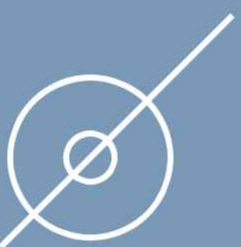
사이버 공격



2023

한국사이버안보학회
KACS

한국사이버안보학회 KACS

한국사이버안보학회 워킹페이퍼 2호
발간일: 2023년 12월 27일

윤민우 (가천대학교)

〈요 약〉

오늘날 안보문제는 연계성과 융합성, 그리고 전일성을 특성으로 한다. 서로 다른 차원에서 존재했던 다양한 문제와 이슈들이 서로 얽히고, 관계 맺고, 하나로 어우러지면서 해당 문제나 이슈의 질적인 변화가 일어나게 된다. 사이버 안보의 문제는 이 같은 안보의 초연결성과 영역의 붕괴, 그리고 전일적 혼재성이 나타나는 신흥안보의 대표적인 사례 가운데 하나이다. 사이버 상에서 나타나는 범죄와 테러, 그리고 간첩 행위는 서로 혼재되어 있으며, 긴밀하게 연계되어있다. 이 같은 신흥안보의 대표적인 사례 가운데 하나인 사이버 안보는 궁극적으로 지정학적 문제로까지 진화하게 된다. 사이버 범죄, 테러, 간첩과 같은 미시적 또는 중층적 문제들이 점점 더 중요한 거시적 국가안보의 아젠다로 들어오게 된 것은 이 때문이다. 이 글의 주요 목적은 전쟁 이전 단계에서 나타나는 다양한 사이버 상에서의 범죄, 테러, 간첩 활동들에 대한 기본 개념을 탐색하는 것이다. 이 글에서는 러시아-우크라이나 전쟁과 같은 본격적인 전쟁(a full-scale war) 이전 단계에서 벌어지는 다양한 사이버 공간에서의 공격과 침해행위들의 기본개념을 탐색하고 국가안보 및 국제안보의 함의를 도출하고자 하였다. 이 같은 공격과 침해행위들은 사이버 범죄, 사이버 테러, 사이버 간첩행위의 형태로 나타난다. 여기에서 제시하는 다양한 사이버 공격, 침해행위들에 대한 기본개념의 구분과 이해는 여전히 만족스럽지는 않지만 애매모호하게 뒤섞여 있어 규정하기 어려운 여러 사이버 안보위해의 양태들을 이해하고 규정하는데 하나의 시각틀 또는 분석틀을 제공할 수 있을 것이다. 그리고 이를 통해 어떤 사이버 안보의 이슈들을 국가안보 및 국제안보의 의제로 다루어야 할지에 대한 어떤 잣대를 제시할 수 있을 것이다.

Ⅰ. 머리말

오늘날 안보문제는 연계성과 융합성, 그리고 전일성을 특성으로 한다. 서로 다른 차원에서 존재했던 다양한 문제와 이슈들이 서로 얽히고, 관계 맺고, 하나로 어우러지면서 해당 문제나 이슈의 질적인 변화가 일어나게 된다. 예를 들면, 반도체 공급망과 같은 경제적인 문제는 미-중 사이의 지정학적 패권충돌과 연계된다. 중동이나 북아프리카로부터 유럽으로 들어가는 이민 또는 난민의 문제는 유럽 국가들에서의 애국적 극우극단주의와 연계되며, 이는 다시 유럽 국가들과 러시아, 미국 등과의 지정학적 관계설정에 영향을 미친다. 최근 들어 국내에서 논란이 되고 있는 후쿠시마 오염처리수 방류의 문제는 국내 정치뿐만 아니라 동북아시아 역내에서의 미-중 간의 세력충돌에도 영향을 미친다.

이처럼 오늘날은 많은 다양한 문제들과 이슈들이 서로 긴밀히 연계-통합되어 있으며, 이는 궁극적으로 국제정치학에서의 안보문제에 영향을 미친다. 일부에서는 이를 지나친 안보화(securitization)라고 비판적으로 지적하기도 하지만 바꾸어 말하면, 전통적으로 안보의 문제와는 별개로 존재했던 범죄, 경제, 과학기술, 환경, 기후, 식량 등의 많은 다양한 문제들이 오늘날에는 안보의 영역으로 들어왔고 국제정치에 중요한 영향을 미치게 되었다는 의미이기도 하다(김상배, 2015: 1-40). 예를 들면 과거 한국은 통상적으로 안미경중(안보는 미국 경제는 중국)이라고 하여 안보의 문제와 경제의 문제를 따로 떼어 생각하고 국익의 최대화를 위해 각각 분절된 영역에서 긴밀한 파트너 국가를 각기 다르게 설정하고 접근하는 전략을 취했다. 하지만 오늘날 이 같은 차별적인 접근 방식은 더 이상 적절하지 않아 보인다. 이는 오늘날 경제와 과학기술, 군사안보, 그리고 국가안보의 문제가 서로 결박되는 현상 때문이다. 반도체 공급망, 희토류, 그리고 다른 다양한 첨단과학기술 및 정보통신과 관련된 소재, 부품, 장비의 문제는 경제의 문제인 동시에 군사 및 국가안보의 문제이다. 이 같은 전통적으로 안보의 문제로 고려되지 않았던 여러 다양한 문제와 이슈들이 안보화되는 경향을 “신흥안보(emerging security)”의 개념으로 감싸 안을 수 있다. 이는 21세기 인류사회가 경험하는 초연결성, 영역의 해체, 그리고 전일적 통합성 때문이다.

사이버 안보의 문제는 이 같은 안보의 초연결성과 영역의 붕괴, 그리고 전일적 혼재성이 나타나는 신흥안보의 대표적인 사례 가운데 하나이다. 사이버 상에서 나타나는 범죄와 테러, 그리고 간첩 행위는 서로 혼재되어 있으며, 긴밀하게 연계되어있다. 사이버 공간에서는 범죄자들과 해커들, 핵티비스트들, 테러리스트들, 민간 사이버 보안업체 직원들과 같은 비국가행위자들과 군과 정보기관의 요원들과 같은 국가행위자들이 뒤섞여 있다. 그리고 종종 이들은 서로 긴밀히 연계되어 있으며, 특히 비국가행위자들이 국가행위자들의 전략목표를 달성하기 위한 프록시(proxy)로 활용된다(윤민우, 2020:275-318). 이 같은 다양한 행위자들의 연계는 은밀히 비밀스럽게 구축되어 작동하기 때문에 특정 사이버 범죄나, 테러, 또는 간첩활동이 누구에 의해 어떤 의도로 수행되었는지를 파악하기는 매우 어렵다(해리스, 2015: 17-18).

더욱이 최근 들어서는 사이버 상에서의 범죄와 테러, 간첩 행위 등이 분업화되고 서로 긴밀히 연계된 하나의 비즈니스 생태계를 이루고 있다. 예를 들면, 멀웨어 제작, 해킹, 스파이웨어나 백도어 설치, 랜섬웨어나 봇넷 인프라 구축, 그리고 실제 사이버 공격의 실행 주체들이 서로 다르고, 이들은 서로 위계적이거나 전략적으로 긴밀히 조직화되어 있지도 않으며, 단지 사이버 비즈니스 생태계에서 분업과 협업, 계약의 논리에 따라 서로 느슨하게 연계되어 있다. 이들은 다크넷 등의 은밀한 사이버 거래시장에서 서로 전문성이 특화되어 거래 관계를 구축하고 있다. 따라서

다양한 범죄, 핵티비즘, 테러, 간첩행위, 영향력 공작, 사이버 공격 등이 혼재되고 연계된 상태로 공존하고 있다. 이 때문에 여러 사이버 안보위해 행위들에 대한 공격특성과 의도, 공격행위자의 파악, 예방 및 대응 등이 더욱 어려워지고 있으며, 낮은 수준에서의 범죄나 핵티비즘 등과 같은 사이버 안전의 문제가 테러와 국가적 사이버 침해행위들과 같은 높은 수준의 사이버 안보의 문제로 질적인 변환을 겪게 되는 경우들이 점점 더 보편화되고 있다(윤민우, 2022a: 555).

이 같은 신흥안보의 대표적인 사례 가운데 하나인 사이버 안보는 궁극적으로 지정학적 문제로까지 진화하게 된다. 사이버 범죄, 테러, 간첩과 같은 미시적 또는 중층적 문제들이 점점 더 중요한 거시적 국제정치학의 아젠다로 들어오게 된 것은 이 때문이다. 김상배는 이 같은 과정을 신흥안보 갈등의 분석틀로 설명하고 있다. 그에 따르면, 사이버 안보는 미시적인 안전의 문제로 시작하여 다양한 이슈들과 연계되는 메커니즘을 따라 복잡화되고 국가들 간의 탈지정학 공간에서의 경쟁으로 발전하면서 궁극적으로 국제정치에서 물질적 또는 지리적 요소에 기반을 둔 고전지정학적 사안들과 통합되는 과정을 거쳐 복합지정학적 게임의 양상으로 창발(emergence)하게 된다(김상배, 2022: 21-26). 이 같은 오늘날 복합지정학적 특성 때문에 전통적으로 국제정치학에서 다루지 않았던 미시적 수준에서의 사이버 범죄나, 핵티비즘, 온라인 상에서의 폭력적 극단주의나 극단적 애국주의의 전파나 확산 등이 중요한 국제정치의 이슈들로 다루어지게 되었다.

오늘날 미국-서방과 중국-러시아가 전지구적 차원에서 지정학적 단층선(geopolitical fault lines)을 따라 충돌하는 신냉전은 복합지정학의 성격을 가진다 (윤민우, 2022b: 2). 논쟁의 여지는 있으나 미국-서방과 중국-러시아의 글로벌 패권충돌이 더욱 격렬해지고 있는 마치 과거 냉전시대의 귀환처럼 보이는 이 같은 오늘날의 국제정세의 흐름을 다수의 학자들과 전문가들은 대체로 “신냉전”으로 정의한다(김열수, 2021: 47-77; 김충근, 2023: 25-48; 반길주, 2021: 1-53). 오늘날 신냉전이 과거의 냉전과 다른 가장 중요한 특징 가운데 하나는 두 충돌하는 진영 간의 전선이 뚜렷이 나누어지지 않는다는 점이다. 과거의 냉전은 자유민주주의 진영과 공산전체주의 진영이 대체로 뚜렷이 분리되었으며, 충돌하는 두 진영 사이의 무역과 정보, 문화, 인적이동 등의 연계는 거의 철저히 단절되었다. 하지만 오늘날 신냉전에서는 두 적대적인 진영이 서로 충돌하고 배제하면서도 동시에 여전히 경제, 과학기술, 문화, 인적교류, 환경, 기후, 사이버 등 여러 부문들에서 서로 뚜렷이 단절되지 않고 연계되는 특성을 보인다. 이는 오늘날의 신냉전이 과거의 냉전과 뚜렷이 구분되는 지점이다. 이 같은 현상은 고전지정학에 신흥안보의 이슈들이 통합되어 나타나는 복합지정학적 특성에 기인한다.

사이버 안보는 이 같은 오늘날의 복합지정학적 충돌의 핵심전장이자 수단이다. 과거 냉전은 “공포의 균형”에 기초한 상호 배제와 단절, 그리고 대치의 모습으로 전개되었고 핵 무력(nuclear power)은 이 같은 냉전의 핵심전장이자 수단이었다. 하지만 오늘날 신냉전에서는 이 같은 핵의 중요성이 여전함에도 불구하고 가장 핵심적인 아젠다는 사이버로 이동한 것처럼 보인다. 이는 신냉전이 충돌하는 두 진영이 여전히 서로 긴밀히 연계되는 복합지정학적 특성을 띠기 때문이다. 두 진영은 본격적인 전쟁(a full-scale war)이전의 단계에서 서로 대치하고 배제하면서 서로를 향해 비키네틱(non-kinetic) 수단을 사용하여 서로에게 영향을 미치고 스스로의 의지를 관철시키려는 도발적 공격행위 등을 지속적으로 수행한다. 사이버 공격 또는 침해행위는 이 같은 비키네틱 수단의 대표적인 사례이다. 따라서 오늘날 신냉전에서는 충돌하는 두 진영에 속한 국가들 간에 사이버 공간을 통한 사이버 공격-방어가 항상적으로 이루어진다. 국가 행위자와 그 프록시에 의해 수행되는 사이버 범죄, 사이버 테러, 그리고 사이버 스파이 행위들은 그와 같은 항상적 비키네틱 공격-방어의 대표적인 사례들이다(박동휘, 2022: 45-66). 이 같은 맥락에서 보면 오늘날의 신냉전은 재래식 군사력 또는 핵 무력이 동원되는 본격적인 전쟁 이전단계에서 사이버 수단

과 같은 비키네틱 열전(hot war)이[1] 진행되는 변형된 성격을 가지는 것으로 볼 수 있다.

물론 사이버 수단은 핵전쟁을 포함한 본격적인 전쟁(a full-scale war)에서도 중요한 전략적 가치를 가진다. 이는 2008년 러시아-조지아 전쟁 사례와 특히 최근 2022년 러시아-우크라이나 전쟁 사례에서 확인할 수 있다. 이 경우에 사이버 공격-방어는 진정한 의미에서의 사이버전(cyberwarfare)으로 정의될 수 있다. 사이버전은 본격적인 전쟁 개시 직전 단계에서 임박한 군사적 침공의 선도공격 또는 예비공격으로서의 성격을 갖거나 땅과 바다, 하늘 등과 같은 물리공간에서의 키네틱 전쟁수행과 병행하여 사이버 공간에서 치러지는 비키네틱 전쟁을 의미한다. 오늘날과 미래의 전쟁은 땅, 바다, 하늘, 우주, 인간의 인지(human domain), 그리고 사이버 공간에서 함께 복합적-다면적으로 치러지는 다영역 전쟁의 성격을 가진다. 사이버전은 이 같은 다영역 전쟁의 한 국면에 해당하며, 다른 도메인(domain)에서의 전쟁과 긴밀히 연계되고, 다영역 전쟁 전체의 승패에 결정적인 영향을 미칠 수 있는 중요한 한 수단이 된다(박동휘, 2022: 125-133).

사이버 공격-방어는 본격적인 전쟁의 시작을 기점으로 전쟁이전의 단계와 전쟁 이후의 단계 모두에서 활용될 수 있다. 이 같은 현상은 2022년 2월 발발한 러시아-우크라이나 전쟁의 사례에서 잘 관찰된다. 대체로 전쟁이전의 단계에서 사이버 공격-방어는 사이버 범죄, 핵티비즘, 사이버 테러, 사이버 간첩, 사이버 영향력 공작 등으로 나타났다. 이는 대체로 2010년대 중반에서부터 진행되어 왔다. 따라서 일각에서는 러시아-우크라이나 전쟁이 2022년에 시작된 것이 아니라 그 이전부터 수년에 걸쳐 진행되어 오고 있었다고 보기도 한다. 2022년 2월 본격적인 전쟁개시 이후의 단계에서는 물리공간에서의 치열한 키네틱 전투와 함께 사이버 공간에서도 본격적인 사이버 기술전과 사이버 인지전이 수행되었다. 이 같은 맥락에서 이번 러시아-우크라이나 전쟁은 우주전과 더불어 사이버전이 본격적인 전쟁의 한 양식으로 포함된 진정한 의미에서의 미래전의 서막이라고 평가되기도 한다.

전쟁 이전과 이후 단계 모두에서 활용되는 사이버 공격이나 침해행위의 특성 때문에 사이버 안보는 전쟁과 평화라는 전통적인 이분법적 경계 구분의 타당성에 의문을 던진다. 사이버 안보의 관점에서 보면 전쟁-평화의 이분법적 구분보다는 의지와 이해관계, 목표가 충돌하는 두 국가 또는 진영 간에 형성되는 항상적인 평화적 전쟁(또는 전쟁적 평화)상태가 더 현실에 가깝다. 사실상 사이버 안보의 측면에서 평화와 전쟁은 이분법적으로 구분되는 개념 보다는 연속된 스펙트럼으로 이해하는 것이 더 타당하다. 두 충돌하는 국가나 진영 간의 현 국면은 스펙트럼 상의 양 끝단에 위치한 절대평화와 절대전쟁의 사이 어딘 가에 위치하며, 이는 늘 이동하는 과정에 있는 것처럼 보인다. 이런 측면에서 러시아의 개념구분은 시사점이 크다. 러시아는 평화-전쟁 스펙트럼을 4개의 하위유형으로 구분한다. 이는 ① 평화적 공존, ② 이해관계의 갈등 또는 자연적 경쟁, ③ 무장충돌, 그리고 ④ 전쟁(a full-scale war)이다. 러시아의 개념으로 전쟁은 어떤 특정 시기에 국한된 의미가 아니며 단계적으로 이해갈등과 충돌이 격화되어 가는 과정이다(Nikkarila & Ristolainen, 2017: 194). 사이버 안보는 특히 이 평화-전쟁의 스펙트럼으로 이해하고 접근하는 것이 보다 타당하다. 충돌하는 두 세력 사이의 사이버 공격 또는 침해행위는 “이해관계의 갈등 또는 자연적 경쟁”, “무장충돌”, 그리고 “전쟁”의 단계 모두에서 국가 행위자들의 전략-전술적 의지(will)나 이해(interest)를 관철하고 목표(objective)를 달성하기 위한 주요한 수단(means)이 된다.

이 글에서 다룰 내용의 범위는 “전쟁” 이전 단계에서의 사이버 공격 또는 침해 행위들이다. 이

1) 냉전(cold war)에 대비되는 개념으로서의 열전(hot war).

는 러시아의 구분에 따르면, “② 이해관계의 갈등 또는 자연적 경쟁”와 “③ 무장충돌”의 단계에 해당한다. 이 단계들에서의 사이버 공격행위들은 사이버 범죄, 핵티비즘, 사이버 테러, 사이버 간첩(또는 사이버 스파이)활동 등으로 나타난다. 개념적으로 사이버전(cyberwarfare)은 전쟁 단계에서 이루어지는 사이버 수단 또는 공간을 이용한 공격, 침해 행위로 규정하여 이 글에서는 다루지 않을 것이다. 물론 실제 키네틱 전쟁이 발생하지 않은 상태에서 순수한 사이버전이 가능한지의 여부는 이론적, 추상적인 수준에서는 논의될 수 있다. 하지만 이 같은 사례가 현실적으로 나타난 경우는 없다. 물론 2007년 러시아의 에스토니아 사이버공격을 사이버전으로 볼 수도 있다는 주장이 제기될 수는 있다. 하지만 이는 여전히 논쟁의 대상이다. 따라서 사이버 범죄, 사이버 테러, 사이버 간첩활동 이외에 전쟁(a full-scale war) 이전단계에서 별도로 사이버전에 대해 이 글에서 다룰 필요는 없을 것으로 판단된다. 바꾸어 말하면 이 글에서는 전쟁 이전의 단계에서 사이버 수단을 사용하거나 사이버 공간을 통해서 수행되는 다양한 공격 또는 침해행위들에 초점을 맞추어 논의할 것이며, 이러한 행위들은 대체로 사이버 범죄, 사이버 테러, 그리고 사이버 간첩활동 등으로 구분될 수 있다.

이 글의 주요 목적은 전쟁 이전 단계에서 나타나는 다양한 사이버 상에서의 범죄, 테러, 간첩활동들에 대한 기본 개념을 탐색하는 것이다. 이 같은 다양한 사이버 공격 또는 침해행위들은 다양한 국가 및 비국가행위자들에 의해 수행되며, 종종 복잡하고 혼재된 형태로 사이버 공간 상에 뒤섞여 있다. 따라서 국제정치학에서 사이버 안보의 문제를 다루기 위해서는 우선 다양한 사이버 안보의 문제들을 개념적으로 규정하고 그 관계들을 보다 명확히 정립할 필요가 있다. 이 글은 이와 같은 필요를 반영한다.

또한 이 글은 이와 같은 다양한 미시적-중층적-거시적 수준에서의 사이버 공격 또는 침해행위들이 어떤 국제정치적 함의를 가지는 지에 대해 논의한다. 오늘날의 국제정치질서는 신냉전으로 규정되며 이와 같은 다양한 형태의 사이버 공격 또는 침해행위들은 본질적으로 신냉전 질서의 현상과 변화방향에 주요한 영향을 미친다. 이 글은 이 같은 사이버 안보의 이슈들과 신냉전 국제정치질서의 관계에 대해 살펴본다. 이를 위해 이 글은 사이버 범죄자들과 해커들, 핵티비스트들과 같은 다양한 비국가행위자들을 다루지만 본질적으로 신냉전의 핵심 주체인 국가행위자들에 대해 보다 주목한다. 대체로 오늘날 사이버 공간상에서 다양한 비국가 행위자들이 국가행위자들과 연계되어 이들의 프록시로 활용되는 경향이 두드러지고 있다. 이러한 경향성은 비국가행위자들과 국가행위자들이 제기하는 다양한 사이버 안보의 위협들이 국제정치에서 중요한 함의를 가지도록 만든다.

Ⅱ. 사이버 공간에서의 위협동향과 범죄-테러-간첩의 통합(nexus) 현상

사이버 범죄, 테러, 스파이 활동 등이 뒤섞여 있는 사이버 공간상에서의 위협 동향 파악은 매우 어렵다. 사이버 공격의 피해가 발생했는지 여부를 피해 당사자들이나 제3자가 정확히 인지하기도 어려울 뿐만 아니라 피해를 인지했을 경우에도 피해 사실 자체를 여러 가지 이유로 외부에 공개하지 않는 경우도 많다. 이 때문에 해킹과 사이버 위협의 상당 부분은 암수(dark figure)로 남는다(Kirwan & Power, 2017: 80-82).

그럼에도 불구하고, 해킹과 핵티비즘, 사이버 공격 등은 상당히 심각한 국제정치에서의 안보위

협으로 받아들여지고 있으며, 전세계적으로 그 발생빈도 역시 상당히 높은 수준인 것으로 인식되고 있다. 사이버 공격에 대해 전문가들은 다음과 같은 위협적이면서 암울한 가능성을 경고한다. 레망-랑글르와는 "특정 국가에 막대한 경제적 손실을 가하기 위해 중요 기반 시설을 표적으로 하는 '사이버 진주만 공격'이 현실로 다가올 수 있으며,... 가장 중요한 핵심 기반 시설을 집중 공격함으로써 중요 기반 시설 전체가 붕괴될 가능성이 있다"고 지적한다(Leman-Langlois, 2008: 2-3). 휘태커는 "몇 번의 스위치 작동으로 적대 국가의 전력망을 차단시키고 통신망을 교란시키며, 도로, 철도, 운송, 항공 통제 시설 등 중요 사회 기반 시설을 붕괴시킬 것이다.... 바이러스 프로그램들이 제대로 작동한다면 전체 시스템이 완전히 붕괴될 것이다. 공작원들은 기밀 정보들을 빼내고, 파괴시킬 수 있다. 우리는 우리를 지켜보고 있는 적이 누구인지도 모르는 상태에서 파괴와 죽음만이 난무하는 혼동 속에서 헤어나지 못할 수도 있다"고 경고한다(Whittaker, 2004: 123).

2022년 상반기 6개월(1월-6월) 동안 전 세계적으로 핵티비즘과 DDoS 공격이 급격히 증가했다. 이와 같은 해킹과 핵티비즘, 사이버 공격의 가파른 증가세는 미국과 아시아, 유럽 전역에 걸쳐 보편적으로 관찰되었다. 예를 들면, 악의적인 DDoS 공격의 빈도수는 2021년 상반기 6개월 동안과 비교할 때 2022년 같은 기간에 203% 증가했다. 또한 2022년 상반기 동안의 악의적인 DDoS 공격 사례 수치는 2021년 전 기간(1월-12월) 동안의 공격 빈도수에 비해서도 60% 증가한 것이다. 애국적 핵티비즘을 포함한 사이버 영향력 공작 역시 2022년 같은 기간 동안 극적으로 증대했다. 특히 애국심 또는 이데올로기 등의 대의(cause)를 목적으로 한 영향력 공작은 2016년 이후 2022년 올해 들어 전 세계적으로 수백만 명의 삶에 영향을 미치는 주요한 위협 요인으로 등장했다. 이와 같은 종류의 사이버 위협은 전 세계적으로 다양한 전략적 목적이나 대의를 실현하기 위한 최고 수준의 하나의 무기가 되고 있다(Lohrmann, 2022).

이와 같은 최근 사이버 위협의 눈에 띄는 증가추세는 다른 자료들에서도 확인된다. 2020년에 이미 사이버 공격은 전 세계적으로 다섯 번째 순위의 중대한 위협이었고 공공과 민간 부문 전반에 걸쳐 중대한 위협이라는 점은 상식이 되었다. IoT(Internet of Things) 사이버 공격 한 분야만 해도 2025년까지 2022년 수치의 두 배가 될 것이라고 예상된다. 반면에 사이버 공격에 대한 탐지 비율은 극히 낮다. 세계경제포럼 2020 글로벌리스크보고서(World Economic Forum's 2020 Global Risk Report)에 따르면, 사이버 공격 탐지 비율은 미국의 경우 0.05퍼센트 밖에 되지 않는다(Embroker, 2023). 또 다른 자료 역시 사이버 공격 위협의 최근 동향이 매우 우려할 만한 수준임을 보여준다. 해당 자료에 따르면, 전세계적으로 매일 30,000개의 웹사이트가 해킹된다. 전 세계 64퍼센트의 민간 기업들이 적어도 하나의 유형 이상의 사이버 공격을 경험했다. 2021년 3월에 2천만 건의 사이버 침해 기록(20M breached records)이 있었다. 2020년에 랜섬웨어(ransomware) 사례가 150퍼센트 증가했다. 이메일은 약 94퍼센트의 모든 종류의 멀웨어(malware)와 관련이 있다. 매 39초마다 웹상에서 새로운 사이버 공격이 어디에선가 발생한다. 평균 대략 24,000개의 악성 모바일 앱(malicious mobile apps)이 인터넷에서 매일 차단된다. 300,000개의 새로운 멀웨어가 매일 만들어지며, 이와 같은 멀웨어는 바이러스(viruses), 애드웨어(adware), 트로전스(Trojans), 키로그스(keyloggers) 등을 포함한다. 2020년에 데이터 침해의 63퍼센트 정도는 금전적인 동기로 발생했다. 2021년에 이와 같은 사이버 침해를 복구하기 위해 전 세계 민간 기업들이 6조 달러(USD)를 지불했다(Bulao, 2022).

최근 들어, 전 세계적으로 사이버 공격위협 수준이 급격히 증대된 것은 다음과 같은 이유들 때문이다. 먼저, 2020년부터 시작된 코비드-19(COVID-19) 팬데믹 영향으로, 사람들의 일상 활동이 오프라인에서 온라인으로 대거 이동하였다. 이와 같은 추이에 맞춰 범죄 역시 오프라인에서

온라인으로 대거 이동한 것으로 관찰된다. 사이버 절도에서 횡령, 데이터 해킹과 사이버 파괴에 이르는 거의 모든 유형의 사이버 범죄가 코비드-19 발생 이후에 600퍼센트 증가하였다(AP, 2020).

또한, 2022년 2월 발생하여 1년 반 넘게 이어지고 있는 러시아-우크라이나 전쟁의 영향도 전 세계적인 사이버 공격의 증대에 영향을 미쳤다. 러시아와 우크라이나 양측에 속한 러시아어 사용 행위자들의 사이버 공격과 언더그라운드 해킹이 급격히 증가했으며, 동시에 애국적 핵티비즘 역시 두 전쟁 당사국과 제3국 등에서 증대하였다. 이와 같은 핵티비즘에는 러시아-우크라이나 양측 핵티비스트들뿐만 아니라 우크라이나 또는 러시아를 지지하는 제3국 해커들과 핵티비스트들도 자신들의 신념과 대의에 따라 자원 참전하였다. 여기에는 러시아를 상대로 전쟁을 선언한 어나니머스 등도 포함된다(Radware, 2022).

이 밖에도 중국을 포함한 세계 도처에 산재한 다양한 국가행위자들의 전략적, 정치적, 경제적 이해와 이와 연계된 프록시들의 활동이 사이버 스파이활동과 영향력 공작, 그리고 애국적 핵티비즘의 증가에 영향을 미쳤다. 중국의 사이버 스파이활동과 영향력 공작은 상당히 높은 수준으로 지속되고 있다. 맨디언트의 2022년 특별보고서에 따르면, 중국의 2021년 14차 5개년 계획(14th Five-Year Plan)의 시행과 계속적인 BRI(Belt and Road Initiative) 추진 지원을 위해 필요한 기술, 금융, 에너지, 텔레커뮤니케이션, 그리고 헬스케어 등의 과학기술 확보와 맞물려 사이버 스파이활동과 사이버 과학기술절도가 더욱 기승을 부릴 것으로 예측되었다(Kutscher, 2022: 79-81). 댓글공작 등을 포함한 중국의 사이버 영향력 공작 수준 역시 최근 들어 더욱 급격히 증대되었다. 트위트는 2019년 12월 발표 자료에서, 중국 댓글부대의 핵심 계정이 2만3750개에 달한다고 밝힌바 있다(송의달, 2023).

한편 한국의 가장 큰 사이버 위협의 출처인 북한 역시 사이버 공격 또는 침해활동에 적극적이다. 국제사회의 대북경제제재, 코비드-19 봉쇄, 그리고 계속되는 핵과 미사일 개발 소요 등으로 인해 외화가 절실하게 필요해진 북한이 자금 조달을 위해 사이버 해킹과 절도에 몰두한 것도 최근 국제적 해킹과 사이버 범죄의 증가에 기여하였다. 2021년 한 해에만 북한 해커들이 암호화폐 플렛폼(cryptocurrency platforms)에 대해 최소 7번 공격하여 약 4억 달러 가치의 디지털 자산을 훔쳤다. 이와 같은 공격의 대부분은 라자루스(Lazarus)라고 불리는 해킹 그룹에 의해 실행되었으며, 이 그룹은 북한의 핵심 정보기관인 정찰총국(The Reconnaissance General Bureau)에 의해 통제된다(BBC News, 2022). 미국 ODNI(The US Office of the Director of National Intelligence) 2021 연례 위협 평가(2021 Annual Threat Assessment)에 따르면, 북한의 사이버 에스피오나지, 사이버 절도, 그리고 사이버 공격 위협은 매우 증대되고 있으며, 특히 북한은 핵과 미사일 개발을 위한 자금 조달을 위해 전 세계 금융 기관들과 암호화폐거래소에 대한 사이버 절도에 주력한다. 북한과 관련된 주요한 해커조직들로는 라자루스 그룹(Lazarus Group), APT38, 블루노로프(BlueNoroff), 스타더스트 천리마(Stardust Cholloima) 등이 있다(US Government Homepage, 2023).

사이버 범죄, 사이버 테러, 그리고 사이버 간첩행위의 통합현상은 행위 그 자체의 연계-통합과 행위자의 연계-통합이 함께 나타나고 있다. 다양한 사이버 침해행위들과 행위자들에 의한 사이버 공격이 서로 뒤섞여 있으며, 최근으로 올수록 이러한 연계-통합 현상이 강화되고 있다. 예를 들면, 조직적 사이버 범죄세력이 직접 사이버 공격을 하는 것이 아니라 다크넷 등을 통해 사이버 공격의 기술과 노하우, 도구, 그리고 인프라 등을 제공하고 금전적인 이득만을 취한다. 이들 사이버 범죄 행위자들은 국가행위자나 테러리스트들, 또는 다른 사이버 범죄자들에게 멀웨어나 스파이웨어를 제작하여 제공하거나, 네트워크나 프로그램 등의 보안상 제로데이 (zero-day) 취약성

을 미리 파악하여 이를 알려주거나, 멀웨어나 백도어 등을 미리 심어두고 사이버 공격 또는 범죄를 위한 인프라를 구축하여 이를 판매하거나 하는 등의 사이버 공격과 관련된 각종 서비스를 제공하고 금전적 대가를 받는다. 또한 다크넷 상에서 다양한 의도를 가진 행위자들이 정보기관이나 사법당국의 감시를 피해 안전하게 자료나 정보를 업로드하거나 유포하도록 하는 블렛프루프 호스팅(Bulletproof Hosting)과 같은 플랫폼 서비스를 제공한다. 이와 같은 방식으로 사이버 범죄-사이버 테러-사이버 간첩 행위들이 서로 긴밀하게 연계되고 통합된다. 상황이 이렇다 보니, 랜섬웨어 또는 멀웨어 공격, 워터링 홀(watering hole) 공격, 백도어 설치, 봇넷 구축 등과 같은 사이버 범죄행위가 언제든 가상화폐절취와 같은 또 다른 사이버 범죄나, 국가핵심기반시설 공격과 같은 사이버 테러, 사이버 공간을 통한 핵심과학기술, 국방기술, 군사전략 등의 절취와 같은 사이버 간첩행위, 민감한 정보의 폭로를 통한 대중여론 조작이나 선거개입과 같은 사이버 영향력 공작으로 이어질 수 있다. 이는 유사한 사이버 공격기법이 범죄와 테러, 그리고 간첩 행위 등에 두루 사용될 수 있는 기술의 상호호환성(interchangeability) 때문이다. 따라서 사실상 특정한 사이버 공격이나 침해행위가 범죄적 목적을 위한 것인지 아니면 그와 연계된 테러나 간첩, 또는 영향력 공작의 의도를 담고 있는 것인지 파악하기가 매우 어려우며 사실상 이것들은 뒤섞여 있다.

다음으로, 행위자의 측면에서 범죄자, 해커들, 핵티비스트들, 테러리스트들, 스파이들은 서로 연계-통합되고 있다. 특히 이 가운데 국가행위자와 비국가행위자들 간의 전략적 연대가 국제정치적으로 중요한 함의를 가진다. 국가행위자들이 이 같은 비국가행위자들을 자신들의 프록시로 활용하는 이유는 국가책임을 부인(deniability)하면서 자신들의 전략적 목표를 효과적으로 달성할 수 있기 때문이다(송태은, 2020a: 8).

러시아의 경우 FSB(연방보안국), GRU(정보총국), SVR(해외정보국) 등 러시아의 주요 정보기관들은 해커들과 범죄자들, 그리고 애국적 핵티비스트들과 같은 민간 프록시(proxies) 병력들과 연계되어 있다. 이와 같은 민간 프록시들은 다양한 사이버 작전들(cyber operations)에 동원된다(Maurer & Hinck, 2018: 47). 네덜란드 정보부(Dutch General Intelligence and Security Service: AIVD)는 러시아 해킹 조직인 코지베어(Cozy Bear)가 SVR에 의해 지휘통제를 받았다고 추론했다. 미국의 민간 사이버보안회사인 크라우드스트라이크(CrowdStrike) 역시 이와 같은 네덜란드 정보부의 추론에 동의한다(SOCRadar, 2021). 사이버베르쿠트(CyberBerkut)라는 해커그룹은 러시아 정보기관의 사주를 받아 2014년 우크라이나 선거 기반시설에 대해 공격한 것으로 알려졌다(Connell & Vogler, 2017: 23-24). 트롤팜(troll farm)이라고 불리는 IRA(Internet Research Agency) 역시 프록시 행위자에 해당한다. IRA는 러시아 정부로부터 금전적 지원을 받는 민간회사로 알려져 있다(송태은, 2020b: 22-23). 2022년 러시아-우크라이나 전쟁 발발 초기에 GRU와 연계된 엘리트 러시아 해킹팀인 샌드웜(Sandworm)을 포함한 러시아 해커들은 멀웨어, 피싱(phishing), DDoS 등으로 우크라이나 주요 타깃들에 대한 전방위적 사이버 공격을 감행하였다(Greenberg, 2022; Lewis, 2022; Pearson & Bing, 2022). 러시아의 해외국가들에 대한 영향력 공작인 프로젝트 락타(Project Lakhta)에 IRA(Internet Research Agency), 미디어 신테즈(MediaSintez), 노보인포(NovInfo), 넵스키 뉴스(Nevskiy News), 이코노미 투데이(Economy Today), 내셔널 뉴스(National News), 페더럴 뉴스 에이전시(Federal News Agency), 그리고 인터내셔널 뉴스 에이전시(International News Agency) 등의 다수의 민간 참여자가 조직적으로 동원되었으며, 이들의 배후에는 러시아 정보기관이 있었던 것으로 파악되었다(Ibid).

중국 역시 러시아와 유사한 경향을 보인다. 중국의 해커들과 핵티비스트들은 중국 정부에 의

해 전략적으로 지휘, 통제된다. 이들의 은밀한 실행 컨트롤타워는 중국인민해방군(PLA), 전략지원군(SSF), 또는 중국의 정보기관인 국가안전부(MSS)이다(Parcels, 2018: 3). 특히 인민해방군의 61398부대와 61486부대는 중국 해커들을 지휘, 통제하는 핵심 기관들이다. 미국과 독일의 연방정부 정보관계자들에 따르면, 중국의 해커 규모는 10만 명에 달한다. 이들 10만 명의 해커들은 중국 전역에 흩어져 있지만, 61398부대의 명령에 의해 움직이는 것으로 추정된다. 해커에 의해 정보가 수집되면 어학 전문가가 나서 번역을 하고 종합적 시각에서 분석·평가·전망한다. 정확한 수는 아무도 모르지만, 해커 외에 10만 명 정도의 지원세력들이 따로 존재하는 것으로 알려져 있다(유민호, 2014). 61486부대 내 12국은 또 다른 명령체계와 목적으로 운용되는 별도의 중국 해커집단이다. 이 부대는 주로 방위·우주·통신 분야에 특화된 해커로, 수준이 종래의 61398부대를 훨씬 능가한다고 알려졌다(유민호, 2014). 한편 MSS 역시 다수의 사이버 에스피오나지 해커 그룹들을 운용한다. MSS 관련 해커그룹들로는 APT3(또는 Gothic Panda)과 APT10(MSS TSSB(Tianjin State Security Bureau)에 의해 지휘통제를 받는) 등이 있으며, 2020년 MSS와 계약을 맺고 모더나 사를 해킹한 바 있다(Cimpanu, 2018; Bing & Taylor, 2020; Spring, 2017). 중국의 해커들 및 핵티비스트들은 모두 애국적(nationalistic)이며, 중국 정부를 위해 직접 일하거나 또는 계약을 맺고 일하는 것으로 파악되었다. 알려진 바에 따르면, 중국 정부에 연계되지 않는 중국 해커나 핵티비스트들은 거의 없다(Parcels, 2018: 5).

이와 같은 사이버 상에서의 범죄-테러-간첩 행위들의 연계성-통합성 때문에 간첩이나 테러 행위뿐만 아니라 통상적인 사이버 범죄 행위 역시 국제정치적인 함의를 갖게 된다. 다양하고 뒤섞여 있는 사이버 공간상에서의 위협들은 하나의 총합(A sum of all threats)으로 중대한 국가안보의 위협이 된다. 또한 이 같은 위협은 다른 도메인에서의 국제안보의 이슈들과 연계된다. 예를 들면, 북한의 사이버 가상화폐 절취는 북한의 핵 무기 개발과 긴밀히 연계되어 있다. 중국의 첨단 과학기술과 국방기술의 사이버 절취는 미-중 간의 국제정치적인 정치, 군사, 경제 부문에서의 패권충돌에 중대한 영향을 미친다. 같은 맥락에서 러시아와 중국의 미국과 서방국가들에 대한 영향력 공작과 선거개입은 미국-서방 대 중국-러시아의 지정학적 패권충돌의 향방에 의미 있는 영향을 미칠 수 있다. 결국 사이버 상에서의 다양한 수준의 공격과 침해행위들은 국제정치의 틀에서 이해되어야 한다. 이런 측면에서 이 같은 다양한 행위들의 기본개념들을 국제정치적 맥락에서 탐색하고 이해할 필요가 있다.

Ⅲ. 사이버 범죄, 테러, 간첩행위의 기본 개념에 대한 탐색

사이버 상의 여러 공격들과 침해 행위들은 미시적 수준, 중층적 수준, 그리고 거시적 수준으로 나누어 분류해 볼 수 있다. 미시적 수준에서의 사이버 공격과 침해행위들은 사이버 범죄로 정의된다. 사이버 테러는 중층적 수준에서의 사이버 상에서의 공격과 침해행위들로 규정될 수 있다. 사이버 간첩행위는 가장 거시적인 수준에서의 사이버 공격과 침해행위들에 해당할 수 있다. 이는 사이버 간첩행위가 한 국가의 전략목표나 국가이해를 관철하기 위해 수행되기 때문이다. 이 같은 사이버 범죄와 사이버 테러, 그리고 사이버 간첩 행위들의 기본 개념들을 각각 살펴보면 다음과 같다.

사이버 범죄는 컴퓨터, 통신, 인터넷 등을 악용하여 사이버 공간에서 행하는 범죄 또는 사이버 공간을 이용한 범죄행위를 통칭한다. 일반적으로 사이버 범죄에는 금전을 목적으로 하거나 개인

적 흥미, 스릴, 쾌락을 추구하거나 또는 다른 사람들을 괴롭히거나 공격하여 피해를 입히기 위한 목적 등으로 행해지는 불법행위들이 포함된다. 사이버 테러 행위가 사이버 범죄에 포함될 수도 있으나 여기에서는 사이버 테러를 별도로 다루고 있기 때문에 사이버 테러를 제외한 나머지 범죄행위들이 모두 이 사이버 범죄의 카데고리에 포함될 수 있다.

사이버 범죄는 오프라인에서의 일반적인 범죄들과 마찬가지로 범죄 수법, 동기 및 범죄의 심각성 수준이 매우 다양하며, 국가별 형사 사법 시스템에 따라 처리 방식 또한 천차만별이다. 또한 국가별 법률체계에 따라 사이버 범죄로 처벌되는 경우도 있고 그렇지 않은 경우도 있다. 가상 세계에서 발생하는 범죄들의 경우 가상 세계별 허용 가능한 행위 수준이 상이하기 때문에 동일한 법률을 적용시키기는 힘들다(Kirwan & Power, 2017, 24-25).

그럼에도 불구하고 이 같은 다양하고 이질적인 사이버 범죄들을 유형별로 구분지어 볼 수는 있다. 먼저 사이버 범죄는 인터넷 이용 범죄와 인터넷 특정 범죄로 구분된다. 인터넷-이용 범죄들(internet-enabled crimes)은 디지털 성범죄, 아동 포르노 유포, 마약거래, 사이버 불링(bullying), 악성댓글 등과 같이 금전이나 다른 개인적 쾌락, 스릴, 분노의 표출 등과 같은 다양한 사적 목적을 위해 실행된다. 이 같은 범죄들은 오프라인에서 수행될 수도 있으나 인터넷을 이용함으로서 쉽고, 빠르게 범죄가 실행되는 경향이 있다. 인터넷-특정 범죄들(internet-specific crime)은 온라인 혹은 컴퓨터를 통해서만 범죄가 가능한 유형으로 대표적으로 악성코드 배포, 웹 사이트 서비스 거부 공격, 랜섬웨어 공격 등이 있다. 이 같은 범죄들은 금전적인 목적을 위해서 수행되거나 아니면 공격자 개인의 과시욕구, 쾌락, 스릴추구 등과 같은 동기추구 때문에 일어난다(Kirwan & Power, 2017). 한편 사이버 범죄는 대인범죄와 재산범죄로도 나누어 볼 수 있다. 대인범죄는 사이버 공간을 통해 특정 인물이나 대상에 대해 공격 또는 침해행위를 실행하는 것이다. 여기에는 아동에 대한 성적학대, 사이버 불링(bullying)과 같은 사이버 공간을 통한 괴롭힘, 웹디페이싱 등이 포함될 수 있다. 한편 재산범죄는 금전적 이득을 목적으로 한다. n번방 사건 등과 같은 사이버 공간을 이용한 디지털 성범죄, 사이버 공간을 이용한 마약거래, 금전을 갈취하기 위한 랜섬웨어 공격, 가상화폐 절취 등이 여기에 해당할 수 있다(Kirwan & Power, 2017). 이 같은 두 개 쌍의 카데고리들은 2X2로 네 개의 세부적 유형들로 분류될 수 있다. 예를 들면, ① 인터넷-이용 범죄/대인 범죄, ② 인터넷-특정 범죄/대인 범죄, ③ 인터넷-이용 범죄/재산 범죄, ④ 인터넷-특정 범죄/재산 범죄 등이다. ①의 대표적인 사례로는 사이버 불링 등을 들 수 있다. ②의 대표적인 사례로는 보복성 개인정보 해킹, 랜섬웨어 공격이 해당된다. ③에는 디지털 성착취물 거래나 온라인 마약거래 등이 대표적이다. 마지막으로 ④는 가상화폐 절취나 금전을 목적으로 한 랜섬웨어 공격 등이다.

사이버 테러는 ISIS, 알카에다 등의 이슬람 극단주의 테러세력이나 극우 또는 극좌 테러단체 등에 의해 수행되는 사회전반에 대한 공포의 조장, 혼란, 사회 핵심기반시설에 대한 마비 등을 목표로 한 사이버 공격행위이다. 테러단체 또는 테러행위자들은 자신들의 정치적, 종교적, 사회적, 이념적, 가치적 의지를 사회일반에 강요하여 관철시키려 한다. 가장 대표적인 사이버 테러는 원자력시설, 발전소, 정보통신망, 항만, 철도교통망, 에너지 공급망, 전력망, 항공교통망 등 국가의 핵심기반시설에 웹기반 공격이나 시스템기반 공격 등과 같은 대규모 사이버 공격을 감행함으로서 국가나 사회전반의 일상을 마비시키고 사회전반에 공포를 조장함으로서 테러단체나 행위자의 전략적 목표를 달성하려는 행위이다(윤민우, 2022a: 546).

사이버 테러 역시 사이버 범죄와 유사하게 두 가지 유형으로 구분될 수 있다. 하나는 디도스 공격이나 랜섬웨어나 멀웨어와 같은 사이버 공격수단을 사용하여 정보통신망이나 핵심기반시설, 또는 웹사이트나 컴퓨터 프로그램, 시스템, 또는 디바이스 등을 파괴, 불능화, 침해, 하이재킹 하

는 사이버-기술 공격이다. 다른 하나는 테러단체나 테러리스트 등이 선전, 선동, 프로파간다, 자금모금, 테러이용수단 및 훈련, 공격기법 전파, 지원 및 공포의 조장 등과 같은 목적을 위해 사이버 공간을 이용하는 행위이다. 전자는 인터넷-특정 범죄와 유사하며, 후자는 인터넷-이용 범죄와 유사하다. 하지만 범죄와 달리 사이버 테러의 경우는 사회전체에 대한 공포의 조장이나 영향력의 행사, 그리고 자신들의 아젠다의 관철 등과 같은 전략적 목표를 실현하기 위한 수단으로 이용된다는 점에서 사이버 범죄와는 차별성을 가진다. 이 같은 테러행위자들의 전략적 목표 때문에 사이버 테러는 사이버 범죄보다는 더 높은 수준의 사회전반에 대한 위협이 된다.

사이버 테러의 경우는 보다 낮은 수준의 사이버 범죄나 보다 높은 수준의 사이버 간첩활동과는 달리 더 과장되고 부풀려진다는 특성을 보인다. 이는 테러세력의 전략적 이해 때문이다. 테러세력의 핵심 전략 목표는 대규모 살상과 파괴 또는 그러한 위협으로 유도되는 공포의 조장(terrorizing)을 통해 자신들의 세력을 과시하고 이를 지렛대로 정치적, 사회적, 종교적 메시지를 전달하고자 하는 것이다. 이런 측면에서 사이버 테러리스트들은 일반 범죄자들이나 국가행위자들과는 달리 자신들의 존재를 감추고 은밀히 작전을 수행할 이유가 없으며, 자신의 존재를 드러내고 과시할 개연성이 크다. 이 때문에 사이버 테러리스트들은 다른 행위자에 의한 사이버 공격이나 의도치 않은 사이버 재난이나 사고(예를 들면, 2022년에 발생한 카카오 서비스의 데이터센터 화재와 같은) 등을 마치 자신이 수행한 것처럼 가장 또는 과장하여 선전할 개연성이 크다(Chopitea, 2012: 37).

어나니머스와 같은 핵티비즘이 사이버 테러에 해당하는가는 논쟁의 여지가 있다. 하지만 이 같은 핵티비즘은 정치적, 사회적, 가치적 아젠다를 사회일반에 투영하고 이를 관철시키려 한다는 점에서 사이버 테러와 유사한 측면이 있다. 이 같은 측면에서 사이버 테러와 핵티비즘은 공통적으로 중충수준의 사이버 안보위협에 속하는 것으로 간주할 수 있다.

핵티비즘은 사이버 공격과 행동주의(activism)가 합쳐진 개념이다. 일반적으로 분산 디도스(DDoS) 공격이나 웹사이트 훼손(web defacement) 등의 형태로 정치적, 사회적, 종교적, 이념적 의사표현을 위해 사이버 상에서 행동하는 형태의 공격이다. 주로 사회적 이슈가 되는 낙태/반낙태, 환경, 동물보호, 인터넷 자유와 정보의 투명성, 국가의 억압적 권력에 대한 저항, 애국주의 등이 주요한 핵티비즘의 테마가 된다. 어나니머스의 사례는 이와 같은 핵티비즘의 대표적인 사례이다(윤민우, 2022a: 546). 러시아나 중국 등의 사례에서 종종 발견되는 애국주의적 핵티비즘 운동도 핵티비즘으로 간주될 수 있다. 하지만 이 같은 애국주의적 핵티비즘은 국가의 사주나 개입 없이 순수한 민간 행위자들에 의한 자발적인 활동에 국한된다. 만약 국가의 정보기관이나 군 등이 배후에 개입되어 민간 행위자들을 프록시로 활용하여 애국적 핵티비즘을 활용하는 경우라면 핵티비즘이 아니라 국가의 사이버-인지 공격 또는 영향력 공작으로 간주되어야 할 것이다. 이에 대한 사항은 뒤에 사이버 간첩과 관련하여 논의될 것이다.

핵티비즘은 종종 사이버 테러나 사이버 간첩활동과는 다른 특성을 보인다. 이들은 공격 타깃 선정에서 정부의 핵심 군사시설이나 보안시설 등과 같은 사이버 보안정도가 견고하여 침투-공격이 어려운 대상보다는 취약성 때문에 비교적 공격이 용이한 대상을 선택하는 기회주의적(opportunistic) 특성을 보인다. 또한 이들은 국가핵심기반시설과 같은 사이버 공격으로 인해 사회전반에 막대한 피해를 초래하거나 공포를 조장할 수 있는 공격타깃을 피하는 경향이 있다. 이는 이들이 자신들의 메시지를 더 많은 청중들에게 전달함으로서 자신들의 대의(cause)를 대중들에게 알리고 이들의 공감과 지지를 끌어내며, 자신들이 악(evil) 또는 부정의(injustice)로 규정한 대상에 대해 저항과 응징을 통해 교훈을 주려는 의도를 갖기 때문이다(Chopitea, 2012: 33). 따라서, 이들은 미디어의 관심을 끌면서 대중들의 주목도를 높일 수 있는 적절한 공격 대상의

취약성이 제공하는 기회를 이용하는 속성을 보인다(Chopitea, 2012: 32, 37).

이런 맥락에서 핵티비즘에는 고도의 기술수준과 자원과 시간, 역량의 지원을 필요로 하는 멀웨어를 이용한 APT 공격이 아니라 비교적 간단하고 용이한 공격기법들이 주로 이용된다. 대표적으로 핵티비즘에 이용되는 공격기법들은 독싱(doxing), 분산디도스(DDoS), 소셜미디어하이재킹(social media hijacking), 웹디페이스먼트(web defacement) 등이 있다(Threat Intelligence and Analysis, 2016: 5-9). 핵티비즘에서 분산디도스 공격 등과 같은 비교적 낮은 기술수준의 공격기법을 자주 활용하는 데는 중요한 이유가 있다. 이는 공격대상에 피해를 주는 것도 중요하지만 핵티비즘의 과정에서 많은 참여자들을 모집하여 함께하는 것 역시 매우 중요하기 때문이다. 이는 그들의 대의에 함께 하는 사람들의 참여규모의 크기와 확장성이 중요한 내러티브의 의미를 가지기 때문이다. 따라서 기술수준이 낮은 해커들이나 일반인들 역시 핵티비즘에 함께 할 수 있기 위해서는 공격툴을 온라인에서 쉽게 내려 받고 간단한 클릭으로 분산디도스와 같은 공격을 실행함으로서 함께 참여할 수 있어야 한다. 이런 측면에서 분산디도스나 웹 디페이스먼트와 같은 핵티비스트 공격은 사이버 기술공격의 측면도 있지만 동시에 대의를 공유하는 다수의 사람들이 함께함으로서 자신들의 대의의 정당성과 지지의 정도를 과시하는 사이버 심리 공격 또는 내러티브 확장의 측면도 동시에 가진다(Hampson, 2011: 7-9, 21-22).

하지만 핵티비즘이 비교적 낮은 기술수준의 공격기법을 사용하고, 대규모 파괴나 패닉, 공포를 야기하기보다는 다수의 참여를 유도하고 자신들의 대의를 주장하고, 환기시키고, 확장하려한다고 해서 사이버 공격의 피해가 반드시 치명적이지 않은 것만은 아니다. 미국 정부와 군에 깊이 연계되어 있었던 미국의 기술보안회사(technology security company)인 에이치비 게리 페더럴(HBGary Federal)은 어나니머스의 SQL injection 공격으로 평판에 치명적인 손상을 받았으며, 해당 회사의 CEO였던 아론 바(Aaron Barr)는 곧바로 사임했다. 결국 1년 뒤에 회사는 사라졌고 만텍 인터내셔널(Man Tech International)에 팔렸다. 굴지의 글로벌 기업인 소니(SONY)사 역시 룰즈섹의 SQL injection 공격으로 회사 평판에 치명적 손상을 입었다. 평판은 소니사의 공식 사과와 함께 천천히 회복되었으나, 소니사 주가는 반드시 해킹 공격에 의한 것이라고 단정하기는 어렵지만 이후 지속적으로 하락했다(Chopitea, 2012: 20-29).

사이버 간첩활동은 다른 말로 사이버 스파이활동 또는 사이버 에스피오나지(espionage)라고도 불린다. 사이버 간첩은 주로 국가행위자나 국가행위자의 사주를 받은 민간 프록시(proxy)들에 의해 수행된다. 스노든이 폭로한 바에 따르면, 미국은 NSA(National Security Agency) 주도로 높은 수준의 광범위한 사이버 간첩 활동을 오랫동안 실행해 왔다. 중국 역시 미국 못지않게 사이버 간첩에 가장 적극적인 행위자로 알려져 있다. 중국은 특히 BRI(Belt and Road Initiative), 경제와 국방부문의 과학기술의 지속적인 발전, 글로벌 패권추구를 위한 해외 주요 국가들에 대한 외교, 안보, 그리고 군사부문의 전략정보 수집 등의 다양한 필요에 따라 광범위하고, 무차별적이며, 끈질긴 사이버 간첩활동을 지속해왔다. 최근 중국의 국방과 산업부문의 빠른 과학기술발전은 상당 부분 사이버 간첩활동을 통한 기술절취에 힘입은 것으로 알려져 있다(윤민우, 2022a: 546-547).

사이버 간첩활동에 적극적인 미국, 중국, 러시아 등 주요 국가들은 군이나 정보기관에 사이버 간첩활동의 전담부서나 기관이 설치되어 있다. 미국의 경우 NSA의 TAO(특수목적접근작전팀), CIA의 IOC(정보작전센터), FBI의 DITU(데이터포착기술팀) 등이 그와 같은 조직들이다. 그리고 여기에 민간부문의 '엔드게임', '크라우드 스트라이크', '팰런티어 테크놀로지', '바나' 등과 같은 특화된 민간보안기업(또는 사실상의 사이버 용병들)과 마이크로소프트, AT&T, 버라이존, 구글 등 정보통신, 컴퓨터 네트워크, 소프트웨어, 및 인터넷 운영자와 플랫폼 등 일반 기업들, 그리고 다

양한 해커들이 연계되어 있다(해리스, 2015: 179-208). 중국과 러시아의 경우에도 이 글의 앞 부분에서 서술한 바와 같이 정보기관과 군의 은밀한 해커조직과 다양한 민간 해커들과 애국적 핵티비스트들이 연계되어 있다.

사이버 간첩활동은 사이버-기술 공격과 사이버-인지 공격의 두 하위 유형으로 구분될 수 있다. 사이버-기술 공격은 전형적인 사이버 간첩활동에 해당한다. 주로 APT나 워터링홀 공격 등을 통해 공격대상의 정보통신망이나 컴퓨터나 다른 정보통신디바이스, 데이터센터, 웹사이트, 이메일 등에 침투하여 과학기술, 국방기술, 국가 또는 군사전략, 외교안보정책, 또는 중요 개인정보 등을 수집하여 절취하는 행위이다. 이 같은 사이버 기술-공격은 컴퓨터 네트워크 내의 하드웨어와 소프트웨어에 침투하여 중요하거나 민감한 정보를 수집하거나 아니면 국가 최고정책결정권자가 제기한 비밀공작(Covert Operation)의 소요에 따라 공격대상의 하드웨어와 소프트웨어를 파괴, 훼손, 장악-통제하기도 한다. 이를 위해서는 주로 악의적인 소프트웨어를 도구로 사용한다. 간첩 또는 스파이활동은 대체로 첩보의 수집활동과 암살, 테러, 사보타지, 소규모 특수작전 수행 등의 다양한 비밀공작 활동들을 포함하는데 이 같은 전통적인 오프라인에서의 간첩 활동은 사이버 공간 상에서도 악성코드와 같은 기술수단을 사용하여 유사하게 수행된다(연합뉴스, 2023a; 연합뉴스, 2023b; 연합뉴스, 2023c).

사이버-인지 공격은 악의적 정보를 이용하여 사이버 영역에서 인간 행위자의 생각, 감정 및 심리에 영향을 미치고 이를 선전, 선동, 조작함으로서 이들의 의견과 행동변화를 이끌어내는 일련의 활동들을 의미한다. 이 같은 인지공격은 전통적으로 오프라인에서 미디어, 도서, 방송, NGO 등을 활용한 전략커뮤니케이션(strategic communication), 공공외교(public diplomacy), 공보, 홍보, 프로파간다 등의 형태로 이루어져 왔다. 사이버-인지 공격은 이 같은 전통적인 오프라인에서의 영향력 공작, 선거개입, 대중여론조작 등의 활동들이 사이버 공간 상에서 수행되는 것이다. 원론적으로 이 같은 사이버-인지 공격은 간첩활동 가운데 비밀공작의 범주에 속한다. 비밀공작에서는 앞서 언급한 스턱스넷 등과 같은 공격용 사이버무기를 통해 공격대상을 은밀히 기술적으로 파괴, 혼란시키는 것과 악성정보를 사용하여 대상청중에게 영향력을 행사하여 의도한 결과로 이어지게끔 유도하는 것이 함께 포함된다.

사이버-인지 공격은 사이버 영향력 공작으로도 불리며, 해외정보 조작 및 개입(FIMI: Foreign Information Manipulation and Interference)으로도 불린다. 이 같은 사이버-인지 공격은 국가 간의 경계를 초월하며, 평화와 전쟁의 시기 모두에 걸쳐 수행될 수 있다. 이는 또한 군사 및 비군사 영역과 정부 및 민간 부문을 모두 포함한다. 이 같은 사이버-인지 공격의 주요한 사례들로는 러시아의 2016년, 2020년 미국 대통령 선거 개입, 테러리스트 및 추종자의 확산 및 급진화(radicalization)를 위한 프로파간다, 중국의 우마오당 등과 같은 애국적 핵티비스트들을 동원한 댓글조작, 가짜뉴스, 역정보(disinformation) 공작, 그리고 북한의 유튜브와 웹사이트 등을 이용한 선전, 선동 공작 등이 있다(Ottewell, 2020). 오늘날의 첨단 정보통신환경에서 이 같은 해외로부터의 사이버-인지 공격은 매우 심각한 안보위협이 된다. 특히 러시아와 중국의 영향력 공작과 오정보, 가짜뉴스, 여론조작, 대중선동, 선거개입 등의 위협이 미국과 유럽 등 서방 동맹국들에서는 매우 중대한 위협이 되고 있다. 이에 따라 미국은 ODNI(Offiece of the Director of National Intelligence) 산하에 FMIC(The Foreign Malign Influence Center)를 2022년 9월 23일에 새로 설치하고 악성 해외 영향력 위협에 대응하고 있다(The Foreign Malign Influence Center, 2023). 또한 EU는 EEAS(European External Action Service) Stratcom Division을 2022년에 설치하고 해외로부터의 정보개입 및 조작의 위협에 대해 대응하고 있다(EEAS, 2023).

최근으로 올수록, 사이버-기술 공격과 사이버-인지 공격은 점점 더 융합되고 있는 추세이다. 예를 들어, 악성코드를 이용한 해킹을 통해 입수한 민감한 정보를 미디어나 위키리크스와 같은 폭로전문 사이트에 공개함으로서 선거개입이나 여론선동, 또는 특정 주요 인물이나 정부에 창피주기 등과 같은 영향력 공작을 수행하는 현상이 관찰된다. 한편 영향력 공작에 악성코드 확산을 통해 구축한 좀비 PC 및 봇넷이 경유지로 이용되기도 한다. 또한 AI(Artificial Intelligence), 딥페이크, 기계적 트롤(troll)들은 댓글 조작, 좋아요 추천, 또는 다른 수단을 이용한 선전, 선동에 활용된다. 이 경우에 사이버-기술 공격은 사이버-인지 공격의 전략적 목표를 달성하기 위한 수단이나 인프라로 활용된다(EEAS, 2023).

Ⅳ. 맺음말

앞서 논의한 사이버 범죄-테러-간첩 행위의 기본개념을 종합적으로 정리해 보면 다음과 같다. 이는 수준별, 공격수단별, 그리고 공격대상과 목표의 세 가지 잣대에 따라 다양한 사이버 공격 또는 침해행위들을 유형별로 분류한 것이다. 먼저, 수준별로 거시적 수준, 중층수준, 그리고 미시적 수준으로 구분해 볼 수 있다. 이 같은 수준별 스펙트럼에서 중층수준을 기준으로 거시적 수준에 해당할수록 국가 간의 복합지정학적 패권충돌에 주요한 영향을 미치고, 보다 국가들 간의 심각한 안보갈등을 야기하며, 핵심적인 국제정치학의 의제로 다루어지게 된다. 반면 미시적 수준으로 내려갈수록 이는 국제정치학의 이슈라기보다는 범죄, 사회문제, 또는 치안의 의제로 다루어질 개연성이 크다. 한편 이와 같은 낮은 수준의 사이버 침해행위들에 대해서는 국가들 간의 협력이나 합의(consensus)가 이루어질 개연성이 높아진다.

공격수단별로는 악성코드를 이용한 기술공격과 인터넷 또는 사이버 공간을 이용하거나 악성정보를 사용하여 사람들의 생각과 감정, 정서를 자극함으로서 전략적 목표를 달성하려는 공격으로 구분될 수 있다. 이 같은 공격수단에 따라 사이버 공격의 양태가 뚜렷이 구분되는 현상은 범죄, 테러, 간첩 행위 모두에서 관찰된다. 한편 핵티비즘의 경우는 기술공격 또는 영향력 공작으로 뚜렷이 구분되기 어렵다. 이는 핵티비즘이 악성코드와 악성정보에 의한 공격을 모두 포함하고 있는 통합공격의 성격을 갖기 때문이다. 핵티비즘은 본질적으로는 사이버 인지공격에 해당한다고 볼 수도 있지만 이를 위해 사이버 기술공격을 핵심 수단으로 사용하고 있다는 점을 고려할 때 두 측면을 모두 포함하고 있는 것으로 보는 것이 타당해 보인다.

공격대상과 목표에 따라, 사이버 간첩-테러-범죄 행위를 구분할 수 있다. 사이버 간첩행위의 경우 공격 대상은 상대 국가 그 자체가 된다. 물론 이 경우에도 특정 인물, 다수의 대중들, 또는 민간 기업이나 단체 등이 공격대상이 될 수 있지만 궁극적으로 이 같은 공격의 목표는 공격대상 국가일반의 과학기술, 전략, 정책에 관련된 첩보를 수집하거나 해당 국가의 전략 또는 정책에 영향을 미치기 위한 것이다. 사이버 테러의 경우는 사회일반이 공격의 대상이 된다. 사이버 공격 또는 침해행위를 통해 일반대중에 “공포”를 조장하거나 자신들의 믿음, 가치, 의지 등을 확산, 유포함으로서 사회일반에 영향을 미치려고 한다. 이 때문에 사이버 테러의 경우 특정 개인이나 단체, 시설 등을 대상으로 공격이 일어나더라도 궁극적으로 이 같은 공격의 목표는 직접 공격의 피해를 겪는 당사자가 아니라(즉 1차 피해자), 이 같은 공격을 통해 메시지를 전달하고자 하는 사회일반(2차 피해자)이 된다. 마지막으로 사이버 범죄의 공격대상은 직접적 피해당사자에 국한된다. 이 같은 공격대상이나 목표는 사람과 돈으로 구분해 볼 수 있다. 사람의 경우는 공격자가

피해대상이 되는 사람 그 자체에 대한 괴롭힘, 폭력, 학대를 목적으로 가하는 공격행위이다. 돈의 경우는 사람 그 자체가 아니라 금전적 이득을 취할 목적으로 행해지는 침해행위이다. 대체로 이 같은 사이버 범죄 행위는 보다 높은 수준의 사이버 테러나 사이버 간첩 행위와는 달리 직접적 공격대상(1차 피해자) 그 자체에 공격목표가 국한되는 특성을 가진다. 국제정치의 측면에서는 공격목표가 1차 피해자에 국한되는 사이버 범죄가 아니라 직접적인 공격의 피해당사자를 넘어서 사회일반이나 국가전체와 같은 2차 피해자에게 영향을 미치는 사이버 테러와 사이버 간첩이 주요한 의제가 된다. 반면 사이버 범죄는 사회적 문제나 치안의 문제로 다루어지게 되며, 국제정치적 함의는 크지 않다 (하단 <그림 1> 참조).

<그림 1> 사이버 범죄/테러/간첩행위의 기본 개념에 대한 탐색과 유형별 구분

<table>
<tr><td>수준</td><td colspan="3">행위</td><td>공격대상/목표</td></tr>
<tr><td rowspan="4">거시적 수준</td><td rowspan="2">사이버 간첩</td><td>사이버 간첩/스파이 (기술적 침해행위/공격)</td><td>사이버 인지-공격/영향력 공작</td><td rowspan="2">국가</td></tr>
<tr><td colspan="2">악성코드 (사이버 기술 공격, 해킹 등)</td><td>악성정보 (사이버 공간의 이용, 인지공격)</td></tr>
<tr><td colspan="3">공격수단</td></tr>
<tr><td rowspan="3">중층 수준</td><td rowspan="2">사이버 테러</td><td>사이버 테러 (기술공격)</td><td>테러리스트의 사이버 공간 이용</td><td rowspan="2">사회일반</td></tr>
<tr><td colspan="2">핵티비즘</td></tr>
<tr><td rowspan="2">미시적 수준</td><td rowspan="2">사이버 범죄</td><td>인터넷-특정 범죄/대인 범죄</td><td>인터넷-이용 범죄/대인 범죄</td><td>사람</td></tr>
<tr><td>인터넷-특정 범죄/재산 범죄</td><td>인터넷-이용 범죄/재산 범죄</td><td>돈/재산</td></tr>
</table>

출처: 글쓴이 작성

사이버 공격행위자가 누구인가에 따라 국제정치적 함의가 달라질 수 있다. 사이버 공격행위자들로는 개인, 민간보안회사, 민간 핵티비스트 그룹, 민간 범죄조직, 민간 네트워크, 테러단체, 애

국적 핵티비스트 그룹, 국가 행위자 등이 있다. 이와 같은 행위자 기준으로 일반 개인, 범죄조직, 범죄네트워크, 해커들, 민간보안회사들이 사이버 공격이나 침해행위를 주도하였을 경우에는 국제정치적 의제로 다루어질 개연성이 낮아진다. 이 경우에는 치안, 보안, 범죄, 사회적 일탈의 문제로 다루어질 개연성이 높다. 반면 국가행위자에 의한 공격일 경우에는 이는 국제정치적 의제가 된다. 이 경우에 국가행위자는 주로 군이나, 정보기관이거나 이들의 사주를 받은 프록시들(즉, 민간보안회사, 사이버 용병, 해커들, 애국적 핵티비스트들, 범죄네트워크들)을 포함한다. 한편 사이버 테러리스트들이거나 국가와 연계되지 않은 순수한 민간 핵티비스트들은 중층수준의 사이버 테러와 관련이 있다. 이 경우에 이 같은 비국가적 위협들은 신흥안보의 의제로 국제정치학에서 다루어질 수 있으며, 주로 국가 간 협력과 국제거버넌스의 이슈가 된다.

그러나 이와 같은 구분은 상대적인 것에 불과하다. 통상적으로 국제정치적 의제가 아닌 사이버 범죄의 경우에도 얼마든지 사안에 따라 국제정치적 함의를 내포할 수 있다. 위의 그림에서 국가행위자에 의한 사이버 침해행위는 회색으로 그리고 순수한 비국가 행위자에 의한 사이버 침해행위는 흰색으로 표시하였다. 한편 “핵티비즘”의 경우 종종 국가행위자가 민간 프록시 등을 사주하는 경우가 발생하기 때문에 국가-비국가 행위자가 뒤섞여 있다는 점을 강조하기 위해 빗금으로 표시하였다. 위의 그림에서 “인터넷-특정 범죄/재산 범죄” 역시 빗금으로 표시되었는데 이 역시 민간 행위자와 마찬가지로 국가 행위자가 금전탈취를 목적으로 사이버 범죄를 수행할 수 있다는 점을 부각하기 위해서이다. 북한의 경우가 이에 해당하는 대표적인 사례인데 북한의 “가상화폐절취”의 사례에서 보듯 국가행위자가 마치 범죄단체나 해킹조직처럼 금전을 목적으로 사이버 범죄를 수행할 수 있다. 이 경우에 순수한 사이버 범죄의 문제가 국제정치적 함의를 가질 수 있는데 이는 북한의 사이버 범죄를 통한 금전적 수익의 취득은 핵 무력과 재래식 군사력의 증강을 통한 동북아시아 지정학적 안보위기의 증대라는 국제정치적 의제가 긴밀하게 연계되기 때문이다.

이 글에서는 러시아-우크라이나 전쟁과 같은 본격적인 전쟁(a full-scale war) 이전 단계에서 벌어지는 다양한 사이버 공간에서의 공격과 침해행위들의 기본개념을 탐색하고 국제정치학적 함의를 도출하고자 하였다. 이 같은 공격과 침해행위들은 사이버 범죄, 사이버 테러, 사이버 간첩행위의 형태로 나타난다. 사이버전(cyberwarfare)이 이른바 평화시기라고 통상적으로 받아들여지는 본격적인 전쟁이전 단계에서도 가능한지에 대해서는 여러 논쟁이 있을 수 있다. 하지만 여기서는 사이버전이 본격적인 전쟁을 동반한다고 보고 사이버전에 대한 논의는 제외하였다. 여러 사이버 범죄, 테러, 간첩행위들은 이 글에서 살펴본 대로 수준과 공격수단, 공격대상과 목표, 공격 행위자의 성격 등에 따라 다양하게 분류될 수 있다. 여기에서 제시하는 다양한 사이버 공격, 침해행위들에 대한 기본개념의 구분과 이해는 여전히 만족스럽지는 않지만 애매모호하게 뒤섞여 있어 규정하기 어려운 여러 사이버 안보위해의 양태들을 이해하고 규정하는데 하나의 시각틀 또는 분석틀을 제공할 수 있을 것이다. 그리고 이를 통해 어떤 사이버 안보의 이슈들을 국제정치적 의제로 다루어야 할지에 대한 어떤 잣대를 제시할 수 있을 것이다.

〈참고문헌〉

김상배, 미중 디지털 패권경쟁, (서울: 한울, 2022), 21-26.

김상배. (2015). 사이버 안보의 복합지정학: 비대칭 전쟁의 국가전략과 과잉 안보담론의 경계, 국제지역연구, 24(3).

김열수. (2021). 미국의 반중봉쇄정책과 신냉전기 한국의 전략, 신아세아 28(4).

김충근. (2023) 한반도 신냉전 체제의 강화: 미북 정상회담 결렬의 경위와 후과 분석, 신아세아 30(1).

박동휘. (2022). 사이버전의 모든 것, 서울: 플래닛 미디어.

반길주. (2021). 냉전과 신냉전 역학비교: 미중패권 경쟁의 내재적 역학에 대한 고찰을 중심으로, 국가안보와 전략 21(1) (2021).

송의달. (2023). 돈·선물·성관계...세계 휩쓰는 중공의 국내정치공작, 한국에선?, 조선일보

송태은. (2020a). 하이브리드 위협에 대한 최근 유럽의 대응," IFANS 주요국제문제분석, 2020-31, 국립외교원 외교안보연구소.

송태은. (2020b). 디지털 허위조작정보의 확산 동향과 미국과 유럽의 대응, 주요국제문제분석 2020-13, 국립외교원 외교안보연구소.

연합뉴스, (2023a.1.26.). 중국 추정 해킹그룹, 학회·연구소 등 12곳 해킹, 연합뉴스. Https://www.youtube.com/watch?v=46YnHWcxRTE.

연합뉴스, (2023b.6.7.). 북 해킹조직 '김수키' 국내 안보 관계자 해킹…의도는?, 연합뉴스. Https://www.youtube.com/watch?v=vwm3BpOx7C0.

연합뉴스, (2023c.4.19.). 국내 언론사 등 61곳 해킹…북한 '라자루스' 소행, 연합뉴스. Https://www.youtube.com/watch?v=fHnXhE_0Dcw.

유민호. (2014.7.18.). 상하이 소재 61486부대 12국에 주목 교통대 출신의 중국 최고 해커들 암약, 주간조선. Http://weekly.chosun.com/news/articleView.html?idxno=7379

윤민우. (2020). 신흥 군사안보와 비국가행위자의 부상: 테러집단, 해커, 국제범죄 네트워크 등," 김상배 엮음 4차산업혁명과 신흥 군사안보, 서울: 한울.

윤민우. (2022a). 물류가 멈추면 세상이 멈춘다: 사이버 안보가 중요한 물류산업," 한국해양수산개발원 미래물류기술포럼 엮음, 물류트렌드 2023, 서울: Beyond X.

윤민우. (2022b). 미국-서방과 러시아-중국의 글로벌 전략게임: 글로벌 패권충돌의 전쟁과 평화, 평화학 연구 23(2).

해리스, 세인. (2015). 보이지 않는 전쟁 @ WAR, 진선미 옮김, 서울: 양문.

An official website of the United States government. (2023). North Korea Cyber Threat Overview and Advisories," CISA, Department of Homeland Security, the US, Https://www. cisa.gov/uscert/northkorea

AP(Associated Press). (May 23, 2020). The Latest: UN warns cybercrime on rise during pandemic, abc News. Https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542.

BBC News. (14 January 2022). North Korea hackers stole $400m of cryptocurrency in 2021, report says, BBC News. Https://www.bbc.com/news/business-59990477

Bing, Christopher and Taylor, Marisa. (July 31, 2020). Exclusive: China-backed hackers

targeted COVID-19 vaccine firm Moderna, Reuters.
Bulao, Jacquelyn. (2022). How Many Cyber Attacks Happen Per Day in 2022?, Techjury. https://techjury.net/blog/how-many-cyber-attacks-per-day/#gref
Chopitea, Thomas. (2012). Threat modelling of hacktivist groups, Master of Science Thesis, Chalmers University of Technology, University of Gothenburg, Sweden.
Cimpanu, Catalin. (December 20, 2018). US charges two Chinese nationals for hacking cloud providers, NASA, the US Navy, ZDNet.
Connell, Michael and Vogler, Sarah. (2017). Russia's Approach to Cyber Warfare, CNA.
EEAS(European External Action Service) Stratcom Division. (2023). 1st EEAS Report on Foreign Information Manipulation and Interference Threats. EEAS.
Embroker. (2023). 2023 Must-Know Cyber Attack Statistics and Trends, Embroker. Https://www.embroker.com/blog/cyber-attack-statistics/
Greenberg, Andy. (April 12, 2022). Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine, WIRED. Https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/
Hampson, Noah, C. N.. (2011). Hacktivism, Anonymous & A New Breed of Protest in a Networked World, Boston College International and Comparative Law Review 35(6).
Kirwan, Grainne and Power, Andrew. (2017). 사이버 범죄 심리학, 학지사.
Kutscher, Jurgen, Mandiant Special Report. (2022). M-Trends 2022, Mandiant. Https://www.mandiant.kr/.
Leman-Langlois, Stephane. (2008). Introduction: technocrime, In Leman-Langlois, Stephane (ed.), Technocrime: Technology, Crime and Social Control, (Cullompton, UK: Willian.
Lewis, James A.. (2022). Cyber War and Ukraine, CSIS(Center for Strategic & International Studies) Report. Https://www.csis.org/analysis/cyber-war-and-ukraine.
Lohrmann, Dan, (2022). Hacktivism and DDOS Attacks Rise Dramatically in 2022, Government Technology. Https://www.govtech.com/blogs/lohrmann-on-cybersecurity/hacktivism-and-ddos-attacks-rise-dramatically-in-2022.
Maurer, Tim and Hinck, Garrett. (2018). Russia: Information Security Meets Cyber Security, in Confronting an "Axis of Cyber?" edited by Fabio Rugge, ISP.
Nikkarila, Juha-Pekka and Ristolainen, Mari (2017). RuNet 2020-Deploying traditional elements of combat power in cyberspace?" in Juha Kukkola, Mari Ristorainen, and Juha-Pekka Nikkarila (eds.). Game Changer Structural Transformation of Cyberspace. Puolustusvoimien tutkimuslaitoksen julkaisuja 10 (Finnish Defence Research Agency Publications 10), Finnish Defence Research Agency.
Ottewell, Paul. (December 7, 2020). Defining the Cognitive Domain, OTH (Over the Horizon) Journal. Accessed on March 7, 2023.

Https://othjournal.com/2020/12/07/defining-the-cognitivedomain/.

Parcels, Sadra W.. (2018). Chinese Hacker Groups, IDC HERZLIYA, International Institute for Counter-Terrorism.

Pearson, James and Bing, Christopher. (May 10, 2022). The cyber war between Ukraine and Russia: An overview, Reuters. Https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/.

Radware. (2022). 2022 H1 Global Threat Analysis Report, Radware. Https://www.radware.com/getattachment/ba8a3263-703b-4cc7-a5d0-741dc00e9273/H1-2022-Threat-Analysis-Report_2022_Report-V2.pdf.aspx

SOCRadar. (November 16, 2021). APT Profile: Coza Bear/APT29, SOCRadar. Https://socradar.io/apt-profile-cozy-bear-apt29/.

Spring, Tom. (May 17, 2017). APT3 LINKED TO CHINESE MINISTRY OF STATE SECURITY, Archived 2017-06-15 at the Wayback Machine.

The Foreign Malign Influence Center. Https://www.dni.gov/index.php/fmic-home

Threat Intelligence and Analysis. (2016). Hacktivism A defender's playbook. Deloitte.

Whittaker, David J.. (2004). Terrorists and Terrorism in the Contemporary World, London, Routledge.

이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.