ISSUE PAPER 2015-18

신흥안보의 부상과 과학기술의 역할

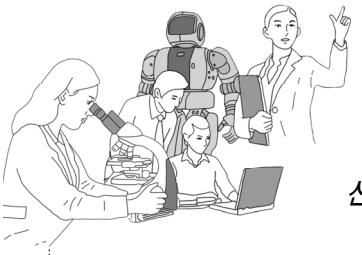
김상배

KISTEP 한국과학기술기획평가원
Korea Institute of S&T Evaluation and Planning

ISSUE PAPER 2015-18

신흥안보의 부상과 과학기술의 역할

김상배



발간사

글로벌화, 정보화 등 세계 환경 변화는 에너지・환경, 원자력, 사이버, 보건・식량, 이주・난민 등 신흥 안보(emerging security) 분야의 위협이 국경을 넘어서 급부상하는 조건을 창출했다. 신흥 안보 위협은 20세기 냉전 시대를 지배했던 국가 단위의 군사안보 개념만으로는 우리 삶과 사회 공동체를 안전하게 꾸려나갈 수 없게 하고 있다. 안보 패러다임의 새로운 전환이 모색되어야 하는 시점에 도달한 것이다. 이러한 변화에도 불구하고 우리의 안보 체계는 여전히 전통안보에 머물러 있는 듯하다. 남북한 대결의 시대를 사는 우리에게 전통 안보는 여전히 중요하지 않을 수 없다. 그러나 전통안보와 신흥안보의 이슈가 복잡하게 얽혀 있는 소위 '위협 융합(threat convergence)'의 시대를 적절히 대응하지 않고서는 더 큰 위험에 봉착할 수도 있다. 특히, 신흥 안보 분야 중 많은 분야는 과학기술의 발전을 통해 야기되거나, 과학기술을 통해 해결할 수 있는 분야이다. 이러한 측면에서 신흥 안보 분야의 이슈를 발굴하고, 이를 효율적이고 효과적으로 대응할 수 있는 거버넌스와 과학기술의 역할에 대한 논의가 시작되어야 한다.

이러한 문제의식을 바탕으로 본 이슈페이퍼는 새롭게 부상하는 신흥 안보의 성격과 과학기술이 담당할 역할을 제시하고 있다. 과학기술계에서는 생소할 수 있는 신흥 안보에 대한 이해를 제고하고, 과학기술의 기여와 역할을 모색할 수 있는 계기가 될 것으로 기대해 본다.

끝으로 본 이슈페이퍼의 내용은 필자의 개인적인 견해이며, KISTEP의 공식적인 의견이 아님을 밝힌다.

2015년 12월

한국과학기술기획평가원 원장 박 영 아

Ⅰ. 머리말 : 새로운 안보 패러다임의 부상

- 탈냉전, 지구화, 정보화 등을 배경으로 한 초국적이고 글로벌한 차원에서 발생하는 문제들의 증가는 국민국가 단위에서 주로 군사안보를 중시하는 전통안보의 발상과 개념만으로는 파악할 수 없는 새로운 위협을 생성하고 있음

  - 지난 5년여 동안 기후변화와 자연재해, 후쿠시마 원전 사태, 북한의 사이버 공격과 미·중 사이버 갈등, 에볼라와 메르스(MERS) 발병과 확산 등과 같은 새로운 위협에 대한 국가사회적 관심이 증대됨

    * 이밖에도 에너지 안보, 식량안보, 인구안보(저출산 · 초고령 사회) 등의 문제도 새롭게 관심을 끌고 있음

  - 천재지변의 형태로 발생하는 안보의 위협 외에도 정치적, 사회적, 문화적 맥락에서 발생하는 초국적 위협 요인들에 대한 관심도 커지고 있음

    * 동북아 차원에서만 보아도 난민안보와 탈북자, 통일과 사회통합, 민주화와 인권, 청년실업과 경제양극화, 문화정체성의 위기 등이 제기됨

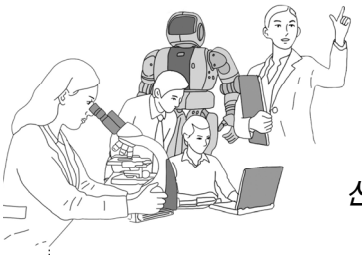
  - 이러한 초국가적이고 글로벌한 위협 요인들의 증가는 단순한 전문영역의 쟁점을 넘어서 국가안보에 영향을 미치는 새로운 위협으로 인식되고 있음

    * 기존의 전통안보 관념만으로는 이러한 위협의 본질을 제대로 파악할 수 없다는 현실이 또 다른 과제를 낳고 있음

- 이러한 맥락에서 볼 때 기존의 전통안보의 발상을 넘어서 새로운 안보 위협을 개념화하는 노력의 필요성이 제기됨

  - 새로운 안보 위협의 급속한 확산은 전통안보(traditional security)와 대비되는 의미에서 비전통 안보(non-traditional security)라고 개념화되었던 종전의 소극적인 시도를 넘어서 신흥안보(emerging security)라는 좀 더 적극적인 개념화의 시도를 벌이게 함

    * 신흥안보의 개념은 일국 단위를 넘어서 발생하는 초국적이고 글로벌한 안보 문제, 예를 들어 원자력안보, 보건안보, 사이버 안보, 에너지 · 환경안보, 식량안보 등과 같은 새로운 위협의 증대를 배경으로 출현함



- 이러한 신흥안보의 이슈들은 국가 간의 갈등을 유발하는 전통안보 이슈들과 연계되면서 그 위협의 위력이 확대되고 있음

  * 오늘날에는 그야말로 전통안보의 이슈와 신흥안보의 이슈가 밀접히 연계되는 '위협융합(threat convergence)'의 시대를 맞이하고 있음

● 신흥안보의 개념은 이슈영역의 확대뿐만 아니라 안보 문제를 인식하고 해결하는 행위자의 숫자와 범위의 확대 및 안보 영역에서 벌어지는 권력게임의 양상의 변화도 배경으로 하여 출현하였음

- 다시 말해 신흥안보 게임에서는 국가 행위자 이외에도 국제기구, 다국적 기업, 글로벌 시민사회 등과 같은 비(非)국가 행위자의 역할이 늘어나고 있음

  * 또한 신흥안보 분야에서는 개별 국가의 대응노력과 함께 지역 거버넌스 및 글로벌 거버넌스를 구축하려는 노력이 중요함

- 이렇듯 위협의 성격과 범위뿐만 아니라 그 해결에 나서는 행위자의 확대라는 차원에서 볼 때 신흥안보의 출현은 단순히 전통안보의 틀에 잡히지 않던 새로운 안보 문제의 등장이라는 차원을 넘어서 새로운 '안보 패러다임(security paradigm)'의 부상이라는 관점에서 이해해야 하는 문제임

● 새로운 안보 패러다임의 부상에 직면하여 한국의 안보 거버넌스는, 최근의 변화 노력에도 불구하고, 여전히 전통안보에 대응하는 발상 위주로 추진되는 경향을 보이고 있음

- 전통안보와는 질적으로 다른 성격을 지닌 신흥안보의 본질을 제대로 이해하고 적절히 대응하지 않고서는 더 큰 총체적인 위험에 봉착할 우려가 있음

  * 신흥안보 문제의 중요성을 인식하고, 이슈별 위협의 성격을 정확히 이해하는 발상의 전환과 추진체계의 정비가 시급히 필요함

  * 아울러 신흥안보 이슈에 대처하는 정부의 역할뿐만 아니라 민간 행위자들의 참여를 독려하고 그 역할을 적극적으로 설정하는 발상과 노력이 필요함

- 그럼에도 최근 정부가 추진하는 안보 관련 대응체계 마련의 움직임을 보면 신흥안보의 특성에 대한 이해뿐만 아니라 좀 더 구체적인 실천방안 도입이 미흡함

* 예를 들어, 사이버 안보 컨트롤타워 구축 과정과 원자력안보, 보건안보 등에 대한 대응양식을 보면, 이들 신흥안보가 지닌 고유한 특성, 예를 들어 그 위협의 기원이 되는 (또는 해결의 실마리가 되는) 과학기술적 특성에 대한 이해가 부족함

* 다양한 신흥안보 분야의 이슈별 위협의 성격을 정확히 이해하고 구체적인 대응방안을 모색하는 차원에서 과학기술의 역할을 자리매김하는 작업은 의미가 있음

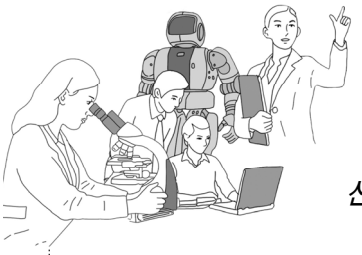
- 본 이슈페이퍼에서는 새로운 안보 패러다임을 개념화하는 차원에서 신흥안보의 부상과 이러한 구도 속에서 과학기술의 역할을 설정하는 작업을 필치고자 함

  - 탈냉전 이후 국내외에서 이루어졌던 새로운 안보이론들을 검토하고 이 글에서 제시하는 신흥안보에 대한 논의가 지닌 연구사적인 위상을 설정

  - 복잡계 이론의 개념적 논의를 원용하여 '신흥'의 의미와 '안보'의 개념, 그리고 신흥과 안보의 조합을 통해서 만들어진 신흥안보의 개념 고찰

  - 신흥안보가 단순한 미시적 안전의 문제가 아니라 거시적 안보의 문제로 창발하는 과정에서 발생하는 글로벌 위험 요인들의 스펙트럼 분석

  - 신흥안보 분야에서 과학기술이 담당해야 할 적절한 역할에 대한 논의를 사이버 안보 분야 사례를 통해 제시



Ⅱ. 코펜하겐 학파의 안보론을 넘어서

코펜하겐 학파의 복합안보론

탈냉전 이후 안보론은 군사안보에 치중해온 전통안보의 개념을 넘어서 비군사적 영역에서 제기되는 안보 문제에 관심을 가지면서 부상

- 실제로 탈냉전 시대에는 국지전과 내전, 테러, 경제적 위협과 난민 등과 같이 냉전 시대와는 전혀 다른 양상의 위협들이 제기되었음

  * 이처럼 위협의 양태가 빠르게 바뀌면서 전통안보의 개념은 더 이상 적절한 개념적 도구가 아니라는 인식의 확산됨

- 특히 과거의 안보론에서는 큰 비중을 두지 않았던 신념체계와 주관적 의식 등에 대한 관심이 크게 늘기 시작함

  * 주류 안보이론이 기반을 이루고 있는 현실주의 국제정치이론의 시각에 대안을 제시하는 구성주의(constructivism) 시각에서 본 안보담론을 바탕으로 함

이렇게 전통 안보론을 넘어서려는 대표적인 시도는, 베리 부잔(Barry Buzan) 등으로 대표되는 이른바 코펜하겐 학파(Copenhagen School)의 안보론에서 찾을 수 있음

※ 코펜하겐 학파로 분류되는 안보이론가들의 저작으로는 Buzan et al.(1998), Buzan and Hensen(2009), McSweeney(2007), Huysmans(2007), Hough, Malik, Moran and Pilbeam(2015) 등을 참조

- 코펜하겐 학파는 탈냉전기의 변화하는 안보 환경을 개념화하는 차원에서 기존 안보이론의 국가 중심성과 군사안보 중심성을 비판하고 탈냉전기 안보의 복합성과 안보담론의 규범성을 지적한 것으로 유명함.

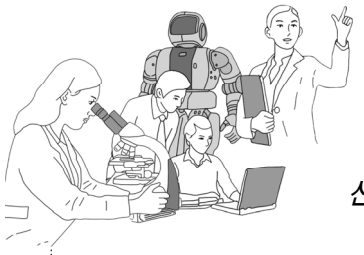
- 특히 코펜하겐 학파의 안보화(securitization) 개념은 안보담론이 사회적으로 형성되는 과정을 지칭하는 개념으로서 구성주의 시각에서 안보행위를 이해하는 데 기여함

※ 안보화 이론에 대해서는 Wæver et al.(1993), Wæver(1995), Balzacq ed.(2011), Hansen and Nissenbaum(2009) 등을 참조

- 코펜하겐 학파의 안보화 이론에 의하면, 안보란 객관적(또는 주관적)으로 실재하는 어떤 조건이라기보다는 현존하는 위협이 무엇인가에 대한 사회적 합의를 간(間) 주관적으로 구성하는 정치적 담론임
  - 다시 말해, 안보는 객관적으로 존재하기보다는(또는 존재하더라도) 안보 행위자에 의해서 현존하는 위협의 대상, 즉 안전이 보장되어야 할 안보의 대상이 무엇인지를 정치적으로 쟁점화하는 과정에서 구성되는 것이라는 인식을 제시함
    * 이러한 과정에서 안보화란 어떤 문제에 여타 비(非)안보 문제가 결여하고 있는 지위와 우선성을 부여하여 그것을 '안보 문제'로서 구성하는 과정임
  - 이러한 시각에 입각할 때, 보통의 경우라면 직접적인 위협으로 간주되지 않았을 문제라도 안보 행위자에 의해서 중대한 위협으로 부각되고 비상의 조치를 강구하는 정치적 행위의 계기가 될 수 있음
- 한편 탈냉전 시대 코펜하겐 학파의 안보론이 제기한 성과 중의 하나는 사회안보(societal security) 개념의 제시에서도 발견됨
  - 사회안보의 개념은 국가와 더불어 시민사회가 안보주체로 중요하다는 점을 인식하는 데서 출발함
    * 사회안보는 사회의 정체성(identity)을 강조하는데, 이러한 점에서 정체성 변수가 안보 문제와 어떻게 연결되는가의 문제를 제기함
  - 사회안보는 변화하는 환경이나 실재하는 위협 하에서도 본질적인 속성을 유지하는 사회의 능력을 유지하는 데 관심을 둠

코펜하겐 학파에 대한 비판

- 코펜하겐 학파의 안보론은 1990년대 탈냉전기를 시대적 배경으로 하고 유럽을 지역공간적 배경으로 하여 출현한 안보론이라는 측면에서 비판적으로 인식할 필요성도 있음
  - 시대적 배경이라는 측면에서 코펜하겐 학파의 안보론이 탈냉전 안보론을 모색했다면, 오늘날의 안보론은 좀 더 본격적으로 지구화와 정보화를 배경으로 하는 복합 네트워크 시대의 안보 현상을 개념화해야 함



- 지역공간이라는 차원에서 코펜하겐 학파의 안보론이 유럽에서의 안보 경험을 바탕으로 이를 보편화하려는 시도를 펼쳤다면, 오늘날의 안보론은 유럽 이외 지역의 특수 안보 문제를 좀 더 적극적으로 포함하여 보편이론을 개발하려는 시도를 보여야 할 것임

- 코펜하겐 학파가 화행(speech-act) 행위를 통한 안보화(securitization)의 구성주의적 메커니즘을 주로 탐구했다면, 신흥안보론은 안보현실(security reality) 자체에서 발생하는 실제 변환을 좀 더 구체적으로 다루려는 시도라고 할 수 있음

  - 이러한 차이를 굳이 명명하자면 코펜하겐 학파의 '위협의 사회적 구성론'과 21세기 신흥안보론의 '위협의 객관적 창발론'이라고 할 수 있음

    * 다시 말해 21세기 신흥안보론은 미시적 '안전' 문제에서 거시적 '안보' 문제가 실제로 창발하는 좀 더 구체적인 안보 현실의 변화를 문제시함.

  - 이러한 맥락에서 볼 때 코펜하겐 학파가 복합안보라는 이름으로 위협요인들을 나열하는데 그쳤다면, 신흥안보론은 여러 가지 위협요인들이 서로 얽히면서 안보를 위협하는 변수로 창발하는 구조를 밝히는 데 초점을 둠

  - 이러한 과정에는 위협의 주체로서 인간 행위자이외에도 물리적 환경이나 과학기술의 도구 등과 같은 비인간(non-human) 행위자의 역할도 고려해야 한다는 문제제기를 함

    * 오늘날의 신흥안보론에서는 컴퓨터 시스템이나 전염병 바이러스 등과 같은 비인간 행위자의 행위능력(agency)에 대한 많은 관심을 기울임

- 지역공간의 배경이라는 차원에서 볼 때 코펜하겐 학파는 주로 유럽의 안보현실을 설명하는 데 주안점이 있었음

  - 따라서 코펜하겐 학파의 논의를 그대로 적용하여 동아시아 안보현실을 분석하는 시도를 벌이기에는 두 공간의 현실과 코펜하겐 학파 이론의 간격이 존재하는 것이 사실임

    * 즉 코펜하겐 학파에 의한 위협의 개념화와 해법의 제시는 모두 탈냉전과 탈근대의 과제를 안고 있는 유럽의 현실에서 잉태된 문제의식을 바탕으로 함

- 이러한 시각에서 보면 코펜하겐 학파에서는 중요한 안보 문제일지라도, 근대의 숙제와 함께 탈냉전 및 탈근대의 도전을 동시에 맞고 있는 동아시아의 맥락에서는 안보의 우선순위 설정이 다르게 나타날 가능성이 큼

  * 예를 들어 코펜하겐 학파가 제시하는 유럽에서의 사회안보(societal security)의 문제는 동아시아에서는 그 정도와 형태가 다르게 체감되고 있음

- 요컨대 동아시아와 한반도의 안보상황이 코펜하겐 학파에서 상정하는 모습보다도 훨씬 더 복잡한 형태로 전개되고 있음을 고려한 안보론이 필요함

신흥안보론의 국내적 기원

- 이러한 문제의식을 염두에 둘 때 1990년대부터 국내에서 발전해온 복합세계정치론과 복합안보론의 시도에 주목할 필요가 있음(민병원, 2012).

  - 1990년대 초반 탈냉전기 초기에 국내 학계에서 제기된 '복합안보'의 개념은 근대의 프로젝트가 완성되지 않은 상황에서 곧바로 탈근대의 물결을 맞이해야만 했던 한반도의 이중적 과제를 담아내려는 시도였음(하영선 편, 1993)

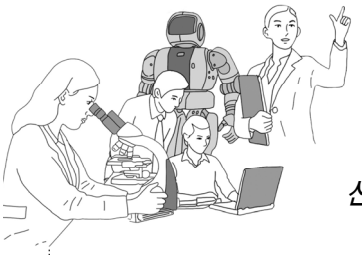
    * 당시 '복합안보' 개념은 초강대국의 쇠퇴와 지역 안보질서의 자율성 증가, 국제기구의 역할 증가 등과 같은 행위주체의 변화와 행위영역의 변화를 동시에 담아내려는 문제제기였음

  - 이러한 점에서 한반도와 동아시아의 근대-탈근대의 복합성을 고려한 '복합안보'의 개념은 탈냉전이라는 맥락에서 안보주체와 안보대상의 다양성을 강조한 코펜하겐 학파의 문제의식을 앞서가는 것이었음

    * 근대와 탈근대의 병존 그리고 그로 인해 야기되는 복합 안보질서의 모습은 21세기에도 여전히 동아시아와 한반도의 안보담론을 자극하는 독특한 성격으로 작동하고 있음

- 2000년대 중후반 코펜하겐 학파의 복합안보론을 수용하면서도 이를 보완하고 비판하려는 국내학계의 시도에도 주목할 필요가 있음

  - 코펜하겐 학파의 안보개념을 동아시아의 맥락에 적용한 비전통 안보(non-traditional security, NTS)나 지역 안보 복합체(regional security complex)의 논의가 있었음



※ 코펜하겐 학파의 국내적 수용에 대해서는 민병원(2006)을 참조. 동아시아 맥락에서 본 비전통 안보론에 대해서는 이신화(2006)를 참조.

- 한편 코펜하겐 학파의 이론을 뛰어넘는 새로운 안보 패러다임으로서 네트워크 사고와 위험사회 개념의 도입 필요성을 강조한 시도에도 주목할 필요가 있음(민병원, 2007).

* 새로운 안보 패러다임의 문제제기는 구조적 차원에서 세계정치가 네트워크화되어 가는 추세와 복합적인 세계위험사회(world risk society)의 부상이라는 인식을 바탕으로 함

※ 울리히 벡(Ulrich Beck)이 제창한 세계위험사회의 개념은 초국가적 상호연계성이 심화되고 불확실성과 불안정성이 증대되는 현실 속에서 빠른 전파력과 예측 불가능한 폭발성을 지닌 21세기 안보 문제의 위험성을 지적함(Beck, 2005)

- 오늘날의 안보에 대한 위협이 네트워크의 속성을 지니고 있음을 지적하는 국내 학계의 연구는 2010년대에 이르러 '복합 세계정치'와 '네트워크 세계정치'에 대한 이론화의 작업을 바탕으로 지속됨(하영선 · 김상배 편. 2010; 2012; 김상배. 2014).

- 네트워크의 시각에서 본 안보론의 문제제기는 각각의 안보 이슈들이 네트워크라는 맥락에서 어떻게 복합되는지에 대한 공식과 새로운 환경에 적합한 작동 메커니즘을 밝히려는 '네트워크 안보(network security)'에 대한 논의와 통함

* 이는 기존의 복합안보론에서 취했던, 탈냉전 이후 새로이 부상한 안보 이슈들을 망라하는 방식을 넘어서는 문제의식이라고 할 수 있음

- 이러한 네트워크 안보의 개념은 미시적 '안전' 문제에서 거시적 '안보' 문제가 창발하는 과정 및 이를 가능케 하는 현실의 구조를 탐구하려는 신흥안보론의 문제의식과도 통함

* 물론 이러한 신흥안보로서의 네트워크 안보의 개념은 근대적인 의미의 전통안보와 탈근대적인 의미의 비전통 안보를 함께 고려해야 한다는 국내 복합안보론의 문제의식을 바탕에 깔고 있음

- 이러한 의미에서 보면 신흥안보의 개념은 복합안보와 네트워크 안보의 개념이 제시한 문제의식을 모두 반영하는 방향으로 모색되어야 할 것임

Ⅲ. 신흥안보, 그 창발의 개념화

신흥(新興, emergence)과 안보(安保, security)

신흥안보의 개념을 살펴보기에 앞서 먼저 신흥과 안보, 그리고 신흥안보의 말뜻을 이해하는 것이 의미가 있음

- 먼저 '신흥'의 의미를 한자 형성문자의 의미를 살펴보는 것이 흥미로움

  * 신(新)은 도끼(斤)로 나무를 베어 땔나무를 만들어 쌓아 놓는다는 뜻인데, 이는 베다→새롭다→새롭게 하다 등으로 뜻이 전성되었음

  * 흥(興)은 동(同)과 여(舁)의 합성어인데, 이는 여럿이 들어 올리다, 일으키다, 일어나다를 뜻함

  * '신'과 '흥'의 합성어로서 '신흥'은 새롭게 일어나다는 뜻 정도로 이해할 수 있음

- 그러나 신흥안보에서 안보를 수식하는 형용어로 사용한 '신흥'이라는 말은 단순히 '새롭게 일어나다'라는 뜻만은 아님

  * 다시 말해 신흥안보라는 말은 예전에는 없었는데 최근 새롭게 등장한 안보, 즉 '신(新) 안보'라는 의미를 넘어서는 좀 더 복잡한 뜻을 담고 있음

이 글에서 사용하는 '신흥(新興)'은 복잡계 이론에서 말하는 'emergence'의 번역어임.

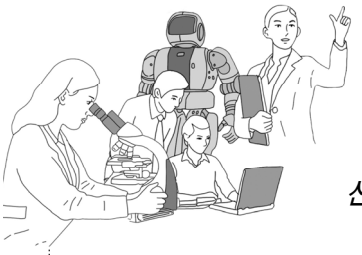
- 'emergence'는 국내 자연과학계에서 흔히 창발(創發)이라고 번역되는데 이 글에서는 안보라는 말과의 합성을 고려하여 '신흥'이라고 번역하였음.

  ※ 그러나 'emergence'라는 용어를 안보와 합성하지 않고 따로 사용하는 경우에는 학계에 이미 통용되고 있는 창발이라는 용어를 사용하였음

  * 창(創)은 칼(刂=刀)로 상처를 내다(倉) 또는 시작하다의 뜻

  * 발(發)은 발을 좌우로 벌리고(癶), 활(弓)로 물건을 치거나 튀기게 한다는 뜻

- 글자 자체로서 창발의 뜻은 새로이 일을 시작한다는 정도의 의미로 이해할 수 있음



- 그러나 개념어로서 복잡계 이론에서 말하는 창발(emergence)이란 복잡계에서 자기조직화의 과정을 통해 새롭고 일관된 구조나 패턴, 속성 등이 나타나는 현상을 의미함

  - 창발이란 미시적 단계에서는 볼 수 없던 존재들, 즉 자체적인 속성을 드러낼 수 없던 소규모・단순한 존재들이 복잡한 상호작용을 통한 연계성의 증대에 의해서 거시적 단계에서는 일정한 패턴(pattern)과 규칙성(regularities)을 드러내는 것을 의미함.

    * 창발 현상은 비선형성(non-lineality), 자기조직화(self-organization), 비평형(far from equilibrium), 유인자(attractors) 등을 특징으로 하는 복잡계 현상을 배경으로 해서 발생함

  - 다시 말해 창발이란 미시적 단계에서는 무질서한 카오스(chaos)였지만 자기조직화(self-organization)의 과정을 통해서 거시적 단계에서는 질서(order)가 생성되는 것을 의미함

    * 생물계 현상에서 창발의 사례로서 가장 많이 거론되는 것은, 전체 디자인이 없이도, 지능이 낮은 개별 개미들의 활동을 통해서 건설되는 거대한 개미탑을 들 수 있음

    * 물리현상에서 발견되는 창발의 사례로는 눈송이에서 발견되는 복합적인 대칭 구조, 즉 프랙털(fractal) 패턴의 형성을 들 수 있음

- 복잡계 이론 진영에서는 많은 이론가들에 의해서 창발(emergence)과 유사한 개념들이 많이 제시되어 왔음

  - 일리야 프로고진(Ilya Prigogine): 요동을 통해서 생성되는 질서(order through fluctuation)

  - 스테판 볼프램(Stephen Wolfram): 카오스에서 질서로 바뀌는 상전이(phase transition)와 생명의 질서를 가능케 하는 '카오스의 가장자리(edge of chaos)'

  - 움베르토 마투라나(Humberto Maturana): 자기생성(autopoiesis)

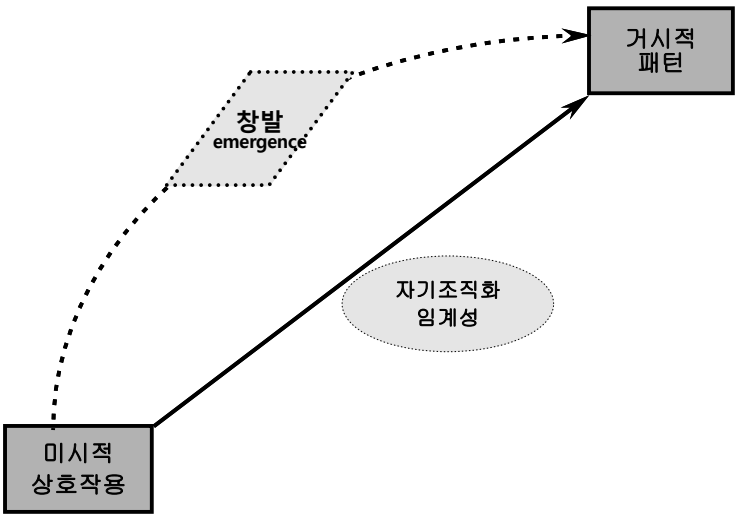
  - 페르 박(Per Bak): 자기조직적 임계성(SOC, self-organized criticality)

    * 시스템의 거시적 격변(catastrophe) 현상은 자기조직적 임계현상으로서 갑작스럽게 발생하는 듯 보여도 그 내부에서는 복잡한 상호작용이 끊임없이 이루어지고 있는 현상으로 이해해야 함. 지진, 산불, 도시의 발달, 생태계 붕괴, 전쟁, 혁명 등의 사례

  - 토마스 셸링(Thomas Shelling): 미시적 동기와 거시적 행위

    * 인간사회의 다양한 영역에서 미시적 규칙의 반복을 통해 혁명, 전쟁, 협력 등 거시적 현상이 생성됨을 설명. 백인과 흑인 거주 지역의 분리 현상을 설명한 사례.

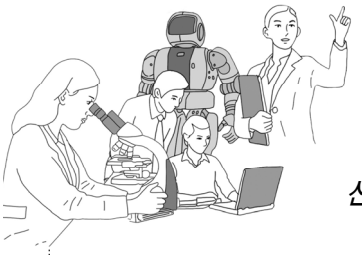
- 말콤 글래드웰(Malcolm Gladwell): 자기조직적 임계성의 응용 사례로서 티핑 포인트(tipping point)의 개념을 경영학의 마케팅에 적용



〈그림-1〉 창발(emergence)

- 이러한 창발의 개념에 입각해서 볼 때, 신흥안보란 미시적 차원에서는 단순히 소규모 단위의 안전(安全, safety)의 문제였는데 거시적 차원으로 가면서 좀 더 대규모 단위의 안보(安保, security) 문제가 되는 과정을 의미함. 〈그림-1〉 참조.
  - 즉 신흥안보란 미시적 안전이 거시적 안보가 되는 문제 또는 개인안전이 국가안보가 되는 문제를 의미함
  - 이렇게 창발의 맥락에서 안보 문제를 보면 우리가 이전에 알고 있던 '안보'의 개념 자체를 재조정할 필요성이 제기됨

* 예전에는 거시적 안보만을 논했지만 이제는 창발의 가능성이 있는 미시적 안전에 대해서도 안보의 관점에서 관심을 기울여야 하는 현실의 변화가 발생하고 있음



- 신흥안보의 창발성은 비선형 메커니즘, 자기조직화, 분산형 상향식 네트워크 구조, 미시적 규칙, 협력의 진화를 특징으로 하는 복잡계 현상을 전제로 해야 함
  - 예를 들어, 자기조직화 임계성(SOC)의 개념에 의하면 신흥안보 분야에서 재난은 갑작스럽게 발생한 것으로 보여도 그 내부에서는 복잡한 상호작용이 끊임없이 이루어지고 있는 것으로 보아야 함
    * 모래탑의 사례: 모래탑을 쌓을 때마다 크고 작은 붕괴(avalanche) 현상이 발생하는데, 이것은 모래탑이라는 시스템 내부에서 일어나는 모래알 사이의 역학관계로부터 비롯됨(페르 박, 2012)
  - 신흥안보의 문제들은 미시적 행위자들이 대강의 규칙만 가지고 수많은 시행착오를 거쳐서 거시적 문제를 해결하는(또는 격변이 발생하는) 상향식 접근법을 통해서 발생하는 특징을 지님
  - 그렇다면 여기서 관건이 되는 것은 창발을 가능케 하는 규칙을 찾아내서 격변이나 붕괴 현상이 언제 어떻게 발생하는지를 밝히는 데 있을 것임
    * 즉 신흥안보 거버넌스의 이론을 만드는 것이 관건이 될 것임. 그런데 이게 쉽지 않다는 사실이 문제임

신흥안보, 그 창발의 조건

- 이상에서 살펴본 복잡계 이론과 창발의 개념에 대한 논의를 좀 더 구체적으로 신흥안보의 개념에 적용해 볼 필요가 있음
  - 강조컨대, 신흥과 안보의 두 개념이 만나서 구성된 신흥안보는 선형적(linear) 인과관계로 파악되는 단순계(simple system)가 아닌 비선형적(non-linear) 상관관계로 파악되는 복잡계(complex system) 현상을 배경으로 하여 부상함
  - 복잡계의 맥락에서 보는 신흥안보는 미시적 상호작용이 양적으로 증대되어 임계점(critical point) 또는 티핑 포인트(tipping point)를 넘어서 거시적 차원에서 특정한 패턴이 발생하는 문제로 이해해야 함
  - 그렇다면 신흥안보 분야에서 미시적 안전의 문제가 거시적 안보의 문제로 창발(emergence)하는 조건은 무엇인가?
    * 어느 수준에서는 미시적 안전의 문제이고 어느 수준을 넘어서면 거시적 안보의 문제가 되는가?

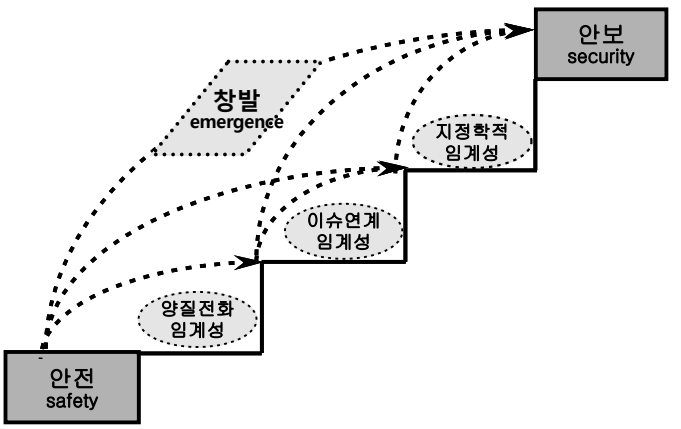
- 복잡계 이론의 다양한 논의를 응용하여 신흥안보 문제는 대략 3단계의 문턱을 거쳐서 미시적 안전으로부터 거시적 안보로 창발하는 것으로 개념화해 볼 수 있음.

  - 개별안전(individual safety)의 문제가 집합안전/안보(collective safety/security)의 문제가 되고 더 나아가 일반안보(general security)의 문제가 되는 과정을 연상해 볼 수 있음

    * 이러한 신흥안보의 3단계 창발론은 마치 곤충이 유충의 단계를 거쳐서 번데기가 되고 더 나아가 성충이 되는 3단계의 과정을 따라서 변태하는 것을 연상케 함

  - 이러한 3단계 창발론은 1)신흥안보 이슈 내에서의 미시적 상호작용의 양적 증대, 2) 여타 신흥안보 이슈들과의 상호 연계성의 증대, 3) 전통안보의 지정학적 이슈들의 개입 등으로 나누어서 이해할 수 있음. 〈그림-2〉 참조.

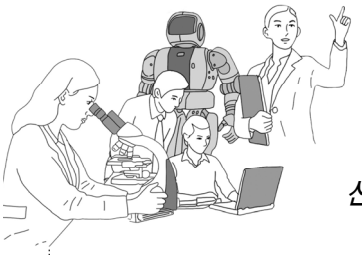
    * 물론 이러한 3단계 창발의 티핑 포인트는 순차적으로 발생하는 것이 아니라 상호 종첩되어 발생하며 이 글에서는 다만 분석적 편의를 위해서 나누어서 살펴봄



〈그림-2〉 신흥안보의 3단계 창발론

- 첫째, 양질전화 임계성. 가장 포괄적인 의미에서 신흥안보는 이슈 영역 내에서의 안전사고가 양적으로 증가하여 일정한 수를 넘는 경우에 창발하는 것으로 개념화할 수 있음

  - 신흥안보의 위협은 기본적으로 양적증대가 질적변화를 야기하는 문제, 즉 양질전화(量質轉化)의 문제로 이해되어야 함



* 개별 단위차원의 안전이 관건이 되는 정도의 우연적 확률의 문제였던 것이 양질전화의 문턱을 넘어서 갑작스럽게 수면(즉 임계점) 위로 떠올라 필연적 발생이 예측되는 안보의 문제로 전화되는 성격을 지님

- 이는'양질전화의 창발 사다리'라고 부를 수 있는데, 안보 개념의 범위라는 점에서 안보(security)와 안전(safety)의 경계를 무너뜨리는, 즉 거시적 안보를 넘어서'일상적 안보'의 개념을 생성함

Q 신흥안보 이슈영역 내에서 안전사고의 수가 증가하여 안보 문제가 되는 사례는 다양한 분야에서 발견됨

- 지구온난화와 관련하여 일인당 에너지 소비량의 증가는 어느 순간에 북극의 빙하를 녹이고 해수면을 상승시키는 원인으로서 지목되고 있음

- 최근 유럽에서 논란이 되고 있는 이민과 난민 문제에서 보는 바와 같이 국경을 넘는 불법 이민자들의 수적 증가는 수용국 내 사회갈등과 범죄의 증가, 이민자 집단의 정치세력화, 테러 위협의 가능성 증가 등의 문제를 야기하고 있음

- 보건안보에서 어느 가정에서 1명이 감기 걸리는 것과 어느 도시 전체 인구에 맞먹는 100만 명이 감기 걸리는 것은 차이가 있을 수밖에 없으며 후자는 명백한 국가사회의 안보 문제임

- 컴퓨터 하나에서 발견된 악성코드가 널리 전파되어 국가 기반시설로서 컴퓨터 시스템을 다운시킬 정도로 확산되면 이는 더 이상 컴퓨터 보안이나 정보보호의 문제가 아니라 사이버 안보 문제가 됨

Q 둘째, 이슈연계 임계성. 신흥안보는 다른 신흥안보 이슈들과의 상호 연계가 밀접해 지면서 그 영역 내에서는 단순한 미시적 안전의 문제였지만 거시적 안보의 문제로 창발할 가능성을 갖게 됨

- 이는 단순히 여러 가지 신흥안보 이슈들이 상호 연관되어 있다는 의미를 넘어서, 즉 단순히 링크 하나가 더해진다는 의미를 넘어서 분절 네트워크에서 '구조적 공백'을 잇는 것과도 같은 의미를 가진

* 즉 신흥안보의 이슈연계성이 창발한다는 의미는 끊어진 링크를 하나 잇는 것이 신흥안보 전체 이슈구조를 재조정할 정도의 파장을 갖는다는 시스템 효과가 발생한다는 의미를 지님

- 이는 '이슈연계의 창발 사다리' 또는 '통섭의 창발 사다리'라고 부를 수 있는데, 이슈연계성이 증대됨으로써 해당 신흥안보 이슈 자체가 전체 신흥안보의 이슈연계도에서 중심성을 갖게 되고 그 이슈를 중심으로 클러스터를 이루게 됨

- 신흥안보 이슈들 간의 연계성이 증대됨으로 인해서 미시적 안전의 문제가 거시적 안보의 문제로 창발하는 사례는 여러 분야에서 발견됨

  - 기후변화는 이슈연계성이 가장 큰 사례 중의 하나인데, 이는 수자원위기, 극단적 기후 사태, 자연적 및 인위적 자연재해 등의 다른 환경적 위험요인과 깊이 연계되어 있음

  - 식량위기는 주기적으로 왔다가 해소되는 주기를 보였지만, 에너지 문제 해결을 위한 정책(곡물을 이용한 바이오 연료의 생산)과 연계되면서 식량안보의 문제가 됨

  - 이민과 난민 문제는 환경 문제의 악화에 의해서 증폭되며 기존 거주자들의 사회적 정체성, 해당 사회의 실업유발, 사회질서의 불안정, 문화적 갈등의 가능성, 이주 과정에서 발생하는 인간안보의 위협 등과 연계되면서 위험이 증폭될 가능성이 많은 문제임

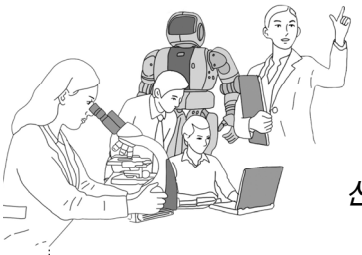
  - 컴퓨터 해킹 공격이 원자력 발전소나 기타 국가기간 시설에 해당하는 컴퓨터 시스템을 상대로 하여 감행될 경우 그 위험은 증폭되며 이러한 해킹이 정치사회적 목적과 결부된 테러와 범죄에 활용될 경우 그 위험성은 매우 커짐

- 셋째, 지정학적 임계성. 신흥안보 분야에서 안전사고의 양적증가와 이슈간 상호연계성이 일정한 수준을 넘어서는 경우 국가 행위자들의 개입이 이루어지게 되며, 이 경우에는 전통안보의 관점에서 본 지정학적 안보 이슈로 창발함

  - 이는 비전통 안보의 문제가 전통안보 문제와 연계되면서 신흥안보가 되는 것

    * 이는 비전통 안보와 신흥안보의 개념적 차이를 의미하기도 함

  - 신흥안보 이슈에 국가 행위자들이 참여하여 양자 간 또는 다자 간의 갈등이나 협력의 대상이 되는 문제



- 이는 '지정학적 창발 사다리'라고 부를 수 있는데, 전통안보 이슈와 연계되면서 국가 행위자가 개입할 근거가 발생하고 국가(일종의 거시적 행위자로서)의 본격적인 관여가 필요하게 되는 현상이 발생함

Q 신흥안보의 이슈가 전통안보의 관심사가 되면서 거시적 안보 문제로 창발한 사례는 다양한 영역에서 발견됨

- 자연재해와 환경악화로 인한 난민의 발생은 지정학적 차원에서 국가간 분쟁을 야기하며 이러한 문제를 해결하기 위한 국제협력의 필요성을 제기하면서 국가 행위자들의 주요 관심사가 됨.

  * 이러한 과정에서 발생하는 비자발적 이주의 문제는 사회적 불안정성은 물론 국가 간 무력충돌 및 국가체제의 전복까지 유발할 수 있는 그 파급력이 매우 높은 위험요인으로 부상

- 저출산・고령화 사회의 도래와 같은 인구문제는 경제성장을 이끄는 노동력의 부족과 국방을 위한 병력부족의 문제를 야기함은 물론 인구를 보충하기 위한 이민정책의 추진은 또 다른 사회적・경제적 문제를 야기하여 국가의 개입을 초래함

- 평화적 목적의 원자력 발전이 군사적 목적의 핵무기 개발과 연계되는 문제나 사이버 안보의 중요성이 부각되면서 국가 행위자들이 개입하여 군사적 차원에서 접근하는 문제, 보건안보 분야에서의 생화학무기 문제 등은 기술 변수가 전통안보의 문제와 만나는 현상을 보여줌

- 정체성 안보의 문제는 최근 종교적 정체성이 테러와 국가 간 분쟁의 중요한 원인으로 등장하고 있으며 경제적 불평등 문제는 이러한 갈등을 증폭시킴

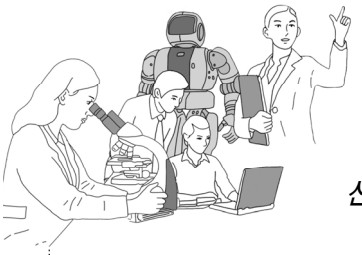
신흥안보의 독특한 성격

Q 이상에서 살펴본 바와 같이 신흥안보는 일정 정도는 수면 아래 있다가 수면 위로 떠오르는 것과 같은 창발의 메커니즘을 따르기 때문에 몇 가지 독특한 성격을 지님

- 특히 수면 위에서 보이는 위협인 전통안보의 경우와는 달리 신흥안보는 대부분의 경우 아직 수면 위로 떠오르기 전의 보이지 않는 위협으로서 거론되기 때문에 발생하는 특성

- 이러한 신흥안보의 특성은 크게 다음과 같은 세 가지에 주목할 필요가 있음

- 첫째, 신흥안보 이슈는 객관적으로 '실재하는 위험'이기도 하지만 그 이전에 안보 행위자에 의해서 '구성되는 위험'의 성격이 강함
  - 이는 앞서 살펴본 코펜하겐 학파의 안보화(securitization) 개념과 맥이 닿는 부분
  - 따라서 신흥안보의 위험을 논하는 경우 과잉 안보화(hyper-securitization)의 위험이 항시 존재하고 이는 일종의 '안보괴담'의 형태로 등장
  - 이러한 안보괴담이 생성 및 유포되는 과정에서 인터넷 미디어나 소셜 미디어와 같은 커뮤니케이션 변수가 중요한 역할을 함
- '구성되는 위험'으로서 신흥안보의 특성은 주로 기술환경을 배경으로 해서 발생하는 신흥안보 문제에서 나타남
  - 지구온난화가 야기하는 위험에 대한 예측은 어느 정도 이러한 안보화의 성격을 가짐
    * 영국 환경운동가인 마크 리나스(Mark Lynas)는 그의 저서 '6도의 악몽'에서 지구 온도가 1도 상승하면 빙하가 소멸하고, 2도 상승하면 대홍수 · 대가뭄이 발생하고, 6도 상승하면 인류 · 동식물 멸종을 예측
  - 2008년 미국산 쇠고기 수입에 반대하는 촛불집회 당시 유포된 광우병 괴담, 후쿠시마 원전 사태 이후 국내에서 일었던 방사능 괴담, 유전자조작농산물(GMO)와 관련된 보건안보 분야의 괴담 등의 사례
  - 아직까지도 그 위협의 실체와 효과가 명시적으로 입증되지 않은 사이버 안보 분야는 전형적인 안보화의 메커니즘이 작용하는 사례임.
    * 2014년 발생한 한수원 사태는 사이버 안보 분야의 괴담이 일종의 심리전의 수단으로 활용된 사례를 보여줌
- 둘째, 신흥안보 이슈에서는 인간 행위자뿐만 아니라 다른 수많은 사물(또는 기술) 변수들과의 상호작용이 중요함
  - 이러한 사물 및 과학기술 변수는 행위자-네트워크 이론(actor-network theory, ANT)에서 말하는 비인간 행위자(non-human actor)에 해당됨
    * ANT에 의하면, 인간이 다른 인간의 행위에 영향을 미치는 것처럼 비인간 행위자도 인간의 행위에 영향을 미칠 수 있다는 의미의 행위능력(agency)을 가지고 있는 것으로 설정됨



* 따라서 물질적 환경이라는 변수도, 통상적으로 이해하는 것처럼, 수동적인 존재가 아니라 능동적인 존재로 그려짐

- 이러한 논의를 신흥안보의 사례에 적용하면 이 분야에서 발생하는 위협은 인간 행위자에 의해서만 생성되는 것이 아니라 비인간 행위자 변수에 의해서 생성되는 성격이 강함

❑ 비인간 행위자가 야기하는 위험의 사례는 다양한 신흥안보 분야에 걸쳐서 발견됨

- 사이버 안보 분야에서 해킹에 사용되는 컴퓨터 바이러스, 악성코드, 디도스(DDoS, Distributed Denial of Service) 공격에 동원되는 좀비 컴퓨터와 봇넷, 경우에 따라서는 네트워크 그 자체가 사이버 테러와 공격에 독특한 성격을 부여하는 일종의 비인간 행위자로서 작동함

- 신흥안보 이슈로서의 테러와 범죄, 첩보와 감시 등에 활용되는 인터넷과 소셜 미디어도 중요한 비인간 행위자 변수

- 환경안보와 관련하여 환경 관련 기술, 에너지 집약적 농법 등이 사례

❑ 셋째, 신흥안보 이슈의 창발은 지역에 따라서 다르게 나타남

- 정치, 사회, 문화적 다양성으로 인해서 창발성을 결정하는 수면의 높이가 지역마다 다르며 이러한 수면은 대부분의 경우 사회문화적으로 구성되는 성격을 가짐

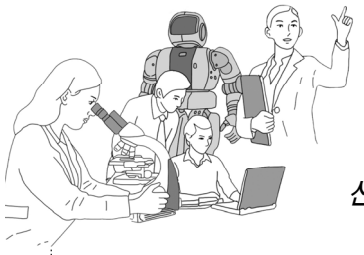
- 신흥안보의 위험은 창발하기 전에는 수면 아래에서 보이지 않는 현상이기 때문에 동일한 종류의 위험이라도 어떤 지역에서는 수면 위, 다른 지역에서는 수면 아래에 존재하는 것으로 인식될 수 있음

* 예를 들어 사회안보는 아직까지는 동아시아 지역에서 큰 문제가 아닌데 유럽에서는 이미 매우 큰 신흥안보의 문제가 되었음

- 코펜하겐 학파가 말하는 바처럼 지역 안보 복합체(regional security complex)라는 것이 있듯이 신흥안보 분야에서도 이러한 지역 개념을 반영할 수 있음

신흥안보의 창발이 지역적 차이를 갖는 사례들은 다수 발견됨

- 각 지역에 따라서 천연자원의 보유 정도와 기후 변화에 적응하는 사회적 능력의 차이 등으로 기후 변화가 인간안보를 약화시키는 정도의 차이가 존재
- 유전자조작 농산물에 대한 지역적 인식 차이가 존재
- 인간안보와 관련하여 정치체제의 다양성, 인권 규범의 다양성, 종교적 다양성 등이 변수가 됨
- 사이버 안보 분야에서도 인프라 의존성의 차이가 존재하기 때문에 발생하는 위협인식의 차이가 있음



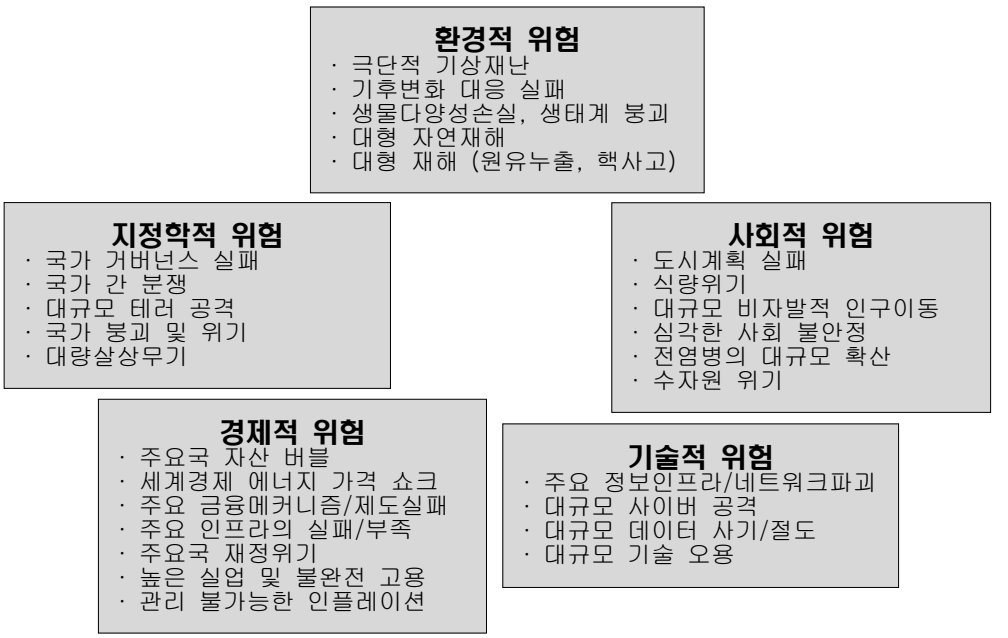
Ⅳ. 신흥안보 분야의 글로벌 위험 요인들

최근 다양한 분야에서 이상에서 언급한 신흥안보의 특성을 갖는 글로벌 위험들이 발생하고 있음.

- 세계경제포럼(WEF)은 900명의 전문가 의견조사를 바탕으로 작성한 '글로벌 리스크 2015'라는 보고서를 통해서 전 세계가 직면하고 있는 새로운 위험을 지적한 바 있음

  * 이 보고서에서는 기후변화, 자연재해, 대형인재, 생태계 손실, 물 위기, 정보인프라 파괴, 사이버 공격, 데이터 사기와 절도, 식량위기, 유행병, 만성질병, 항생제 내성 박테리아 등과 같은 신흥안보의 이슈들을 지적함

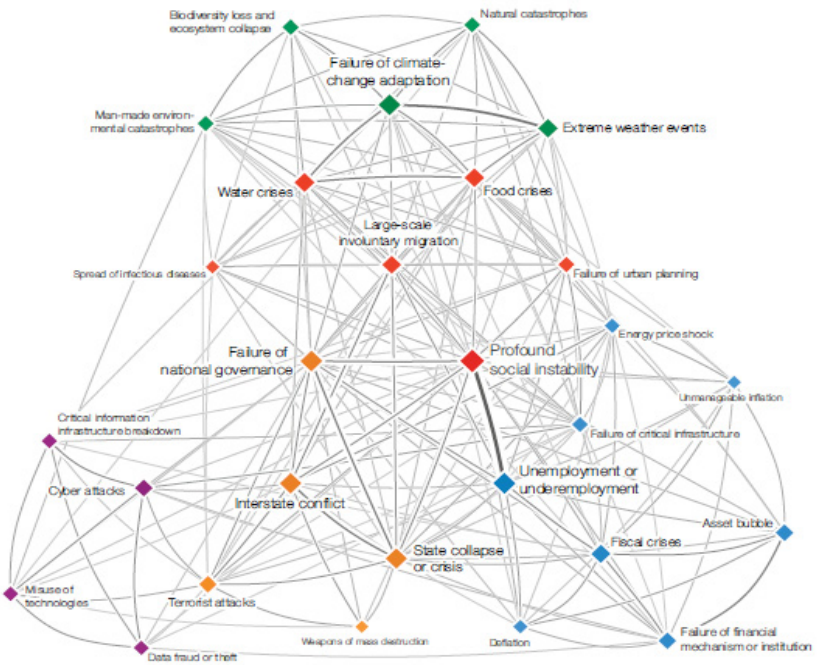
- 경제적 위험, 환경적 위험, 지정학적 위험, 사회적 위험, 기술적 위험 등 5개 분야에 걸쳐 향후 10년 내 다수 국가와 산업에 부정적 영향을 미칠 28개 위험요인과 함께 위험요인 발생 및 확산에 영향을 주는 트렌드를 도출. 〈그림-3〉 참조.



출처: World Economic Forum. 2015. Global Risks 2015, 10th Edition.

〈그림-3〉 28개 글로벌 위험요인

- 이들 위험들은 그 위험의 성격과 피해의 범위라는 점에서 초국적이고 글로벌 차원에서 발생하는 안보 문제인 동시에 국지적이고 개인적인 안보의 문제까지도 영향을 미치는 다층적인 안보 문제임
  - 신흥안보 문제는 한 국가의 안보뿐만 아니라 지역적 및 지구적 차원에서 중층적이며 복합적인 접근을 통해서만 해결이 가능한 사안이기도 하여 매우 복잡하고도 긴급한 문제로 인식할 필요가 있음



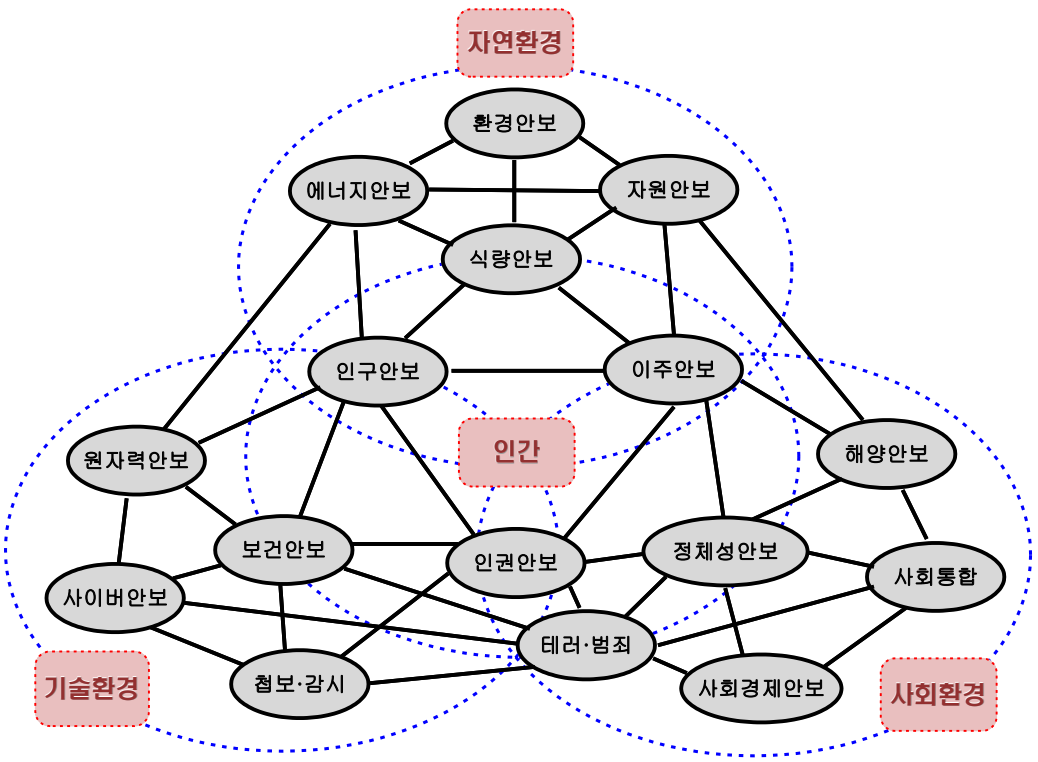
출처: World Economic Forum. 2015. Global Risks 2015, 10th Edition.

〈그림-4〉 WEF의 글로벌 리스크의 상호연계도, 2015

- 게다가 이러한 신흥안보 이슈들은 서로 밀접하게 연계된 특징을 지니고 있음
  - WEF의 글로벌 리스크 보고서도 이러한 이슈연계성의 중요성을 인식하고 〈그림-4〉와 같은 글로벌 리스크 상호연계도를 작성하였음(WEF, 2015).

- 글로벌 위험 또는 유럽 차원의 위험을 염두에 두고 작성된 리스크의 상호연계도를 참고로 하면서 동아시아와 한반도의 신흥안보 현실을 반영한 신흥안보 클러스터의 지형도를 그려보는 것은 의미가 있을 것임

  - 그러나 현재 학계의 연구현황을 고려하면 실상도(實像圖)를 그리는 것은 쉽지 않고, 이를 위한 시론(試論)으로서 〈그림-5〉와 같은 가상의 지형도를 그려볼 수는 있음.



〈그림-5〉 신흥안보 클러스터의 가상 지형도

- 신흥안보의 이슈들을 인간안보를 중심으로 하여 그 주위의 자연환경, 기술환경, 사회환경 등에서 야기되는 안보 위협을 포함한 네 가지 범주로 나누어 클러스터를 설정함. 그리고 각 이슈들의 상호연계성을 고려하여 위치를 설정함.

- 인간안보 분야 신흥안보 이슈

* 일차적으로는 인구안보, 이주안보, 인권안보 등이 클러스터를 형성하고 이차적으로는 식량안보, 보건안보, 인권안보, 테러감시, 정체성안보 등이 연계됨

- 자연환경을 배경으로 하는 신흥안보 이슈

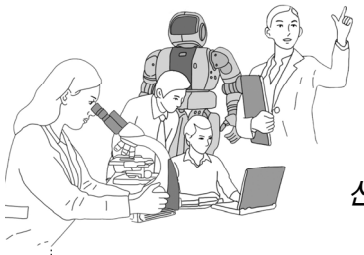
* 일차적으로는 환경안보, 식량안보, 에너지안보, 자원안보 등이 클러스터를 형성하고, 이차적으로는 인구안보와 이주안보, 삼차적으로는 해양안보, 원자력 안보 등이 링크를 형성하는 것으로 그려볼 수 있음

- 기술환경을 배경으로 하는 신흥안보 이슈

* 일차적으로는 원자력 안보, 사이버 안보, 보건안보, 첩보 · 감시 등이 클러스터를 형성하고 이차적으로는 테러 범죄(마약, 인신매매, 국금융사기), 인권안보, 인구안보, 삼차적으로는 에너지안보, 식량안보, 자원안보 등이 연계됨

- 사회환경을 배경으로 하는 신흥안보 이슈

* 일차적으로는 사회경제안보, 사회통합, 문화정체성안보, 테러와 범죄, 해양안보 등이 클러스터를 형성하고 이차적으로는 인권안보, 이주안보, 첩보 · 감시 등이 연계됨



Ⅴ. 신흥안보 분야 과학기술 역할

신흥안보 위협 대응 방안 : 사이버 안보 분야를 중심으로

- 신흥안보 분야에서는 위협의 원인이나 위협에 대응하는 해법의 마련이라는 차원에서 볼 때 다양한 과학기술 변수들이 중요한 역할을 함
  - 이러한 과학기술 변수는 행위자-네트워크 이론(actor-network theory, ANT)에서 말하는 비인간 행위자(non-human actor)에 해당됨
    * ANT에 의하면, 과학기술 변수는 수동적인 존재가 아니라 인간의 행위에 영향을 미칠 수 있는 행위능력(agency)을 가진 비인간 행위자임
  - 이러한 논의를 신흥안보의 사례에 적용하면 이 분야에서 발생하는 위협은 인간 행위자에 의해서만 생성되는 것이 아니라 과학기술 변수 그 자체에 의해서 생성되는 성격이 강함
  - 또한 신흥안보 분야의 문제를 해결하는 데 있어서도 과학기술 변수는 인간 행위자가 활용하는 단순한 도구 이상의 의미를 가짐
- 특히 신흥안보 분야에서 위협의 원인을 파악하고 해법을 마련한다는 차원에서, 〈그림-2〉에서 언급한 바와 같이, '미시적 안전'이 '거시적 안보'가 되는 상승의 고리를 끊는 데 필요한 과학기술을 개발하는 노력이 필요함
  - 신흥안보란 미시적 차원에서는 단순히 소규모 단위의 안전(安全, safety)의 문제였는데 거시적 차원으로 가면서 좀 더 대규모 단위의 안보(安保, security) 문제가 되는 과정
    * 따라서 신흥안보 분야에서 재난을 방지하는 가장 중요한 고리는 바로 이러한 '미시적 안전 – 거시적 안보 상승의 고리' 라고 할 수 있음
  - 이러한 상승의 고리를 끊는 것이 중요한 이유는 거시적 격변(catastrophe) 현상은 자기조직적 임계현상으로서 갑작스럽게 발생하는 듯 보여도 그 내부에서는 복잡한 상호작용이 끊임없이 이루어지고 있는 현상이기 때문임
    * 예를 들어 거대한 지진은 그 발생 이전에 징후를 드러내는 것으로 알려져 있고 이러한 조짐을 관찰하고 감지하는 것은 중요함

- 이러한 상응의 고리를 끊는 데 필요한 과학기술 역량의 확보, 즉 기술혁신과 인력양성의 노력이 중요함.

  * 최근 국가가학기술자문회의에서 펴낸 정책보고서에서도 보건안보나 사이버 안보 등과 같은 신흥안보 분야의 위협에 대응하는 과학기술의 역찰에 주목하였음(잊오구 외, 2015)

Q 사이버 안보 분야를 보면 예방과 탐지 및 복원의 과학기술 역량을 배양하여 이상에서 언급한 상승의 고리를 끊는 것이 중요함

- 해킹과 사이버 테러 및 공격에 대한 대책들은 크게 i) 공격을 미리 예측하고 사고 발생을 최소화하는 예방력 ii) 해킹 공격 루트에 대해 수사하고 공격자를 확인하는 탐지력 iii) 공격이 발생했을 때 최단시간 내에 차단하여 피해를 최소화하고 빠르고 원활하게 복구하는 복원력 등의 세 가지 기술역량을 키우는 것으로 요약됨

  * 이를 위해서 최근 국내에서도 사이버 안보 분야의 연구개발을 위한 예산지원을 늘리고, 정보보호 산업의 육성을 위한 민간 및 정부 지원사업의 확대 등과 같은 대책들이 강구되고 있음

Q 첫째, 사이버 안보 분야에서 공격을 미리 예측하고 사고 발생을 최소화하는 예방력을 키우는 것이 중요함

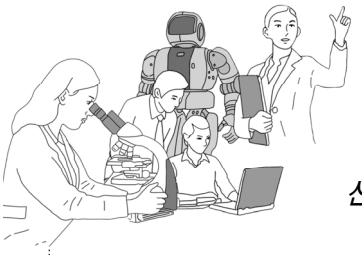
- 이와 관련해서 이른바 '사이버 보안 인텔리전스 네트워크 기반의 국가 통신망 모니터링 체계'의 구축이 거론됨

- 이밖에도 △ 전력 · 금융 · 의료 등 기반시스템 운영기관 및 기업들의 중요 정보 암호화 등 보호조치 강화 △ 주요 핵심시설에 백업센터 및 재해복구 시스템 확대 구축 △ 정부 소프트웨어 개발 단계에서의 보안취약점 사전 진단 제도 의무화 등도 거론됨

- 이는 국민 인식제고나 직원 내부통제, 민감한 조직에 공급되는 소프트웨어를 감시하는 공급망 보안 등의 조치에 의해서 보완돼야 함

- 한편 사이버 테러와 공격을 예방하고 대응하기 위한 국내외 정보공유 네트워크(예를 들어, 사이버위협 정보 종합 수집 · 분석 · 공유 시스템)를 구축하는 것도 중요함

- 이는 해커들의 동향이나 악성코드에 대한 정보, 특히 빅데이터를 공유하는 환경을 구축하여 고도화된 사이버 공격을 막을 수 있다는 인식을 바탕으로 함



- 둘째, 사이버 안보 분야의 대응책을 마련하는 데 있어 해킹 공격 루트에 대해 수사하고 공격자를 확인하는 탐지력을 키우는 것이 중요함
  - 이러한 탐지력은 "근원지를 역추적하고 공격자의 신원을 식별하며, 사이버 공격 증거들을 확보하고 공격 원점을 타격하거나 동일한 수준의 목표물에 대해 부수적 피해 없이 동일한 수준의 대응공격을 할 수 있는 능력"을 의미함(임종인 외, 2013).
  - 특히 공격의 원인을 분석하여 근원지를 역추적하는 대책으로서 '포렌식 준비도(forensic readiness)'가 주목을 받고 있음
    * 포렌식 준비도란 사후 대응 시에 디지털 포렌식 증거 수집 및 분석의 역량을 극대화하고 비용을 최소화하기 위한 환경을 사전에 준비하는 것임. 2009년 영국에서 제도화되어 널리 알려졌지만 아직 국내에서는 제도화되지 못한 상태.
  - 포렌식 준비도가 도입되면 효과적인 사후 대응을 위해 보안 전문인력을 보유하고, 하드웨어(네트워크, 보안 장비)와 소프트웨어(운영체제, 응용프로그램)가 로그를 많이 남기도록 정책을 설정하는 등의 준비를 통해 사이버 공격에 의한 침해 사고가 발생했을 시에 신속한 대응으로 피해를 최소화 할 수 있음(『보안뉴스미디어』, 2013-4-14).
- 셋째, 사이버 안보 분야의 대응책을 마련하는 데 있어 공격이 발생했을 때 최단시간 내에 차단하여 피해를 최소화하고 빠르고 원활하게 복구하는 복원력(resilience)을 키우는 것이 중요함
  - 복원력에 대한 관심은 "이제 해킹은 피할 수 없다"고 인정하는, 해킹과 사이버 공격을 바라보는 발상의 전환을 전제로 함(『전자신문』, 2013-3-26).
  - 다시 말해 그동안 보안 분야의 주된 관심과 투자가 사이버 공격을 막거나 예방하는 데 있었다면, 앞으로는 공격을 당하더라도 피해를 최소화할 수 있는 방향으로 전환하자는 것임
    * 비유컨대 방패가 뚫리더라도 중상을 입지 않고 타박상에 그칠 수 있는 대응 전략이 필요하다는 것
  - 사실 방어가 기술적으로 쉽지 않은 상황에서 완벽한 사이버 방어 시스템을 구축하겠다는 계획은 합리적이지도 않으며 바람직하지 않음
    * 이러한 맥락에서 일각에서는 기업경영이나 국정운영, 에너지 · 자원 등 사이버 공격이 예상되는 분야를 중심으로 '해킹 리스크'를 상수로 설정하자는 의견도 제기됨

○ 사이버 안보 분야에서 이러한 기술역량을 강화하는 데 있어 인력양성은 중요한 이슈임

- 효과적인 사전 예방과 사후 대응을 위해서는 하드웨어, 소프트웨어, 네트워크, 정보보호, 디지털 포렌식 등의 지식을 두루 갖춘 고도의 전문가가 필요함. 그러나 현재 국내 상황은 이들 인력이 부족한 상황임.

- 예를 들어, 공공 영역에서 사이버 방어에 종사하는 이른바 '사이버 전사' 인력 부족. 사이버 전사를 양성하기 위한 국가적인 차원의 체계적인 계획이 부족하고 이들에 대한 활용계획과 적절한 대우와 포상정책 또한 없으며, 사이버 전사들을 효과적으로 활용하기 위한 사이버 병과도 없는 상황임 (임종인 외, 2013).

- 또한 민간 영역에서도 주요 기반시설의 보안관리와 정보보호 산업에 종사할 전문인력 육성의 필요성도 강력하게 제기되고 있음

  * 그러나 현재는 정보보호 전문기업 대부분이 중소업체 위주로 되어 있고, 대학의 전문인력 배출도 미흡한 상황임

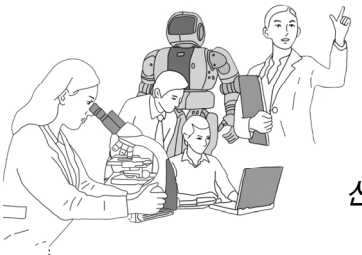
○ 이러한 상황을 인식하고 정부는 공공 및 민간 부문에서 사이버 전문 인력을 양성하기 위한 대책들을 내놓고 있음

- 그림-6〉은 이른바 '화이트 해커'로 알려진 사이버 안보 분야 인력을 양성하기 위해서 정부가 내놓은 계획의 요약임 (『조선닷컴』, 2015-7-25).

- 그 골자를 보면, 사이버 능력이 우수한 특기자 전형의 사이버 특화 고교 · 대학을 확대하고, 국내 대학의 컴퓨터 및 정보보호 학과 졸업자들이 민간 기업에 채용될 수 있도록 기회를 제공하는 것으로 되어 있음

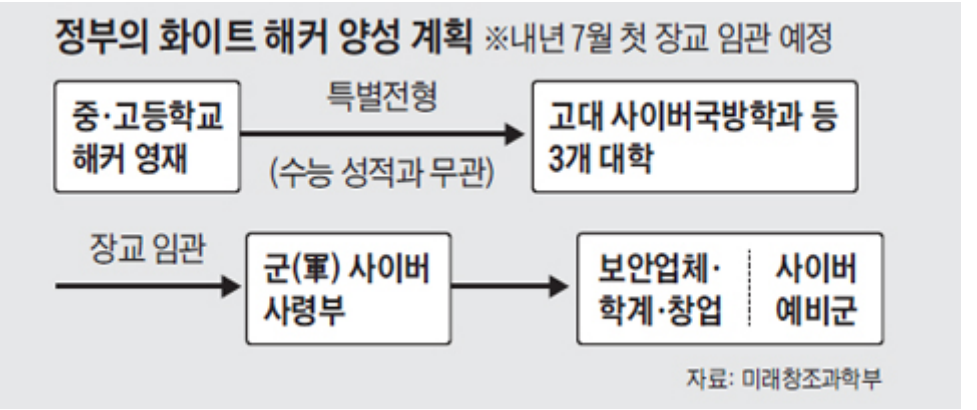
  * 이렇게 양성된 인력이 안정적인 취업과 지속적인 재교육을 통해 전문 인력으로 성장할 수 있도록 틀을 마련

  * 군에서도 전문 인력을 효과적으로 양성할 수 있는 교육훈련체계와 사이버병과체계, 공공과 민간의 사이버인력 활용체계를 마련하고 합당한 대우와 보상체계를 제공함으로써 안정적인 사이버 전사 육성·활용체계를 마련



* 또한 군 적역 후에도 사회 각 분야에서 활용되도록 사이버 인력 생태계를 조성하는 방안도 거론되는데, 이른바 사이버예비군제도 도입의 필요성이 제기되고 있음

* 군에서 양성된 정예오원이 민·관·산·학과 연계해 군의 노하우를 사이버 안보에 걸맞은 창업으로 이어지게 하는 시스템을 마련하겠다는 것임



출처: 『조선닷컴』, 2015-7-25.

〈그림-6〉 정부의 화이트 해커 양성 계획

● 사이버 안보를 포함한 신흥안보 분야에서 재난을 미리 탐지하는 빅데이터 관련 과학기술 역량이 최근 관심의 대상이 되고 있음

- 휴대폰이나 인터넷, 소셜 미디어에서 생성되는 빅데이터를 활용하여 자연재난 및 전염병 발생 징후의 조기 감지, 발생 후에 인구 이동 패턴, 실시간 주민 필요 파악, 조기경보를 통한 신속한 대응책의 마련이 가능함

- 빅데이터는 개도국에서 발생하는 재난에 대한 인도적 지원을 최적화하는 데에도 활용될 수 있으며, 구호물자를 효율적으로 전달하는 데에 도움을 줄 수 있음

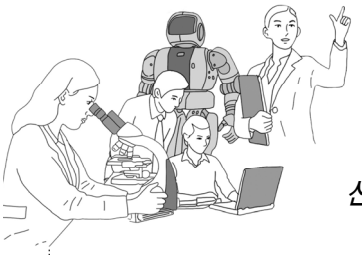
* 실제로 2013년 필리핀 하이엔 태풍의 구호 활동에서 수천 개 트위터 메시지의 키워드를 이용하여 구호물자가 필요한 지역과 최단거리 경로지도가 작성되었고 유엔도 이에 기초하여 구호활동을 전개한 바 있음

- 보건안보 분야에서도 인터넷 검색어를 통해서 질병 발병을 예측하거나, 발병에 대한 정보를 신속하게 전달하고, 휴대폰 사용 자료와 센서스 자료를 결합하여 전염병 등의 확산에 대한 신속한 대응이 가능함

- 이러한 과정에서 휴대폰의 CDR(call-data records)은 유용한 빅데이터를 생성하는데, 발신자의 신원, 전화번호, 통화의 시간과 정소 등과 같은 빅데이터를 분석할 수 있음

- 빅데이터는 기후변화 분야에서 초국적 환경오염의 원천파악, 글로벌 생태계에의 장기적인 효과 분석 등에 활용되어 국가 간 환경 분쟁 해결에 도움을 줄 수도 있음

- 사이버 안보 분야에서도 사이버 공격을 전후 한 시점에 발생하는 온라인상에서의 이상 징후를 감지하거나 사이버 공격에 사용된 악성코드를 기존의 것과 비교하는 빅데이터 분석이 가능함(Hansen and Porter, 2015, pp.14-15).



Ⅵ. 맺음말

- 전통안보를 넘어서는 신흥안보 이슈들의 부상은 국내외 정치 전반에서 새로운 안보 패러다임의 부상을 전망케 함

  - 오늘날 위협의 성격과 위협의 대상이라는 차원에서 기존의 전통안보 위협과는 질적으로 다른 신흥안보 이슈들이 등장하고 있음

  - 예를 들어, 환경안보, 식량안보, 에너지안보, 자원안보, 인구안보, 이주안보, 인권안보, 원자력안보, 사이버안보, 첩보·감시, 테러·범죄, 보건안보, 정체성 안보, 사회경제안보, 사회통합, 해양안보 등의 분야를 들 수 있음

  - 이러한 변화는 안보담론의 변화뿐만 아니라 안보게임에 관여하는 행위자의 성격과 이들이 벌이는 안보게임 또는 권력게임의 양상을 변화시키고 있음

- 신흥안보의 부상으로 인해서 위협의 인식과 해결의 주체 변화는 행위자의 변환과 이들이 벌이는 안보게임의 변환이 야기됨

  - 신흥안보의 부상은 새로운 위협요인의 출현뿐만 아니라 안보문제의 해결 주체라는 점에서 기존의 국가 행위자 위주의 안보 관념도 조정케 함

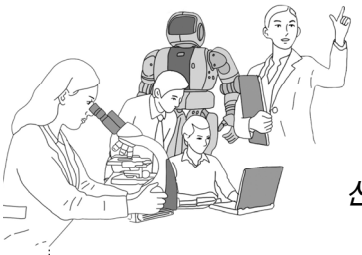
    * 신흥안보에 대응하기 위해서는 국가 행위자 혼자서는 안 되고, 국가 행위자와 비국가 행위자(민간기업, 시민사회, 지역공동체, 국제기구 등), 그리고 더 나아가 비인간 행위자(컴퓨터 악성코드, 전염병 바이러스, 원자력 발전소 등)까지도 모두 참여하는 복합 행위자의 개념을 활용해야 함

  - 이들 행위자들의 벌이는 안보게임의 양상도 새로운 방향으로 전개되고 있음

    * 이는 국내외 정치에서 권력게임의 성격도 변화시키고 있는데, 신흥안보 분야에서 복합 행위자들이 벌이는 안보/권력 게임의 성격은 기존의 자원권력 게임이라기보다는 새로운 권력게임의 양식으로서 '네트워크 권력'의 게임임

  - 이러한 점에서 신흥안보의 부상은 단순히 전통안보를 대체하는 새로운 안보 이슈들의 등장이라는 차원을 넘어서 전통안보와 비전통 안보를 모두 아우르는 의미에서 새로운 안보 패러다임의 부상이라고 볼 수 있음

- 이상에서 살펴본 신흥안보의 부상에 따라 각 이슈발 과학기술의 적절한 역할을 살펴보는 문제를 향후 연구과제로 제시할 수 있음
  - 신흥안보 분야의 위협들이 과학 · 기술 · 지식 · 정보 집약적인 성격을 지니고 있으므로 구체적인 국가 대응전략을 마련함에 있어 과학기술의 핵심적인 역할을 탐구할 필요가 있음
  - 예를 들어, 신흥안보에 대비하는 과학기술과 R&D 전략 수립 및 로드맵 구축 등과 같이, 과학기술 전반을 횡단면적으로 아우르는 안보관련 정책·기술에 대한 종합적인 대응 전략을 수립할 필요가 있음



참 고 문 헌

김상배. 2014. 『아라크네의 국제정치학: 네트워크 세계정치이론의 도전』 한울.

민병원. 2006. "탈냉전시대의 안보개념 확대: 코펜하겐 학파, 안보문제화, 그리고 국제정치이론." 서울대학교 국제문제연구소 편. 『세계정치와 동아시아 안보』. 인간사랑, pp.13-61.

민병원. 2007. "탈냉전기 안보개념의 확대와 네트워크 패러다임." 『국방연구』 50집 2호, pp.23-55.

민병원. 2012. "21세기의 복합안보: 개념과 이론에 대한 성찰." 하영선 · 김상배 편. 2012. 『복합세계정치론: 전략과 원리, 그리고 새로운 질서』 한울, pp.118-146

이신화. 2006. "동아시아 인간안보와 글로벌 거버넌스." 서울대학교 국제문제연구소 편.서울대학교 국제문제연구소 편. 『세계정치와 동아시아 안보』 세계정치 시리즈 5. 인간사랑. pp.263-286

이종구 외. 2015. "과학기술기반 신흥안보 대응 방안." 국가과학기술자문회의 정책연구보고서. 2015-02.

임종인 · 권유중 · 장규현 · 백승조. 2013. "북한의 사이버전력 현황과 한국의 국가적 대응전략." 『국방정책연구』 29(4), pp.9-45.

페르 박. 2012. 『자연은 어떻게 움직이는가?: 복잡계로 설명하는 자연의 원리』 한승.

하영선. 편. 1993. 『탈근대지구정치학』 나남.

하영선 · 김상배 편. 2006. 『네트워크 지식국가: 21세기 세계정치의 변환』 을유문화사.

하영선 · 김상배 편. 2010. 『네트워크 세계정치: 은유에서 분석으로』 서울대학교출판문화원.

하영선 · 김상배 편. 2012. 『복합세계정치론: 전략과 원리, 그리고 새로운 질서』 한울.

Ansell, Christopher K. 2000. "The Networked Polity: Regional Development in Western Europe," Governance, 13(3), pp.303-333.

Ansell, Christopher K. and Steven Weber. 1999. "Organizing International Politics: Sovereignty and Open Systems." International Political Science Review. 20(1), pp.73-93.

Balzacq, Thierry, ed. 2011. Securitization Theory: How Security Problems Emerge and Dissolve. London and New York: Routledge.

Beck, Ulrich. 2005. "World Risk Society and the Changing Foundations of Transnational Politics," Edgar Grande and Louis W. Pauly, eds. 2005. Complex Sovereignty: Reconstituting Political Authority in the Twenty-first Century. Toronto: University of Toronto Press.

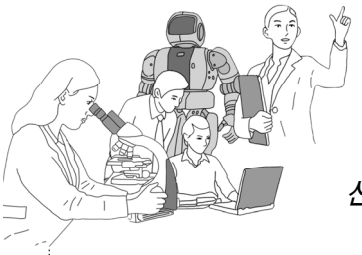
Buzan, Barry and Lene Hensen. 2009. The Evolution of International Security Studies. Cambridge: Cambridge University Press.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. Security: A New Framework for Analysis. Boulder: Lynne Rienner.

Carnoy, Martin, and Manuel Castells. 2001. "Globalization, the Knowledge Society, and the Network State: Poulantzas at the Millennium." Global Networks. 1(1), pp.1-18.

Clark, Ian, 1999. Globalization and International Relations Theory, Oxford: Oxford University Press.

Hansen, Hans Krause, and Tony Porter. 2015. "What do Big Data do in Transnational Governance?" Paper Presented at the International Studies Association Meetings, New Orleans, February 21, 2015.



Hansen, Lene and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." International Studies Quarterly, 53(4), pp.1155-1175.

Hough, Peter, Shahin Malik, Andrew Moran and Bruce Pilbeam. 2015. International Security Studies Theory and Practice. Routledge: Londond and New York.

Huysmans, Jef. 2007. "Revisiting Copenhagen: Or, on the Creative Development of a Security Studies Agendas in Europe." in Barry Buzan and Lene Hensen. eds. International Security. v4. Los Angeles, SAGE, pp.43-66

Jessop, Bob. 2003. The Future of the Capitalist State. Cambridge: Polity Press.

McSweeney, Bill. 2007. "Identity and Security: Buzan and the Copenhagen School." Barry Buzan and Lene Hensen. eds. International Security. v3. Los Angeles, SAGE, pp.121-134

Wæver, Ole, Barry Buzan, Morten Kelstrup, and Pierre Lemaitre. 1993. Identity, Migration and the New Security Agenda in Europe. London: Pinter.

Wæver, Ole. 1995. "Securitization and Desecuritization." in Ronny Lipschutz. ed. On Security. New York: Columbia University Press, pp.46-86.

World Economic Forum(WEF). 2015. Global Risks 2015, 10th Edition.

저자 소개

■ **김 상 배**
- 서울대학교 정치외교학부 교수
- 전화 : 02) 880-6848
- e-mail : sangkim@snu.ac.kr

KISTEP Issue Paper 2015-18

| 발 행 | 2015년 12월
| 발행인 | 박 영 아
| 발행처 | 한국과학기술기획평가원
서울시 서초구 마방로 60(양재동) 동원산업빌딩 9~12층
전화 : 02) 589-2866 / 팩스 : 02) 589-2280
http://www.kistep.re.kr
| 인쇄처 | (주)비전테크시스템즈 [TEL : 02)3432-7132]