CENTER FOR FUTURE WARFARE STUDIES
INSTITUTE OF INTERNATIONAL STUDIES
SEOUL NATIONAL UNIVERSITY

서울대학교 국제문제연구소
미래전 연구센터
08826 서울시 관악구 관악로 1
서울대학교 종합교육연구동 220동 517호

Tel. 02-880-6311
Fax. 02-871-4115

Center for Future Warfare Studies,
Institute of International Studies at Seoul National University |
국제문제연구소 미래전 연구센터 워킹페이퍼 No. 60 (발간일: 2020.12.11.)

스마트 메가시티의 복합안보위협과 거버넌스 대응전략

군의 역할을 중심으로

이웅 육군미래혁신연구센터

〈차 례〉

Ⅰ. 서론

전 세계적으로 나타나는 미래의 주요 트렌드인 스마트 메가시티의 확산 추세와 더불어 그 이

면에는 상주인구의 밀집현상과 각종 기반체계의 복잡성으로 인해 안보적 측면에서의 취약성이 노정되고 있다. 국내에서도 서울, 대전, 부산, 광주 등 주요 도시들을 중심으로 스마트 시티화가 추진 중이나, 이로 인한 안보 측면에서의 잠재적 위험성(risk)이 증대되고 있는 가운데 실질적인 거버넌스 차원에서의 복합안보위협 관리체계는 아직 충분히 갖춰지지 않은 상황으로 판단된다. 특히, 서울과 그 주변 지역(인천, 경기)를 포함하는 수도권 지역은 상주인구 규모와 면적 측면에서 이미 세계 5위 수준의 메가시티에 도달하였기에 각별한 범정부적 관심과 거버넌스 차원에서의 대응이 요구될 것으로 보인다. 하지만, 이러한 스마트 메가시티의 본질적 속성은 안보위협에 대한 기존의 논의를 다소 무색하게 만드는 측면이 존재한다.

도시는 살아있는 생명체와 유사하다. 도시는 그 자체로서 일종의 시스템(system)이며, 구성요소로서의 다양한 하위 시스템과 복합적으로 상호작용하며 유지되고 있다. 정보 시스템(information system)의 측면에서, 도시는 각종 ICT 인프라로 정교하게 구성되어 있으며, 이러한 ICT 인프라가 그 기능을 발휘하고 제대로 작동하기 위해서는 반드시 전기공급을 필요로 한다. 비록, 간과되고 있는 측면이 있지만, 도시에서의 전기 공급은 생명체의 혈액과도 같은 것이며, 이를 안정적으로 공급하기 위한 각별한 관리가 필연적으로 요구된다. 만일 전 국민의 약 50%가 상주하는 수도권과 같은 스마트 메가시티의 주요 기반 체계에 심각한 문제가 발생할 경우, 이는 도시로서의 기능을 마비시킬 뿐만 아니라 국가의 PMESII체계[1]를 손상시킴으로써 국가통치 기능의 마비효과를 일으키게 되고, 국가안보 측면에서의 공백을 야기하게 된다. 또한, 스마트 메가시티[2]의 확산과 더불어 서로 상이한 안보 이슈가 상호 연계될 때, 복합적인 재난의 형태로 전화되고 그 파급효과가 국가안보차원에서 치명적일 것이라는 우려 섞인 전망이 나타나고 있다. 따라서 이러한 도시 기반 체계는 반국가적 적대세력에게는 유용한 표적(target)으로써 인식될 가능성이 충분한 것이다. 따라서 오늘날에 이르러 국가 차원에서의 안보위협이 반드시 전면전 형태의 전쟁(warfare)이 될 것이라고 단정할 수 없는 것이며, 기존의 방식으로 충분한 대처가 불가능한 것이다.

그리하여 본 연구는 미래의 주요 트렌드(trend)로서 스마트 메가시티(smart-mega city)에서의 복합안보위협에 대응하는 거버넌스 접근 전략에 대한 고찰에 중점을 두었다. 특히, 상주인구 규모가 약 2,616만 명(기준 : 2020년)으로 세계 5위 수준의 메가시티를 형성하고 있는 서울 및 수도권 지역에 중점을 두고 안보위협 주요 이슈 및 이슈 간 상호작용을 살펴볼 필요가 있을 것으로 보았다. 이러한 거버넌스적 접근전략에 있어서는 스마트 메가시티에서의 비전통적 복합안보

---

1) 합동작전 수행을 위해 분석하는 국가의 6가지 주요 기능요소로서, 정치(Politic), 군사(Military), 경제(Economy), 사회(Society), 정보(Information), 기반시설(Infrastructure)를 의미한다.

2) 스마트시티(smart city)와 메가시티(mega-city)의 특성을 동시에 갖추고 있는 도시. (※ 참고 : 육군 교육사령부. 2020.『월간작전환경분석 (2020년 1월)』.
- 스마트시티(smart-city) : 도시의 경쟁력과 삶의 질의 향상을 위하여 건설 · 정보통신기술 등이 융 · 복합된 도시기반시설을 바탕으로 다양한 도시서비스를 제공하는 지속가능한 도시
- 메가시티(mega-city) : 인구 · 도시학적 관점에서 대도시권(metropolitan; 중심도시+위성도시+배후지역) 지역 내 1,000만명 이상의 인구가 거주하는 지역

위협에 대해 중점을 두고 살펴보았으며, 군사 노드의 개입 필요성을 군사적 관점에서 민 · 관 · 군 상호 융합적 측면에서 군의 기여도를 제고할 수 있는 방안을 모색하였다. 이러한 탐색적 · 선제적 연구를 통해 미래 스마트 메가시티에서의 안보위협에 대한 거버넌스(governance) 관점에서의 대응 전략을 모색해보고자 하였다.

이에 따라 본고의 제2장에서는 이론적 배경으로서 복합안보위협 창발 메커니즘에 대한 논의를 통해 신흥안보위협의 특징과 창발 과정에 대해 살펴보고, 시스템의 결합도 및 복잡성에 의해 구분되는 복합안보위협에 대응하는 거버넌스 유형에 관하여 검토하였다. 이어서 제3장에서는 스마트 메가시티의 본질적 속성으로부터 비롯되는 취약성과 주요 안보이슈에 대해 살펴보았다. 그리하여 제4장에서는 스마트 메가시티의 복합안보위협에 대한 거버넌스 대응전략에 대해 주로 군사적 관점에서 다루었다.

II. 이론적 배경

1. 복합안보위협 창발 메커니즘에 대한 논의

최근 지구적 차원에서 초국가적으로 발생하는 새로운 위험들이 국가안보의 관심사로 떠오르고 있다. 탈냉전, 지구화, 정보화, 민주화 등의 현상을 배경으로 출현한 이러한 위험들은 예기치 않은 천재지변 외에도 인간이 개발한 기술 시스템의 오류나 사회 시스템의 위기 등으로 나타나고 있다. 지난 5년여 동안 동북아에서 발생한 사례만 보아도, 중국발 스모그와 미세먼지의 초국경적 피해, 일본에서 발생한 쓰나미와 후쿠시마 원전 사태, 북한의 사이버 공격과 미 · 중 사이버 갈등, 동남아와 한국에서 발병한 사스(SARS)와 메르스(MERS)의 확산, 북한의 인권과 탈북자 문제 등을 들 수 있다. 이러한 문제들은 여태까지 알려져 있지 않았던 종류의 재난을 야기할 가능성이 클 뿐만 아니라 시스템 내 여러 요소들이 서로 밀접하게 연계되어 해당 분야의 안전 문제를 넘어서 국가안보 전반에 피해를 주는 새로운 위험으로 인식되고 있다. 이러한 새로운 성격의 안보이슈는 전통적인 군사안보 이외에도 비군사적 영역, 즉 환경안보, 인간안보, 자원안보, 사이버 안보 등을 포괄한다. 이러한 위험의 부상은 안보영역이 새로이 확대되는 현상뿐만 아니라 안보주체의 숫자와 범위의 확대 및 안보 세계정치의 양상을 변화시키고 있다. 이들 위험은 그 성격과 파급력의 측면에서 지구적 차원에서 초국가적으로 발생하는 안보문제인 동시에 지역과 국가 차원의 국지적이고 개인적인 안보문제에도 영향을 미치는 다층적이고 복합적인 성격을 지니고 있다. 게다가 국가 행위자 이외에도 국제기구, 다국적 기업, 글로벌 시민사회 등과 같은 비(非)국가 행위자들, 그리고 더 나아가 기술 및 사회 시스템 자체가 위험을 야기하는 원인으로 떠오르고 있는 상황이다(정민섭, 2020).

따라서 새로운 안보문제를 해결하기 위해서는 필요시 개별국가 차원을 넘어서 지역 및 글로벌 차원에서 모색되는 중층적이고 복합적인 거버넌스의 매커니즘을 마련하는 것이 필요하다. 새롭게 대두되는 안보의 이슈는 대개 일상생활의 미시적 차원에서 발생하는 안전의 문제들이 특정한 계기를 만나 거시적 국가안보의 문제로 증폭되는 특징을 보인다(김상배, 2016). 다양한 국가 및 비국가 행위자, 하물며 비인간 행위자까지도 관여하기 때문에 그 발생원인과 확산경로 및 파급효과를 예측하는 것이 쉽지 않다. 신흥안보 분야의 위험은 전례 없던 극단적 사건의 형태로 발생할 가능성이 높을 뿐만 아니라 그 위험의 발생 및 확산의 양상도 개별 신흥안보 분야들 간의 상호 연계성이 증폭되는 과정에서 발생하는 경향이 있다. 따라서 철저한 예측과 대비를 하지 않으면 전통적 위협보다 큰 피해를 받을수 있다고 본다.

최근의 안보분야 신조어로서 '신흥안보'라는 단어는 단순히 '새로운 안보'만을 의미하는 것은 아니며, 복잡계 이론에서 다루는 'emergence'의 개념을 담고 있다. 이는 자연과학계에서 흔히 말하는 '창발(創發)'이라고 번역하는데, 안보라는 말과 합성을 고려하여 신흥이라고 번역하였다(김상배, 2016). 개념어로서의 신흥 또는 창발이란 의미는 미시적 단계에서 단순하고 무질서한 존재에 불과했던 현상들이 복잡한 상호작용을 벌이는 가운데 상호 연계성을 증대시킴으로써 거시적 단계에 이르러 일정한 패턴과 규칙성, 즉 질서를 드러내는 현상을 의미한다. 이를 안보의 개념과 연결시키면 신흥안보란 미시적 차원에서는 단순히 소규모 단위의 안전의 문제였는데, 거시적 차원으로 가면서 좀 더 대규모 단위의 안보문제가 되는 현상을 의미한다.[3] 이러한 신흥안보의 개념은 '비전통 안보'로 대변되던 기존의 소극적인 개념화를 넘어서 좀 더 적극적으로 오늘날의 안보현상을 이해하려는 문제의식을 반영한다. 이러한 신흥안보 위협의 특징은 주로 '잠재성, 불가측성, 다양성, 초국가성, 연계성'으로 요약되는데, 그 구체적인 내용은 다음의 〈표 1〉과 같다.

〈표 1: 신흥안보 위협의 특징〉

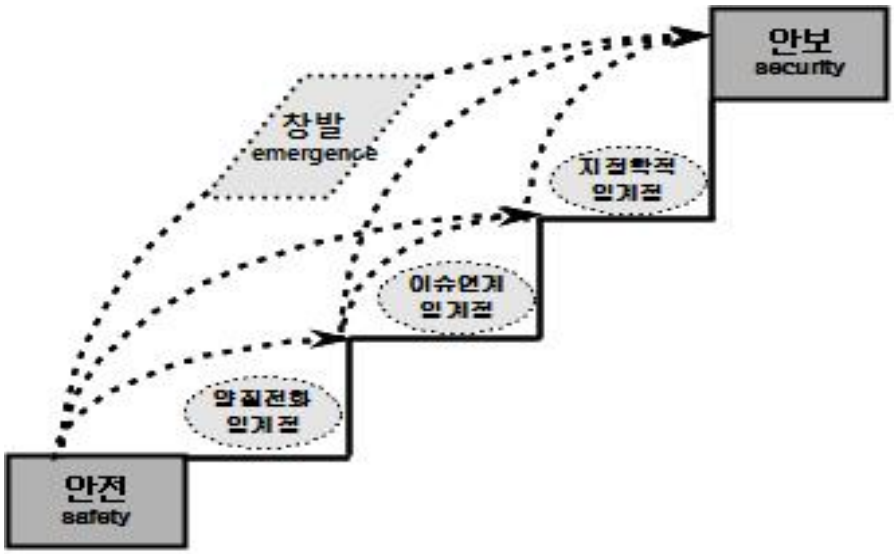
구 분	내 용
① 잠재성	평소 겉으로 드러내지 않거나 미미한 형태로 나타나 심각한 위협인식을 못하나 양적 확대, 질적 심화과정을 거치면서 일정단계를 넘어서면 위협이 급격히 상승
② 불가측성	잠재성이 있어 언제, 어디서, 어떤 형태로 발생할지 예측이 어려움. 위협의 근원이 인간의 통제영역을 벗어나는 자연현상이나 눈에 보이지 않는 바이러스 등에서 시작, 사이버, 테러는 은밀한 공간으로 사전 탐지나 대응 제한
③ 다양성	전통안보는 국가가 주체이자 대상이나 신흥안보 위협은 미세먼지, 바이러스 사이버 공격 등 비인간적 영역 포함
④ 초국가성	어느 한 지역에서 발생한 피해가 일정지역에 국한된 것이 아니라 국경을 넘어 확산되는 특징, 위협에 대응하는 방식도 국가간 긴밀한 협력이 필수
⑤ 연계성	여러 형태로 발생하지만, 이슈상호간 밀접한 관계 속에서 서로 영향을 주고 받으면서 위협의 수준도 상승

3) 김상배, 2017.『신흥안보의 미래전략』. 서울대학교 국제문제연구소 총서 7. p38.

※ 국가전략연구원. 2018,『신안보총람』. pp.4-9. 저자 재구성

복합시스템의 맥락에서 보는 신흥안보는 시스템 내 미시적 상호작용이 양적으로 작용하여 늘어나고 질적으로 변화하여 이른바 양질전화의 임계점을 넘어서게 되면, 거시적 차원에서 국가안보를 위협하는 심각한 문제로 전화되는 현상을 지칭한다. 신흥안보는 다양한 분야에서 발생하는 위험들의 이슈연계성이 높아지면, 어느 한 부문에서는 미시적 안전의 문제였던 것이 국가 전체의 거시적 안보문제가 되는 현상을 지칭한다. 이와 같은 신흥안보의 창발 메커니즘은 다음의 〈그림 1〉과 같다. 이렇게 양질전화와 이슈연계의 연쇄작용을 거쳐 창발하는 종류의 위험에 대해서 전통안보인지 비전통 안보인지에 대한 구별이 다소 무색해질 수 있다. 창발의 가능성을 지니고 있는 신흥안보의 이슈들은 언제, 어떻게 국가적 중대사안이 되어 국가 행위자들간 갈등의 빌미가 되거나 협력이 필수가 될지에 대해 불확실성이 크다.

〈그림 1: 신흥안보의 3단계 창발론〉



※ 김상배. 2017.『신흥안보의 미래전략』. 재인용. p.40.

〈그림 1〉에서 제시하듯이 3단계 창발과정에서 발견되는 임계점은 순차적으로 형성되는 것이 아니라 상호 중첩될 뿐만 아니라 경우에 따라서는 동시에 발생하기도 한다. 첫째, 양질전환 임계점은 신흥안보 이슈 내의 안전사고가 양적으로 증가하여 일정 수준을 넘는 경우에 창발한다. 즉, 양적 증대가 질적 변화를 야기하는 현상을 의미한다. 이러한 예는 1인당 에너지 소비량의 증가는 어느 순간에 빙하를 녹이고 해수면을 상승시키는 지구온난화의 주범이 된다. 한명이 감기에 걸리는 것은 위험이 아니지만, 도시전체에 치사율이 높은 신종플루는 국가안보의 문제가 된다. 컴퓨터 한 대의 해킹은 무시할수 있겠지만, 국가기반시설을 통제하는 컴퓨터시스템의 해킹은 국가차

원의 중대한 위협이다. 둘째, 신흥안보 이슈들 간의 질적 연계성이 높아지게 되면, 어느 한 부문에서 발생한 안전의 문제가 임계점을 넘어서 거시적 안보의 문제가 될 가능성이 커진다. 이러한 사례는 여러 분야에서 발견된다. 기후변화는 이슈연계성이 높은데, 홍수, 가뭄 등과 같은 재해뿐만아니라 수자원 및 식량부족과 연계되면서 환경안보로 창발된다. 이주와 난민문제는 실업문제와 사회질서 불안정, 테러 등의 국가안보의 문제로 확산된다. 셋째, 양질전화나 이슈연계성을 통해서 창발하는 신흥안보 이슈가 전통안보 이슈와 연계되는 경우는 국가안보의 문제가 된다. 지정학적 임계점을 넘어서 국가 간 분쟁의 대상이 되면 국가 행위자가 개입할 근거가 발생되고 문제해결을 위한 국제협력의 메커니즘이 필요하다. 자연재해와 환경악화로 인한 난민발생은 국가 간 갈등이 되고, 종교적 문화적 · 정체성문제는 테러 등의 문제와 연계되면서 국가안보의 중요한 이슈가 된다.[4)]

우리는 신흥안보 이슈가 갖는 이러한 특징과 메커니즘으로 인해 보편적 해법의 마련하는데 더욱 큰 어려움을 겪고 있다. 기존에 인식되지 않았던 위협에 대해서 그 본질에 대한 다양한 담론과 억측이 난무하고 있는 실정이다. 게다가 기존의 안보위협이 상존하는 가운데 새로운 안보위협 요소가 가중되고 상호 연계되면서 더욱 복잡하고 풀기 어려운 '난제(wicked problem)'로 비화되고 있는 상황이다. 이러한 복합적인 위협에 대해서는 기존의 군사적 요소만을 중시하는 안보적 개념만으로는 효과성을 충분히 발휘하기 어렵다. 그리고 이러한 위협의 규모와 성격이 기존의 국가간 전면전 양상과 다르다고 해서, 혹은 그 수준으로 문턱(threshold)을 넘어서지 않았다는 이유로 군사적 요소를 배제하고 민(民) · 관(官)의 노력만으로 해결해내겠다는 것은 국가안보 차원에서 매우 위험한 발상이 될 수 있다.

2. 복합안보위협에 대응하는 거버넌스 접근에 대한 논의

복합안보위협의 창발 · 연계 · 확산은 이에 대처하는 기존 국가통치체제의 변화 필요성에 대한 인식을 확산시키고 있다. 과학기술의 혁명적 발전으로 인한 초연결 사회 구조와 시민들의 생활양식 변화는 개인의 권력과 사회적 경쟁력을 증대시키는 반면, 국가와 정부의 사회에 대한 통제와 영향력은 약화될 것으로 보인다. 개인이나 단체들은 그들의 경쟁력을 강화하고 힘을 합치기 위해 네트워크를 활용하여 서로 비슷한 무리들이나 동일한 목적을 가진 단체들끼리 지역을 넘어 국제적으로 결집하는 현상이 보편화될 수 있다. 거대한 경제력과 권력을 가진 개인들이 원하는 형태로 특정 지역을 운영하거나 스페인의 몬드라곤[5)]과 같이 이익집단들이 연합한 거대 협동조합 혹

4) 김상배, '신흥안보와 메타 거버넌스 : 새로운 안보 패러다임의 이론적 이해', 「한국정치학회보 50」, 2016. 3. pp.83~85

5) 스페인 바스크 지역에 있는 노동자 단체의 협동조합으로 생산협동조합, 교육협동조합 주택협동조합, 농업협동조합 등 총 166개의 협동조합과 약 120여개의 기업을 보유하고 있는 세계적으로 가장 성공한 이익집단 조직이다. 몬드라곤 협동조합은 구성원들에게 사회보장, 고용, 교육, 보건 등 많은 분야의 국가 기능을 제공하고 있는 것으로 알려져 있다.

은 국가 대체 조직, 글로벌 시민 연대 등 새로운 형태의 거버넌스가 등장할 수 있다. 이에 따라 지금까지 국가에 의해 독점되었던 신분 및 거래정보 입증과 발행, 금융 통제 등 많은 부분의 국가 기능이 대체될 것으로 예상된다. 이때 과학기술의 발전은 개인 · 조직 · 국가 간 상호의존도를 증대시키는 동시에 진입장벽과 국경의 제약을 낮추는 등 경계를 초월하는 여건의 조성을 촉진할 것이다. 결국, 향후 국가의 국민에 대한 통제력은 많은 분야에서 약화될 것이며, 국가의 역할은 안보, 외교, 치안, 방재 등 사회를 유지하는데 필요한 최소한의 기능으로 축소될 가능성이 높다.

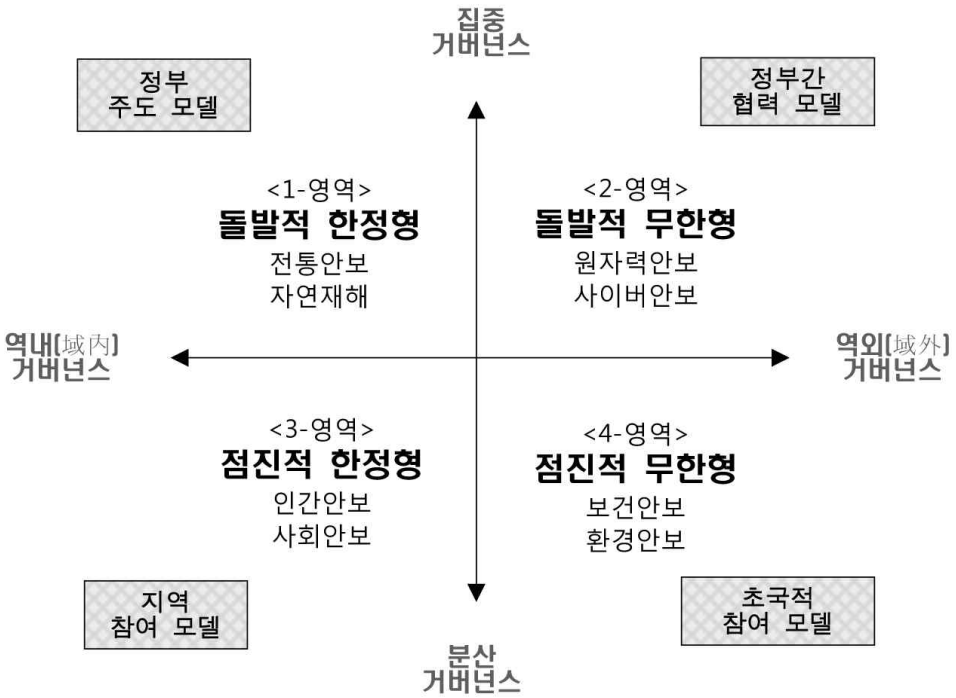
이러한 거버넌스에 대한 논의를 신흥안보 분야에 적절히 적용하기 위해서는 복잡계 환경에서 발생가능한 위험의 성격을 규명하고, 이를 바탕으로 적합한 거버넌스의 형태를 살펴보기 위한 위험의 유형 구분이 필요하다(김상배, 2016). 이와 관련하여 허버트 키첼트(Herbert Kitschelt, 1991)는 찰스 퍼로우(Charles Perrow, 1984)와 올리버 윌리엄슨(Oliver Williamson, 1985)의 조직이론을 원용하여 분석틀을 개발하였다. 키첼트에 의하면, 모든 시스템은 그에 적합한 거버넌스 구조의 선택에 영향을 미치는 두 가지의 특징으로서 시스템의 결합도(degree of coupling)와 시스템 내 인과적 상호작용의 복잡도(complexity of causal interactions)를 제시하고 있다(Kitschelt 1991; 김상배 2007).

먼저, '시스템의 결합도'란 각기 다른 구성요소 간의 시공간적 연결의 필요 정도를 의미한다. 높은 결합도의 시스템은 어느 한 부문에서 발생한 문제가 인접한 다른 부문으로 급속히 전화되는 것을 방지하기 위해 집중 거버넌스 구조를 도입하는 것이 효과적이다. 반면, 낮은 결합도의 시스템은 어느 한 부문의 문제가 시스템 전체로 확산될 가능성이 적기 때문에 분산 거버넌스 구조를 도입해도 무방하다. 이러한 논의는 신흥안보 분야에서 위험의 발생속도(speed)에 대한 논의에 적용할 수 있다. 다시 말해 시스템의 결합도가 높을수록 위험이 갑작스레 시스템 전체로 번져서 위험이 돌발할 가능성이 크기 때문에 집중 거버넌스가 요구되고, 결합도가 낮은 시스템의 경우에는 위험이 점진적으로 발생하여 시스템 전체가 급작스레 붕괴할 위험이 적기 때문에 분산 거버넌스가 도입되어도 무방하다. 또한, '인과적 상호작용의 복잡도'란 시스템의 원활한 작동을 위해 발생하는 구성요소 간 피드백의 정도를 의미한다. 복잡한 상호작용의 시스템인 경우 집중 거버넌스를 도입할 경우 정보의 과부하가 걸리기 쉽기 때문에 주로 분산 거버넌스가 도입된다. 반면, 단선적 상호작용의 시스템인 경우 집중 거버넌스를 도입하여 시스템 내 구성요소간의 상호작용에 직접적으로 개입하더라도 정보처리 과정에서 과부하가 걸릴 가능성이 적다(김상배, 2016).

이러한 논의는 신흥안보 분야에서 위험의 파급범위(scope)와 위험의 조기인지 및 피해예측에 응용해서 적용해 볼 수 있다. 다시 말해 시스템의 복잡도가 높을수록 위험의 파급범위가 무한(無限)해서 그 위험을 즉각 인지하고 그 피해결과를 상정하고 대처하기 어렵기 때문에 경계를 정하지 않은 방식의 역외(域外) 거버넌스가 적합하다. 반면 복잡도가 낮을수록 위험의 파급범위가 한정(限定)되어 있어 그 위험을 조기인지하고 결과를 예측하여 통제할 수 있기 때문에 경계를 정하

는 방식의 역내(域內) 거버넌스를 도입해도 무방하다. 이러한 두 가지 시스템의 속성에 비추어 신흥안보 분야에서 발생하는 위험의 유형을 살펴보면, 〈그림 4〉에서 보는 바와 같은 네 가지 유형으로 나누어 볼 수 있다.

〈그림 3: 시스템의 속성과 위험 발생 유형〉



※ 김상배. 2016. "신흥안보와 메타거버넌스 : 새로운 안보패러다임의 이론적 이해". 재인용. p.92.

이러한 유형의 분류에 있어서, 스마트 메가시티의 본질적 특성과 관련하여 주목하고 있는 영역은 바로 〈2-영역〉이다. 해당 영역은 시스템의 결합도가 높아 위험이 돌발적으로 발생할 가능성이 높으며, 복잡도 역시 높아서 위험의 파급범위가 무한하여 위험을 조기에 인지하기 어렵고 그 결과를 예측하여 통제하는 것도 쉽지 않은 유형이다. 이러한 '돌발적 무한형 위험'에는 일반적으로는 원전사고나 사이버 공격 등과 같은 기술 시스템과 관련된 위험들이 해당된다. 하지만, 스마트 메가시티의 특성을 고려 시 〈1-영역〉 돌발적 한정형, 〈3-영역〉 점진적 한정형, 〈4-영역〉 점진적 무한형의 특성을 갖는 안보위협이라도 시골이 아닌 도시, 그것도 스마트 메가시티에서 발생하면 집중형 거버넌스의 대응소요가 증대되는 측면이 존재한다. 즉, 스마트 메가시티가 그 자체로써 복합안보위협 측면에서의 주요 변수로써 작용할 수 있다는 것이다. 이는 기존의 논의에서 충분히 다루어지지 않았던 사항이며, 이러한 안보위협이 동시다발적으로 발생하여 피해 효과가 누적될 경우에는 도시 그 자체가 안보위협의 취약성이 증대시키는 요인으로 작용하게 될 수 있

음을 의미한다.

Ⅲ. 스마트 메가시티가 갖는 취약성과 주요 안보이슈

1. 스마트 메가시티의 특성 및 취약점

글로벌 트렌드인 스마트 메가시티(smart-mega city) 현상을 살펴보면, ICT기술이 집약되어 스마트化 되면서도 동시에 거대화된 규모를 지닌 도시의 특성과 취약성으로부터 국가안보에 영향을 미치는 모습이 식별된다. 미래에는 물리적 공간, 디지털 공간, 생물학적 공간의 경계가 희석되고 도시의 제반 기능들이 초지능 · 초연결되어 유기적이고 조화롭게 작동하는 스마트시티의 기능이 고도화될 전망이다. 앞으로 등장하는 대부분의 신기술들이 도시의 기능 안에 집약되고 데이터가 상호 연계되어 스마트 홈, 자율주행 차량 및 자율 비행체, 공간정보, 에너지, 헬스 케어, 안전 등의 서비스를 창출하게 될 것이다. 이로 인해, 경제 및 생활 등의 이점을 누릴 수 있는 스마트시티로 인구가 더욱 집중되어 2050년경에는 세계 인구의 70% 이상이 도시에 거주하고, 그 결과 인구 1,000만 명 이상의 메가시티들이 늘어날 것으로 보인다.[6] 이러한 스마트 메가시티에 대해 질적 개념이 부각되는 스마트시티(smart city)와 양적 개념이 부각되는 메가시티(mega city)의 본질적 특성과 취약점을 각각 살펴보면 다음과 같다.

가. 스마트시티의 특성과 취약점

먼저, 미래 스마트시티(smart city) 측면에서의 안보위협 요인은 주로 정보통신 기반체계와 연계되어 부각된다. 정보통신기술(ICT)은 인간 삶의 질을 획기적으로 향상시키는 이점이 있으나 한편으로는 범죄 조직이나 개인 또는 적의 사이버 공격이나 물리적 테러, 미사일 공격 등에 매우 취약할 것이다. IoT, 네트워크, 자동화 · 자율화 등 초연결 기술을 기반으로 하는 도시 운영 시스템에 대한 사이버 공격은 스마트시티의 에너지, 식수, 통신, 행정 서비스, 안전, 금융 시스템 등을 파괴시키고 국민 여론에 결정적인 영향을 미치는 등 핵무기에 버금가는 위협 요인이 될 것이다. 이러한 특성으로 인해 도시 자체가 특정의 목적을 달성하기 위한 범죄 조직이나 테러 단체 또는 적국의 중요한 핵심 표적이 될 가능성이 높다[7]. 이는 전 세계가 개인 · 조직 · 국가 단위의 다양한 노드로써 인터넷 플랫폼을 통해 복합적으로 연결되어 있고, 그와 연관된 수많은 디바이스가

---

6) OECD, 2012, *Environmental Outlook to 2050*.
7) 미군은 이러한 세계적인 도시화 추세와 더불어 향후 도시에서의 군사작전은 '불가피한 표준(inevitable norm)'이 될 것으로 규정하였다(US Military, 2017, Army Technique Publication[ATP] 1-1).

스마트 네트워크로 연결되어 있기 때문이다. 앞으로 AI · BIG Data 융합으로 모든 기술사업 구조가 센서로 상호 연동됨에 따라서 다양한 형태의 사이버 테러공격[8]에 대한 취약성이 증대되고 있다. 향후 사이버 공간의 발전은 사이버 용병, 국가지원 공격자 등으로 주체가 다변화하고, 공격목표도 단순범죄가 아닌 파괴적, 목표 지향적으로 심화될 것으로 보인다.

반면, 스마트 시티에서는 이러한 연결성을 이용해서 안보를 강화하는 수단으로 활용하고자 하는 대응 추세가 나타나고 있다. 즉, 도시의 특성을 이해하고 전략적으로 활용한다면 이는 공자에게 뿐만 아니라 방자에게 있어서도 충분한 이점(advantage)을 제공해준다는 것이다(US Military (Mosul Study Group), 2017, 28-39). 예컨대, 2020년에는 서울시와 육군 수도방위사령부, 국토교통부가 협력해 서울시내 폐쇄회로(CC)TV를 통합 모니터링 하는 '스마트서울 CCTV 안전센터'와 수도방위사령부 상황실 간 연계망을 구축할 예정이다[9]. 이는 방범, 교통, 시설물 관리 등 대시민 서비스를 위해 각 자치구별로 설치한 CCTV 등 정보시스템을 군과 공유하고, 테러발생 등 국가안보와 관련된 위기상황이 발생할 경우 군이 현장 상황을 신속하게 파악, 초동대처에 나서고 서울지역의 안보태세를 높일 수 있도록 시의 스마트도시 통합플랫폼 시스템을 연계한다는 개념이다. 이를 통해 유사시 현장 상황을 신속히 파악하고 관련 정보를 작전부대에 즉시 제공, 지휘통제 능력이 크게 향상되고 군부대의 작전수행 능력도 개선될 것으로 보인다. 이와 마찬가지로 용인시에서도 2020년 8월, 국토교통부 · 국방부 · 서울시 등 4개 기관이 참여하는 '스마트시티 안전망 구축 업무협약'을 체결했다[10]. 용인시가 구축한 스마트시티 통합플랫폼 영상정보를 범인 검거나 화재 진압 뿐만 아니라, 군 작전 통제나 훈련지원 등에도 활용할 방침이다. 이러한 스마트시티 통합플랫폼을 경찰 · 소방 · 군과 영상정보를 공유함으로써 지역사회 안전은 물론 국가안보에도 기여한다는 측면에서 이러한 추세는 보다 확산될 전망이다. 이러한 스마트도시 영상정보 활용개념은 다음의 〈그림 4〉와 같다.

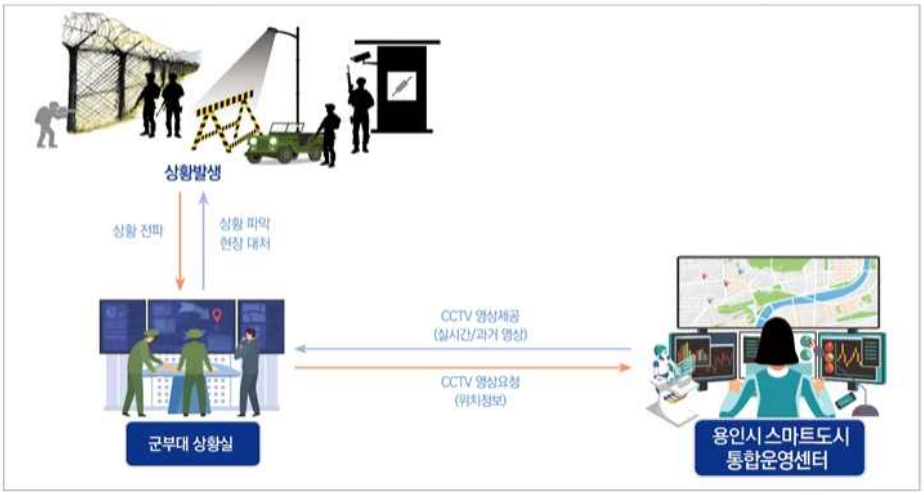
---

8) 인터넷 유 · 무선망, 전자파, 원격 접점, 전력선 등을 이용한 자료절취 · 변조는 물론 물리적 · 심리적 타격을 할 것이다.

9) 예병정. 2020. "서울시, CCTV 통합플랫폼 수도방위사령부와 연계… 안보 태세↑". 파이낸셜뉴스. 2020.8.23. https://www.fnnews.com/news/202008212212019301. (검색일 : 2020.8.25)

10) 김승희. 2020. "용인시, 스마트도시 영상정보 군 작전 활용". 이뉴스투데이. 2020.8.24. http://www.enewstoday.co.kr/news/articleView.html?idxno=1409491. (검색일 : 2020.8.25)

〈그림 4: 스마트도시 영상정보 활용 개념도〉



※ 김승희. 2020. "용인시, 스마트도시 영상정보 군 작전 활용". 이뉴스투데이. 2020.8.24. http://www.enewstoday.co.kr/news/articleView.html?idxno=1409491. (검색일 : 2020.8.25)

주변국의 사이버 안보 대응동향에 대해 살펴보면, 미국은 9.11. 테러이후 사이버공간을 제 5 전장으로 규정하고 국토안보부, 국가정보국, 사이버안보 총국에서 사이버 안보분야를 전담하도록 하면서, 최소한의 인터넷규제와 더불어 민 · 관 · 학이 사이버를 주도케하고 법 · 제도를 정비하고 있다. 또한, 국가사이버 안보전략에서 사이버 위협 행위[11]를 명시하였다. 그리고 중국은 '사이버 안보가 국가안보'라고 천명하고, 사이버공간을 동시에 강화하면서 전문가를 양성하고 있다. 또한, 미국을 견제하기 위해서 '인터넷 안전 없이 국가 안전이 없다'는 점을 강조하며 미국이 주도하는 인터넷 거버넌스 질서에 반대하고 나섰으며, 러시아 등 주변국과 더불어 미국에 대한 견제를 강화하고 있다. 중국은 사이버 안보전략[12]의 일환으로서 사이버 공간 국제협력의 4대 기본원칙으로 6대 전략목표[13]를 설정하였다. 한편, 일본은 2009년 한국의 D-DOS 공격이후 국가정보보호센터를 출범후 체계적인 사이버 업무를 강화하고 있다. 특히, 사이버 방어역량 구축을 위해 군 자위대 조직과 결부하여 중앙집권화 체제로 안보와 군사를 통합하면서, 미 · 일 사이버 안보협약을 체결하여 미국의 사이버 안보우산 체계로 전환, 경제적 · 기술적인 우위를 바탕으로 중 · 러 · 북의 사이버 위협에 적극 대응할 방침이다(조상근, 2020).

11) ①금전적 이득을 목적으로 정보절취, 또는 시스템을 무력화하는 행위, ②정부나 민간 정보시스템으로부터 기밀정보나 정보자산을 절취하는 행위, ③특정국가를 지원하기 위해 사이버 공격을 배양하거나 실천하는 행위, ④비금적적 이익을 목적으로 정보시스템에 침입하는 해킹공격, ⑤비국가 행위자 또는 특정국가의 지원을 받아 사이버 공격을 자행해온 테러리스트 행위 등이다.

12) 사이버 공간 주권수호, 국가안보 수호, 핵심정보인프라 보호, 사이버 문화 건설 강화, 사이버 테러와 불법 범죄단속, 사이버 통치체계 완비, 사이버 보안 기초 마련, 사이버 공간 방호능력 향상, 사이버 공간 국가협력 강화 등 9가지 과제를 제시하였다.

사이버 안보위협은 핵티비즘의 기조가 형성되어 점차 공격기법이 진화하고 있다. 초기에는 호기심, 앙갚음, 금전취득 등 개인적 수준에서 단순한 방식으로 시작되었으나, 미래에는 국가 · 군사시설 보안취약점을 활용한 군사적 공격, 국가 · 계층간 갈등을 야기하는 정치적 사이버 공격, 기술적 편향성과 정보격차 심화에 따른 비대칭 위협, 보복응징이 제한되는 스모킹건 공격 등 사이버 공격이 보다 지능화 복잡화된 형태를 보일 것으로 예상된다. 그리고 정교한 악성코드와 사회 공학적 기법을 사용하여 사회혼란이나 정치적 목적을 가진 국가 단위의 테러리즘 형태로 진화하는 양상을 보여줄 것으로 보인다(정민섭, 2020).

나. 메가시티의 특성과 취약점

이어서, 메가시티(mega city) 측면에서의 안보위협 요인은 주로 도시 규모의 확장과 밀집도의 증가로부터 비롯된다. 밀집된 인구와 경제사회적 제반시설은 자연재해와 인재에 취약하며 메가시티 핵심기능의 손상은 국가기능의 마비를 초래할 수 있다. 또한, 이러한 본질적인 취약성을 보완 및 예방하기 위한 각종 정책을 실행하기 위해서는 천문학적인 비용이 동반되므로 국가 재정에 있어서 막중한 부담으로 작용한다. 따라서 메가시티의 대표성 및 영향력이 증대될수록 그에 따른 취약성이 필연적으로 증가하게 되는 구조를 갖고 있다고 할 수 있다.

실제로, 도시에서는 통상 제한된 공간 내 인구재화기반시설이 집중됨에 따라 소규모 사건재해에도 큰 손실을 초래할 위험성이 내재되어 있으며, 이는 군사적 측면에서 더욱 민감하게 작용한다(Townsend, 2018). 그리고 도시 확장과 도시구조의 변화는 구도심부의 슬럼화 및 공동화를 초래하며 범죄, 교통체증 등의 사회문제와 행정력의 사각지대 양산 등 각종 사회불안요소가 증대되고 있는 실정이다. 게다가 도시의 상주인구 밀집도가 과도하게 높아지면서 도시 기반시설의 수용 용량을 초과하게 되면서 자원부족 문제를 비롯하여 수질 및 대기오염, 대량 폐기물 등 다양한 형태의 환경오염을 촉발시키고 있다. 고도로 산업화되고 고령화, 저출산 현상이 진행되는 선진국의 메가시티에서는 국제 이주민이 증가함에 따라 계층 및 인종갈등 등의 사회문제가 새롭게 대두되고 있다.

이와 같은 스마트 메가시티의 주요 특성에 대해 국가안보 · 군사적 관점에서 도출된 키워드로는 ▲역동성(dynamicity), ▲고밀집성(high density) 및 복잡성(complexity), ▲연결성(connectedness), ▲거대한 영향력(massive influence) 및 대표성(representativeness), ▲취약성(vulnerability), ▲규모(scale) 및 분권화(decentralization)가 있다(교육사, 2020). 이를 토대로 스마트 메가시티의 특성과 취약성을 구체적으로 살펴보면 다음과 같다.

첫째, 역동성(dynamicity)이다. 사회 · 역사 · 문화 · 지리 · 국제적 요소 등의 복합적 환경요인에 의해 형성 및 성장한 메가시티는 각기 다른 고유의 특성을 지니고 있다. 메가시티의 중심도시와 주변도시들은 생태계의 군집과 같이 역동적으로 상호작용하면서 변화하고, 내부의 구성요소

들도 세포의 생애주기처럼 끊임없이 생성 · 진화 · 쇠퇴 · 소멸을 반복한다. 이러한 메가시티를 이해하기 위해서는 특정 도시에 대한 맞춤식 분석이 필요하다는 관점이 존재한다.

둘째, 고밀집성(high density) 및 복잡성(complexity)이다. 메가시티는 거주인구, 기반시설, 인공구조물, 전자기 등 모든 면에서 과거의 도시와 비교할 수 없을 만큼 높은 밀집도를 보이고 있다. 예컨대, 세계 주요 메가시티(중심도시)의 중심지 단위면적(1km2) 당 인구밀집도를 살펴보면, 뭄바이 29,650명, 파리 20,870명, 선진 17,150명, 서울 16,358명, 도쿄 14,312명, 뉴욕 11,014명의 현황을 나타내고 있다[14]. 인구 및 인공구조물의 높은 밀집도는 물리적 유동성(도보 이동, 교통)의 저해 요소로 작용하게 되며, 높은 전자기 밀집도는 통신망 대역폭의 혼잡을 야기하게 된다. 그리고 모든 형태의 유 · 무형적 영역(평지, 인공구조물, 산악, 하천, 바다, 지하, 사이버 등)이 도시내에 복합적으로 존재함에 따라 복잡성 · 불확실성이 증대되며, 이는 메가시티를 이해하고 시각화하는 데 큰 장애요소로 작용한다.

셋째, 연결성(connectedness)이다. 메가시티는 내부 구성원간 또는 외부와의 강력한 물리적(도로, 항공망 등), 사회적(S.N.S., 정보망 등, 경제적(물류망 등) 연결성을 보인다. 이러한 연결성은 메가시티 내에서 거대하고 통제하기 어려운 유동성을 발생시키는데, 뉴욕시 맨하탄에서는 일일 평균 약 280만명의 통근자와 헤아리기 어려운 관광객 등 유동인구가 존재한다. 따라서 메가시티를 평상시 외부로부터 완전하게 고립 · 단절시키는 것은 불가능에 가깝다는 관점이 존재한다.

넷째, 거대한 영향력(massive influence) 및 대표성(representativeness)이다. 메가시티는 고급인력, ICT, 교통 등 국가를 대표하는 다양한 기반이 집중되어 있으며, 1,000만명 이상 밀집된 인구가 형성하는 거대한 소비시장, 주요 행정 · 기업 · 연구기관이 입지로 인해 경제적, 정치적 영향력이 보다 증대되고 있다. 세계적으로도 GDP의 8%가 10대 메가시티에서 발생하고 있으며, 일부는 국가 수준의 경제력(뉴욕시의 GDP가 한국보다 높은 수준)을 갖추고 있다. 세계 각국은 메가시티를 거점으로 하여 국가경쟁력을 제고하기 위한 비전을 설정하고 도시와 국가의 동반 발전전략을 추진 중이다. 특히, 메가시티 거주인구의 증가로 인해 정치적 의사결정에 미치는 영향력을 증대시키는 측면이 존재하며, 도시의 특성을 반영한 자치권 행사를 법적으로 제도화하는 추세(뉴욕시의 '자치헌장', 런던의 '런던대도시법' 등)이다. 이와 같이 심화되는 메가시티化는 국정운영의 중심을 국가 단위에서 도시단위로 변화시킬 것이며, 국가안보와 메가시티 보호의 개념이 동일시 될 것이라는 전망이 존재한다.

다섯째, 취약성(vulnerability)이다. 밀집된 인구와 경제 · 사회적 제반시설은 자연재해와 인재(人災)에 취약하며, 메가시티 핵심기능의 손상은 국가기능의 마비를 초래할 수 있다는 위기의식이 증대되고 있다. 또한, 취약성을 보완 · 예방하기 위한 각종 정책의 실행은 천문학적 수준의 비용을 동반하게 되므로 국가 재정에 큰 부담으로 작용하게 된다. 따라서 메가시티에 국가의 주요

14) 육군 교육사령부. 2020. 『월간작전환경분석 (2020년 1월)』.

시설 및 기능이 집중되는 추세가 지속될 경우, 그 영향력 및 대표성도 함께 증대될 것이다. 하지만, 이로 인해 메가시티의 취약성도 그와 더불어 증대되는 것은 필연적이다.

여섯째, 규모(scale) 및 분권화(decentralization)이다. 메가시티는 모든 특성에서 일반적인 도시와 차별화되며, 이는 발생 가능한 문제의 수와 파급효과가 지수적으로 증가됨을 의미한다. 또한 AI, Big Data, IoT 등 첨단 정보통신기술(ICT)을 활용하는 스마트시티[15]가 미래의 메가시티 운영을 위한 새로운 모델로써 등장하게 되었다. 이를 통해 과거 중앙집권적 · 하향적 도시행정으로는 메가시티의 거대한 규모를 제어 · 관리할 수 없으며, 미래의 도시 행정은 분산적 · 상향적으로 진화해나갈 전망이라는 견해가 중론(衆論)을 형성하고 있다.

하지만, 이러한 특성과 취약성에도 불구하고 도시화는 주요 트렌드로서 확산되고 있는 추세이다. 실제로, 전 세계적으로 경제성장에 따른 급속한 도시화(urbanization)가 진행 중인데, 1일 평균 약 18만명이 도시지역으로 이주하고 있으며, 현재 세계인구의 약 55%가 도시지역에 거주하고 있다. 이러한 추세를 토대로 2030년에는 세계인구의 약 60% (약 50억명) 이상, 2050년에는 약 70% (약 64억명) 이상이 대도시권에 거주할 것으로 전망되며, 정치 · 경제 · 사회적 기능이 집중되고 자립적 경제기반이 형성된 도시는 메가시티로 성장하게 될 것이다. 이러한 글로벌 메가시티는 2018년 기준으로 총 33개(선진국 7개, 신흥국 26개)였으나, 2030년에는 43개로 증가될 것으로 보고 있다(UN, 2018)[16].

2. 스마트 메가시티의 주요 안보이슈

스마트 메가시티에서의 주요 안보이슈는 본질적 속성으로부터 기인한다. 스마트 메가시티에서의 핵심기능이 원활하게 발휘되기 위해서는 해당 프로세스 상에서의 주요 기능을 담당하는 허브와 노드가 외부의 다양한 영향으로부터 충분히 보호되어야만 한다. 만일, 이러한 프로세스에 문제가 발생하면 스마트 시티의 상호연계성이 제대로 발휘되지 못할 것이며, 앞서 언급한 양질전화 및 이슈연계의 연쇄 과정을 거쳐 전통적 위협과 연계되어 심각한 안보문제로 확대될 수 있다.

앞서 언급한 스마트 메가시티의 본질적 속성인 연결성(connectedness), 고밀집성(high density), 복잡성(complexity), 거대한 영향력(massive influence), 취약성(vulnerability)으로부터 비롯되는 주요 안보이슈를 도출해보면 다음과 같다. 먼저, 메가시티 운영의 기반을 이루는 스마

15) 메가시티와 스마트시티의 관계에 있어서, 메가시티는 생존(도시화 문제 해결)을 위해 스마트化가 필요하다는 인식이 증대되고 있다. 도시의 외형적 확장(메가시티化)은 도시문제를 심화시켜 관리 소요가 증가하게 되며, 에너지 · 교통 · 자원 · 폐기물처리 등 문제해결 과정에 신속한 데이터 처리가 필요하다. 하지만, 도시에서 발생하는 광범위한 데이터의 수집 및 처리속도와 관련된 문제로부터 적시성의 문제가 점증하고 있는 상황이다. 따라서 혁신기술들의 속성인 연결성을 활용하여 부족한 자원의 공유를 유도하고, 보다 효율적으로 도시문제를 해결해야만 생존(지속적인 번영)이 가능할 것이라는 인식이 확산되고 있는 추세이다.

16) 2020년 중국은 최다 메가시티(6개)를 보유하고 있으며, 향후 10년 이내에 2개(청두, 충칭)가 추가되어 전 세계 메가시티의 18%를 보유할 전망이다.

트 시티(smart city)의 핵심역량은 정보통신기술에 토대를 둔 상호연계성에서 비롯된다는 점을 인지할 필요가 있다. 도시에서의 네트워크 기반의 상호연계성을 보장하는 것은 정보통신 인프라이고, 그 기능을 원활히 작동시키기 위해서는 근본적으로 에너지 공급이 보장되어야 한다. 이러한 통신 네트워크를 침해하는 의도적인 사이버 공격이 발생하거나, 통신 인프라의 주요 노드가 천재지변, 우발적 사고 등에 의해 기능 고장이 발생할 경우에는 도시의 본질적 속성인 연결성(connectedness)을 손상시키며, 이는 다시 고밀집성(high density)과 복잡성(complexity)으로 인해 연쇄적인 파급효과를 일으키게 되는 것이다. 그리고 도시 기능의 저하로 인해 야기되는 혼란이 확산되면, 국가 통치 기능의 손상 혹은 마비를 불러일으킬 우려가 존재하며, 전통적 안보위협(북한, 주변국 위협 등)과 연계되면 걷잡을 수 없는 안보문제로 확대 · 재생산될 소지가 크다. 이러한 상황에서 안보적 관점에서 이러한 근본적인 취약성이 내재되어 있는 스마트 메가시티에서 에너지 문제는 과연 어떠한 파급효과를 일으킬 것인지에 대해 심도 깊은 검토가 필요할 것으로 판단된다.

향후 발생가능한 스마트 메가시티의 주요 안보이슈로는 ▲대규모 정전, ▲통신(네트워크) 장애, ▲중요시설 화재, ▲감염병 확산 등이 거론되고 있다.

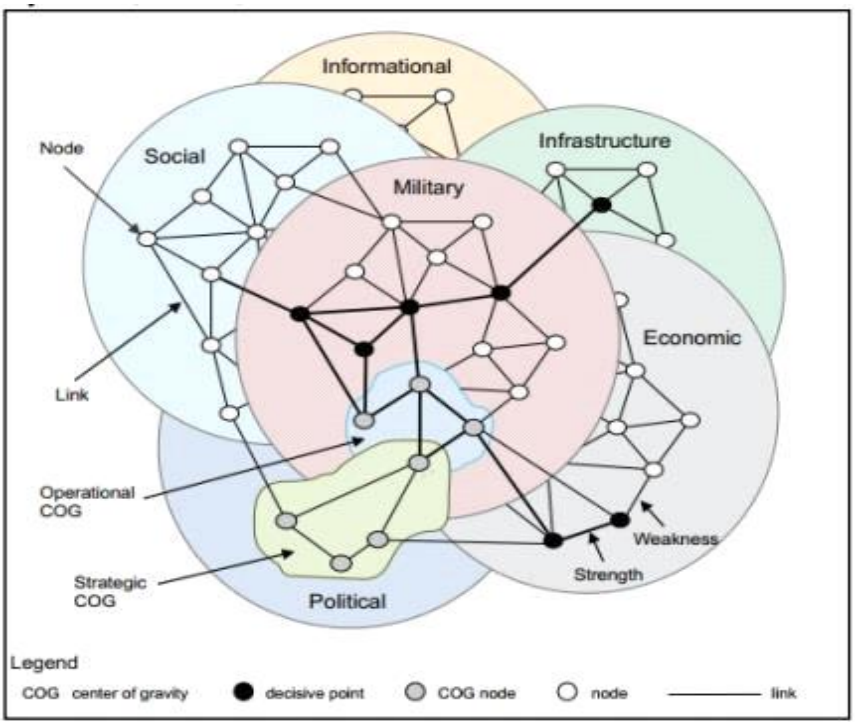
첫째, 메가시티에서의 대규모 정전 문제는 유기체의 혈액공급이 일시에 중단되는 것과 같은 위험을 초래한다. 비록 현재로서는 이에 대한 위기의식이 심각하게 표면화되지는 않았으나, 우리는 스마트 메가시티에서의 에너지는 생명체에게 있어서 혈액에 비견될 수 있을 정도로 가장 기본적이면서도 절대적으로 중요한 역할을 담당하고 있다는 점을 인식할 필요가 있다. 그리고 유사시 에너지의 생산 · 공급 순환이 원활하지 않을 경우에는 국가의 주요 기능이 어느 한 순간에 마비될 수도 있다는 잠재적 위험성(risk)을 자각하고, 이에 대해 범국가적 차원에서 대비할 필요가 있을 것이다. 이러한 에너지 안보위협에 대한 접근은 군사적 관점과 연계되어 재해석될 필요가 있다.

일례로써, KT 아현지사 지하 통신구 화재사건(2018.11.24.)에서는 화재로 인해 서울 중구 · 마포 · 서대문구로 통하는 유무선 케이블 16만8천회선과 광케이블 220묶음이 손상되면서, 서울 서부지역 일대는 갑작스런 통신 마비 사태가 발생하였다. 이로 인해, KT 휴대전화와 인터넷뿐 아니라 카드결제 장애가 발생되어 소상공인들에게 경제적 피해를 초래하였으며, 일반 시민들에게는 큰 불편과 혼란을 야기하였다. 당시 KT는 화재로 인해 약 469억원 규모의 물적 피해를 입었으나, 단지 경제적 측면에서의 손실 뿐만아니라 국가안보적 관점에서는 새로운 위협의 도래를 직관적으로 인식하게 되는 계기가 되었다. 그 외에도 도시에서는 너무나 많은 위협 요소가 상존하는데, 제2롯데월드와 같은 초고층 건물의 대형화재, 출근시간대 지하철에서의 생화학테러, 한여름 · 한겨울의 대규모 정전 사태 등 상주인구 밀집지역에서의 각종 재해, 재난, 테러 등 위협의 가능성을 배제하기 어렵다.

이러한 개념을 군사적 관점에서 '중심 분석(Center of Gravity Analysis)' 메커니즘을 적용하

면 다음과 같다[17]. 스마트 메가시티로서의 수도권은 '국가통수권자의 의지'라는 국가전략적 수준에서의 중심(center of gravity : COG)이 국민 여론을 수렴하는 물리적 공간에 해당되며, 핵심능력(critical capability)인 국가통치능력이 원활히 발휘되도록 하는 주요 수단으로써 ICT 기반체계는 핵심요구조건(critical requirement)으로 기능한다. 그리고 ICT 기반체계의 원활한 기능발휘를 보장하는 필수요소이자, 적대세력으로부터 반드시 지켜내야만 하는 에너지 공급 시스템은 바로 핵심취약점(critical vulnerability)으로 간주될 수 있다. 즉, 적대세력의 결정적 지점(decisive point)[18]으로서 군사적 · 비군사적 목표로 선정되어 필히 공략이 예상되는 취약 지점이 바로 도시기반체계를 유지케 하는 에너지 공급시스템이며, 국가안보차원에서는 이에 대한 각별한 대비가 필요하다는 것이다. 이러한 스마트 메가시티에 대한 군사적 관점에서의 작전환경 인식 개념을 정리하면 다음의 〈그림 5〉와 같다.

〈그림 5: 스마트 메가시티에서의 군사적 작전환경 인식 개념〉



17) 중심(center of gravity)이란 '정신적 또는 물리적인 힘, 행동의 자유 또는 전투의지를 제공하는 능력이나 힘의 원천'이다. 군사이론가인 클라우제비츠가 중심을 "모든 힘과 운동의 중심점으로서, 전체가 의존하며, 우리의 모든 에너지를 지향해야 하는 지점"이라고 강조한 바 있다. 적 중심 분석은 통상 합동작전환경정보분석(JIPOE)의 한 과정이며, 이하에 언급된 중심분석에 관한 사항은 美. 해군전쟁대학(Naval War College) 교육참고 Joint Operation Planning Process Work Book (Jan, 2008)과 대한민국 합동군사대학교의 합동작전 교육자료(2020. 6월)을 참고하였다.

18) 결정적 지점이란 '어떠한 행동이 취해졌다면 지휘관으로 하여금 적에 대해 현저한 이점을 획득하게 하며, 승리 달성에 실질적으로 기여하는 지리적 장소, 특정 주요사태, 핵심요소 또는 기능'이라고 정의되고 있다.(JP 5-0, Joint Planning, 16 June 2017)

※ Kaune, Patrick N. 2016. Analysis of US Army Preparations of US Army Preparation for Megacity Operations. US Army War College-Civilian Research project. Syracuse, NY 13244 : Syracuse University. p.36.

앞서 언급했듯이, 특히 스마트 메가시티에서의 안정적인 에너지 기반체계의 유지는 필수적이다. ICT기반으로 상호 연계성이 극대화되는 스마트 메가시티는 첨단과학기술로써 초연결 · 초지능 · 초융합을 구현해냄으로써 마치 살아있는 하나의 생명체와 같이 생동하게 될 것이나, 동시에 대규모 상주인구의 밀집이 심화됨에 따라 문제 발생 시 막대한 파급효과가 순식간에 확산될 수 밖에 없는 취약점을 갖고 있기 때문이다. 스마트 메가시티가 국가안보 차원에서 차지하는 중요도가 높아질수록 이러한 안보측면에서의 취약점에 대한 방호 필요성은 더욱 부각될 것이다. 그리고 그와 아울러, 스마트 메가시티에서의 안정적인 에너지 공급을 보장하기 위한 안보분야 유관기관 간의 협조는 더욱 중요해질 것이다.

둘째, 메가시티에서의 통신(네트워크)과 관련된 사이버안보 위협은 국가차원의 치명성을 증대시키고 있다. 메가시티는 4차 산업혁명과 맞물려 초연결을 통한 사이버 공간을 확장시키고 사이버 활동을 촉진하게 될 것이며, 그 과정에서 네트워크와 네트워크, 네트워크와 모바일이 연결되는 지점이 기하급수적으로 증가될 것으로 전망된다. 이로 인해 초연결된 메가시티는 필연적으로 사이버 공간에서의 공격, 테러 등 침해행위에 대해 취약해질 수 밖에 없는 구조를 형성하게 된다. 메가시티에서 사이버 공간에 접속할 수 있는 인구가 1,000만 명 이상 존재하며, 이들은 실제의 현실 세계에서 밀집되어 복잡하게 활동하고 있기에 사이버 안보의 치명성이 극대화될 수 있는 충분조건이 갖추어진 것으로 보인다. 이로 인해 인간안보를 침해하는 다양한 사이버 안보이슈가 발생할 수 있다. 예컨대, 경제활동이나 사회활동을 위해 네트워크에 접속하는 개인 단말기(Point of Sales)나 모바일은 사이버 위협의 표적이 되기 쉽다. 특히, 메가시티는 사이버 활동 인구가 많아서 개인 사이버 위협이 증가할 것이고, 사이버 테러나 범죄도 개인 단말기나 모바일을 통해 최종 목표에 도달하는 방식으로 전환될 가능성이 있다.

한편, 사이버 양극화를 통한 사회문제가 심화될 수 있다. 메가시티에서도 인구구조 변화 트렌드에 의해 아날로그 방식에 익숙하여 디지털 장비를 능수능란하게 다루는 것이 제한적인 노년층의 비중이 커질 것이며, 이들은 인터넷을 능수능란하게 다루지 못함으로써 사이버 서비스로부터 소외될 수 있다. 또한, 메가시티에서의 사회경제적 약자 및 극빈층은 인터넷 등 네트워크 서비스에 접속조차 하지 못함으로써 사이버 공간 · 활동으로부터 고립될 우려가 크다. 특히, 인공지능과 결합되어 사회의 혼란을 야기하는 새로운 안보문제에 직면하게 될 가능성이 존재하는데, 이러한 문제는 인공지능 기술이 발전할수록 더욱 정교해질 것이고 더욱 큰 파급효과를 일으킬 것으로 우려된다[19]. 이로 인해, 국민들은 인지 조작에 쉽게 현혹되어 사실과 거짓을 구분할 수 없는 사

[19] 'Deepfake'는 'Deep-learning'과 'Fake'의 합성어로서 인공지능에 의해 조작된 음성과 영상을 의미한다. 실제

이버 회색지대(Grey Zone)에 서게 될 것이다. 따라서 거대한 사이버 공간에서는 데이터 조작이나 합성, 비정상 접속, 해킹 등을 조기에 식별할 수 있는 지능형 사이버위협이 증대되고 있다.

군사적으로는, 전쟁의 패러다임(Paradigm)이 사이버전 중심으로 전환되고 있는 가운데, 메가시티가 사이버전 격전지로 떠오르고 있다(조상근, 2020). 미 · 일 · 중 · 러의 움직임에서 볼 수 있듯이 미래 전장(戰場)은 지상 · 해상 · 공중 · 우주뿐만 아니라, 사이버 공간으로도 확대되고 있다[20]. 이로 인해, 미래 전쟁은 물리적 공간과 비물리적 공간의 수단과 방법이 복합된 하이브리드(Hybrid) 형태로 진행될 것이고, 무엇보다도 전쟁의 주체, 시기, 목적 등을 쉽게 식별할 수 없게 될 것이다. 여기에 4차 산업혁명의 주요기술(AICBM : AI, IoT, Cloud, Big Data, Mobile)은 전 세계를 하나의 거대한 네트워크망으로 초연결하고 있다. 또한, 이번 코로나-19로 열린 온택트(Ontact) 시대는 전 세계의 인터넷 보급률을 급상승시킬 것으로 보인다. 미래 전쟁에서 사이버전이 차지하는 비중이 높아질 수밖에 없는 상황이 조성되고 있는 것이다.

셋째, 국가의 주요시설과 더불어 (초)고층건물[21]이 밀집해 있는 메가시티에서의 소방 및 방재 문제는 보다 큰 파급력을 지닌다. 이러한 공간에서 발생하는 화재는 메가시티에서 막대한 인명피해를 야기할 뿐만 아니라 직 · 간접적으로 국가의 주요 기능에 부정적인 영향을 초래할 우려가 크다. 고층건물에서의 화재는 순식간에 확산되며 대형참사로 이어질 가능성이 높으며, 우리나라에서도 대형 참사의 가능성이 높은 빌딩들이 적지 않다는 점을 유념할 필요가 있다.

더불어민주당 홍익표 의원실이 소방청으로부터 확보한 자료(2020.8.10)에 따르면, 우리나라 30층 이상 고층 건축물 135동에 가연성외장재가 설치된 것으로 드러났다. 구체적으로 보면, 아파트 등 공동주택 건축물이 97동으로 가장 많았고, 업무용 건축물 34동, 숙박 건축물은 2동, 기타 2동이었다. 문제는 가연성 외장재를 사용한 건축물이 불연성 외장재 사용이 의무화 된 2012년 이전에 지어진 건물들이어서 강제로 외장재를 교체할 수 없다는 점이다. 소방청은 일반적인 30층 건축물의 외장재를 바꾸는 비용이 약 30억원 정도로 추산하고 있다. 이런 가운데 최근 5년간 고층건축물(30층 이상)에서 발생한 화재는 계속해서 늘어나는 추세다. 2013년 고층건축물에서 발생한 화재는 86건이었는데, 2014년 107건, 2015년 107건, 2016년 131건, 2017년 145

로 2018년 4월 오바마 전 대통령이 트럼프 대통령을 비난하는 가짜 영상이 유포되어 미국 정계가 요동치기도 했다.

20) 러시아군은 인터넷, SNS, 언론 등을 활용하여 공세적인 심리 · 정보작전을 전개한 결과 돈바스 전쟁(War in Donbass)에서 유리한 여건을 조성하였다(2014년). 그리고 중국군은 본격화되는 사이버 전쟁에 대비하기 위해 10만 명 규모의 해커로 구성된 '사이버공간작전부대(網絡空間作戰部隊)'를 창설하였다(2016년). 이에 대응하여 미군은 지상뿐만 아니라, 해상, 공중, 우주, 사이버 · 전자기 등 모든 영역을 활용하는 다영역작전(Multi-Domain Operations) 개념을 발표하였다(2018년). 또한, 일본 방위성은 우주 감시와 사이버 방위 능력 강화를 위해 110명 규모의 우주 · 사이버사령부를 발족하였다(2020년).

21) 대한민국에서 초고층 건물은 건축법 시행령 제2조 18에 의하면 높이 200m 이상 또는 50층 이상인 건축물을 말한다. (c.f. 브리태니카 사전에서의 정의를 살펴보면, 고층건물에 대한 다양한 기준이 존재하는데, 통상 20세기 이후에는 40~50층 이상의 건물을 고층건물로 간주한다. (The term skyscraper originally applied to buildings of 10 to 20 stories, but by the late 20th century the term was used to describe high-rise buildings of unusual height, generally greater than 40 or 50 stories. (from : https://www.britannica.com/technology/skyscraper) (검색일 : 2020.8.25.)

건이었다. 5년 만에 약69%가 증가한 것이다[22]. 일례로써, 영국 런던의 그렌펠타워 화재사건(2017.6.14.)에서 순식간에 불길이 건물 전체를 뒤덮고 72명의 사망자를 냈던 경우를 볼 수 있다. 이때 화재가 대형참사로 번진 주요 원인으로는 건물 외벽에 설치된 가연성 복합패널이 지목되었는데, 알루미늄 복합 판넬내부 단열재가 연소되면서 공간이 형성 됐고, 이 공간이 굴뚝효과를 유발하면서 불길이 급속히 위로 확산되었다는 것이다. 이와 관련하여 대한민국 건설기술연구원(2020)에서 실시한 주상복합건물에서의 화재발생 시뮬레이션에 따르면, 4층에서 시작된 불이 38층 꼭대기까지 번지는 데 20분밖에 걸리지 않았던 결과를 보였던 것을 상기할 필요가 있다[23].

이런 초고층건물 상층부에서 발생한 화재를 진압하기는 쉽지 않다. 통상 화재진압작전에서는 외부에서 내부로 진입해 화재를 진압하지만, 초고층건축물은 외부에서 진입할 방법이 마땅치 않기 때문이다. 물론, 물대포가 장착된 소방헬기를 이용해 화재진압에 나서는 방법이 있지만, 물대포가 장착된 소방헬기는 단 1대뿐이며, 고성능(CAFS) 소방펌프차의 방수 거리도 300m 안팎이어서 400m 이상 되는 초고층건축물 화재 진압에는 충분치 못하다. 최근에는 (초)고층건물에 소방용 드론을 투입하고자 하는 시도가 이루어지고 있으나, 아직 실험적 수준에 머물고 있으며 화재 현장에서 실질적인 화재진압 효과를 기대하기에는 다소 요원한 실정이다.

이 뿐만 아니라, 메가시티에서의 화재와 연계되어 발생하는 대형폭발사고와 유독물질 등에 대한 피해 우려도 증대되고 있는 상황이다. 최소 135명이 숨지고 약 18조원의 경제적 피해가 발생했던 레바논 베이루트 대폭발 참사(2020.8.4.)[24] 이후, 국내 최대 규모의 석유화학공단이 위치한 울산에서는 폭발사고에 대한 불안감이 확산되고 있다. 울산석유화학단지는 전국화학단지 면적의 53%, 저장 액체위험물의 42%, 특히 고위험 화학물질의 연간 유통량 27%이상을 차지할 정도로 국내 최대 규모를 자랑한다. 위험물제조소 등의 설치를 허가 받은 업체는 8126곳에 이르며 특히 유해화학물질 영업허가를 받은 곳은 723곳이나 된다. 특히, 이번 베이루트 대폭발의 원인으로 지목된 질산암모늄의 경우 울산지역 내 취급업체가 18곳에 이르고 있지만 실태 파악은 전혀 이뤄지지 않고 있어 우려를 키우고 있다. 기껏 공개된 정보는 업체 9곳과 5만t가량 뿐 이 외에는 실제 얼마나 많은 양이 저장돼 있고 어떤 곳에 사용되는지 울산시조차 정확히 알지 못하고 있다. 관련 정보가 기업의 영업비밀로 비공개 분류된 데다 국민총리실 대테러센터의 비공개 요구 때문이다. 이번 베이루트 폭발 당시 현장에는 약 2750t의 질산암모늄이 보관 중이었던 것으로

---

22) 김구연. 2018. “英 그렌펠타워 대참사…한국도 빌딩 135동 '화재 무방비'”. CBS노컷뉴스. 2018.10.11. https://www.nocutnews.co.kr/news/5042924. (검색일 : 2020.8.25.)

23) KBS뉴스. 2019. “고층건물에서 불이 나면?…화마 피하는 ‘화장실’”. KBS뉴스. 2019.7.15. http://news.kbs.co.kr/news/view.do?ncd=4242054&ref=A. (검색일 : 2020.8.25.)

24) 미셸 아운 레바논 대통령은 베이루트 폭발 참사로 인한 피해액이 150억 달러(한화 17조7천억원)를 넘는다고 밝혔다(2020.8.12.). 아운 대통령은 이날 트위터에 스페인 국왕 펠리페 6세와의 전화통화 소식을 전하면서 "폭발로 인한 피해의 초기 추정치가 150억 달러를 넘는다"고 전했다. 베이루트에서는 지난 4일 항구 창고에 보관돼 있던 인화성 물질 질산암모늄이 대규모로 폭발, 200명 넘는 사망 · 실종자와 5천명 이상의 부상자가 속출했다. (백나리. 2020. “레바논 대통령 "베이루트 폭발 피해액 17조원 넘어"”. YTN. 2020.8.13. https://www.yna.co.kr/view/AKR20200813002800071?input=1195m. (검색일 : 2020.8.25.))

알려졌다.

이 같은 상황은 공단 내 폭발, 화재사고와 유독물질의 누출사고와도 연결된다. 최근 3년간(2017~201) 해마다 30여 건씩 97건의 화재, 폭발 사고가 발생했다. 특히 유해물질 관련 사고는 최근 5년간 272건(2019 울산시정백서)이나 발생했으며 누출로 이어진 사건도 104건이나 된다. 질산암모늄과 관련해서도 지난 2013년 공단 내 비료공장에서 화재가 발생한 바 있다[25]. 이에 따라 베이루트 사고를 반면교사 삼아 고위험 우려 물질의 처리 정보를 의무적으로 공개할 수 있도록 관련법을 개정하고, 국가가 직접 고독성 · 고위험물질 관리센터를 울산에 건립해야 한다는 목소리가 높아지고 있는 실정이다.

넷째, 메가시티에서의 감염병 확산은 국가차원에서의 심각한 안보 위협요소이다. 메가시티의 취약성(vulnerability)은 근본적으로 높은 밀집도에서 비롯되며, 이는 다시 메가시티의 인구이동, 유통, 물류 등이 이루어지는 복잡한 교통(交通) 흐름으로 인해 더욱 배가된다. 메가시티에서의 교통의 경로는 현재 지하, 지표면, 수로 등 다영역 교통로들을 보유하고 있고, 근미래에는 드론과 같은 공중 기동체의 등장으로 공중 공간이 추가적으로 활용될 전망이다. 이러한 다영역 교통로(multi-domain traffic routes)들은 상호 촘촘히 연결되어 하나의 거대한 복합교통망을 형성하고 있는데, 지하철, 기차, 버스, 택시, 선박, 드론 등 고속으로 이동하는 대중교통수단은 메가시티의 역동성(dynamicity)과 복잡성(complexity)를 증대시키는 요인이다. 특히, 타지역으로부터 다양한 교통로가 집중되고, 주변의 국제공항 · 항구와 연결되는 메가시티의 지리적 특징은 인구 및 물류의 흐름이 집중되는 국내 · 외 교통의 허브(hub)로써 기능케한다. 이는 유사시 발생할 수 있는 여타의 다른 취약요인과 상호작용하며, 문제의 부정적 영향력이 순식간에 전방위로 확산되는 구조적 취약성을 필연적으로 동반하게 되는 속성을 갖게 한다. 예컨대, 이런 초연결된 메가시티의 복합교통망을 따라 바이러스 감염자들이 이동한다면, 바이러스 확산 속도와 범위는 상상을 초월할 것이다. 특히, 서로 다른 영역의 교통로가 중첩되는 지점은 바이러스를 전이시키는 핵심지점이 될 것이므로 다른 영역과의 교통로가 중첩된 교통의 요충지는 집중적으로 관리될 필요가 있다.

일례로써, 2020년 발생한 코로나-19는 전 세계로 확산되어 각국의 주요 도시를 위협하고 있다. 이 중에는 도쿄, 베이징, 뉴욕 등 인구 1,000만 명 이상의 메가시티들도 포함되어 있다. 코로나-19로 인해 우리나라뿐만 아니라, 전 세계가 멈춰 섰다. 각국은 코로나-19의 확산을 방지하기 위해 안간힘을 쓰고 있지만, 코로나-19는 전 세계를 팬데믹(pandemic)의 공포에 몰아넣고 있다. 이러한 상황에서 메가시티가 새롭게 조명되고 있다. 메가시티는 1,000만 명 이상의 인구가 거주하는 거대한 도시로서 인구밀도가 높아 전염병에 취약하기 때문이다. 메가시티를 포함한 주요 도시의 인구밀도는 상당히 높아서 감염률과 치사율이 치솟을 수 있고, 이미 이와 같은 전망은 현실화되고 있다. 각국에서는 코로나-19의 확산을 차단하기 위해 강도 높은 사회적 거리두기

25) 최수상. 2020. ""레바논 대폭발, 남의 일 아냐" 울산석유화학공단 불안 커졌다". 파이낸셜뉴스(2020.8.23.). https://www.fnnews.com/news/202008231657063393. (검색일 : 20.8.25)

(Social Distancing)를 시행하고 있지만, 백신이 개발되기 전까지는 임시방편에 불과할 것으로 보이며 각종 부작용이 속출하였다. 전 세계적으로 장기간 이어지는 '사회적 거리두기(social distancing)'으로 인해 각국에서는 국민의 피로가 한계에 다다르고 있으며, 경제활동도 위축되고 있다.

이와 관련하여 전문가들은 코로나-19 이후의 사회 변화에 대해 분야별로 예상되는 문제점을 예측하고, 대응책을 마련해야 한다고 말하고 있다. 이와 관련하여 메가시티에서 전망되는 주요 변화는 다음과 같다.

정치(Political) 분야에 있어서, 유권자들의 주요 활동이 물리적 공간이 아닌, 사이버 공간에서 이루어질 전망이다. 앞으로 코로나-19와 같은 신종 전염병이 더욱더 빈번하게 발생할 것으로 예측되고 있기 때문이다. 이로 인해, 전염병이 확산되는 상황에서도 선거 활동에 지장을 받지 않는 사이버 정치 활동이 더욱 중요해질 것이다. 특히, 인구밀도가 높은 메가시티에서는 사이버 국민투표도 추진될 수 있을 것이다. 군사(Military) 분야에서는 메가시티에서의 신속대응능력을 갖춘 군의 역할이 더욱더 확대될 것이다. 우리 군은 이번 코로나-19 사태에서 국민의 생명을 보호하기 위해 의료 · 방역 분야의 전문인력, 장비, 물자를 감염자가 급증하는 도시지역에 투입하였다. 이처럼 군이 긴급하게 투입된 이유는 상시 출동태세를 갖추고 있는 군은 전방위로 확산하는 전염병에 신속하게 대응할 수 있기 때문일 것이다. 앞으로 군의 역할은 전통적인 안보뿐만 아니라, 전염병, 재해재난, 환경오염 등 신흥안보위협(new emerging threats)이 포함된 비전통적인 안보분야로 확대될 것이다. 경제(Economy) 분야에서는, 메가시티는 국가 경제의 중심지로서 비접촉(non-contact) 경제활동이 활성화될 것이다. 메가시티의 경제활동이 장기간 정지되면, 국가 경제가 침체될 수 있으므로 사회적 거리두기가 진행되더라도 메가시티의 경제활동은 지속되어야 할 것이다. 사물인터넷(IoT), 클라우드(Cloud), 모바일(Mobile) 기술을 이용하면 재택근무 환경을 조성될 가능성이 높다. 사회(Social) 분야에서는, 주변과의 소통, 교육 등 사회 제 분야의 활동이 원격시스템으로 이루어질 것으로 전망된다. 하지만, 이때 메가시티의 거대 와이파이 존(Wifi Zone)에 사각지대가 발생할 경우, 사이버 양극화로부터 파생되는 전혀 예상치 못한 새로운 사회 문제가 발생할 수 있다. 즉, 코로나-19 이후, 메가시티에서는 4차 산업혁명 주요기술(AI, IoT, Cloud, Big-data, Mobile, Drone-Bot 등)이 적용되어 메가시티가 초연결 · 초지능화됨으로써 강도 높은 전염병 예방과 확산 방지 노력을 기울이면서도, 경제활동을 병행할 것이다.

이와 같이, 한반도의 전통적 위협이 상존하는 가운데, 새로운 안보위협요소의 발생 가능성을 염두에 두고 이를 조기에 통제하기 위한 범국가적 위기관리체계가 마련되어야 할 것이다. 특히, 스마트 메가시티에서의 안보위협은 각각의 위협요소들이 개별적으로 또는 복합적으로 상호작용하면서 다양한 층위에서 증폭되고 있다. 이는 오늘날 복합적인 위협을 관리하는 메커니즘을 발전시키기 위해서 민 · 관 · 군 · 산 · 학 · 연 및 NGO · IGO 등의 상호 협력이 필수적이며, 이러한 다양한 안보분야 노드(node)간 수평적 · 수직적 상호협력을 극대화시키는 거버넌스 관점에서의 통

합된 접근에 대한 개념 발전이 이루어져야할 시점이라는 점을 환기시킨다.

서 언급되었듯이, 스마트 메가시티에서는 시스템의 결합도가 높아 복합안보위협의 발생속도 측면에서 돌발적 발생 가능성이 높으며, 영향 요소 간 상호작용의 복잡도가 높기에 복합안보위협의 파급범위가 커질 가능성이 높다. 이러한 복합안보위협을 효과적으로 통제하기 위해서는 그 본질적 속성을 파악하고 유형화하여, 유형별 대응전략을 발전시켜나갈 필요가 있다. 즉, 유형 구분의 기준으로서, 문제가 발생하고 파급효과가 미치게 되는 시간(time)과 공간(space)의 개념을 적용함으로써 문제 유형을 세분화하고 각각의 효율적인 대응 전략을 마련해야 한다는 것이다. 먼저, 시간(time)의 측면에서는 복합안보위협의 피해에 대한 '확산 속도'의 관점에서 확산 속도의 '급속'과 '완만'으로 개념적 구분이 가능할 것이다. 또한, 공간의 측면에서는 복합안보위협을 촉발하는 원인행위의 '발생 원점'의 관점에서 크게 '물리적 공간(실제 공간)'과 '비물리적 공간(가상 공간)'으로 구분할 수 있을 것이다. 이러한 개념적인 구분 영역 내에서 각각 효율적인 거버넌스적 복합위협관리 메커니즘[26]이 확립되고 작동할 수 있다면, 민 · 관 · 기타 역량의 집중소요가 상대적으로 큰 영역과 군사적 역량의 집중될 소요가 상대적으로 큰 영역에서 국가역량을 가장 효과적으로 발휘할 수 있는 효율적인 거버넌스적 접근이 가능해질 것이다.

이와 같은 스마트 메가시티의 주요 안보이슈들은 단독으로 발생하기 보다는, 서로 상호작용하며 복합적으로 발생하고 안보이슈를 돌발적으로 부각시킬 가능성이 클 것이다. 이러한 스마트 메가시티의 주요 안보이슈에 관한 위협 유형 및 내용을 정리하면 다음의 〈표 2〉와 같다.

〈표 2: 스마트 메가시티의 주요 안보이슈〉

구분	주요 속성	위협 유형	내 용
스마트 시티	초연결성	통신 · 전자기	통신인프라 침해, 사이버 테러, 네트워크 마비 등
		에너지	대규모 정전 발생, 에너지 공급 노드 침해 등
메가 시티	밀집성, 복잡성, 취약성, 결합성, 상호작용,	소방 · 방재	고층건물 화재, 대형밀집시설 화재, 위험물질 특수 화재, 대형 건축물 붕괴, 지하철 사고 등
		보건	감염병 확산 (*교통 연계/확산), 식 · 용수 오염, 수질오염 등

Ⅳ. 스마트 메가시티의 복합안보위협 거버넌스 대응전략

[26] 미래 위협의 진화(evolution) 양상을 고려할 때, 불확실성이 더욱 증대되는 추세이므로 군사적 조치만으로는 효과적인 대응이 부족해질 가능성이 클 것으로 판단하였으며, 복합위협에 관한 '예측, 예방, 대비, 대응 복구' 측면에서의 거버넌스적 접근 개념이 필요함을 전제로 하였다. (참고 : 김흥수. 2014. "한국적 특성에 부합한 국가위기관리체계 구축방안". 『국방정책연구』제30권 3호. 134-135.)

1. 범정부 차원의 복합안보위협 대응 실태

앞서 살펴본 스마트 메가시티에서의 주요 안보이슈는 이슈 간 상호작용을 통해 파급효과가 증폭되며, 전통적 안보위협과 연계될 경우에는 국가차원에서의 심각한 위기상황을 초래할 수 있다. 따라서 범국가적 차원에서 이러한 복합적인 안보위협요소를 통제하는 거버넌스 협력체계를 갖추어야 하며, 민 · 관 · 군의 모든 유관 조직이 상호 연계된 대응전략을 발전시켜야 할 것이다. 현재의 범정부 차원에서 이루어지고 있는 복합안보위협 대응 실태를 살펴보면 다음과 같다.

현재 범정부 차원에서 대응은 국가안전관리기본계획(재난 안전관리 기본법 제22조)에 의거 각종 재난 및 사고로부터 국민의 생명 · 신체 · 재산을 보호하기 위한 일환으로 국가의 재난 및 안전관리의 기본방향을 설정하고 있다. 국가안전관리기본계획은 도시화 · 인구집중, 고령화, 기후변화, 신종감염병의 발생 등 재난환경 변화에 대응하여 국가가 국민을 재난 및 안전사고로부터 보호하기 위한 계획[27]이며, 다음과 같은 내용을 포함하고 있다. 첫째, 향후 5년간 국가 재난 및 안전관리 정책을 통합적으로 운영할 수 있는 방안과 이를 이행하기 위한 중점추진과제들을 제시한다. 둘째, 중앙행정기관과 지방자치단체를 포함한 각종 재난관리책임기관들이 세부대책을 수립 · 운영할 수 있는 지침을 제공한다. 셋째, 국가적 안전관리를 위한 자원의 통합적 운영 및 예방 · 대비 · 대응 · 복구의 각 단계별로 국가적 역량을 통합, 조정할 수 있는 방안을 제시한다. 이 계획에서 다루는 재난의 정의는 국민의 생명 · 신체 · 재산과 국가에 피해를 주거나 줄 수 있는 것을 말한다. 재난에는 자연재난과 사회재난이 있는데, 먼저, 자연재난은 태풍, 홍수, 호우(豪雨), 강풍, 풍랑, 해일(海溢), 대설, 한파, 낙뢰, 가뭄, 폭염, 지진, 황사(黃砂), 조류(藻類) 대발생, 조수(潮水), 화산활동, 소행성 · 유성체 등 자연우주물체의 추락 · 충돌, 그 밖에 이에 준하는 자연현상으로 인하여 발생하는 재해이다. 사회재난은 화재 · 붕괴 · 폭발 · 교통사고(항공사고 및 해상사고를 포함) · 화생방사고 · 환경오염사고 등으로 인하여 발생하는 것[28]을 말한다. 국방재난관리 훈령에 반영된 재난 유형 및 주관 기관은 다음의 〈표 3〉과 같다.

〈표 3. 재난 유형에 따른 주관 기관[29]〉

27) 행정안전부, 「제 4차 국가안전관리기본계획(안)」, 2019.7 pp3.~4.
28) 재난 및 안전관리 기본법 제 3조 정의
29) 행정안전부. 2020. 「국가안전관리 기본계획」 제5장 피해유형별 재난안저관리대책 참고로 재작성

구 분	관리번호	재 난 유 형	주관기관
자연재난 분야 (10유형)	1	풍수해(태풍 · 호우 · 대설)	행정안전부
	2	지진(지진해일 포함)	행정안전부
	3	대형 화산폭발	행정안전부
	4	산사태	산림청
	5	낙뢰	행정안전부
	6	한파	행정안전부
	7	폭염	행정안전부
	8	조수재난	해양수산부
	9	우주전파 재난	과기부
	10	자연우주물체 추락 · 충돌	과기부
사회재난 분야 (22유형)	11	지하철 사고	국토교통부
	12	고속철도 사고	국토교통부
	13	산불	산림청
	14	다중밀집시설 대형화재	소방청
	15	다중밀집시설 건축물 붕괴	국토교통부
	16	공연장 안전사고	문화체육관광부
	17	해양분야 환경오염사고	해양수산부
	18	수질분야 환경오염사고	환경부
	19	유해화학물질 유출사고	환경부
	20	댐 붕괴 사고	국토부, 산업부
	21	공동구 재난	국토부, 행안부
	22	감염병 재난	보건복지부
	23	가축질병	농림축산식품부
	24	해양선박사고	해양수산부
	25	해양 유도선 사고	해양경찰청
	26	전력 분야	산업통상자원부
	27	원전안전사고	산자부, 원안위
	28	육상 화물운송 분야	국토교통부
	29	식·용수 분야	국토부, 환경부
	30	보건의료 분야	보건복지부
	31	GPS전파혼신	과기부
	32	정보통신 분야	과기부
해외재난	33	해외재난 긴급구호 군 수송 지원	외교부

우리나라 재난 관리는 재난의 발생 원인을 크게 자연적 요인과 사회적 요인으로 구분하고 각각의 분류에서 관리대상 재난을 나열하는 방식을 제시하고 단일부처에서 담당하고 있다. 그러나 최근 어떤 재난이 자연적 요인인지 사회적 요인인지 구분하기 어려운 새로운 현상들이 발생하고

있다. 사회재난으로 정의되었으나 풍속, 풍향과 황사 등의 자연적 영향이 매우 큰 미세먼지나 인위적 요인으로 촉발된 포항 지진 등은 대표적인 사례이다. 게다가 향후 미래의 주요 트렌드로써 확산되고 있는 도시화 현상에 대한 고려가 미흡하며, 특히 스마트 메가시티에서의 다양한 안보위협에 대한 대응체계는 현재의 국가 재난 및 안전 관리계획 상에 반영되어 있지 않은 실정이기에 상황이 매우 심각하다.

현재 국가차원에서 위기관리절차는 〈표 4〉과 같이 예방(prevention), 대비(preparedness), 대응(response), 복구(recovery) 등 4단계로 되어있다. 국가 위기관리는 위기의 시간대별 진행과정을 중심으로 위기 발생 前(예방-대비단계), 위기발생 後(대응-복구단계)로 구분한다.

〈표 4. 국가위기관리 절차〉

구 분	개 념	방 법
① 예방 (prevention)	국가위기 발생요인을 사전에 제거 감소시켜 위기발생 자체를 억제하거나 방지	제도개선 및 정책적 대안 강구, 취약점 보완 · 관리하는 활동
② 대비 (preparedness)	국가위기 상황하에서 수행해야 할 제반 사항을 사전에 계획하고 준비	교육훈련 시행 및 위기징후, 상황 · 경보 수준에 따라 비상근무 태세를 유지하여 대응능력 제고시키는 활동
③ 대응 (response)	국가위기 발생시 국가의 자원과 역량을 효율적으로 활용하고 신속하게 대처하여 피해를 최소화	2차적인 위기 발생 가능성을 감소시키는 실제적인 활동
④ 복구 (recovery)	국가위기로부터 발생한 피해를 발생 이전 단계로 회복	평가 등에 제도개선과 운영체계 보완을 통해 재발을 방지하고 위기관리 능력을 보완하는 활동

※ 김홍수. 2014. "한국적 특성에 부합한 국가위기관리체계 구축방안", 『국방정책연구』 30-3, p.134.

위와 같은 국가안전관리 기본계획은 우리나라 재난 위협에 대응하는 주요 계획으로 5년 단위 중장기적 정책 발전 방향을 제시하는 등 발전해 왔으나, 계획의 실행력이 부족했고, 타 부처의 다양한 계획 간 연계가 미흡하다는 지적이 존재했으며, 이와 관련하여 다음과 같은 근본적인 문제점 및 개선 소요[30]가 거론되었다.

첫째, 국가의 안전 범위가 너무 넓어 실효성이 떨어졌다. 국가안전관리 기본계획은 전세계적으로 유례를 찾을 수 없는 재난관리와 모든 안전관리를 포함하는 종합계획이다. 미국, 일본, 영국 등 대부분의 선진국의 경우 종합계획으로는 재난관리계획만 수립하고 있으며, 종합적 안전관리계획은 수립하지 않는다. 안전관리계획의 경우 교통, 환경, 원자력 등 주요 부분별로 분산화된 계

30) 행정안전부,「국가안전관리 기본계획」,(2019.7), p10.

획체계를 유지하는 것이 일반적이다. 계획의 통합성과 조정성이 떨어졌다. 법적 최상위 계획으로 국가안전관리기본계획에 따라, 각 부처와 지방자치단체 및 공공기관에서는 개별 기본계획 및 집행계획을 수립해야 한다. 그러나 기본계획과 집행계획, 그리고 지역안전관리계획의 내용이 방대하고 각 계획 간 계획기간이 모두 다른 등, 상호 연계성이 부족하여, 통합성과 조정성이 떨어졌다. 둘째, 실효성 있는 재정투자계획의 수립이 미흡했다. 국가재정법에 의한 국가재정운용계획과의 상호연계를 통하여 계획의 실효성 및 예산집행 여부를 확인 · 평가하는 후속조치가 부족했다. 셋째, 평가를 통한 개선노력이 부족했다. 기본계획 및 집행계획 등 하위계획에 대한 평가를 통한 개선 노력과 환류가 부족했다. 넷째, 국제적 동향에 대한 관심과 연대가 부족했다. UN 등 국제기구와 재난관리의 주요 선진국의 동향 및 정책적 흐름에 대한 반영이 제대로 이루어지지 않았다. 특히 UN-ISDR 등이 강조한 재난관리에서 회복력(resilience) 개념에 대한 고려가 부족했다.

넷째, 재난발생시 군사적 측면에서의 조치 및 조기 개입을 통해 거둘 수 있는 피해예방 효과를 간과하였던 측면이 존재한다. 법제적 측면에서, 군은 적의 침투 · 도발 및 우발사태 등 군사적 위기상황에 대해서만 통합방위법에 의거 주도하며, 재난분야 위기 시에는 행정안전부 주도 하에서 지원하는 역할만을 수행하도록 설정되어있는 상황이다. 이로 인해 재난 발생 시 군이 주도적인 역할을 수행하는 것은 극히 제한되는 실정이며, 사회재난 시 주관부처인 행안부, 보건복지부와 연계하는 범정부 차원의 대응체계에서는 단지 군의 인력 및 물자를 지원하는 수준에 머물고 있다. 또한, 군은 국방망 · 전술통신망 을 운용하고, 정부 행정기관은 행안망 · 재난안전통신망 운용함에 따라 국가위기시 군 및 정부 행정기관별 상황조치 및 관리를 위한 일원화된 소통도 제한되고 있기에 비효율성이 증대되고 있다. 최근 COVID-19 상황을 비롯하여, 2000년대 이후 각종 재난, 테러 등의 비전통적 위협에 대한 대응이 중요성이 부각되는 가운데 군의 적극적인 역할 확대가 필요하다는 인식이 확산되고 있다.

그러므로 향후 다양한 안보위협 요인이 연속적 혹은 동시다발적으로 발생하는 복합안보위협에 대해 포괄적으로 대응하는 접근방식이 필요한 것으로 판단된다. 이를 위해서는, 우선 자연적, 사회적 요인을 포괄적으로 설명할 수 있는 새로운 재난 정의가 필요할 것이며, 전 세계적으로 통용되는 '전재해 접근법'(all hazards approach)에 따라 자연재난과 사회재난을 모두 포괄하여 국민의 생명 · 신체 · 재산과 국가에 피해를 주는 모든 현상을 재난으로 통칭하여 민 · 관 · 군 · IGO · NGO 등 모든 주요 노드가 통합적으로 연계되는 통합적인 플랫폼 형태의 거버넌스 운용을 고안할 필요가 있다.

2. 스마트 메가시티의 복합안보위협 거버넌스 구축 방안

앞서 식별한 스마트 메가시티에서의 주요 안보 이슈(통신 · 전자기, 에너지, 소방 · 방재, 보건)

와 연계하여, 이러한 복합안보위협에 대한 거버넌스 대응전략 구상(안)은 다음과 같다.

첫째, 스마트 메가시티에서의 복합안보위협 거버넌스 대응체계 구축에 대한 범국민적 공감대 형성이 필요하다. 오늘날 대한민국 인구의 절반이 상주하는 서울 및 수도권과 같은 스마트 메가시티에서는 기존의 전통적 안보위협이 상존하는 가운데, 그와는 다른 양상으로 새로운 위협요소가 작용하며 안보 측면에서의 불확실성이 증대되고 있다. 이러한 비전통적 위협요소는 전통적 안보위협요소와 연계되어 복합적으로 작용하면서 일순간에 국가의 주요 기능을 마비시키고 안보공백을 야기할 수 있다는 우려에 대한 국민적 위기의식을 환기시키는 것이 중요한 시점이다. 이와 같은 새로운 복합안보위협은 기존의 대응 메커니즘으로는 효과적인 대처가 불가능하므로 변화하는 안보상황에 부합되는 새로운 범국가적 대응체계의 구축 필요성이 반드시 언급되어야 할 것이다. 그리고 이 과정에서 군의 재난대응 역할이 강조되어 군사분야의 인적 · 물적 자원이 조기에 투입됨으로써 안보위협 요인의 창발 이전에 피해의 확산 · 증폭을 예방해야 할 필요성이 부각될 필요가 있다. 이를 토대로 국가의 안보정책분야 주요 이슈로서 스마트 메가시티의 복합안보위협에 대한 대국민 소통 및 논의의 장을 마련하고, 전문가들의 연구와 토론을 활성화시킴으로써 집단지성의 활성화 여건을 조성하며, 각계각층의 폭넓은 인식을 형성함으로써 정치적 차원에서도 해당 이슈의 중요성에 대한 의사결정권자의 인식수준이 제고되어야 한다.

둘째, 복합안보위협 거버넌스는 대응체계의 조직화 및 법제화를 통해 민 · 관 · 군 · IGO · NGO 등 모든 주요 노드에 대한 실질적 통제력을 발휘할 수 있는 여건을 조성해야 한다. 이를 위해서는 민 · 관 · 군 · 산 · 학 · 연이 융합되어 기능하는 거버넌스 협력체계 및 컨트롤타워(가칭 : 복합안보위협대응본부)의 구성이 필요할 것이다. 위기대응 관련 국가조직의 제 기능을 통합 · 관리할 수 있는 컨트롤타워 기능 수행하는 조직을 구축하는 것은 허브와 각 노드에 대한 플랫폼 역할을 수행함과 동시에, 유사시 효과적으로 유관 조직 간의 노력의 통합을 달성해내기 위함이다. 여기에는 이러한 모든 조직들이 국가위기대응체계 상에서 단계별 노드로써 기능하도록 권한 및 책임 범위가 구체적으로 설정되어야 한다. 그리고 집단지성이 발휘될 수 있는 학습조직 플랫폼을 구축함으로써 기존의 사례를 분석하고 대응책을 마련하며, 새로운 위협에 능동적으로 대처할 수 있는 역량을 구비해야 한다. 그리고 이러한 조직설계에 관한 사항의 법제화를 통해 복합안보위협 대응에 필요한 각 유관 조직의 인적 · 물적 자원의 원활한 투입여건이 보장되어야 할 것이다. 아울러, 이러한 거버넌스 협력체계가 현실적으로 작동하기 위해서는 운용에 대한 소요 예산이 충분히 확보될 수 있도록 통합방위법 등에 추가하여 법제적 근거가 마련되어야 한다.

셋째, 복합안보위협 거버넌스 대응체계에서 군사분야 노드의 역할이 강화되어야 한다. 스마트 메가시티의 밀집된 환경(dense urban environments)으로부터 비롯되는 주요 취약성을 고려하면, 군사적 요소가 개입됨으로써 보다 체계적이고 효율적인 대응이 가능해질 것으로 판단된다(US Military (TRADOC), 2014, 8). 복합안보위협의 특성을 고려 시, 초기 단계에서는 통치질서의

혼란이 가중되는 수준에 머물다가 순식간에 양질전화 및 이슈연계의 프로세스를 거쳐, 전통적 안보위협요소와 결합되고 증폭되는 양상을 보이기 때문이다. 따라서 안보 이슈의 발생 초기에 적극적인 군사적 개입이 효과적일 것으로 판단된다. 이를 위해서는 군사적 관점에서 도시의 각종 기반체계에 대한 위협요소에 대한 유형 분석이 필요하며, 이에 대해 중심 분석(CoG Analysis) 개념 하에서 핵심취약점(critical vulnerability) 방호에 중점을 두고 스마트 메가시티에서의 복합안보위협에 대해 보다 구체적인 접근을 시도할 필요가 있다. 그리하여 모든 위기 상황을 상정하고 그에 따른 대응 시나리오를 발전시켜나가야 할 것인데, 이러한 시나리오는 평시 민·관·군 통합대응훈련으로 확장되어 시행까지 연결되어야 한다. 이는 미국 연방재난관리청(FEMA : Federal Emergency Management Agency)을 중심으로 유관 조직이 연계되어 평시 훈련체계를 갖추고 시행하는 것과 같이 유사시에 대비하여 범국가적 차원에서의 실질적 훈련이 이루어져야 함을 의미한다. 그리하여 국방재난대응 정보공유 및 지휘 체계를 구축하고, 재난 유형별로 특화된 대응부대(구조, 탐색, 대응 등)를 편성하며, 재난관리 전문가를 양성하는 등 군사적 측면을 포괄하는 구체적인 재난관리정책으로 발전되어야 할 것이다. 그리고 민·관·군 재난 대응훈련과 연계되어 유사시 민간 분야의 최첨단 장비가 즉각적으로 투입될 수 있도록 물자동원 여건을 조성해야 할 것이다.

넷째, 복합안보위협대응을 위한 미래지향적 과학화 훈련체계를 갖추어야 한다. 이를 위해서는 복합위협대응 관련 범정부 R&D체계를 구축함으로써 연구역량을 배양하고, 국가 차원에서의 '지능형 재난관리 플랫폼'을 형성해야 한다. 특히, 디지털트윈(digital twin), 인공지능(AI), 사물인터넷(IoT) 등 4차 산업혁명의 핵심기술을 접목시켜 혼합현실체계(mixed reality system)를 구축하고, 군사분야에서의 합성전장환경(STE)[31]과 연계시킴으로써 가상과 실제의 경계가 사라진 훈련 환경을 조성할 필요가 있다. 밀집된 도시 환경(DUEs) 하에서는 대규모 인력이 소요되는 복합안보위협 상황이 존재할 것이나(Hedges, 2018), 이러한 훈련으로 인해 도시의 혼잡이 가중되기에 현실적으로 어려움이 많다. 따라서 가상의 스마트 메가시티(virtual smart-megacity)를 구성함으로써 복잡한 도시 환경에서의 다양한 변수에 대한 시뮬레이션 분석을 강화하고, 그러한 분석결과를 실제 훈련에 환류시킴으로써 효과적으로 위기대응 역량을 제고할 수 있을 것이다. 이를 통해 위협 유형을 분석하여 그에 적합한 장비와 물자를 식별해낼 수 있을 것이며, 이러한 특화된 물적 자원을 체계적으로 확보해나갈 수 있는 여건을 마련할 수 있을 것이다.

이와 같이 민·관·군의 모든 유관 조직이 상호 연계되어 복합안보위협에 대응하는 거버넌스 전략 구상(안)은 유사시 국가안보에 미치는 영향을 최소화하기 위해서 군사적 요소의 개입 필요성이 부각되는 측면이 있다. 이러한 거버넌스 대응전략(안)에 대해 군사분야 정책개발의 관점에서 '전투발전요소(DOTMLPF) 프레임'을 적용하여 정리한 내용은 다음의 〈표 3〉과 같다.

---

31) 합성전장환경(Synthetic Training Environment)은 과학화훈련의 일환으로서 LVCG 메커니즘(Live(실기동훈련), Virtual(가상훈련), Construction(워게임모의훈련), Game(게임)) 구현하는 훈련환경을 의미한다.

〈표 5: 스마트 메가시티의 거버넌스 대응전략 구상(안)〉

구분	내 용	D 제도	O 조직	T 훈련	M 물자	L 리더십	P 인력	F 시설
#1	[범국민적 공감대 형성] · 복합안보위협 위기의식 인식제고 · 복합안보위협 대응체계 구축방안 논의 · 복합안보위협 거버넌스 대응책 마련	○				○		
#2	[복합안보위협 거버넌스 조직화 · 법제화] · 민 · 관 · 군 · IGO · NGO 협력체계 구축 · 컨트롤타워(복합안보위협대응본부) 구성 · 학습조직 플랫폼 구축 · 법제적 근거 마련을 통한 예산 확보	○	○			○	○	○
#3	[거버넌스內 군사노드 역할 강화] · 스마트 메가시티 방호기능 강화 · 재난대응정보공유 및 지휘 체계 구축 · 복합안보위협 이슈/대응 시나리오 구성 · 민 · 관 · 군 통합 재난대응 교육 및 훈련 시행 · 재난대응부대 편성 · 재난대응전문가 양성 · 재난유형별 물자 · 장비 확보 및 동원		○	○	○		○	○
#4	[미래지향적 과학화훈련체계 구축] · R&D체계 구축 및 연구역량 강화 · 지능형 재난관리 플랫폼 구성 · 군사분야 합성전장환경(STE) 연계		○	○				○

Ⅴ. 결 론

본고에서는 미래의 주요 트렌드(trend)로서 거론되는 스마트 메가시티(smart megacity) 현상에 주목하여 기존의 대응방식으로는 효과적인 대처가 어려운 비전통적 복합안보위협에 대해 이론적으로 살펴보고, 그에 대응하는 거버넌스 접근 전략을 고찰하였다. 이와 관련하여 주요 시사점 및 논의 사항은 다음과 같다.

첫째, 스마트 메가시티의 새로운 복합안보위협에 대응하는 거버넌스 대응체계 구축이 필요하다. 메가시티의 특성상 구성요소의 밀집도 및 결합도가 높아서 문제의 확산 속도가 매우 빠르며,

구성요소 간 상호작용 관계가 복잡하여 대응의 어려움이 가중된다. 이로 인해 안보위협 이슈 발생 시, 복합적인 재난의 형태로 전화되고 그 파급효과가 순식간에 국가안보문제로 증폭될 수 있는 잠재적 위험을 지니고 있는 것으로 판단된다. 이러한 전례없는 위험에 효과적으로 대처하기 위해서는 기존의 국가재해재난대응체계를 개선할 필요가 있을 것이다. 그리하여 안보위협 이슈의 발생 초기에 범국가적 차원에서 모든 인적 · 물적 가용자원이 투입되어 효과적으로 상황을 통제할 수 있는 거버넌스 대응체계를 조속히 구축하고 대응력을 강화할 필요가 있다. 이를 통해 유사시 국가적으로 미치게 될 피해의 규모를 감소시키고, 국가역량과 비용을 절감할 수 있을 것이다.

둘째, 거버넌스 대응체계에서는 다영역(multi-domain)에서의 직 · 간접적인 복합안보위협에 대비하는 군사적 개입이 필요하다. 향후 적대세력은 전통적인 방식만을 통해서 혹은 물리적인 공격을 직접적인 방식으로만 사용할 것으로 단정할 수 없으며, 가짜뉴스(fake news) · 해킹 · 선전 · 선동 등 공세적인 사이버 활동을 전개하여 거대도시민들을 공포에 휩싸이게 하거나 잘못된 정보를 확산시켜 국민 · 정부 · 군 간의 신뢰 관계를 파괴하는 등 간접적인 공격방식을 사용할 것이다. 즉, 상대의 전쟁 의지와 지속능력을 약화시키기 위해 사이버 공간을 활용하여 정보전과 심리전을 전개함으로써 인지적 영역에서의 마비효과를 노릴 가능성이 증대되고 있다는 것이다. 스마트 메가시티에서는 초연결된 거대 네트워크형성, 모바일 빅뱅, 인프라 운용시스템 융 · 복합 등으로 인해 사이버 위협의 최대 격전지가 될 것이다. 따라서 거버넌스 대응체계에서 군사적 역량을 원활하게 발휘하고, 각종 물자를 신속히 투입할 수 있는 민 · 관 · 군 협업 여건을 조성하는 것이 중요할 것이다.

셋째, 미래 트렌드를 고려하여 복합안보위협에 대한 미래지향적 대응 인프라를 수립해야 한다. 미래 트렌드로서 메가시티 확산 추세와 더불어, 4차 산업혁명의 주요 과학기술(AICBM[32])이 발전함에 따라 스마트화가 가속되고 있다. 이러한 상황에서 '가상 스마트 메가시티(virtual smart-megacity)를 구성하고, 이를 군사분야에서의 합성전장환경(STE)과 연계하여 범국가적 스마트 대응 인프라를 갖추는 것은 필수적이다. 이를 통해 과학기술의 이점을 극대화함으로써 위기상황의 불확실성을 능동적으로 극복해내는 미래지향적 학습조직으로 거듭날 수 있을 것이다.

그러므로 전 세계적 트렌드인 스마트 메가시티(smart-mega city) 확산 추세를 고려 시, 도시지역에서는 새롭게 대두되는 안보위협에 대해 기존의 대응방식만으로는 충분치 않으며, 다양한 안보위협요인이 중첩되어 동시다발적 · 복합적으로 발생할 높다는 인식이 점증하고 있다. 따라서 이에 대한 대응체계는 거버넌스 차원에서 새롭게 구축되어야 하며, 지상군 고유의 전장으로서 '스마트 메가시티'를 재조명하고, 복합안보위협의 유형별로 군사적 요소가 적극적으로 개입되도록 설계할 필요가 있을 것이다. 이를 통해 복합안보위협 발생 초기부터 위협에 대한 선제적 통제를 가능케하고, 피해 확산에 따른 부정적인 'n차 파급효과'를 최소화할 수 있을 것이다.

---

32) AI(인공지능), IoT(사물인터넷), Cloud(클라우드), Big Data(빅데이터), Mobile(모바일)

〈참고문헌〉

〈국문〉

국가전략연구원. 2018.『신안보총람』. 4-9.

김근식. 2019. "기후변화 및 에너지 안보 인식의 긍정적 부정적 판단에 따른 원자로 에너지 수용성 영향 분석".『정책분석평가학회보』. 29(2), 29-64.

김기봉 외. 2018. "4차 산업혁명시대의 스마트시티 현황과 전망".『한국융합학회논문지』. 제9권 제9호. 191-197.

김병운. 2016. "초연결산업 사회 사이버보안 정책".『과학기술법연구』. 제22집 제3호. 85-122.

김상배. 2016. "신흥안보와 메타 거버넌스 : 새로운 안보 패러다임의 이론적 이해".『한국정치학회보』. 2016 봄, 75-102.

------. 2017.『신흥안보의 미래전략』. 출판사 소재지 : 출판사 이름, 40-41.

김서용, 김근식. 2018. "위험사회와 에너지 체제 전환 에너지 선호 구조 분석 및 정책적 함의".『행정논총』. 제54권 제2호, 287-318.

김인태. 2013. "국가위기관리기본법(안) 제정 발전방안".『위기관리이론과실천』. 9(6). 141-165.

김흥수. 2014. "한국적 특성에 부합한 국가위기관리체계 구축방안".『국방정책연구』제30권 3호. 134-135.

마이클 더글라스. 2014. "The Urban Transition in Disaster Governance : Scaling up from Neighborhood to City and Transborder Region in Asia".『국정관리연구』. 제9권 제2호, 61-90.

박재완. 2019. "북한의 EMP 위협과 한국의 대응방안".『한국군사』. 제5호(2019.6). 93-129.

박진경, 김상민. 2017.『인구구조 변화에 대응한 유형별 지역발전전략 연구』. 한국지방행정연구원 연구보고서 2017-13. 강원 원주 : 세일포커스(주).

신범철. 2018. "북한 핵능력 고도화에 따른 북한의 전략적 의도와 목표의 변화".『한국국가전략』. 제6호(2018.3). 139-172.

육군 교육사령부. 2020.『월간작전환경분석 (2020년 1월)』.

정민섭. 2020. "미래 신흥안보위협과 육군의 대응방향".『육군미래혁신저널(Army Future Innovation and Technology)』. 제20-2호.

조상근, 차도완. 2020. "미래 한국의 메가시티 출현에 따른 위협 양상과 대응방안에 관한 연구".『사회융합연구』. 4(3). 11-16.

조석현. 2014. "한반도 작전 환경 변화에 따른 도시지역 전투수행 발전방안".『전략논단』. 제20호, 126-154.

조재성. 2020. "한국의 메갈로폴리스 혁신도시 정책 시즌2에서 메가시티 전략으로".『도시정보』. 제458호(2020.5). 56-57. 진대욱. 2014. "재난안전분야 : 4가지 회복력 갖춰야".『Future

Horizon 21』, 20-23.

조화순, 권웅. 2017. "한국과 미국의 사이버안보 거버넌스 : 사이버 위협의 안보화 관점에서의 비교". 『Information Society & Media』. Vol.18, No.2. 97-120.

조화순, 김민제. 2016. "사이버 공간의 안보화와 글로벌 거버넌스의 한계". 『Information Society & Media』. Vol.17, No.2. 77-98.

〈영문〉

Arnold, Thomas, D. & Fiore, Nicolas. 2019. "Five Operational Lessons from the Battle for Mosul". In 『Military Review(Jan-Feb 2019)』. 56-71.

Bălcescu, Nicolae. 2019. Training Military Leaders For Urban Irregular Warfare. International Conference KNOWLEDGE-BASED ORGANIZATION. Vol. XXV, No. 1. 32-39.

Dilegge, Dave, et al. 2019. "Blood and Concrete: 21st century conflict in urban centers and megacities". In : Ash Rossiter. (ed). 『Small Wars & Insurgencies』. Vol. 31, Issue. 4. Washington DC, USA. Maria-Louise Clausen. 920-923.

DiMarco, Louis. 2012. 『Concrete Hell』. Osprey Publishing. 151-168.

Hedge, William. 2016. "An Analytic Framework for Operations in Dense Urban Areas". Small Wars Journal(11 Mar 2016). Accessed 17 Sep 2020, https://smallwarsjournal.com/jrnl/art/an-analytic-framework-for-operations-in-dense-urban-areas.

Kaune, Patrick N. 2016. Analysis of US Army Preparations of US Army Preparation for Megacity Operations. US Army War College-Civilian Research project. Syracuse, NY 13244 : Syracuse University.

Jensen, Benjamin M, et al. 2019. Complex Terrain : Megacities and the Changing Character of Urban Combat. Marine Corps University Press.

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

Kleer, Jerzy, et al. 2018. Rise Of Megacities : The Challenges, Opportunities And Unique Characteristics. Danvers, MA 01923, USA: World Scientific Publishing Europe Ltd.

Loper, Margaret L. 2018. "Situational Awareness in Megacities". In : Kosal M. (ed). 『Technology and the Intelligence Community : Advanced Sciences and Technologies for Security Applications』. Springer, Cham. 205-235. (https://doi.org/10.1007/978-3-319-75232-7)

OECD, 2012. Environmental Outlook to 2050.

Sharma, Sharad, et al. 2017. "Megacity: A Collaborative Virtual Reality Environment for Emergency Response, Training, and Decision Making". Visualization and Data Analysis. 70-77. (https://doi.org/10.2352/ISSN.2470-1173.2017.1.VDA-390).

Townsend, Stephen J. 2017. "Multi-Domain Operations in Megacities" (presentation, Association of the United States Army 2017 LANPAC Symposium & Exposition, Honolulu, 23 May 2018).

US Military. 2013. Joint Publication (JP) 3-06, Joint Urban Operations. Washington, DC: U.S. Government Printing Office, November 2013, I-6.

————. 2014. TRADOC Pamphlet 525-3-1, The U.S. Army Operating Concept: Fight and Win in a Complex World (Fort Eustis, VA: TRADOC, 31 October 2014), 8.

————. 2017. JP 5-0, Joint Planning, (16 June 2017).

————. 2017. Field Manual(FM) 3-0, Operations. Washington, DC: U.S. Government Publishing Office (GPO), October 2017.

————. 2017. Army Techniques Publication (ATP) 3-06, Urban Operations. Washington, DC: U.S. GPO, December 2017), 1-1.

————. 2017. Mosul Study Group 17-24U, What the Battle for Mosul Teaches the Force (Fort Eustis, VA: U.S. Army Training and Doctrine Command [TRADOC], September 2017), 28-39.