국가전략연구위원회 이슈브리핑 8호 (발간일: 2023.09.02.)

‘파이브 아이즈(Five Eyes)’와 사이버 안보[1)]

유인태 (단국대학교)

1. 부상하는 사이버 안보와 파이브 아이즈의 변화

파이브 아이즈(The Five Eyes)는 2차 세계대전 중, 미국과 영국의 정보(intelligence) (공유)협력으로 시작해서, 호주, 캐나다, 뉴질랜드를 포함하며 확장해 왔다. 더 효과적인 전쟁 계획을 세우기 위해 정보를 공유할 필요가 있었던 것이 그 기원이다. 역사가 짧지 않은, 그리고 지구상에 많지 않은 높은 수준의 첩보 협력 체계를 이룬 국제 첩보 협의체이지만, 최근 눈에 띄는 두 가지 변화가 생겼다.

첫째, 다양한 영역으로의 확장이다. 과거에는 첩보 수집이 주요 업무였다면, 최근에는 외교, 국방, 경제(산업) 등 관련 부서들과의 협업의 채널이나 회의가 자주 열리고, 파이브 아이즈 회원국 외의 국가들도 필요에 따라 초대하여 같이 회의를 갖는다. 이러한 변화를 가져온 배경과 함의에 대해서는 본문에서 상론한다.

둘째, 파이브 아이즈는 주로 눈에 띄지 않는 비밀스러운 행보로 특징지어왔지만, 사이버 안보의 중요성이 더 커짐에 따라, 공개적인 양상을 더 보이는 중요한 변화를 보이기 시작했다. 이러한 경향은 특히, 전 미 국가안보국(National Security Agency, NSA) 소속의 에드워드 스노우든(Edward Snowden)의 미 첩보기관들의 (적어도 2009년 이후부터 지속적으로 해온) 활동에 대한 2013년 6월의 폭로에서부터 시작되었다고 할 수 있다. 파이브 아이즈에

1) 이 글은 2023년 8월 30일 제3차 KACS 국가전략포럼에서 발표된 발표문을 수정보완한 것이다.

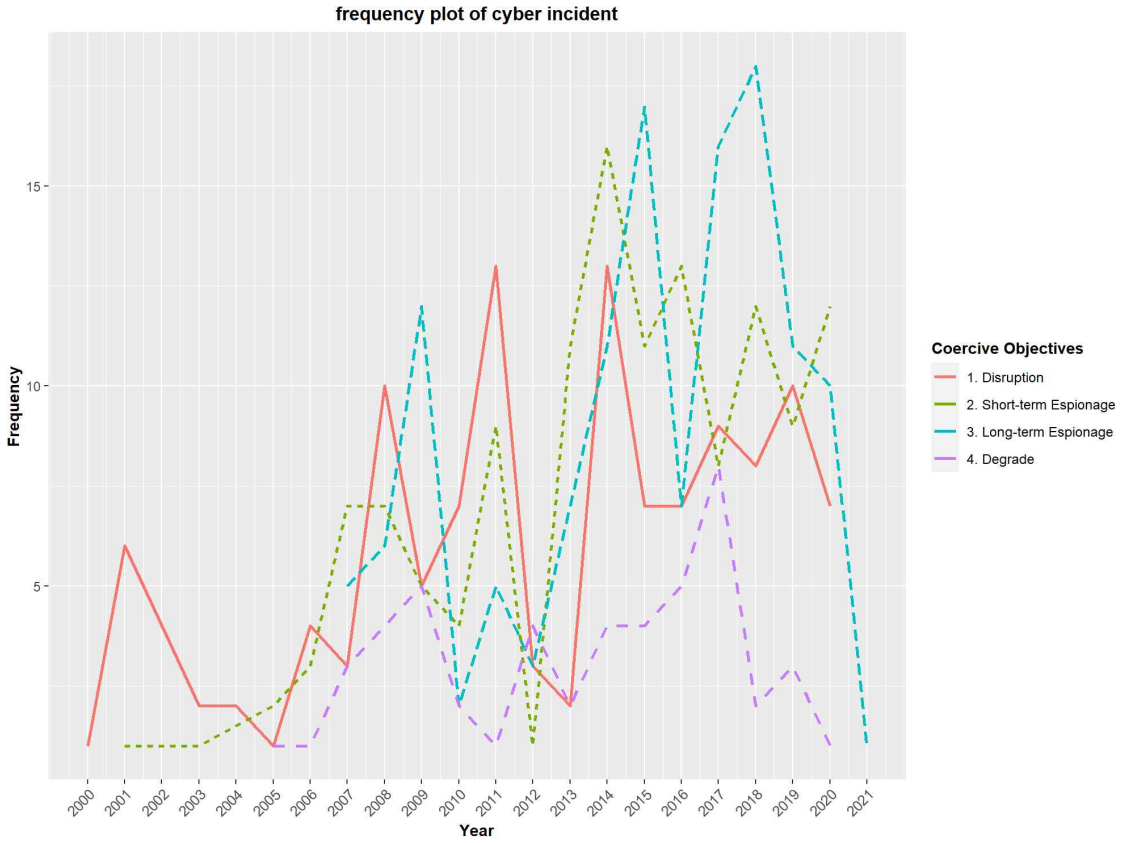
관한 공개적 기사들이 나오기 시작하는 것도 이때 즈음부터이다. 그러나 파이브 아이즈 첩보 기관들은 이러한 공개성을 오히려 국익을 실현하는 방법으로 역이용하고 있다.

첩보 기관들이 이전보다 더 공개적인 장소에 출현하며, 특정한 위협 및 활동 정보를 공개하는 것은 그만한 이익과 목적이 있기 때문이다. 우선, 파이브 아이즈의 공개적 성격이 증가한, 그리고 국가안보상으로도 더 중요한 이유는, 특정한 위협 및 (잠재적) 악의적 행위에 대처(즉, 공격하거나 억지)하기 위함이다. 예를 들어, 공개적 귀속(attribution)을 들 수 있다. 공개적 귀속을 통해 악의적 행위(자)를 규탄할 수 있다.[2] 공개적으로 규탄함으로써, 자국이 도덕적 우위 또한 점할 수 있다. 위협 정보의 타국과의 공유는, 국가들을 규합하여 집단적 행동을 취할 수 있는 기반이 되기도 한다. 그뿐 아니라, 위협에 대한 인지/탐지 역량을 보이기 위함이기도 하다. 이는 후술할 사이버 억지 역량과도 밀접한 관련이 있다.

특히 사이버상의 사건이 더욱 심각하게 인식되면서 위와 같은 변화가 뚜렷하게 되었다(그림 1. 참조). 사이버상의 공격의 빈도수가 2000년대에 비해 2010년도에 들어서면서 급증하게 되었고, 특히 그 대상으로 파이브 아이즈 주요 국가들이 포함되었다. 이러한 새롭게 부상한 사이버 공간에서의 새로운 유형의 위협에 대한 각 정부의 반응은 일국 차원에서 그리고, 인터넷의 초국적 특성상, 국제협력을 피할 수 없게 하였다.

[2] 유사한 맥락에서 사이버 공간에서의 규범 설립 노력을 볼 수 있다(Finnemore and Hollis 2016). '이름 불러 망신주기(naming and shaming)'라는 개념은 종종 거론되어 온 대표적 방법이다. 사이버상의 진화에 대해서는 Finnemore and Hollis (2020)를 보아라. 이 모든 대응 방식의 본질적 이유는, 자국의 행위/이익에 대한 정당성을 부여하고, 악의적 행위자의 행동 비용을 증가시키기 위함이다.

<그림 1> 사이버 사건의 강압적 목적 (using R-4.3.1).



출처: Maness, Ryan C., Brandon Valeriano, Kathryn Hedgecock, Benjamin M. Jensen, and Jose M. Macias. 2022. The Dyadic Cyber Incident and Campaign Dataset, version 2.0.의 데이터를 사용하여 시발자의 시발점 기반으로 저자가 그래프화.

또 다른 파이브 아이즈의 공개적 성격이 증가한 이유는, 특히 사이버 안보의 중요성이 대두되면서, 정보 소통의 중요성이 증가했기 때문이다. 사이버 사건에 대한 정보가 필요한 민간에게, 정부가 보유하고 있는 정보를 전달하는 과정이 원활해야 할 필요가 있는데, 이 과정에서 공개적인 채널을 사용하게 된다. 그리고 사이버 사건에 대한 민간의 정보도, 정부 기관들이 필요로 하기 때문에, 공개성은 더욱 증가하게 된다. 소통되는 정보의 신뢰성을 위해, 정부 기관들은 공개적 활동 등을 통해 투명성을 높이는 것이 바람직하게 된다. 정부와 민간 간의 정보공유 때문만은 아니다. 다양한 정부 내 부서 간의 협업의 필요성도 증대하였다. 과거에는 개별적으로 활동하는 경향이 컸으나, 이제는 다른 사안 영역과 연계되어 타부서들과의 협업이 불가피하게 되었다.

특히, 정보 동맹으로서의 파이브 아이즈 회원국 간에는, 정부 부처 간뿐 아니라 국경을

넘어, 전통적으로 담당하던 영역을 넘나드는 국제적 부처 간 협업이 보인다. 파이브 아이즈 첩보 기관들은, 과거의 공개적 석상에 모습을 드러내는 것을 자제하고 비밀스러운 활동으로만 점철하던 행태에서 벗어나 공개적 무대에서의 활동성을 증가시켰다. 위와 같이 파이브 아이즈의 역할과 성격은 사이버 안보의 부상과 함께 중요한 변화를 경험하였고, 기존의 첩보에 집중되었던 파이브 아이즈의 성격과 활동이 변화할 수밖에 없었던 이유는 디지털 정보통신기술의 발전과 그에 따른 사이버 안보의 중요성의 대두라는 변화가 기저에 존재한다.

그러나 이러한 파이브 아이즈에 대한 거시적 변화 외에도, 구체적 사이버 안보 활동 방향에도 변화가 생겼다. 특히, 괄목할 만한 것이 사이버 작전상의 특징이다. 이하에서는 파이브 아이즈를 주도하고 있는 미국에 초점을 맞추어 보인다.

2. 미국 사이버 작전의 발전: 변화된 파이브 아이즈 사이버 전략의 기원

미국이 다른 파이브 아이즈 국가들보다도 더, 공세적 사이버 역량의 중요성을 인식해 왔으며, 공세적 사이버 작전에 대한 전략을 구상하고, 행동으로 옮기는 것에 적극적이었다. 미국의 사이버 작전, 특히 공세적 사이버 역량에 대해 잘 표명된 것으로 미군의 2018년 '합동 간행물(US military's 2018 Joint Publication)'을 들 수 있다. 사이버 작전이란 국가의 목적을 지원하기 위해 외국의 사이버 공간을 통해서 혹은 내에서 힘(power)을 투사하는 것을 의미한다. 공세적 사이버 역량이란 일차적으로는 사이버 공간에 효과를 나타내지만, 물리적 영역에까지 파급될 수 있다. 따라서 적 체계에 물리적 손상이나 파괴를 가하는 힘(force)의 사용에 포함될 수 있다.

또한 2018년 합동 간행물은 '사이버 공간 공격(cyberspace attack)'[3]에 의해 의도한 '부인 효과(denial effects)'와 물리적 영역에서의 '부인 효과'로 이어지는 '조작(manipulation)'에 대해서도 상세한 정의를 내리고 있다. '부인 효과'는 Degrade, Disrupt, Destroy로 분류한다. 사이버 공간의 '대항책(countermeasures)' 또한 특정 조건을 만족하는 어떠한 사이버 작전상의 행동을 의미한다. 상당히 폭넓은 범위를 포함하여, 대내적 그리고 대외적 대항책이 존재하며, 사전적(preemptively)으로도 반응적(reactively)으로도 사용될 수 있다.

2018년 국가 사이버 안보 전략(National Cyber Strategy)에서도 사이버 공간에서의 공세적 접근을 담는 '선제적 방어(defend forward)'와 '지속적 관여(persistent engagement)' 개념을 내놓는다. 2018년 국방부 사이버 전략(DOD Cyber Strategy)에서도 선제적 방어(defend forward) 개념을 반복적으로 제시하며, 사이버사령부가 핵심적인 이 개념의 수행에 핵심적 역할을 맡게 되었다. 선제적 방어란, 사이버사령부의 '지속적 관여(persistent

3) 미군이 '사이버 공간 공격(cyberspace attack)'이라는 용어의 기원에 대해서는 알 수 없다. 다만, 보통 국제법 학자들이 '사이버 공격(cyber attack)'이라는 말을 엄밀하게 사용할 것을 주장하며, 해당 용어가 국제법상의 주권을 침해하는 사이버상의 공격을 의미하기 위해 사용될 것을 규정하기 때문에(Schmitt and Vihul. 2016), 이와 구별되는 용어로 사용하는 것으로 생각된다.

engagement)'의 개념에 근거하여, 빈번히 일어나는 무력 갈등(armed conflict) 이하에서 행해지는 행동들에 대해, 근본적인 차원에서 차단하고자 하는 것을 의미한다. 즉, 사이버 작전을 통해 적의 약점을 파고들어 비용을 부과함으로써, 그들의 자원을 방어로 전환하는 것을 강제하고 하는 것이다.[4] 이러한 사이버 작전에는 공세적 사이버 역량을 활용할 수 있으며, 사이버 억지의 한 수단으로 동원될 수 있다.

1년 전인 2017년 미 국회는, 국방수권법(National Defence Authorization Act, NDAA)를 통해 미 국방부의 사이버 사령부(U.S. Cyber Command, CYBERCOM)를 폴 나카소네(Paul Nakasone) 장관의 지휘하에서 활동하는 하나의 통합된 전투 사령부로 승격시켰다. CYBERCOM은 사이버 작전의 이행에 있어 주요 기관이며 2010년도에 최초로 전략 사령부(U.S. Strategic Command) 예하에 설치되었었다. 미 육·해·공·해병·우주군은 CYBERCOM에 배치될 인력을 훈련시키고 관리하며 배치할 책임을 지며, 이들은 통합되어 '사이버 임무군(Cyber Mission Force, CMF)'이라 불린다. CMF는 CYBERCOM이 내리는 임무를 사이버 작전을 통해 수행한다. CMF는 공세적 사이버 공간 작전, 방어적 사이버 공간 작전, 그리고 국방부 정보네트워크 작전의 세 유형의 임무를 담당한다.[5]

이듬해인 2019년도의 국방수권법(National Defence Authorization Act, NDAA)에서는, 이후의 NDAA에서 보이지 않을 정도의, 사이버 작전에 대한 더욱 구체적인 내용이 담기는데, 미국의 사이버 작전의 핵심을 잘 표현하고 있다. 즉, 미국은 사이버 공간, 사이버 안보, 사이버 전과 관련해서, 미국이 모든 국력의 도구를 사용할 것을 주문하고 있으며, 이에는 외국 세력의 모든 사이버 공격 및 활동을 억지하기 위한, 공격적 사이버 역량의 사용도 포함된다고 적고 있다(House Armed Services Committee 2019).[6]

---

4) "Persistent engagement ... [t]his approach prevents adversary nations and non-state actors from launching disruptive and destructive cyberattacks in the first place." (https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/). 그에 반해 파트너 국가들과의 'hunt forward' 개념은 방어적 사이버 작전에 국한되는 개념이다.

5) 미국의 사이버 사건과 사이버 안보에 대한 책임은 크게 국내와 대외 책임으로 나뉘어진다. 국토안보부(DHS)는 국내 주요 인프라에 대한 보호를 맡고 있다. DHS산하의 사이버보안인프라보안국(Cybersecurity and Infrastructure Security Agency, CISA)은 2018년의 법을 통해 동년 11월 16일에 통해 만들어졌다. 전신은 '국가 보호 프로그램 관리국(National Protection and Programs Directorate, NPPD)'이며, DHS의 사이버안보 관련 모든 일을 관리했었다. CISA는 두 개의 주요 센터가 있다. 하나는 '국가사이버보안 및 통신통합센터(National Cybersecurity and Communications Integration Center, NCCIC))'는 사이버안보와 관련하여 공공 및 민간 행위자들을 조율하는 역할을 한다. 또 하나는 국가위기관린센터(National Risk Management Center, NRMC)로, 주요 인프라에 대한 위험 등을 식별하고 대처한다. 국내 사이버 안보 책임을 담당하는 또 하나의 기관은 법무부(DOJ)이며, 연방수사국(Federal Bureau of Investigation, FBI)을 통해 위협 대응과 법집행을 수행한다.

6) "... the United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter .... all cyber attacks or other malicious cyber activities of foreign powers ..." (https://www.congress.gov/bill/115th-congress/house-bill/5515/text)

2019년도 NDAA는 구체적으로 적국을 상정하며, 이들에 대해 공세적 사이버 작전을 수행할 수 있는 권위를 부여했다. 러시아, 중국, 북한 그리고 이란이 만일 민주주의적 과정을 포함한 정부나 민간 대상으로 공격을 가할 경우 적절하고 비례하는 행동, 예를 들어, "방해, 굴복, 그리고 억지(disrupt, defeat and deter)" 할 수 있는 행동을 취할 수 있음을 재가하고 있다(House Armed Services Committee 2019, 497).

따라서 2019년도 NDAA의 기술을 미국의 공세적 사이버 작전에 대한 의회 차원의 공식적 인가(認可)라고 볼 수 있다. 2018년 8월까지만 해도 미 대통령 정책 지시(US Presidential Policy Directive 20, PPD-20)에 따라 언제, 어떻게, 누구에 의해 공세적 사이버 작전이 허가될 수 있는가에 대해 엄격한 제한이 걸려 있었기 때문이다. 2018년 여름 트럼프 대통령에 의해 이러한 요구사항이 개정되고 느슨해졌다고 보도되었었다.[7] 2018년 8월의 국가안보대통령제안서(National Security Presidential Memorandum 13)은 미군이 무력 사용에 못 미치는 행위에 더욱 쉽게 대처할 수 있도록, 그리고 사망, 파괴 그리고 심각한 경제적 충격을 일으킬 수 있는 수위의 행위를 더욱 용이하게 했다.

비록 미국은 일국 차원에서도 사이버 작전을 계속 수행할 의지와 역량을 가지고 있지만, 동맹국들과 파트너 국가들과 같이 하고자 하는 의향을 계속 내비쳐 왔으며, 또 그러할 때 더 효과적일 수 있다고 표명해왔다. 사이버 억지의 한 차원이었던 미국의 사이버 작전은 국제협력의 맥락에서 공동 귀속과 집단 억지를 위한 국제 전략, 정책 그리고 행동으로 이어진다.

합동 공개적 귀속의 예로 최근에는 파이브 아이즈 회원국들의 사이버 안보 관련 주무기관들이 합동으로, 악의적 사이버 행위자들에 의해 노출된 취약점들을 합동보안권고문을 통해 알리고 있다.[8] 공동으로 취약성을 투명하게 공유한다는 것과 대처 방식(혹은 모범 사례)들도 공유되고 있기 때문에, 사이버상의 안정성을 더 높이는 데 기여하고 있다. 그뿐 아니라, 공동의 적을 지목하고 그들의 악의적 행동 방식(혹은 전술, 기법, 절차(tactics, techniques, procedures, TTPs))을 공개하여 한편으론 공동으로 대처 방식을 공유하면서, 다른 한편으론 '이름 불러 망신 주기'를 펼치고 있다.

예를 들어 중국과 러시아에 대한 활동에 대한 파이브 아이즈의 대응을 볼 수 있다. 중국이 후원하는 '볼트 타이푼(Volt Typhoon)'으로 알려진 사이버 행위자가 미국의 주요 인프라(critical infrastructure) 부문에 영향을 미쳤으며, 따라서 다른 부문이나 다른 국가에게 같

7) Ellen Nakashima, "White House authorizes 'offensive cyber operations' to deter foreign adversaries," *The Washington Post* (September 20, 2018). https://www.washingtonpost.com/world/national-security/trump-authorizes-offensive-cyber-operations-to-deter-foreign-adversaries-bolton-says/2018/09/20/b5880578-bd0b-11e8-b7d2-0773aa1e33da_story.html

8) Cybersecurity & Infrastructure Security Agency, "2022 Top Routinely Exploited Vulnerabilities," (August 3, 2023). https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a#:~:text=for%20Critical%20Function-,MITIGATIONS,-Vendors%20and%20Developers

은 기법(techniques)을 활용할 수 있다고 공표했다.[9] 또 다른 예로, 글로벌 네트워크에 영향을 미치는 러시아가 만든 스네이크(Snake) 멀웨어를 파이브 아이즈가 공동으로 차단한 사건이다.[10] 러시아 Federal Security Service(FSB)의 Center 16(혹은 미 사법부에 의하면 'Turla')이 만든 것으로 비난하고 있으며, 메듀사(Medusa)로 불리우는 합동 작전에 의해 저지되었다. 스네이크 멀웨어는 나토 회원국들을 포함해 적어도 50개국의 컴퓨터 시스템에서 민감한 문서를 훔쳐서 비밀 네트워크를 통해 유출해 왔다. 메듀사 공동 작전의 성공에는, 민관 협력의 중요성과 위협 첩보 정보의 공유가 국제적인 사이버 적대 그룹을 물리치는 데 중요했다고 거론된다.

향후 파이브 아이즈는 협의의 사안 범위가 더욱 넓어지고, 협의에 참가하는 대상도 증가할 것으로 예상된다. 서두에 첩보 동맹이 정부 내외의 다른 유관 부처와의 협력 채널이 증가했으며, 이러한 경향성의 증가는 사이버 안보의 중요성이 부상하면서라고 언급하였다. 사이버 작전의 강조에 의해 대내 및 국제적 첩보, 국방, 사법, 경찰 등의 협력이 중요해졌지만, 미국의 (기술, 원자재, 경제, 연구의) 공급망 안보를 강조하는 경향을 따라 앞으로 국내외 상무부, 무역대표부, 재무부와의 협력도 중요해질 것이다.

첩보 협의체로 시작한 파이브 아이즈는, 사이버 공간의 부상이라는 역사적 시기에, 억지, 작전, 귀속 그리고 공급망 보호 등으로 협업의 대상과 활동의 범위를 넓히는 방향으로 진화하고 있다.

9) Cybersecurity & Infrastructure Security Agency, "People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection," (May 24, 2023). https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

10) Howard Solomon, "Five Eyes countries disable Russia's Snake malware network," *ITWorld Canada* (May 9, 2023). https://www.itworldcanada.com/article/five-eyes-countries-disable-russias-snake-malware-network/538486