커졌다. 이러한 공세에 대해 화웨어도 자사의 제품이 보안위협이 아니라는 명백한 증거를 제시하고 있는 것도 아니다. 화웨이의 입장은 자사 장비의 보안문제가 발생한 적이 아직까지 없으며, 만약에 문제가 발생한다면 회사 문이라도 닫겠다는 식이었다. 마치 ‘블랙박스’를 가운데 두고 누구 말이 맞는지 믿어달라고 말싸움을 벌이는 모습이였다.

화웨이의 통신장비가 미국의 국가안보에 실제 위협인지에 대해서는 논란의 여지가 있을지 몰라도, 화웨이로 대변되는 중국 기업들의 기술추격이 5G시대 미국의 기술패권에 대한 위협임은 분명하다. 화웨이 제품은 가격경쟁력을 보유하고 있을 뿐만 아니라 기술력도 세계 최고의 수준을 자랑하고 있으며, 2018년 현재 화웨이의 글로벌 이동통신 장비 시장점유율은 28%로 세계 1위이다. 화웨이 사태의 이면에 중국의 ‘5G 기술굴기’에 대한 미국의 견제의식이 강하게 깔려 있음을 추측할 수 있게 하는 대목이다. 특히 미국의 불만은, 중국이 기술기밀을 훔치거나 기술이전을 강요하는 행태를 보이면서 성장했다는 데 있다. 미국 정부가 ‘중국제조 2025’와 같이 중국의 정부 주도 정책에 불만을 제기하는 것도 비슷한 맥락에서 이해할 수 있다.

미국의 사이버 동맹외교와 그 균열

2019년에 접어들 무렵 미국 정부와 화웨이가 벌이는 실랑이는 국제적으로 그 전선이 확대되는 양상을 보였다. 2018년 말 트럼프 행정부는 ‘파이브 아이즈’(Five Eyes)로 대변되는 미국의 주요 첩보 동맹국들에게 화웨이 보이콧에 동참할 것을 촉구하였다. 마치 국제적으로 화웨이 장비가 발붙일 곳을 아예 없애려는 듯이 보이는 강경행보를 이어갔다. 이에 호응하여 호주와 뉴질랜드, 영국은 2018년 말 5G 공급망에서 화웨이를 배제하려는 움직임을 보였고, 캐나다는 중국과의 갈등을 무릅쓰고 미국의 요청에 따라 명완저우 부회장을 체포하는 조치를 취했으며, 일본 역시 정부조달 입찰에서 화웨이를 배제하기로 결정했다.

그런데 2019년 2월 하순을 거치면서 화웨이 장비를 사용하지 말라는 미국의 압박에 동참하는 듯이 보였던 미 우방국들이 국제공조의 전선에서 이탈하는 조짐을 보였다. 영국 국가사이버보안센터(NCSC: National Cyber Security Centre)가 화웨이 장비의 보안 위험을 낮출 수 있다는 결론을 내린

데 이어, 독일 역시 화웨이 장비를 배제할 계획이 없다고 밝혔다. 2018년 미국의 요청에 따라 화웨이를 배제했던 뉴질랜드의 경우는 총리가 직접 나서 입장 변화의 가능성을 내비치기까지 했다. 프랑스도 특정 기업에 대한 보이콧은 하지 않겠다는 입장을 내놨다.

이들 국가가 이탈한 데에는 5G 부문의 선두기업인 화웨이를 배제하고 5G 네트워크를 구축하는 현실적 부담 외에도 ‘미국 우선주의’를 내세우며 미중경쟁에서 무리하게 ‘내편 모으기’를 시도하는 미국에 대한 반발심이 작용했다. 파국으로 치달을 수도 있는 사태의 전개에 직면하여 트럼프 대통령은 2019년 2월 21일 자신의 트위터에 “더 선진화된 기술을 막기보다는 경쟁을 통해 미국이 승리 하길 바란다”며 그 동안의 강경자세를 다소 누그러뜨리는 제스처를 취했다. 사실상 미국의 반(反) 화웨이 전선이 와해된 것이 아니냐는 평가가 나오는 대목이었다.

그렇지만 화웨이 사태는 2019년 5월 14일 트럼프 대통령의 행정명령으로 새로운 국면에 접어들었다. 미국 당국은 국가안보를 위협한다는 이유로, 화웨이를 거래 제한 기업 리스트에 올렸고, 주요 민간 IT기업들에게 거래 중지를 요구했다. 트럼프 행정부는 화웨이와 거래하는 자국 기업의 피해를 최소화한다는 이유로 이러한 제재조치를 180일 간 유예했으나, 화웨이의 숨통을 죄기 위한 조치들은 여기서 그치지 않을 전망이다. 실제로 구글, 마이크로소프트, 인텔, 퀄컴, 브로드컴, 마이크론, 암(ARM) 등 주요 기업들은 화웨이와 제품 공급 계약을 중지하고 기술 계약을 해지하기도 했다.

5G 이동통신에서 드론과 CCTV로?

최근의 사태 전개는 민간 영역의 5G 이동통신 상용화와 관련된 화웨이 장비의 보안 문제를 넘어서 좀 더 군사적이고 정치적인 함의를 갖는 여타 기술과 산업 분야로 확산될 조짐마저 보이고 있다. 2019년 하반기에 접어들면서 미국은 화웨이에 이어 민간 드론 업체인 DJI와 CCTV 업체인 하이크비전에 대한 제재카드를 다시 꺼내 들었다. 되돌아보면, DJI는 2018년 9월 미국 기업의 특허를 침해했다는 논란이 일어 제재가 거론되었던 중국의 기업이며, 하이크비전은 2017년 11월 미 당국에 의해서 미국 시장 진출에 대한 우려가 제기된 바 있었던 중국의 기업이었다.

2019년 5월 20일 미국 국토안보부(DHS: Department of Homeland Security) 사이버안보·기간시설 안보국(CISA: Cybersecurity and Infrastructure Security Agency)은 중국의 드론이 민감한 항공 정보를 중국 본국으로 보내고, 중국 정부가 이를 들여다본다고 폭로했다. 이를 두고 CISA는 국가기관의 정보에 대한 ‘잠재적 위협’이라고 경고했다. CISA가 특정 드론을 거론한 것은 아니었지만, 사실상 중국의 DJI를 염두에 둔 발표였다. 이와 관련해서 DJI는 즉각 “우리 기술은 안전하다”고 반박했으나, CISA는 자국 소비자들에게 중국산 드론을 구입할 경우 신중해야 하며 인터넷 장비를 분리해야 한다는 방침까지 내놨다. 화웨이의 백도어에 대해서 제기되었던 기술안보 공방을 연상케 하는 조치였다.

한편 2019년 5월 22일 미국 정부는 중국의 CCTV 업체 하이크비전을 상무부 기술수출 제한목록에 올리는 것을 검토 중이라고 보도했다. 하이크비전은 CCTV 제작기술에서 세계적으로 앞서 갈 뿐만 아니라 안면 인식이나 사람들의 버릇과 신체특성 등을 고려해 특정 인물을 식별하는 기술로 유명하다. 중국 정부는 이러한 기술을 감시도구로 활용해서 소수민족이나 반체제 세력을 통제하는데 적극 활용하고 있다. CCTV의 하이크비전에 대한 압박은 미국이 중국의 기술굴기를 견제하고 중국 정부와 IT기업의 유착을 질타하는 차원을 넘어서, 천안문 사태 30주년을 맞이한 중국의 인권 문제를 겨냥했다는 해석을 낳았다.

데이터 주권과 사이버 공간의 국제규범 문제

이상에서 살펴본 미중 사이버 갈등의 이면에는 데이터 안보에 대한 이해관계도 걸려 있다. 2013년 에드워드 스노든 사건 이후 개인정보보호와 데이터 안보는 미중 국가안보의 쟁점이 됐다. 미국의 다국적 기업에 의한 데이터 유출의 경계는 중국에서 <인터넷안전법>을 출현시켰다. 이 법에 의하면, 중국에서 수집된 개인정보를 다루는 외국 기업들은 반드시 중국 내에 데이터 서버를 두어야 하며, 사업상의 이유로 데이터를 해외로 옮기려면 중국 공안당국의 보안평가를 받아야 한다. 미국 기업들의 중국 내 서비스를 검열·통제하고, 개인정보가 담긴 데이터의 국외 이전을 데이터 주권이라는 명목으로 금지하려는 취지로 해석되었다. 이 법은 2018년 7월부터 본격 시행됐지만 외국 기업들이 반발해 법 시행이 2019년 초로 유예되기도 했다.

실제로 이 법에 의거해서 중국 정부는 구글을 비롯한 페이스북, 유튜브, 인스타그램, 와츠업 등의 외국 기업들의 인터넷 서비스를 규제했다. 2017년 7월 31일 애플은 중국 앱스토어에서 인터넷 검열시스템을 우회하는 가상사설망(VPN: Virtual Private Network) 관련 애플리케이션 60여 개를 삭제해야만 했다. 또한 아마존웹서비스(AWS: Amazon Web Services)도 2017년 11월 중국사업부 자산을 매각했다. 2018년 초 마이크로소프트와 아마존은 자사 데이터를 각기 베이징과 닝샤의 데이터센터로 옮겼다. 또한 <인터넷안전법> 시행 직후 애플도 중국 내 사용자들의 개인정보와 관리권을 모두 중국 구이저우 지방정부에 넘겨야 했으며, 2018년 2월에는 제2데이터센터를 중국 네이멍 자치구에 건설할 계획을 발표했다.

이러한 중국의 행보가 인터넷을 대하는 미중 양국의 정책과 이념의 차이를 반영하는 것이었다면, 2014년부터 시작해서 2018년의 제5회에 이르기까지 중국이 저장성 우전(烏鎮)에서 개최하고 있는 ‘세계인터넷대회’(World Internet Conference)는 사이버 공간의 국제규범 형성에 대한 양국의 입장 차이를 보여주는 사례이다. 중국의 세계인터넷대회 개최는 글로벌 인터넷 거버넌스에 대한 미국의 주도권에 맞불을 놓으려는 의도를 담고 있다. 출범 당시부터 세계인터넷대회는 ‘사이버공간총회’로 대변되는 서방 진영의 행보에 대항하는 성격을 띠었다. 특히 2013년 스노든 사건 이후 중국은 글로벌 인터넷 거버넌스를 주도하는 미국을 견제하고, 중국이 주도하는 비(非)서방 국제진영을 결집하고자 했다. 미국이 주도하는 현행 체제 하에서는 중국의 사이버 주권이 제약될 수밖에 없다는 인식을 바탕으로 한 도전적 행보였다.

이러한 태세의 이면에는 중국 국내체제의 성격뿐만 아니라 사이버 공간의 미래질서를 보는 중국의 구상이 담겨 있다. 이러한 구상은 서방 진영에 대항하여 사이버 공간의 독자적 관할을 모색하는 세계인터넷대회의 정치적 비전과도 통한다. 아마도 중국의 속내는 미국이 주도하는 체제에 단순히 편입하기보다는 중국이 중심이 되는 새로운 질서를 구축하는 데 있을 것이다. 사이버 공간의 미래질서를 구축하는 과정에서 ‘아메리칸 드림’을 대신하여 ‘중국몽’(中國夢)을 밑그림으로 삼고 싶을 것이다. 아마도 그 과정은 과거 화려했던 중국의 천하질서(天下秩序)를 디지털 시대로 옮겨와서 재현하려는 시도일 가능성이 크다.

미중 복합지정학적 경쟁 속의 한국?

복합지정학의 시각에서 본 미중 사이버 안보 갈등은 다양한 영역에 걸쳐서 진화하고 있다. 제일 눈에 띄는 것은 기술패권 경쟁이라는 명목으로 벌어지는 지정학적 경쟁이다. 이는 화웨이 사태와

같은 사이버 안보 논란뿐만 아니라 여타 민군겸용기술과 관련된 정치·군사안보 문제와 연계될 조짐을 보이고 있다. 이러한 갈등은 표면적으로는 미국의 기술경쟁력 하락에서 비롯된 양국 간 통상마찰 문제와 이에 수반된 보호주의적 법·제도의 마찰 문제로 나타나고 있다. 게다가 이렇게 복합적인 양상을 보이는 미중 사이버 갈등의 전면에서 첨단기술의 문제를 국가안보 문제로 ‘안보화’하는 미중 두 나라의 안보담론 경쟁이 벌어지고 있다. 이러한 안보담론 경쟁을 통해 미중 양국은 동맹국들을 결속하고 자국에 유리한 사이버 공간의 국제규범을 마련하려는 경쟁을 벌이고 있다.

이렇듯 복잡지정학적 지평을 펼쳐놓고 있는 미중경쟁에 한국은 어떻게 대응해야 할까? 최근 어느 국내업체의 화웨이 장비 도입을 둘러싼 논란에서도 나타난 바와 같이, 미중 사이버 안보 갈등은 단순한 기술과 산업의 문제가 아니라 안보와 정치의 문제로 다가올 가능성이 있다. 자칫 미중 기술패권 경쟁이 그 사이에 낀 한국에 지정학적 위기를 야기하는 상황이 벌어질지도 모른다. 다시 말해, 미중 사이버 경쟁은 한국으로 하여금 단순한 기술 선택의 문제가 아니라, 전통적인 동맹과 외교의 문제를 포함한, 좀 더 복잡한 지정학적 선택을 강요할 가능성도 없지 않다. 요컨대, 복잡지정학의 시각에서 미중 기술패권 경쟁의 진화과정을 제대로 읽어내서 이에 대한 적절한 대응책을 마련하는 지혜가 절실하게 필요한 시점이다. ■

■ **저자: 김상배** _ 서울대학교 정치외교학부 교수. 서울대학교 외교학과를 졸업하고 미국 인디애나대학교에서 정치학 박사 학위를 취득했다. 주요 연구분야는 국제관계에서 정보, 통신, 네트워크 등이다. 주요 저서로는 <버추얼 창과 그물망 방패: 사이버 안보의 세계정치와 한국> (2018), <아라크네의 국제정치학: 네트워크 세계정치이론의 도전> (2014), <정보혁명과 권력변환: 네트워크 정치학의 시각> (2010), <정보화시대의 표준경쟁: 인텔리즘과 일본의 컴퓨터산업> (2007) 등이 있다.

■ **담당 및 편집:** 김세영 EAI 연구원
문의: 02-2277-1683 (ext. 208) sykim@eai.or.kr

- 인용할 때에는 반드시 출처를 밝혀주시기 바랍니다.
- EAI는 어떠한 정파적 이해와도 무관한 독립 연구기관입니다.
- EAI가 발행하는 보고서와 저널 및 단행본에 실린 주장과 의견은 EAI와는 무관하며 오로지 저자 개인의 견해를 밝힙니다.

발행일 2019년 8월 23일

[EAI 특별기획논평 시리즈] 미중 경쟁과 세계 정치 경제 질서의 변환 - 기술 편

“사이버 안보와 미중 기술패권 경쟁: 그 진화의 복잡지정학” 979-11-90315-03-6 95340

재단법인 동아시아연구원
04548 서울특별시 중구 을지로 158, 909호 (을지로4가 삼풍빌딩)
Tel. 82 2 2277 1683 Fax 82 2 2277 1684

Email eai@eai.or.kr Website www.eai.or.kr