https://doi.org/10.33778/kcsa.2019.19.5.099

사이버 위협의 안보화 동향에 대한 이론적 배경과 비판적 논의

이 광 호*, 이 승 규**, 김 호 길**

요 약

본 연구에서는 사이버 위협이 사회적으로 담론화 과정을 통해 안보화 되는 이론적 배경과 주요 동향을 제시하였다. 특히 사이버 위협의 안보화에 대한 비판적 논의을 코펜하겐학파의 안보화 이론을 바탕으로 설명하였다. 또한 사이버 위협의 안보화 과정을 설명한 비전통적 위협의 안보화와 신흥안보이슈의 안보화를 기존 연구를 바탕으로 제시하였으며 이에 대한 한계점을 설명하였다. 또한 현재 나타나고 있는 사이버 위협의 군사화 현상이 기술담론과 군사담론의 결합을 통해 나타나는 현상임과 이에 대한 경계적 시각을 제시하고자 하였다. 본 연구를 통해 사이버 위협의 안보화 과정에 대한 객관적 통찰력을 바탕으로 보편적 해법 제시의 한계와 함께 군사화의 경계적 시각을 우리군에 제시하고자 한다.

Theoretical Background and Critical Discussion about Securitzation Trend of Cyber Threat

Kwangho Lee*, Swengkyu Lee**, Hokil Kim**

ABSTRACT

In this study present the theoretical background and major trends in which cyber threats are securitization through the discourse process. In particular, this study explained based on the theory of Copenhagen school, which is critical of the security of cyber threats. And presented the security of non-traditional threats and the security of emerging security issues, which explained the process of security for cyber threats, based on existing research, and explained the limitations to this. And tried to provide a cautious point of view that the militarization phenomenon of cyber threats that is currently displayed is a phenomenon that is displayed through the combination of technical discourse and military discourse. Through this study, we aim to show the military the limits of universal solution presentation and the borderline perspective of militarization based on objective insights into the cyber threat security process.

Keywords : Cyber Threats, Cyber Security, Nontraditional Security, Emerging Security, Military Security

접수일(2019년 10월 3일), 수정일(1차: 2019년 12월 27일), 게재확정일(2019년 12월 30일)

* 육군3사관학교 이공학처 사이버전학과(책임저자)

** 육군3사관학교 이공학처 사이버전학과

1. 서 론

정보통신기술의 발달로 창조된 사이버 공간에 대한 의존성의 증가는 그에 비례하여 다양한 위협 유형을 증가시켜왔다. 특히 개인정보 해킹에서 사이버 범죄와 테러에 이어 국가 간의 사이버 충돌까지 위협의 양상이 변화 발전해 왔으며, 행위자 역시 개인의 범죄에서 사이버 범죄조직, 초국적 사이버조직에 이어 사이버 핵티비스트(해커-hacker와 행동주의자-activist의 합성어로 새로운 형태의 행동주의자)들까지 등장하였다[1]. 최근에는 사이버 위협에 대응하는 군 또는 국가의 사이버 조직도 연이어 등장하고 있다[2]. 이와 같은 동향 속에 2015년 발생한 워너크라이 랜섬웨어의 사례는 국가나 물리적 영역을 초월하는 사이버 위협의 특성과 폭발적인 확산 속도, 행위자를 파악하기 어려운 익명성의 기술적 특성과 미국-북한 간의 정치적 이슈 등 사이버 위협의 특징을 복합적으로 보여주고 있다[1].

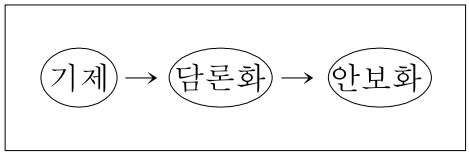
사이버 위협은 발달된 정보통신기술 인프라를 갖추고 있는 선진국 또는 강대국이 후진국 또는 약소국에 비해 더 큰 위협이 되는 비대칭성, 공격자를 파악하기 어려운 기술적 익명성이 특징이다. 이 특징들이 국제 기구나 규범의 미비가 복합적으로 결합되어 위협을 사회적으로 담론화시키고, 안보에 대한 개념적 논의를 불러일으키고 있다. 하지만 이 위협에 대한 개념과 정의는 다양한 시각에서 제시되고 있다. 따라서 본 논문에서는 사이버 위협의 안보화에 대한 이론적 배경을 제시하고 이 이론을 바탕으로 안보화 현상을 설명하고 있는 비전통적 안보의 안보화와 신흥안보이슈의 안보화에 대한 개념을 제시하였다. 또한 각각의 설명이 제시하고 있는 한계점을 비판적 시각에서 제시함으로써 현재 나타나고 있는 사이버 안보의 군사안보화에 대한 경계적 관점을 우리군에 제시하고자 한다.

2. 사이버 위협에 대한 비판적 논의와 안보화의 이론적 배경

사이버위협의 사회적인 담론화와 안보화에 대해 크게 두 가지 비판적 시각이 제시되는데 위협의 실재(real)와 과대 평가에 대한 논의이다. Rid & Thomas는 그들의 연구에서 사이버 위협은 그 실체와 효과가 증명되지 않았으며, 재앙 형태로 발생하는 실재 또는 검증 가능한 형태의 위협이 아니라, 전문가나 정치인들에 의해 가상적으로 존재하는 위협이라고 분석하였다[14]. Hansen & Nissenbaum은 그들의 연구에서 사이버 위협을 안보담론화 하는 과정에서 세 가지 비판적 특징으로 분석하였다. 먼저 '하이퍼 안보화(hypersecuritization)'의 성격으로 아직 발생되지 않은 많은 종류의 다차원적 사이버 재난을 과장해 담론화하여 부각시키고 있으며, 대중들의 일상적인 경험이나 느낌 등에 호소하는 경향이 강하다는 것, 마지막으로 사이버 안보담론은 비밀정보와 전문지식을 갖춘 전문가들에 의한 '기술적 전문담론(technical expert discourse)'을 형성하고 있어 일반인들은 잘 이해하지 못한다고 분석하였다[15]. 이와 같은 연구들을 정리해보면 사이버 안보의 위협은 실재하지 않으며 전문가들에 의해 과장되거나 과대평가되어 있다고 분석할 수 있다.

하지만 다양하고 복잡해지는 위협을 적절하게 다루기 위해 안보의 개념을 확대해야 한다는 주장은 학계에서 지속되어 왔다[3][4][5][6]. 코펜하겐 학파의 안보화 이론은 안보의 복합성과 안보담론의 규범성을 바탕으로 탈전냉기의 안보를 기존의 국가 및 군사안보 중심에서 탈피하여 제시하였다. 특히 안보담론이 사회적으로 형성되는 과정을 통해 구성주의 시각에서 안보행위를 정의한다[7][8][9][10][11]. 여기서 담론으로서의 안보란, 안보와 연관된 다양한 논의 기제(mechanism)에서 비롯된 가정, 이미지, 신념, 합의, 그리고 정책적 선택 등을 종합적으로 분석한다는 것으로, 안보담론은 안보 문제가 직면한 지침을 제시하고 구체적인 영역에서의 실행 방법들을 제공해 준다는 의미를 갖는다. 즉, "사회적으로 구성된다(Socially constructed)'는 것을 뜻한다.[12] 정리하면, 고펜하겐 학파의 안보화 이론에 의하면 안보란 객관적(또는 주관적)으로 실재하는 어떤 조건이 아닌 정치적 담

론을 통해 위협이 무엇인가에 대해 사회적으로 합의하여 구성되는 과정에서 안보화 된다는 것이다[13].



(그림 1) 안보화 과정

3. 사이버 안보의 비전통적 안보화

3.1 비전통적 안보화에 대한 논의

다양한 시각과 이론적 연구의 동향 속에서 나타나고 있는 중요한 현상 중 하나는 전 세계 주요 국가들이 공통적으로 사이버 위협을 안보에 대한 위협으로 인식하고 사이버전 능력을 갖추기 위해 노력하고 있다는 것이다. 그 이유는 앞서 제시하고 있는 안보화가 객관적으로 존재하는 것이 아니라 사회적 합의 및 정치적 과정을 통해 구성되는 담론의 산물이라는 이론적 배경에 있다. 이것은 탈냉전기 시대의 전통적인 군사안보가 아닌 비전통적, 비군사적으로 다양한 이슈가 사회적으로 담론화되고 안보화에 영향을 주게 되었기 때문이다[16].

국가 간의 외환, 식량안보, 중국의 미세먼지나 일본 후쿠시마 원전 사태에 의한 초국경적 환경문제, 동남아에서 발생한 메르스의 확산과 같은 질병 문제를 포함해 북한의 사이버 공격이나 미중 사이버 갈등과 같은 문제들이 지금까지의 전통적 안보위협과는 다른 성격의 재난을 야기할 가능성으로 사회적 담론화되었기 때문이다. 또한 국제사회와 시스템 내 여러 요소들이 서로 밀접하게 연계된 복합적 현상을 배경으로 하고 있어 단순히 안전의 문제를 넘어서 국가안보 전반에 피해를 주는 새로운 위험으로 인식됨에 따라 비전통적 위협이 사회적 담론을 형성하고 안보화에 영향을 미치게 되었다[17].

정리하면 비전통적 위협의 안보화는 냉전 시기의 양극체제에서 변화된 탈냉전기 국제체제의 복합적 내부 역학구조가 결합되어 안보화에 영향을 미쳤다. 국가 간 핵심행위자가 단순히 국가간의 역학관계를 바탕에 둔 전쟁방지와 평화관리의 영역을 넘어서 국제기구, 다국적기업, NGO 등으로 확대 및 다변화 되었다. 또한 행위 유발 요인도 무역 분쟁, 환경오염, 질병 확산, 초국가적 조직범죄나 사이버 공격 같은 문제의 유형으로 다양화되어 공동 대응을 필요로 하는 등 복합적인 양상을 가지게 된 것이다[18]. 따라서 기존의 전통적 군사안보 문제가 국가중심으로 그 해결방안을 모색해 왔다면, 비전통적 안보문제의 해결은 한 국가행위자를 넘어서 국제기구나 NGO들의 공동대처를 요구하고 있다[19]. 특히 동아시아 국가들을 비롯한 세계 여러 나라들이 환경문제, 전염성질병, 불법이민 등을 포함한 모든 비군사적 위협을 비전통적 안보위협으로 간주하는 경향이 뚜렷해지고 있으며, 국가안보를 규정하는데 있어 많은 국가들이 전통적 군사안보와 더불어 환경이나 에너지, 경제 등의 비전통적 위협이 안보화 되었다고 분석하였다[20].

3.2 비전통적 안보화에 대한 비판적 논의

사이버 위협에 대한 안보의 안보담론화는 안보개념의 확대에 따라 비전통적 안보화로 인식되어 발전되었다. 하지만 사이버 위협을 비전통적 안보화로 정의하기에는 한계가 있다. 비전통적 안보화는 크게 세가지 특징을 지니는데, 첫째, 안보연구의 범주를 안보에 대한 비군사적 위협으로 규정하고, 둘째 대부분의 비전통적 위협들은 그 발생 원인과 영향이 초국가적 성격을 가지며, 마지막으로 학문적, 정책적 면에서 국가뿐 아니라 다른 행위자들도 안보의 준거점으로 간주된다는 점이다[21].

사이버 안보는 비전통적 안보이슈의 일부 특징을 포함하지만 사이버 안보를 비전통적 안보의 시각으로 보는 것은 한계가 있다. 먼저 세계의 각국은 사이버 안보에 대해 군사화 경향을 보이고 있으며, 그에 따라 발생 원인과 영향이 국가적 성격과 초국가적 성격의 양면성을 갖고 있으며, 마지막으로 기술적 특성이 행위자가 존재하지만 특정할 수 없다는 특징을 가지기 때문이다.

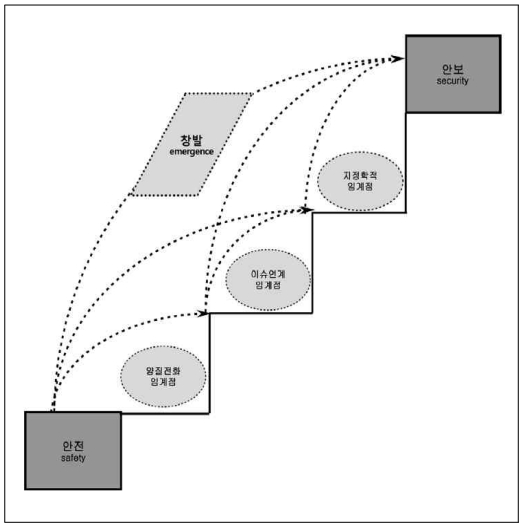
4. 신흥안보 위협과 안보화

4.1 신흥안보 위협의 안보화에 대한 논의

비전통적 안보화의 소극적 개념의 한계에 따라 초국가적으로 발생하는 새로운 위험을 이해하기 위해 제시된 개념이 '신흥안보(emerging security)'이다. 이것은 환경, 원자력, 보건, 인간, 사회 안보 그리고 사이버 안보와 같이 초국가적으로 발생되는 새로운 위협을 이해하기 위한 개념을 제시하고 있다[17][20].

신흥안보 분야의 위협은 새로운 사건의 형태로 발생할 수 있으며 그 위협의 발생 및 확산도 다른 신흥안보 분야들과 연계되어 증폭되는 과정에서 발생하는 경향이 있다. 이 전례없는 극단적 형태의 위험은 그 정체에 대해 담론과 억측이 난무하기도 하며 확산되어 전통안보 이슈들과 연계되면서 국가 간의 갈등을 발생시키거나 특징을 규정하기 어려워 보편적 해법의 제시를 더욱 어렵게 하는 특징이 있다[17].

신흥안보의 개념을 구체적으로 살펴보면 해당 위협에 의한 안전사고가 양적으로 증가하여 일정한 수준을 넘는 경우에 창발(emerging)하는 매커니즘의 특징을 가짐으로써 비전통적 안보와 구별된다. 신흥안보는 (그림)와 같이 3단계의 창발 과정을 거친다.



(그림 2) 신흥안보의 3단계 창발론(김상배, 2015)

양적 안전사고의 위험이 질적인 변화로 전화되는 양질전화의 현상이 나타날 때 위협이 사회적으로 이슈화된다. 작은 안전사고나 사건들이 질적인 변화로 확대되고 안전사고와 안보 위협간의 인식의 경계가 불분명해지고, 결국 거시적 관점에서의 위협으로 접근하게 된다. 이렇게 발생된 위협들이 다른 신흥안보 위협과 질적 연계성이 높아지면서 위험성은 더욱 확대되고 안보화의 가능성이 커지게 된다. 높아진 위험은 전통적 안보 이슈와 연계되는 '지정학적 임계점'을 넘어 국가 간 분쟁의 대상이 되면서 명백한 국가 안보의 문제가 되고, 전통안보의 영역으로 진입함에 따라 지정학적 차원에서 국가 간 갈등이나 충돌도 유발하는 위험요인으로 안보화된다[22].

단순히 해커에 의해 발생되던 해킹이나 개인정보 유출과 같은 안전사고의 문제가 전문적 사이버 범죄 집단이나 정치적 목적의 사이버 테러단체와 결합하게 되어 양질전화의 현상이 나타나기 시작하고, 국가 기반시설의 시스템이나 은행 시스템에 대한 위협으로 확대되는 질적 연계 현상으로 위험성이 확대되게 된다. 이 같은 사이버 위협 현상에 대한 대응으로 전통적 안보화와 결합된 각국의 사이버 보안 조직이 위협에 대한 대응을 넘어 전통적 안보 문제들과 연계됨에 따라 지정학적인 국가 간 갈등이나 충돌까지 유발하게 됨으로써 안보화되는 것이다.

4.2 신흥안보 위협의 안보화와 군사안보화

지금까지 살펴본 이론적 배경과 동향 속에서 현시점에 나타나는 중요한 현상은 전 세계 주요 국가들이 사이버 위협을 안보에 대한 위협으로 인식하고 독자적인 사이버전 능력을 갖추기 위해 노력하는 '군사화'의 현상과 사이버 공간에서 국가 간의 충돌이 발생되는 전통적 군사안보화 현상이다.

전 세계 주요국들이 10여 년 동안 추진해온 사이버 안보 전략에서 대부분 국가들이 사이버 위협을 국가안보의 문제로 인식하고 있으며, 안보화를 넘어 군사화(militarization)를 추진하고 있음을 확인할 수 있다[24]. 특히 군사화에서는 군의 사이버 역량강화, 부대 창설, 선제적 또는 사후 대응 등의

군사적 개념을 도입해 전통적 안보화가 진행되고 있다. 또한 다양한 분야의 전문가들이 국제법과 전쟁법을 적용해 행위자에 대해 응징(punishment)을 하거나, 핵안보의 억지 이론을 적용한 사이버 억지(cyber deterence) 등과 같은 전략을 전통적 군사안보 이론에 기반을 두고 제시하고 있다[25][26][27][28][13].

이와 같은 현상에 대해서도 비판적 논의는 계속해서 제시되고 있다. 사이버 위협이라는 것은 결국 고도의 전문화 지식을 필요로 하는 컴퓨터 시스템을 연구하는 전문가 집단에 의해서만 연구되어 제기되며 인터넷의 연결성 및 확장성, 그리고 상업적 시장성과 결합되어 앞서 제시한바와 같이 사이버 공격의 위험성과 기술적 가능성을 과장하는 경향이 있다. 이러한 기술담론이 다시 군사담론과 결합하면서 사이버 공간의 군사화 현상을 더욱더 강화시켜나가는 경향이 있다. 즉, 일반인들이 잘 이해하지 못하는 과장된 기술적 가능성과 군사적 위협의 가능성이 결합함에 따라, 인력과 예산 투입을 통해 이 위협을 대비할 수 밖에 없도록 현실이 구성하고 다시 이를 통해 군사적 경쟁을 촉발하는 담론과 현실의 상호구성 고리가 형성된다는 것이다[29].

5.. 결 론

본 연구에서는 사이버 위협의 안보화에 대한 이론적 배경을 바탕으로 사이버 위협에 대한 안보화의 동향과 이에 대한 비판적 시각을 살펴보았다.

또한 사이버 위협이 신흥안보로써 안보화된 과정을 살펴보았으며, 현재 진행되고 있는 사이버 위협의 군사화 현상을 분석하였다. 마지막으로 기술담론이 군사담론과 결합하여 군사화되어 구성되는 현실과 이에 경계해야할 '담론과 현실의 상호구성 고리'에 대해서 제시하였다.

한 대의 컴퓨터에서 발생된 악성코드 한 개가 다양하고 복합적인 성격에 따라 국가를 넘어 초국가적 안보에 위협이 되는 문제가 되고 있을 뿐만 아니라, 국가 간의 갈등에서 발생되는 사이버 공간에서의 충돌 현상은 전통적 안보 위협과 연계되어 결과적으로는 사이버 위협이 군사안보화 되어 가고 있음을 확인할 수 있다.

사이버 안보는 신흥안보 위협으로써 그 위협의 속성이 가지는 기술적 특성과 전통적 군사안보로서의 개념적 특성이 결합되어 국가 안보를 위한 보편적인 해법 제시 한계가 있다. 따라서 사이버 안보를 대비하는 우리군에서는 사이버 위협의 실재적 위험을 평가하고 기술담론과 군사담론에서 나타나는 군사화 현상에 대한 경계심을 가지고 사이버 안보 위협에 대비하는 관점을 유지해야 할 것이다. 또한 지금까지의 전통적 안보화의 이론적 배경을 바탕으로 사이버 위협에 대한 보편적 해법 제시의 한계에 따라 향후 연구에서는 보다 다양한 학문적 관점과 이론적 배경을 바탕으로 현상을 설명하고 해법을 제시할 필요가 있다.

참고문헌

[1] Lee & Jung, "A Study on the Quantitative Threat-Level Assessment Measure Using Fuzzy Inference", The Journal of Korea Convergence Security Association' Vol. 18, No.2, pp.19-24, 2018

[2] 한국인터넷진흥원 "주요 국가별 사이버방어 체제 및 대응동향" 심층보고서, 2014

[3] Walt, Stephen M, "The Renaissance of Security Studies." International Studies Quarterly 35, 211-239, 1991

[4] Haftendorn, Helga, "The Security Puzzle: Theory-Building and Discipline-Building in International Security." International Studies Quarterly 35, 3-17, 1991.

[5] Baldwin, David A. 1995. "Security Studies and the End of the Cold War." World Politics 48(1), 117-141, 1995.

[6] Baldwin, David A, "The Concept of Security." Review of International Studies 23, 5-26, 1997.

[7] Waever, Ole, Barry Buzan, Morten Kelstrup, and Pierre Lemaitre. 1993, Identy, Migration and the New Security Agenda in Europe. London: Printer.

[8] Waever, Ole. "Securityzation and Desecuritization." in Ronny Lipschuts. ed. On Security. New York: Colombia

University Press, 46-86, 1995.
[9] Buzan, Barry, Ole Waver, and Jaap de Wilde, Security: A New Framework for Analysis. Boulder: Lynne Rienner, 1998.
[10] Buzan, Barry and Lene Hensen, The Evolution of International Security Studies. Cambridge: Cambridge University Press, 2009.
[11] Balzaq, Thierry, ed, Securitization Theory: How Security Problems Emerge and Dissolve. London and New York: Routledge, 2011.
[12] 박인휘, “탈냉전과 미국의 패권적 안보담론”, 국제정치논총 40(4), pp.45-64, 2000.
[13] 김상배, “사이버 안보의 미중관계: 안보화 이론의 시각”, 한국정치학회보 49(1), pp.71-97, 2015.
[14] Rid, Thomas, Cyber War will not take place. Oxford and New York: Oxford University Press, 2013.
[15] Hansen, Lene and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School." Internation Studies Quarterly 53(4): 1155-1175, 2009.
[16] Whasun Jho, Minje Kim, “Securitization of Cyberspace and the Limits of Cyber Security Governance”, Information Society & Media, vol 17, No. 2, pp.77-98, 2016.
[17] 김상배, “신흥안보와 메타 거버넌스: 새로운 안보 패러다임의 이론적 이해”, 한국정치학회보, 50(1), pp.75-104, 2016.
[18] 이신화, “21세기 글로벌이슈와 국제정치학”, 국제정치논총 46(특별호), pp.197-226, 2007
[19] 한승주, “인권: 국가주권 대 인간주권”, 아산재단 창립 30주년 기념 국제학술대회, 2007년 6월 22일.
[20] Craig, Susan L. "Chinese Perceptions of Traditional an Nontraditional Security." http://www.StrategicStudiesInstitute.army.mil(검색일: 2019.8.3.).
[21] 이신화, “비전통안보와 동북다지역협력”, 한국정치학회보 42(2), pp.411-434, 2006.
[22] 김상배, “신흥안보의 미래전략: 개념적, 이론적 이해” 서울: 사회평론아카데미, 2016.
[23] 이신화, “인구, 이주, 난민안보의 복합지정학”, 아세아연구 60(1), pp.6-50, 2017.
[24] 김상배, “세계 주요국의 사이버 안보 전략”, 국제지역연구 26(3), pp.67-108, 2017.
[25] Morgan, Patrick M, "Applicability of Traditional Deterrence Concepts and Theory to the cyber Realm" , Proceedings of a Workshop on Dettering Cyber Attacks: Informing Strategies and Developing Options for U.S.Policy. National Research council, 2010
[26] Lupovici, Amir, "Cyber Warfare and Detterence: Trends and Challenges in Research" Military and Strategic Affairs 3(3), pp.49-62, 2011.
[27] Singer & Scachtman, "International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed" Havard International Law Journal 54, pp. 13-37, 2011
[28] 장노순, 한인택, 2013, "사이버 안보의 쟁점과 연구 경향" 국제정치논총 53(3), pp.195-230, 2013.
[29] Matusitz, Jonathan A. "Cyberterrorism: A postmodern View of Networks of Terror and How Computer Security Experts and law Enforcement Officials Fight Them. Ph.d. Dissertation. university of Oklahoma, 2006.

〔저자소개〕

이 광 호 (Kwangho Lee)
2007년 3월 육군3사관학교 경제학 학사
2016년 3월 연세대학교 정보보호학 석사
2019년 3월 아주대학교 사이버전학 박사수료
2018년 11월~현재 육군3사관학교 사이버전학교수
email : loveney0106@gmail.com

이 승 규 (SwengKyu Lee)
2000년 3월 육군사관학교 국제관계학 학사
2007년 3월 고려대학교 정보보호학 석사
2015년 3월 숭실대학교 IT정책경영학 박사
2018년 11월~현재 육군3사관학교 사이버전학과장(교수)
email : lsk6464@naver.com

김 호 길 (Hogil Kim)
1992년 3월 육군사관학교 전자공학 학사
1996년 3월 연세대학교 전자공학 석사
2007년 12월 텍사스 A&M 전산학 박사
2007년 12월~현재 육군3사관학교 사이버전학교수 (이공학처장)
email : khglex@gmail.com