법학박사 학위논문

사이버공격의 국제법적 규율을 위한 적극적 방어개념의 도입

2018년 2월

서울대학교 대학원

법학과 국제법 전공

백상미

국문초록

본 논문은 초국경적 성격을 가진 사이버공격이 국가안보에 위협이 되고 있는 현실을 진단하고, 국제법적으로 이를 효과적으로 규율하기 위한 방안이 무엇인지에 대해 연구하였다. 일련의 사건을 통해 국가들이 사이버공격의 위험성을 인지한 이래 사이버공격의 국제법적 규율을 위한 국가들의 논의는 현재까지 활발하게 진행되고 있다. 이는 사이버공간에서 이루어지는 사이버공격이 물리적 공간에서의 활동과는 구별되는 특징을 가지고 있기 때문일 것이다. 그러나 현재 국가들의 논의는 사이버공간의 특성을 반영하기 보다는 사이버공간의 규율을 위해 새로운 체제 마련이 필요한지 현행 국제법을 그대로 적용할 수 있는지 여부에 집중되어 있다.

사이버공격에 대한 국제법적 규율을 위해 반드시 고려해야할 특성으로는 사이버공간의 일반적 특성인 익명성 및 공간에 대한 초월성 외에도 공격자와 공격거점, 공격목표 간의 독특한 관계를 들 수 있다. 사이버공격은 대부분 공격자가 목표대상을 직접 공격하지 않고, 사전에 마련된 공격거점을 거쳐 공격을 실행하는 특성을 가지고 있다. 공격자는 이러한 공격거점을 여러 개 마련할 수 있기 때문에 공격 또한 여러 단계를 거쳐 진행될 수 있다. 따라서 사이버공격의 경우 실제 공격자를 밝히는 귀속의 입증이 더욱 어렵고, 입증을 하는 데에도 적지 않은 시간이 소요된다. 때문에 공격을 즉각적으로 억지하기 위해서는 귀속의 입증보다는 공격거점에 대한 조치가 우선적으로 필요하다.

현재 발생하고 있는 공격의 흐름을 차단시키거나 공격의 거점이 되는 서버 또는 시스템을 직접 셧다운시키는 등의 사이버공간상의 조치를 의미하는 적극적 방어는 바로 이러한 사이버공격의 특성을 반영하여 마련된 대응전략이다. 이는 공격을 실시간으로 억지하기 위해 취하는 조치로 귀속의 증명보다는 위협을 사전에 탐지하고 공격 수단을 처리하는 데 그 초점이 맞추어져 있다.

문제는 적극적 방어조치 시 그 대상이 되는 공격거점이 실제 공격자와

는 관련이 없는 곳에 위치할 가능성이 높다는 점이다. 즉, 공격과는 진정한 관련성이 없는 제3국의 기반시설이나 민간 시스템이 공격거점인 경우가 대부분이기 때문에 조치의 강도 및 결과에 따라 국제법위반의 문제가 발생할 수 있는 것이다. 특히 적극적 방어는 사전적 조치의 개념을 포함하고 있다. 따라서 위협이 목표시스템 내부에 접근하지 않은 외부 네트워크에서 탐지된 단계에서도 타국에 위치한 네트워크에까지 추적해 들어가 찾아낸 봇넷이나 C&C서버를 제어하거나 무력화시키는 조치를 취하게 되는 것이다. 이는 시기상 국제법이 허용하는 것보다 훨씬 앞선 시점에서 이루어지는 조치이며, 조치 그 자체로 대상 시스템에 손상을 초래할 수 있다는 점에서 국제법위반의 문제가 발생할 수 있다.

적극적 방어조치가 사이버공격의 억지를 위한 현실적 필요성에도 불구하고 엄격한 기준을 바탕으로 국제법에 의해 규율되어야 하는 이유가 여기에 있다. 그러나 적극적 방어개념은 국가들이 국내적으로 마련하고 있는 안보전략차원에서 언급되고 있을 뿐, 국제사회 차원에서는 논의된 바가 없다. 사이버공격과 관련한 국제법 연구에서도 국가들이 마련하고 있는 적극적 방어 전략이 국제법 체제 안에서 어떤 문제점을 가지는 지 검토된 바가 없기는 마찬가지다.

이에 본 논문에서는 국제법위반에 해당하는 사이버공격이 발생하기 전에 또는 공격자가 명확하게 밝혀지지 않은 상황에서 공격거점에 우선적으로 조치를 취하는 적극적 방어개념이 현행 국제법체제 내에서 허용될 수 있는지에 대해서 살펴보았다. 이를 위해서 적극적 방어조치 시 그 시기 및 대상과 관련하여 발생할 수 있는 위법성의 문제가 자위권, 대응조치, 긴급피난과 같은 국제법상의 위법성 조각사유에 의해 정당화될 수 있는지에 중점을 두고 분석하였다. 그 결과 국제법상의 위법성 조각사유를 확대적용하여도 적극적 방어조치를 완전히 포섭할 수 없다는 점을 확인하였고, 이에 다자조약체제를 통해 적극적 방어개념을 도입하는 것이 필요하다는 결론에 도달하였다. 아울러 사후 책임자 처벌 및 제재가 가능할 때, 사이버공격에 대한 완전한 규율이 이루어질 수 있다고 보고, 귀속입증을 위한 조

사협조의무의 확립을 다자조약체제에 포함시킬 것을 제안하였다.

주요어 : 귀속, 공격거점, 사이버공격, 사전적 조치, 적극적 방어
학 번 : 2014-30462

목 차

표 목 차

그 림 목 차

주요사건 목록

2007년 에스토니아 사이버공격	에스토니아가 수도 탈린에 있던 구소련 참전 기념 청동동상 이전 정책을 발표한 후 러시아계 주민 및 러시아로부터의 거센 반발이 있었고, 그러한 반발의 일환으로 2007년 4월 국가 주요 기관 홈페이지와 전산망이 분산서비스 거부(DDoS) 공격을 받아 국가 전체에 걸쳐 전산망이 마비된 사건.
2008년 터키 BTC 송유관 폭발	2008년 터키 동부지역에서 카스피해부터 지중해에 이르는 구간을 관통하는 길이 1,760km의 송유관이 폭발한 바 있는데, 6년 후 악성코드 삽입을 통한 사이버공격이 폭발의 원인이었음이 밝혀진 사건.
2008년 그루지야 사이버공격	2008년 러시아와 그루지야 간 전쟁 당시 러시아의 물리적 공격 이전에 그루지야 대통령의 홈페이지 및 의회·국방부·외교부 등의 사이트가 사이버공격을 받아 전산망이 무력화된 사건. 사이버전력이 무력과 결합한 케이스로 주목을 받은 사건.
2010년 스턱스넷 사건	2010년 이란의 나탄즈 핵시설이 스턱스넷이라는 악성코드 공격에 의해 1,000개 이상의 원심분리기가 파괴된 사건. 사이버공격이 물리적 파괴를 초래할 수 있음을 보여주면서 사이버공격에 대한 관심을 촉발시킨 사건.
2014년 우크라이나 대선개입 사건	2014년 우크라이나 대선 4일 전에 우크라이나 중앙선관위 컴퓨터에 대한 사이버공격으로 선거결과가 방송되기 40분 전 악성바이러스가 제거되기 전까지 투표검수 프로그램이 운영 불가 상태가 된 사건.
2014년 소니해킹 사건	미국의 소니 영화사가 북한의 김정은 위원장을 암살을 내용으로 하는 영화 '더 인터뷰' 개봉을 앞두고, 해커집단에 의해 해킹공격을 받은 사건.
2016년 미국 민주당 전국위원회 이메일 해킹사건	2016년 폭로전문 사이트 위키리크스가 민주당의 대선후보인 Hillary Clinton의 캠프 선대본부장 John Podesta의 이메일 수천 건을 공개하면서 촉발되었으며, 위키리크스가 폭로한 이메일 해킹의 배후에 러시아가 있다는 미 당국의 발표에 따라 러시아의 미 대선개

	입 논란이 문제가 된 사건.
2017년 워너크라이 랜섬웨어 공격	WannaCry는 사용자의 파일을 암호화 한 뒤, 이를 푸는 대가로 금전을 요구하는 랜섬웨어로 미 국가안보국이 해킹당한 툴이 사용된 것으로 알려짐. 2017년 5월 12일에 유포되기 시작해 전 세계 100여 개국에 확산되어 피해를 입힌 사이버공격 사건.

용어해설표

용어	내용
공격거점	공격거점은 공격자와는 구별되는 의미로 사이버공격을감행하려는 해커가 자신의 위치를 드러내지 않기 위해 불특정다수의 컴퓨터를 대상으로 악성코드를 유포하여 제어 및 명령 수행이 가능하도록 만든 수단 또는 공격의 매개체를 의미한다. 오늘날 사이버공격을 실행하고자 하는 공격자 대부분은 특정 시스템에 대한 공격을 수행하기 전에 먼저 봇넷과 C&C서버와 같은 공격의 수단을 마련해 놓고 이들 수단에 명령을 내려 공격을 실행한다.
공격자(Attacker)	컴퓨터 기술을 이용해 악성바이러스를 유포하고, 특정 시스템에 침투하여 기밀정보를 탈취하거나 시스템의 운영을 마비시키는 등의 사이버공격을 계획, 준비, 실행하는 사람 또는 단체를 의미하며, 이를 실행하기 위해 사용하는 기기·기술과는 구별되는 개념이다.
루트킷(Rootkit)	루트킷은 해커가 설치한 악성코드가 백신이나 PC 사용자에게 발각되지 않도록 숨겨주는 역할을 한다. 대부분의 루트킷은 일반 프로그램이 동작하는 계층보다 더 하위 계층, 즉 커널이라는 운영체제 핵심 부분에 숨어서 동작하여 탐지가 어렵다.
랜섬웨어 (ransomware)	컴퓨터 사용자의 파일들을 암호화하여 금전을 요구하는 악성코드. 인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 스프레드시트, 그림 파일 등을 제멋대로 암호화해 열지 못하도록 만들고 이메일 주소로 접촉해 돈을 보내주면 해독용 열쇠 프로그램을 전송해 준다며 금품을 요구하기도 한다
멀웨어 (malware)	악의적인 목적을 위해 작성된 실행 가능한 악성 코드(Malicious Code) 또는 악성 프로그램(Malicious Program).
보안패치 (Security Patch)	운영 체계(OS)나 응용 프로그램에 내재된 보안 취약점을 보완하는 소프트웨어. 보안 패치를 할 경우 취약점

	을 악용하는 악성 코드 감염을 방지하고, 각종 개인용 컴퓨터(PC) 오류의 원인을 제거해 준다.
봇(bot)	로봇의 줄인 말로써 데이터를 찾아주는 소프트웨어 도구. 인터넷 웹 사이트를 방문하고 요청한 정보를 검색, 저장, 관리하는 에이전트의 역할을 한다. 보안이 취약한 컴퓨터를 스스로 찾아 침입해 보이지 않는 곳에서 조용히 작동하면서 컴퓨터 사용자도 모르게 시스템에게 명령을 내릴 수 있는 원거리 해킹 툴이다.
봇넷(botnet)	악성 프로그램에 감염되어 나중에 악의적인 의도로 사용될 수 있는 다수의 컴퓨터들이 네트워크로 연결된 형태. 봇넷은 해킹 또는 악성 프로그램에 감염된 컴퓨터를 네트워크로 연결하고, 해커는 봇넷에 연결된 컴퓨터를 원격 조종해 개인 정보 유출, 스팸 메일 발송, 다른 시스템에 대한 공격 등 악성 행위를 한다.
백도어(backdoor)	트랩도어(trap door)라고도 한다. 시스템 보안이 제거된 비밀 통로로, 서비스 기술자나 유지 보수 프로그램 작성자의 액세스 편의를 위해 시스템 설계자가 고의로 만들어 놓은 시스템의 보안 구멍. 대규모의 응용 프로그램이나 운영 체계(OS) 개발에서는 코드 도중에 백도어라는 중단 부분을 설정하여 쉽게 보수할 수 있게 한다. 최종 단계에서 삭제되어야 하는 백도어가 남아 있으면 컴퓨터 범죄에 악용되기도 한다.
수동적 방어 (passive defense)	컴퓨터 보안이라고 흔히 부르는 수동적 방어는 방어벽이나 안티바이러스 소프트웨어 등을 설치하는 것을 의미한다.
유포지	악성코드를 유포하는 장소를 의미하는 것으로 C&C서버나 봇넷을 그 예로 들 수 있다.
에어갭	에어갭 네트워크는 외부의 인터넷과는 완전히 분리된 네트워크를 구축하고 운영되는 방식을 의미한다.
적극적 방어	현재 발생하고 있는 위협이나 공격의 흐름을 탐지하여 공격의 경로와 흐름을 파악하고, 이를 차단시키거나 공격명령 서버(C&C 서버) 혹은 봇넷 을 직접 셧다운시키

	는 등의 사이버역량을 사용하여 공격에 실시간으로 대응하는 사이버공간 상의 조치를 말한다.
제로데이공격	보안 취약점이 발견되었을 때 그 문제의 존재 자체가 널리 공표되기도 전에 해당 취약점을 악용하여 이루어지는 보안 공격. 공격의 신속성을 의미하는 것으로, 일반적으로 컴퓨터에서 취약점이 발견되면 제작자나 개발자가 취약점을 보완하는 패치를 배포하고 사용자가 이를 내려받아 대처하는 것이 관례이나, 제로 데이 공격은 대응책이 공표되기도 전에 공격이 이루어 지기 때문에 대처 방법이 없다.
취약점 (Vulnerability)	기능명세, 설계 또는 구현단계의 오류나 시동, 설치 또는 운용상의 문제점으로 인하여 정보 시스템이나 네트워크가 내포하고 있는 취약한 부분으로 보안의 위협 대상이 된다.
클라우드 컴퓨팅 (Cloud Computing)	인터넷 기술을 활용하여 가상화된 정보 기술(IT) 자원을 서비스로 제공하는 컴퓨팅. 사용자는 IT 자원(소프트웨어, 스토리지, 서버, 네트워크 등)을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 실시간 확장성을 지원받으며, 사용한 만큼 비용을 지불하는 컴퓨팅을 말한다.
트래픽 (traffic)	전신, 전화 등의 통신 시설에서 통신의 흐름을 지칭하는 말이다.
프로토콜 (protocol)	데이터가 전송되는 방식 (특히 네트워크를 통해)을 설명하는 공식화된 규칙의 집합. 저수준 프로토콜은 준수해야 할 전자적, 물리적 표준, 비트 및 바이트 순서, 전송과 오류 검출 및 비트 스트림의 수정을 말한다.
패킷(Packet)	데이터 전송에서사용되는 데이터의 묶음을 말한다. 패킷 전송은 두 지점 사이에 데이터를 연속적으로 전송하지 않고, 전송할 데이터를 적당한 크기로 나누어 패킷의 형태로 구성한 다음 패킷들을 하나씩 보내는 방법을 쓴다. 각각의 패킷은 일정한 크기의 데이터뿐만 아니라 데이터 수신처, 주소 또는 제어 부호 등의 제어 정보까지 담고 있다. 보통 한 패킷은 1,024비트 데이터를 담을 수 있다.

APT공격	특정 공격 대상을 겨냥해 지능적, 지속적으로 은밀하게 공격을 행함으로써 기밀 정보 및 중요 정보를 유출하고 내부 시스템에 피해를 유발하는 해킹 기법으로, 해킹 공격 방법에 제약을 가지지 않는다는 특징이 있다.
C&C서버	좀비 PC를 조정하는 서버를 말한다. 해커는 다른 사람의 PC를 악성 코드로 감염한 뒤 C&C 서버를 통해 각종 명령을 내린다.
DDoS공격	DDoS 공격은 분산 배치된 여러 단말을 통해 특정 서버에 많은 양의 접속 시도를 동시에 수행하여 시스템이 정상적인 서비스를 제공할 수 없도록 하는 공격 방식이다.

제1장 서론

제1절 문제제기

인터넷이 우리 삶에서 차지하는 비중이 커지면서 사이버공간은 더 이상 '가상'이 아닌 실질적 영향력을 가진 영역이 되었다. 사이버활동의 물리적 파괴력을 보여준 2008년 터키 BTC 송유관 폭발 사건[1] 및 2010년 스턱스넷 사건[2]부터 정치적 파급력을 보여준 2014년 우크라이나 대선 개입사건[3]과 2016년 미국 민주당 전국위원회 이메일 해킹 사건[4]까지 사이버공

---

1) 2008년 터키 동부지역에서 카스피해부터 지중해에 이르는 구간을 관통하는 길이 1,760km의 송유관이 폭발한 사건이 발생하였다. 당시 사건의 원인으로는 기기의 오작동 또는 테러조직의 소행이 거론되었다. 그러나 오랜 시간의 조사 끝에 6년이 지난 2014년 당시 사건이 악성코드 삽입을 통한 사이버공격에 의한 것이었음이 밝혀지게 되었다. 공격의 배후로는 러시아가 지목되었다. Bloomberg, Dec. 10, 2014, "Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar", <https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar> (2017.10.31.최종방문).

2) 2010년 이란의 나탄즈 핵시설에 스턱스넷이라는 악성코드 공격에 의해 1,000개 이상의 원심분리기가 파괴된 사건이다. BTC 송유관폭발 사건이 사이버공격에 의한 것임이 밝혀지기 전까지 스턱스넷 사건이 물리적 파괴를 가져온 최초의 사이버공격 사건으로 알려져 있었다. 해당 사건의 공격 배후는 미국과 이스라엘로 기정 사실화되어 있다. 자세한 설명은 David Albright, Paul Brannan, and Christina Walrond, "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?", Institute for Science and International Security Report, Dec. 22, 2010, <http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/> (2018.1.21.최종방문) 참조.

3) 2014년 우크라이나 대선 4일 전에 우크라이나 중앙선관위 컴퓨터에 대한 사이버공격으로 투표 검수 프로그램이 운영 불가 상태가 되었고, 선거 결과가 방송되기 40분 전에 악성바이러스가 제거 되었다. 악성코드를 통해 실제 당선자가 아닌 극우정당 후보가 당선된 것으로 방송되도록 조작되어 있었다.

격의 실제적 영향력은 다양한 양상으로 증명되고 있다. 초국가적 성격의 악의적 사이버활동이 국가안보에 위협을 줄 수 있다는 점에서 이에 대한 국제법 차원의 규제가 필요하다는데 대해서는 국가들 모두가 동의하고 있다. 이에 국가들은 UN사이버안보정보전문가그룹[5], 상하이협력기구[6], 유럽안보협력기구[7] 등 다양한 국제포럼에서 사이버공격에 대한 규율 문제를 논의해왔다.

이러한 논의는 현행 국제법이 사이버공격을 규율하는 데 있어 그대로 적용될 수 있는지 여부에 초점이 맞춰져 있다. 즉, 사이버공격이 일반국제법상의 원칙인 무력사용금지원칙, 국내문제불간섭원칙 등의 위반에 해당할 수 있는지에 관한 논의가 중심이 되고 있는 것이다. 이는 자연스럽게 어떠한 강도의 사이버공격을 무력사용으로 볼 수 있는지, 자위권차원의 대응이 가능한 무력공격으로 볼 수 있는지에 대한 논의로 이어진다. 2017년 UNGGE에서도 사이버공격 규율에 적용 가능한 국제법으로 자위권, 국가책임, 국제인도법과 같은 원칙을 명시하는 데 대한 논의 끝에 적용기준에 대

The Christian Science Monitor, Jun. 17, 2014, “Ukraine election narrowly avoided 'wanton destruction' from hackers”, <http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video> (2017.10.31.최종방문).

4) 러시아가 미국 민주당 전국위원회의 이메일을 해킹하여 공개함으로써 미국 대선에 개입하려 한다는 의혹이 불거진 사건으로 미국연방수사국(FBI)이 공식적으로 수사에 착수하기도 하였다. The New York Times, Sept. 14, 2016, “Sowing Doubt Is Seen as Prime Danger in Hacking Voting System”, <http://www.nytimes.com/2016/09/15/us/politics/sowing-doubt-is-seen-as-prime-danger-in-hacking-voting-system.html> (2017.10.31.최종방문).

5) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 이하 UNGGE.

6) Shanghai Cooperation Organization. 이하 SCO.

7) Organization for Security and Cooperation in Europe. 이하 OSCE.

한 자의적 해석의 가능성을 이유로 국가 간 합의 도출에 실패한 바 있다.[8)]

그러나 진짜 문제는 국제법원칙이 사이버공격에 그대로 적용될 수 있는지, 그러한 국제법 원칙은 무엇인지를 결정하는 것이 아니라 이러한 논의가 사이버공격을 규율하는데 실익이 있는지 일 것이다. 논의의 실익 여부를 판단하기 위해서는 현행 국제법 원칙의 적용이 사이버공격을 억지하는데 실질적인 대응책을 제시하고 있는지를 검토해야 한다.

사이버공격의 가장 큰 특성은 공격의 징후를 포착하기가 어렵고, 위협징후를 포착하더라도 이러한 위협을 발생시킨 행위자, 즉 공격자를 찾기가 어려우며, 물리적 공간에 비해 공격과 피해발생의 시간차가 거의 존재하지 않는다는 점이다.[9)] 따라서 사이버공격을 효과적으로 규율하기 위해서는 이러한 특성을 반영하여 공격의 징후를 포착하는 문제, 공격자를 밝혀내지 못할 경우의 대응문제가 중점적인 논의대상이 되어야 한다. 그런데 국제법 체제는 주로 국제의무 위반이 발생한 경우에 이에 대해 어떻게 대응할 지에 초점이 맞춰져 있고, 그러한 대응도 의무위반의 주체가 밝혀진 경우에 가능하다. 특히 무력사용금지의무, 국내문제불간섭의무, 영토주권존중의무와 같은 일반국제법상 의무의 위반주체는 국가이기 때문에 이들 의무의 위반에 해당하는 사이버공격행위가 국가로 귀속되어야 이에 따른 국제법상의 대응을 할 수 있는 측면이 있다.

이는 물리적 공간의 특성과 사이버공간의 특성이 가장 대비되는 지점이다. 사이버공간은 물리적 공간에서와는 달리 다양한 기술을 사용하여 행위

---

8) The Diplomat, Jul. 31, 2017, “UN GGE on Cybersecurity: The End of an Era?”, <https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/> (2017.10.30.최종방문)

9) Eric Talbot Jensen, “Cyber Deterrence”, Emory International Law Review, Vol. 26 (2012), p. 800; Kim Taipale, “Cyber Deterrence”, in Pauline C. Reich & Eduardo Gelbstein (eds.), *Law, Policy and Technology: Cyber Terrorism, Information Warfare, Digital and Internet Immobilization* (IGI Global, 2010), pp. 3-4.

의 흔적을 지울 수 있고, 추적기술을 통해 공격에 사용된 네트워크를 찾는다 해도 그것이 곧 공격 행위자를 찾았다는 것을 의미하지는 않는다.[10] 즉, 사이버공격은 물리적 공간에서의 공격과는 달리 공격 행위자가 직접 무기를 소지하지 않고, 원거리에서 자신이 획득한 악성 파일 유포지-C&C 서버[11]나 봇넷(botnet)[12]-를 매개로 공격을 수행한다는 특징이 있다. 따라서 공격의 거점[13]으로 사용하기 위한 C&C 서버나 봇넷도 이미 공격자가 해킹을 통해 마련한 수단으로서 사이버공격의 또 다른 피해자에 불과할 가능성이 높다.

이는 공격자와 공격대상과의 물리적 거리가 중요하지 않다는 것을 의미할 뿐 아니라 공격자와 공격자가 공격의 거점으로 사용하는 유포지와의

---

10) Lipson, H.F., "Tracking and Tracing Cyber-Attacks: Technical Challenges and Golbal Policy Issues", CERT Coordination Center (2002), pp. 13-14; Scott J. Shackelford, "State Responsibility for Cyber Attacks: Competing Statndards for A Growing Problem", in Czosseck C and Podins K(eds.), *Conference on Cyber Conflict Proceedings* (CCD COE Publications, 2010), p. 200.

11) C&C 서버(Command & Control Server)는 좀비 PC를 조정하는 서버를 말한다. 해커는 다른 사람의 PC를 악성 코드로 감염한 뒤 C&C 서버를 통해 각종 명령을 내린다. 한국정보통신기술협회 정보통신용어사전, <http://word.tta.or.kr/dictionary/dictionaryView.do?word_seq=038958-1> (2018.1.4.최종방문).

12) 봇넷은 악성 프로그램에 감염되어 나중에 악의적인 의도로 사용될 수 있는 다수의 컴퓨터들이 네트워크로 연결된 형태를 일컫는다. 봇넷은 해킹 또는 악성 프로그램에 감염된 컴퓨터를 네트워크로 연결하고, 해커는 봇넷에 연결된 컴퓨터를 원격 조종해 개인 정보 유출, 스팸 메일 발송, 다른 시스템에 대한 공격 등 악성 행위를 한다. 한국정보통신기술협회 정보통신용어사전, <http://word.tta.or.kr/dictionary/dictionaryView.do?word_seq=037363-1> (2018.1.4.최종방문).

13) 공격거점은 공격자와는 구별되는 의미로 사이버공격을 감행하려는 해커가 자신의 위치를 드러내지 않기 위해 불특정다수의 컴퓨터를 대상으로 악성코드를 유포하여 제어 및 명령 수행이 가능하도록 만든 수단 또는 공격의 매개체를 의미한다. 오늘날 사이버공격을 실행하고자 하는 공격자 대부분은 특정 시스템에 대한 공격을 수행하기 전에 먼저 봇넷과 C&C서버와 같은 공격의 수단을 마련해 놓고 이들 수단에 명령을 내려 공격을 실행한다.

거리에도 한계가 없음을 의미한다. 공격자와 공격이 실제로 실행된다고 볼 수 있는 거점이 서로 다른 곳에 위치하고 있다는 사실과 공격자가 사용하는 공격의 거점이 공격과 관련된 어떠한 의도도 가지고 있지 않고, 자신이 공격에 이용되고 있다는 사실조차 알지 못하고 있다는 점은 사이버공격에 대한 대응이 물리적 공간에서 이루어진 공격과는 달라야 한다는 것을 시사한다. 즉, 탐지된 사이버 상의 악의적 흐름을 저지하기 위해서는 우선 위협을 유포하고 있는 공격거점에 대한 조치가 필요하고, 공격거점을 마련하고 명령을 내린 공격자를 찾아 처벌하고 책임을 묻는 것은 그 다음 문제이다.

이렇게 볼 때, 물리적 공간을 기반으로 하여 형성된 국제법 체제를 그대로 사이버공격에 적용하는 차원의 논의는 위의 특성을 반영하고 있지 않을 가능성이 높다. 공격과 결과발생의 간격이 0인 사이버공격의 특성을 고려할 때, 이에 대응하기 위해서는 사전적 또는 실시간 대응이 필요하다. 그러나 국제법체제는 일반적으로 위반행위의 발생을 전제로 대응을 하게 되어있어 공격발생 전에 이루어지는 사전적 대응이 현행 국제법의 범위를 넘어서는 것일 수 있기 때문이다. 또한 의무위반주체가 아닌 의무위반행위에 사용된 수단에 조치를 취하는 문제도 국제법원칙을 그대로 적용해서 해소되기 어려운 측면이 있다. 이는 결국 사이버공격에 대한 국제법의 규율에 있어서 현행 국제법체제의 적용을 뛰어넘은 새로운 차원의 논의가 필요함을 나타내 준다고 볼 수 있다.

반면 국가들이 사이버공격과 관련하여 도입하고 있는 국내전략은 국제적 차원의 논의와는 다른 양상을 보이고 있다. 상당수의 국가들은 악의적인 흐름이 탐지된 네트워크에 대한 블로킹이나 즉시 타격과 같이 실제로 피해를 야기하는 공격이 발생하기 전이라도 사전적으로 조치를 취하는 이른바 적극적 방어개념[14]을 사이버안보정책으로 도입하고 있는 것이다. 적

14) 적극적 방어는 원래 적의 위협이 아군 지역에 도달하기 전에 이를 제거하여 부대의 전투력을 보존하는 전략을 뜻하는 군사용어로 적의 미사일 발사 징후 포착 시 위협의 근원지를 선제 타격하는 활동을 포함한다. 국방기술품질원, 국

극적 방어전략은 조치의 내용에서도 짐작할 수 있듯이 탐지된 위협을 억지하기 위해, 공격자를 밝히는 데 보다는 악의적 흐름을 유포하는 공격거점에 대한 직접 대응에 집중한다. 이러한 국가들의 전략은 향후 사이버공격에 대한 국가들의 대응실행을 형성하게 될 것이다.

문제는 적극적 방어조치가 여러 가지 위험성을 내포하고 있다는 점이다. 조치의 성격상 탐지된 위협이 발생하는 유포지를 추적하는 과정에서 초국경적인 네트워크 침해가 일어날 수 있고, 추적된 공격거점에 조치를 취하는 과정에서 파괴적인 결과가 초래될 수도 있다. 앞서도 말했듯이 공격거점은 악성바이러스에 감염된 제1차 피해자일 가능성이 높기 때문에 공격거점을 대상으로 한 적극적 방어조치는 제3국에 대한 또 하나의 사이버공격을 구성하게 될 수도 있다. 특히 이러한 전략이 사이버공격과 마찬가지로 은밀하게 진행될 때, 문제는 더 심각해질 수 있다. 따라서 국가들의 실행이 고착화되기 전에 적극적 방어개념에 대한 국제법적인 검토가 반드시 필요하다.

현재 73개의 국가들이 사이버안보 전략 보고서를 발표[15]하였으나 이에 대한 분석과 보고서에 포함된 전략의 국제법적 함의에 대해 검토한 연구는 찾아보기 어렵다. 적극적 방어와 관련한 선행연구들은 이 개념이 국제법 체계 안에서 법적 정합성을 가지는지와 같이 종합적인 관점으로 적극적 방어 개념에 접근하기 보다는 주로 역해킹이나 방향변경(redirection)과 같이 몇 가지 조치의 강도와 범위에 대해 검토하는 제한적인 수준에 머물고 있다.[16] 무엇보다도 이러한 조치가 적극적 방어개념으로서 국가들

방과학기술용어사전, (국방기술품질원, 2011), p. 742.

15) 이 숫자는 공식적으로 사이버안보전략 보고서를 발간한 국가만을 계산한 것이며, 비공식적인 보고서는 포함하지 않았음을 밝혀둔다. CCDOE, Cyber Security Strategy Documents, 2017년 11월 23일 기준, <https://CCDCOE.org/cyber-security-strategy-documents.html> (2017.12.6.최종방문).

16) 다음의 논문들이 그러한 예로 적극적 방어조치들을 전체적인 관점에서 바라보기 보다는 적극적 방어조치 중 몇 가지를 사이버상의 대응조치 또는 자위의 수단으로서 분석하고 있다. Katharine C. Hinkle, “Countermeasures in the Cyber Context: One More Thing to worry about”, The Yale

의 전략으로 도입되고 있거나 실행에 반영되고 있다는 내용을 담고 있는 연구는 찾아보기 힘든 실정이다. 이는 사이버공격에 대한 민간기업들의 대응에 관한 연구에서 적극적 방어가 그 개념 및 범위, 조치가 가지는 위법성을 중심으로 전체적인 관점에서 다루어지고 있는 것과 대조를 이룬다.[17)]

사이버공격에 대한 국가들의 대응실행이 적극적 방어조치를 중심으로 형성될 가능성이 높다는 점을 생각할 때, 현행 국제법이 그대로 사이버공격에 적용될 수 있는지를 검토하는 차원을 넘어서 적극적 방어개념이 현행 국제법 하에서 정당화될 수 있는지에 관한 종합적인 연구가 필요하다. 여기에는 특히 적극적 방어조치가 어떤 점에서 국제법적으로 문제가 될 수 있는지, 공격자가 아닌 공격거점에 대한 조치가 국제법체제 하의 귀속

Journal of International Law, Vol. 37 (2011), pp. 11-21; Oona A. Hathaway, "The Drawbacks and Dangers of Active Defense", in P. Brangetto, M. Maybaum, J. Stinissen (Eds.), *6th International Conference on Cyber Conflict* (NATO CCD COE Publications, 2014), pp. 39-50; Jan Messerschmidt, "Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm", Colombia Journal of Transnational Law, Vol. 52 (2013), pp. 275-324.

17) 그러나 민간기업의 적극적 방어관련 연구는 아쉽게도 대부분 국내법적 함의를 검토하는 데서 그치고 있다. 이하의 논문들이 그러한 예이다. Jan Kallberg, "A Right to Cyber Counter Strikes: The Risks of Legalizing Hack Backs", IT Professional, vol.17, no.1 (2015), pp.30-35; Irving Lachow, "Active Cyber Defense-A Framework For Policymakers", Center for a New American Security (2013), pp. 1-10; Dennis C. Blair et al., "Into the Gray Zone-The Private Sector and Active Defence against Cyber Threats-", Center for Cyber & Homland Security (2016), pp. 1-69; Wyatt Hoffman and Ariel E. Levite, *Private Sector Cyber Defense-Can Active Measures Help Stabilize Cyberspace?* (Carnegie Endowment for International Peace, 2017), pp. 1-46; Paul Rosenzweig, "International Law and Private Actor Active Cyber Defensive Measures", Stanford Journal of International Law, Vol. 50 (2014), pp. 103-117.

의 법리와 조화될 수 있는지, 위반행위가 발생하기 전에 조치를 취하는 것이 사후 대응을 기반으로 하는 현행 국제법 체제 하에서 수락될 수 있는지 등 구체적인 차원의 분석과 검토가 포함되어야 한다.

제2절 연구의 목적과 범위

본 논문의 목적은 사이버공간에 대한 국제법적 규율에 있어 국가들의 논의 및 학자들의 연구와 국내전략 간의 괴리가 발생하게 된 원인을 파악하고, 사이버공격 억지에 있어 국제법적으로 가장 효율적인 방안을 모색하는 데 있다. 이를 위해서 먼저 일반국제법상의 원칙이 사이버공격에 그대로 적용 가능한지 여부에 관한 논의가 사이버공격의 규율에 있어 어떠한 함의를 가지는지 분석한다. 또한 사이버공격에 적용될 수 있는 조약상의 의무에 대해서도 살펴보고, 이를 바탕으로 현행 국제법을 적용하여 사이버공격을 규율하는 데에 한계가 존재하는지를 검토한다. 국제법 체제의 한계를 규명하는 작업은 사이버공간 및 사이버공격이 가지는 독특한 특성이 국제법의 적용을 통해 해결될 수 있는지와 관련된 문제이다.

사이버공격은 일단 공격이 실행된 것을 발견했을 때는 이미 목표시스템 장악에서 피해의 발생까지의 과정이 모두 완료된 후일 가능성이 크다. 이러한 특성상 공격실행을 기점으로 대응을 하는 것은 사이버공격에 대한 효과적인 규율방안이 될 수 없다. 따라서 사이버공격에 대한 국제법적 규율에는 공격 발생 전 위협의 탐지 및 차단과 관련한 문제가 포함되어야 한다. 다수의 국가들이 국내적으로 도입 및 개발하고 있는 적극적 방어조치는 이러한 사전조치 및 즉각대응을 염두에 두고 고안된 전략이다. 문제는 이러한 대응전략이 국제법과 조화될 수 있는가이다. 사이버공격을 효과적으로 억지하는 것만큼 이를 억지하기 위한 대응이 또 다른 피해를 초래하지 않도록 규제하는 것 또한 중요한 문제이기 때문이다.

이에 본 논문에서는 국가들이 도입하고 있는 적극적 방어조치가 국제법적으로 어떤 문제점을 가지고 있는지 구체적으로 검토한다. 또한 이러한 문제점이 국제법상 위법성조각사유의 범위 내에 포섭될 수 있는지에 대해 각각의 위법성조각사유와 적극적 방어개념의 비교를 통해 분석한다. 이를 바탕으로 현행 국제법체제 안에서 적극적 방어개념의 실행이 가능한지 아니면 다자조약체제 마련을 통해 적극적 방어개념의 도입이 필요한지에 대

해 결론을 도출한다.

아울러 사이버공격을 효과적으로 규율하기 위해서는 사전적 및 즉각적 대응 외에도 추후 행위자를 밝혀 책임을 묻는 사후적 대응도 필요한 바, 이를 위해 현행 국제법 체제 내에 보완이 필요한 부분이 있는지에 대해서 검토한다. 먼저 활동의 흔적을 지울 수 있는 사이버공간의 특성상 공격자를 추적하기 위해 필요한 사항 및 절차를 알아보고, 지금까지 적용되어 온 국가귀속성의 법리가 사이버공격의 귀속을 밝히는 데에도 그대로 적용될 수 있는지 살펴본다.

이상 사이버공격에 대한 즉각적 대응 및 장기적 대응과 관련한 종합적 검토를 바탕으로 결론에서는 사이버공격을 국제법을 통해 실효적으로 규율할 수 있는 궁극적 방안을 제시할 것이다.

본 논문에서 다루는 사이버공격의 범위는 국가안보에 영향을 미치는 초국가적 사이버공격으로 한정하기로 한다. '국가안보에 영향을 미치는'이라는 문구는 사이버공격이 타국의 기반시설에 물리적 파괴를 초래하거나 인명 살상을 하는 것과 함께 물리적 피해는 없더라도 대규모 네트워크 공격으로 정부의 기능이 마비되거나 국가전반에 걸친 경제적 손해가 발생하거나 사이버공격을 통해 정권 교체와 같은 국가의 주권사항에 관련된 문제에 개입하는 경우 모두를 의미한다. 이와 같이 국가안보에 영향을 미치는 사이버공격에는 저강도 공격이나 고강도 공격 모두 포함될 수 있기 때문에 공격의 강도에 관계없이 모든 강도의 실제 공격 사례를 분석의 대상으로 한다.

제2장 사이버공격에 대한 국제법적 규제의 필요성

제1절 사이버공격의 개념

1. 사이버공격의 정의

사이버공격(Cyber Attack), 사이버 테러리즘(Cyber Terrorism), 사이버전(Cyber Warfare) 등의 사이버 행위와 관련하여 국가 및 국제사회가 관심을 가지고 이를 법적으로 규제해야 한다고 인식하기 시작한 것은 최근 20년 사이의 일이다. 이후 2007년 에스토니아 사건, 2010년 이란 핵시설에 대한 스턱스넷 사건 등이 일어나면서 위협적인 사이버활동에 대한 국제법적 관심은 더욱 커졌다. 이에 북대서양조약기구(NATO) 산하의 사이버방어협력센터(Cooperative Cyber Defence Centre of Excellence, CCD COE)가 국제법 학자들과 실무자들의 연구를 통해 2013년 사이버전에 적용가능한 국제법원칙에 대한 사이버 교전 수칙인 탈린 매뉴얼(The Tallinn Manual on International Law Applicable to Cyber Warfare)을 발간하기도 하였으나[18] 이는 국제사회가 공식적으로 채택한 구속력이 있는 문서가 아닌 일종의 가이드라인이다.

한편 구속력 있는 조약으로는 2004년 발효된 사이버 범죄에 관한 협약(Convention on Cyber Crime)[19]이 있다. 그러나 이는 주로 국내적으로 처벌 가능한 컴퓨터 네트워크를 통한 사기, 돈세탁, 사이버공간상의 지적재산권 침해, 아동포르노그래피 유포 등의 사이버 범죄를 다루는 것이어서 국가에 영향을 미치는 사이버 적대행위와는 그 적용범위가 다르다. 이처럼 적대적인 사이버활동을 규제하는 구속력 있는 국제문서가 없고, 이에 대한

18) 2017년 2월에는 Tallinn Manual 2.0이 발간되었다.
19) 2001년 11월 23일 채택, 2004년 7월 1일 발효. 당사국은 49개국이다, Council of Europe, Treaty No.185.

논의가 중점적으로 이루어진지 얼마 되지 않았기 때문에 사이버 관련 용어에 대해 확립된 정의는 찾아보기 힘들다. 이하에서는 각국의 사이버안보 전략 및 연구 문서에 나타난 사이버공격의 정의에 대해 검토해 보고, 공통점을 바탕으로 종합적인 정의를 내려 본다.

2013년 발간된 탈린 매뉴얼은 사이버공격을 “공격적인지 또는 방어적인지에 관계없이 사람에 대하여 위해나 죽음을 야기하거나 사물에 손해 또는 파괴를 야기할 것으로 충분히 예상되는 사이버작전(Cyber Operation)을 의미”하는 것으로 정의하고 있다.[20] 또한 사이버 작전에 대해서는 “사이버공간 안에서 혹은 사이버공간의 사용을 통해 목표를 달성하는 것을 주요 목적으로 사이버역량을 사용하는 것”[21]이라고 정의하고 있다. 이를 종합하면 사이버공격은 “목적을 달성하기 위해 사이버공간에서 사이버역량을 사용하여 사람의 죽음이나 상해 혹은 사물에 대한 손해나 파괴를 야기하는 행위”라고 볼 수 있다.

탈린매뉴얼의 저자는 여기서 말하는 ‘공격’의 개념을 ‘1949년 제네바협약에 대한 추가 및 국제적 무력충돌의 희생자보호에 관한 의정서(제1의정서)’(Protocol Additional to the Geneva Convention of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts(Protocol I) 제49조 제1항에 근거한 것이라고 밝히고 있다.[22] 그러나 제1의정서 제49조 제1항은 공격을 “폭력 행위(acts of violence)”를 의미하는 것으로 정의하고 있어 사이버공격에 적용하는데 주의를 요한다. 매뉴얼에 따르면 “acts of violence”는 재래식 무기를 사용한 행위만을 의미하는 것은 아니라고 하고 있다. 매뉴얼은 타디치 사건에서 화학 또는 생물학무기를 사용한 경우도 공격으로 인정된 것처럼[23]

---

20) NATO Cooperative Cyber Defence Centre of Excellence, *The Tallinn Manual on International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013), p. 106.
21) *Ibid.,* p. 258.
22) *Ibid.,* p. 106.
23) *Prosecutor v. Dusko Tadić, ICTY, Case IT-94-1-A, 1999*, paras. 120,

공격의 의미를 수단이 아닌 발생하는 결과를 가지고 판단하는 것으로 보고 있다.[24] "acts of violence"의 예로는 송전망을 통제하는 SCADA 시스템을 조작하여 화재가 발생하는 것, SCADA 시스템 조작으로 댐을 방류하는 것 등이 제시되어 있다.[25] 즉, 일정 강도 이상의 피해가 발생해야 사이버공격이 일어났다고 판단하고 있는 것이다.

한편 북대서양 조약기구(NATO)가 2014년 발간한 용어집에서는 사이버공격을 컴퓨터 네트워크 공격의 한 종류라고 하면서 "컴퓨터 또는 컴퓨터 네트워크 상의 정보를 교란, 거부, 성능저하 또는 파괴하기 위해 취하는 행동"[26] 이라고 정의하고 있다. 미국 연방표준·기술국(National Institute of Standards and Technology, NIST)이 2013년 발간한 보고서에서는, "기업의 사이버공간 사용을 표적으로 하여 전산 환경/기반시설을 방해, 불능화, 파괴 또는 악의적으로 통제하려는 목적으로 또는 데이터의 통일성을 파괴하거나 통제된 정보를 훔치려는 목적으로 사이버공간을 통하여 행하는 공격"[27]을 사이버공격으로 보고 있다.

한편 국가들도 자국이 발간한 사이버안보전략이나 법령을 통해 사이버공격에 대한 정의를 내리고 있는데, 그 중의 몇 가지를 살펴보면 다음과

124.

24) NATO CCD COE, *supra* note 20, pp. 106-107.

25) *Ibid.,* p. 107.

26) North Atlantic Treaty Organization Standardization Agency (NSA), "NATO Glossary of Terms and Definitions", NATO AAP-06 Edition (2014), p. 71 ; Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself.

27) Richard Kissel eds., "Glossary of Key Information Security Terms, NIST US Department of Commerce" (2013), p. 57.
;(원문) An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information, <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf> (2018.1.4. 최종방문).

같다. 독일은 2011년 발간한 사이버안보 전략(Cyber Security Strategy for Germany)에서 “사이버공격은 사이버공간 내에서 하나 또는 여러 개의 다른 정보기술(IT) 시스템의 보안에 손상을 가할 목적으로 행하는 정보기술 공격”이라고 정의하였다. 독일은 또한 외국의 정보기관에 의한 정보기술 시스템의 기밀성에 대한 사이버공격이 사이버 간첩행위이며, 정보기술 시스템의 통일성과 이용성에 대한 사이버공격은 사이버 사보타주(Cyber Sabotage)라고 하여 이들 개념을 함께 묶어 사이버공격의 종류로 분류하고 있다.[28)]

우리나라는 국가사이버 안전관리 규정[29)]을 통해 사이버공격에 대한 정의를 내리고 있다. 동 규정 제2조 제2호는 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 사이버공격이라고 정의하고 있다. 또한 같은 조 제4호에서 사이버공격으로 정보통신망을 통해 유통·저장되는 정보를 유출·변경·파괴함으로써 국가안보에 영향을 미치거나 사회·경제적 혼란을 발생시키거나 국가 정보통신시스템의 핵심기능이 훼손·정지되는 등 무력화되는 상황을 ‘사이버 위기’로 정의하면서 사이버공격이 국가안보에 직접적인 영향을 미칠 수 있음을 인식하고 있다. 앞서 살펴본 정의와 이 밖의 국가들의 사이버 전략에 나타난 사이버공격의 정의를 표로 정리하면 다음과 같다.

---

28) Germany, “Cyber Security Strategy for Germany” (2011), p. 14, <https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile> (2018.1.4. 최종방문).

29) 대통령훈령 제316호, <http://www.law.go.kr/admRulLsInfoP.do?admRulSeq=2000000100482> 참조.

표1. 사이버공격의 정의

	장소	수단	목적	대상
CCD COE	사이버공간	사이버역량	죽음·위해/손해·파괴	사람/사물
NATO	컴퓨터·컴퓨터 네트워크		정보교란·거부·Degrade·파괴	컴퓨터·컴퓨터 네트워크 상의 정보
오스트리아[30]	사이버공간	정보통신기술	정보통신기술의 보안 약화	정보시스템
독일	사이버공간	정보기술	정보기술 시스템 보안의 손상	정보기술 시스템
영국[31]		이메일 스캠을 포함한 정보기술	정보기반시설에 대한 혼란, 산업시스템에 대한 물리적 혼란	정보기술 기반시설 or 산업시스템
스위스[32]	컴퓨터, 컴퓨터 네트워크, 데이터	데이터 판독·삭제·변경·연결/서비스 과부하/시스템 조작 등	데이터의 통일성·기반시설의 기능 방해, 데이터의 이용성 제한	데이터, 정보채널, 처리시스템
미국	사이버공간		전산환경·기반시설 방해·불능화·파괴·악의정통제/데이터의 통일성 파괴	전산환경/기반시설
한국	국가정보통신망	해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단	국가안보에 영향을 미치는 것, 사회·경제적 혼란 발생, 국가정보통신시스템의 핵심 기능 훼손·정지	국가정보통신망
일본[33]		장착형 장치	정보 절취·손	정보, 데이터

			상·변경을 통한 사회체계 기능 방해 및 사회·경제적으로 물리적 영향을 주는 것	
러시아[34]	정보통신시스템, 정보자원	정보시스템에 대한 접근	정보보안에 대한 위협	정보통신 시스템, 정보자원
뉴질랜드[35]	컴퓨터 기반 시스템	컴퓨터 시스템에 대한 접근 약화, 온라인 이동경로 추적	재정적 손해, 지적재산권 절취, 국가 주요 기반시설에 대한 손상	컴퓨터 시스템의 기능과 정보
캐나다[36]		전자적 수단	전자 및 물리적 기반시설에 대한 접근·사용·조작·방해·파괴 행위	전자 및 물리적 기반시설
공통점	사이버공간	정보통신 기술	정치적·사회적·경제적 혼란	사람, 전자 및 물리적 기반시설

30) Austria, "Austrian Cyber Security Strategy" (2013), p. 21, <https://www.bka.gv.at/DocView.axd?CobId=50999> (2016.7.21. 최종방문).

31) United Kingdom, "Parliamentary Office of Science & Technology, POSTnote Number 389: United Kingdom, "Cyber Security in the UK" (2011) p. 1.

32) Swizerland, "National Strategy for the Protection of Switzerland Against Cyber Risks" (2012), p. 9.

33) Japan, "Cyber Security Strategy", Government of Japan(Cabinet Decision 2015) pp. 5, 12, 30.

34) Russia, "Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space" (2011), p. 3, <https://CCD COE.org/strategies/Russian_Federation_unofficial_translation.pdf>(2018. 1.25.최종방문).

표1에서 정리된 내용을 종합해보면, 사이버공격은 “사이버공간 안에서 정보통신 기술을 사용하여 정치적·사회적·경제적 혼란을 발생시킬 목적으로 사람, 전자 및 물리적 기반시설에 대하여 위해를 가하는 행위” 정도로 정의를 내릴 수 있다.

한편 언론기사와 각국의 국내법, UNGGE 보고서, 앞서 언급한 탈린 매뉴얼 등의 국제문서에서는 사이버공격과 함께 사이버 테러, 사이버전, 사이버 충돌, 사이버 작전 등의 용어가 혼용되고 있는 것을 확인할 수 있다.[37] 이러한 용어들도 사이버공격과 마찬가지로 확립된 정의가 없는 것은 마찬가지이다. 이 중 몇 가지 용어의 정의에 대해 간략히 살펴보면 먼저 사이버전은 한 연구에서 적국을 공격하기 위해 컴퓨터 시스템과 네트워크를 주로 사용하는 군사적 활동을 포함하는 것[38]으로 정의되어 있다.

이를 사이버공격의 정의와 비교해 보면 ‘적국’ 이나 ‘군사적 활동’과 같은 단어를 제외하고는 의미하는 바가 별 차이가 없음을 알 수 있다. 이는 다른 용어들의 경우에도 마찬가지이다. 예를 들어 사이버테러리즘의 정의로 가장 많이 인용되는 Dorothy Denning의 정의는 일반적으로 정치적 또는 사회적 목적을 달성하기 위해 컴퓨터, 네트워크 및 이에 저장된 정보에 대한 불법 공격 및 공격의 위협을 통해 정부 또는 그 국가의 국민을

---

35) New Zealand, “New Zealand’s Cyber Security Strategy” (2011), p. 12 ; New Zealand, “New Zealand’s Cyber Security Strategy“ (2015), p. 3.

36) Canada, “Canada’s Cyber Security Strategy For A Stronger and More Prosperous Canada” (2010) p. 3, <http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf> (2018.1.4. 최종방문).

37) 이정석, 이수진, “북한 사이버공격에 대한 국제법적 검토를 바탕으로 한 국방 사이버전 수행 발전 방향”, 보안공학연구논문지, Vol. 12, No. 4 (2015), p. 320.

38) Johann-Christoph Woltag, “Cyber Warfare”, in Wolfrum (ed.), *Max Planck Encyclopaedia of Public International Law*, (Oxford Public International Law, 2015), para. 8. <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e280?rskey=i8J7z5&result=1&prd=EPIL>

위협 또는 강제하는 것을 사이버테러리즘으로 보고 있다.[39] 여기에서도 '정치적 또는 사회적 목적을 달성하기 위해'라는 문구를 빼고 나머지 부분은 사이버공격의 정의와 거의 다르지 않다는 것을 알 수 있다.

이렇게 볼 때, 각 용어들의 정의에서 몇 가지 특징적으로 강조되는 부분이 있기는 하지만 행위의 수단과 방법이 같고, 국가안보에 영향을 미치는 초국경적 사이버공격은 모두 국제법 규율의 대상이라는 점에서 용어의 세부적인 구별이 국제법적으로 큰 실익이 없다는 점을 알 수 있다. 무엇보다도 사이버공격은 발생 즉시 행위의 성격 및 행위자를 특정할 수 없다는 특징이 있기 때문에 해당 행위가 사이버전에 해당하는지, 사이버 테러에 해당하는지 결정하는 데는 상당한 시간이 걸린다. 이와 같은 점들을 고려할 때, 사전에 행위자를 특정할 필요도 없고, 다양한 공격양태를 아우를 수 있는 사이버공격이라는 용어를 사용 하는 것이 가장 적절하다고 본다.

2. 사이버공격의 발생시점

앞에서 사이버공격에 대한 정의를 내렸지만 이 용어를 적용하여 국제법적 분석을 진행하기 위해서는 사이버공격의 전개과정에 대한 이해가 필요하다. 앞에서 살펴본 바 있듯 기관이나 국가들의 연구보고서에서 사이버공격에 대해 내린 정의나 제시된 예를 보면 시스템 손상 이상의 결과를 발생시키는 행위가 사이버공간에서 실행되었을 때, 이를 사이버공격이 발생한 것으로 보고 있음을 알 수 있다. 재래식 공격의 경우에는 미사일이나 폭탄을 발사하면 인명피해나 기반시설의 파괴와 같은 결과가 발생한다. 그러나 사이버공격은 이와 다르다. 사이버공격은 재래식 공격과 비교했을 때 무기 발사를 위한 스위치를 누르기까지-즉, 시스템에 손상을 가할 수 있

39) Mehmet Nesip Ogun, "Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purposes", Journal of Applied Security Research (2012), p. 209. ; Serge Krasavin, "What is Cyberterrorism?", Computer Crime Research Center (2001-2002). <http://www.crime-research.org/library/Cyber-terrorism.htm>.

는 DDoS 공격[40], APT공격[41], 랜섬웨어 공격[42]을 실행하기까지- 여러 단계에 걸쳐 준비작업을 하기 때문이다. 이에 대해 재래식 무기의 경우에도 사용하기 전에 여러 가지 준비과정을 거친다는 반박이 있을 수 있다. 그러나 무기개발, 무기 이동 및 시험발사 등의 준비과정과 달리 사이버공격을 위한 준비과정은 그 자체로 사이버공간에 악영향을 끼친다는 점에서 차이가 있다. 따라서 앞서 내린 정의대로 실제로 사람, 전자·물리적 기반시설에 위해를 가하는 사이버공격이 실행되는 시점을 이해하기 위해서는 목표한 대상에 사이버공격이 이루어지기까지의 전체과정을 이해하는 것이 필요하다.

오늘날 대부분의 사이버공격은 공격자의 컴퓨터에서 목표시스템으로 바로 실행되는 것이 아니라 봇넷과 봇넷을 제어하고 명령을 내리는 C&C 서버를 공격거점으로 하여 이루어진다. 봇넷은 악성코드에 감염된 개인 컴퓨터들이 하나의 네트워크를 형성하고 있는 것으로 공격자에 의해 원격으로 조종되어 공격자의 명령에 따라 공격을 수행[43]하는 실질적인 공격 수단이다. 공격자는 우선 인터넷 사이트에 악성코드를 심어놓아 해당 사이트에

---

40) 분산 서비스 거부(Distributed Denial of Service, DDoS)공격은 인터넷 사이트에 대량의 트래픽을 보내 서비스를 마비시키는 공격 유형이다.

41) 지능형 지속형 공격(Advanced Persistent Threat, APT)은 기관, 기업 등 목표시스템에 침투하기위해 지속적으로 취약점을 노리며, 내부망에 침투하고 나서도 시스템에 잠복하면서 정보를 수집하여 해킹 혹은 시스템을 파괴하는 공격유형이다. 한국정보통신기술협회 정보통신용어사전, <http://word.tta.or.kr/dictionary/dictionaryView.do?word_seq=035578-2> (2017.12.31.최종방문).

42) 랜섬웨어는 몸값을 뜻하는 Ransome과 제품을 뜻하는 Ware의 합성어로, 이에 감염된 컴퓨터는 시스템 접근에 제한을 받고, 해제를 위해 악성코드 제작자에게 금품을 제공해야 제한이 풀리는 악성프로그램을 말한다. 한국정보통신기술협회, "정보보호기술용어", 한국정보통신기술협회 (2013), p. 24.

43) Christian Czosseck, Gabriel Klein, Felix Leder, “On the Arms Race Around Botnets-Setting Up and Taking Down Botnets”, C. Czosseck, E. Tyugu, T. Wingfield (Eds.), *International Conference on Cyber Conflict* (CCD COE Publications, 2011), p. 108.

방문하는 사용자들이 심어놓은 악성코드를 다운 받게 하거나[44], 이메일 피싱[45] 수법을 쓰거나 또는 웜에 악성코드를 실어 취약성을 가진 컴퓨터를 찾아 감염시키는 등의 다양한 방법을 통해 개인컴퓨터를 악성코드로 감염시킨다. 이렇게 감염된 봇[46]은 C&C 서버에 접속하여 자신의 감염사실을 알리게 된다. C&C는 감염된 봇에게 다른 컴퓨터에 대한 감염을 지시하고, 봇은 새로운 대상들을 감염시켜 이들을 C&C로 연결시키고 추후 지시를 받도록 만든다. 해커는 원격조종을 통해 봇들을 하나의 네트워크로 연결하여 봇넷을 형성하고, 봇넷을 사용한 공격이 필요할 때까지는 이를 휴면상태로 둔다. 그러다가 필요한 시점이 되면 기관이나 기업에 대한 공격 실행에 봇넷을 사용하게 되는 것이다.

악성코드는 주로 언론사 홈페이지 등 사용자들이 일반적으로 방문하는 웹페이지에 심겨져 있는 경우가 많고, 이메일을 통해 감염되는 경우에도 별다른 징후가 나타나지 않기 때문에 대부분의 사용자들은 자신의 컴퓨터가 악성코드에 감염된 사실을 알지 못한 상태에서 모든 과정이 진행된다.[47] 즉, 자신도 모르게 봇넷의 일부가 되어 공격을 수행하게 되는 것이다.

---

44) 최근에는 미국 정부의 사이트가 이용된 경우도 있었다. 데일리시큐, “미정부 웹사이트 해킹당해 케르베르 랜섬웨어 배포 서버로 활용돼”, 2017년 9월 5일, <http://www.dailysecu.com/?mod=news&act=articleView&idxno=23531> (2017.12.31.최종방문).

45) 정부기관을 사칭하거나 사용자가 구체적으로 관심 있는 분야의 이메일을 보내어 사용자가 메일을 확인하도록 유도하는 수법으로 이를 열기위해 클릭하는 순간 악성코드에 감염되어 개인정보가 유출되거나 계정이 탈취된다.

46) 로봇의 줄인 말로써 데이터를 찾아주는 소프트웨어 도구. 인터넷 웹 사이트를 방문하고 요청한 정보를 검색, 저장, 관리하는 에이전트의 역할을 한다. 보안이 취약한 컴퓨터를 스스로 찾아 침입해 보이지 않는 곳에서 조용히 작동하면서 컴퓨터 사용자도 모르게 시스템에게 명령을 내릴 수 있는 원거리 해킹 툴이다. 한국정보통신기술협회, 정보통신용어사전, <http://word.tta.or.kr/dictionary/dictionaryView.do?word_seq=037358-1> (2018.1.25.최종방문).

47) Christian Czosseck, Gabriel Klein, Felix Leder, *supra* note 43, p. 108.

한편 봇넷에 명령을 내리고 봇넷의 활동을 제어하는 C&C 서버는 공격자가 유명 포털사이트나 기관의 서버를 해킹하여 마련하기도 하고,[48] 이미 감염된 봇을 C&C 서버로 사용하기도 한다.[49]

문제는 이렇게 공격의 수단 및 공격의 거점을 마련하는 과정이 인터넷 환경에 해로운 영향을 주기는 하지만[50] 이러한 수단의 존재 자체가 시스템에 손상을 주는 사이버공격이라고 보기는 힘들다는 점이다. 이와 같은 맥락으로 한 연구에서는 "미국의 군대가 매일 수백만 개의 사이버공격에 직면하고 있다"는 미국 사이버 사령부 지휘관의 발언에 대해 비판한 바 있다.[51] 여기에서 언급된 수치가 기관 내 네트워크로 침입하지 못하여 실제적인 손상을 입히는 데까지는 이어지지 못한 위협까지 모두 포함하고 있기 때문이다.[52]

앞에서 살펴본 각국의 전략이나 기관의 연구보고서에서는 목표 대상에 대해 일정 강도 이상의 피해를 야기하는 사이버 상의 행위를 사이버공격으로 정의하고 있고, 국가들도 국제법의 규율이 필요하다는 시각에서 사이버공격 문제에 접근하고 있다.[53] 이에 목표시스템으로의 침투 및 이에 대

---

48) TrendMicro, Mar. 12, 2015, "Investigating and Detecting Command and Control Servers", <http://blog.trendmicro.com/trendlabs-security-intelligence/investigating-and-detecting-command-and-control-servers/> (2017, 12.31.최종방문); SC Media, Apr. 6, 2017, "ROKRAT using Twitter, other social media as command and control link", <https://www.scmagazineuk.com/rokrat-using-twitter-other-social-media-as-command-and-control-link/article/648866/> (2017.12.31.최종방문).

49) Felix Leder, Tillmann Werner and Peter Martini, "Proactive Botnet Countermeasures-An Offensive Approach", In C. Czosseck, K. Geers (Eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press, 2009), p. 213.

50) Ibid., p. 211.

51) P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2014), p. 68.

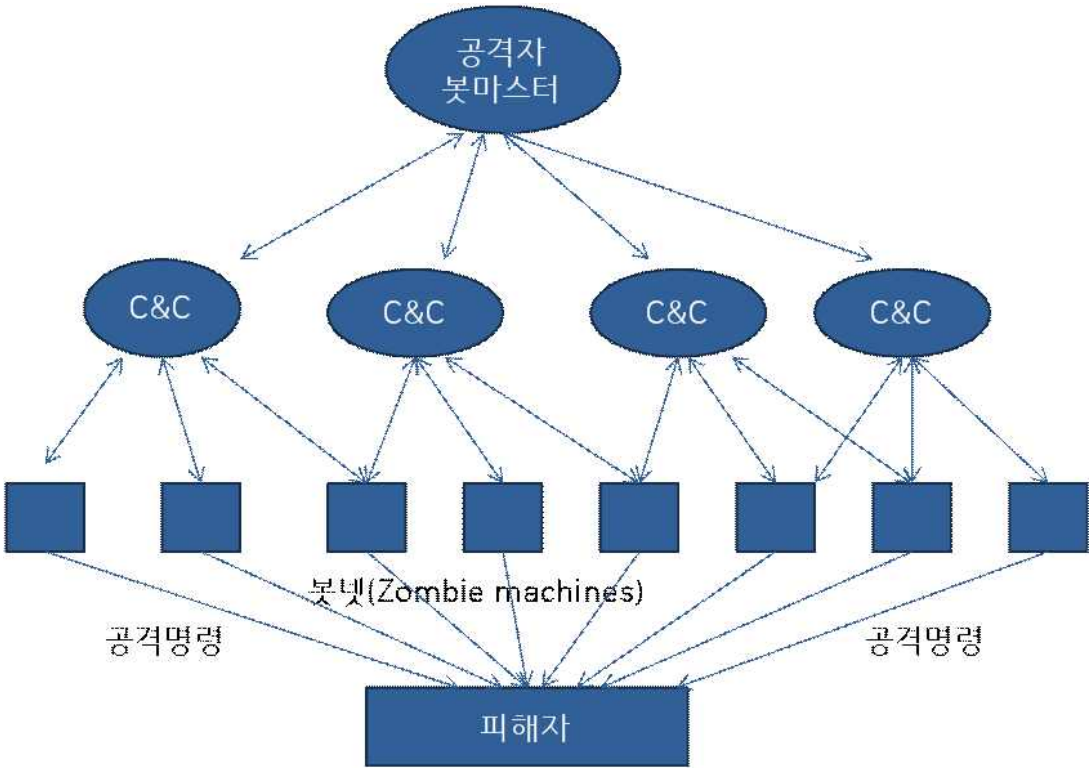
52) Ibid., p. 68.

한 조작이 가능하기 전까지의 사전작업 모두를 사이버공격으로 보는 것은 법적 규율이 미치는 사이버공격의 범위를 지나치게 확대할 위험이 있다는 점에서 바람직하지 않다. 그렇게되면 일상적으로 흔히 일어나는 바이러스 감염과 같은 위협을 모두 법위반의 문제로 접근해야 하는 문제가 발생할 수 있기 때문이다. 따라서 기관이나 기업의 내부시스템에 직접 영향을 미치는 행위의 실행[54]이 있기 전까지 진행되는 사이버상의 활동에 대해서는 사이버공격이라는 용어를 적용하기 보다는 위협이 발생했다거나 위협이 탐지되었다는 용어를 사용하는 것이 적절하다. 사이버공격은 내부시스템에 손상을 주는 행위가 실행되는 시점에 발생한 것으로 보아야 한다. 이는 다음과 같이 사이버공격이 수행되기까지의 기본적인 전개과정을 그림으로 도식화해보면 더욱 분명하게 이해할 수 있다.

53) UN Doc. A/68/98 (2013); UN Doc. A/70/174 (2015). 국가들의 논의에 대해서는 제4장에서 자세히 검토하기로 한다.

54) 2013년에 발간된 탈린매뉴얼에서는 사이버공격의 예로 송전망이나 댐 시설 운영에 사용되는 SCADA 시스템 조작을 든 바 있다. NATO CCD COE, *supra* note 20, pp. 106-107.

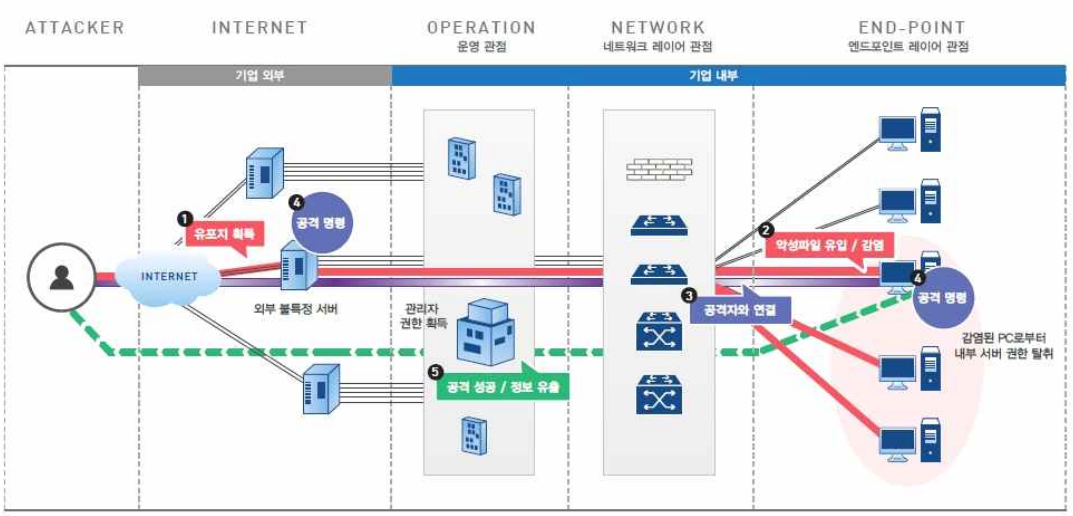
그림 1. 사이버공격의 전개과정



이 과정은 DDoS 공격, 지능형 지속형 공격, 랜섬웨어 공격에 모두 적용될 수 있다. 봇넷에서 피해자로의 공격과정을 좀 더 세분화해서 살펴보기 위해 지능형 지속형 공격의 예를 들어보면 우선 진행과정은 다음과 같다. 공격자의 목표가 A기관의 내부 시스템 관리자 권한을 획득하여 시스템 운영을 마비시키는 것이라고 하자. 우선 공격자는 기관 외부의 인터넷 공간에서 봇넷에 이메일 피싱 등의 위협 유포를 통해 기관 내부의 개인 사용자의 컴퓨터를 감염시킨다. 개인 컴퓨터가 감염되면 이는 사용자 컴퓨터의 파일 공유서버를 통해 다른 개인 컴퓨터로 확산된다. 이후 감염된 개인컴퓨터를 정찰하면서 사내 시스템에 접근하기 위해 패스워드를 대입해 보는 등의 정찰 및 정보수집 작업을 실행하게 된다. 즉, 기관 내 개인 컴퓨터가 악성코드에 노출되었다고 해서 내부 시스템 조작을 위한 공격을

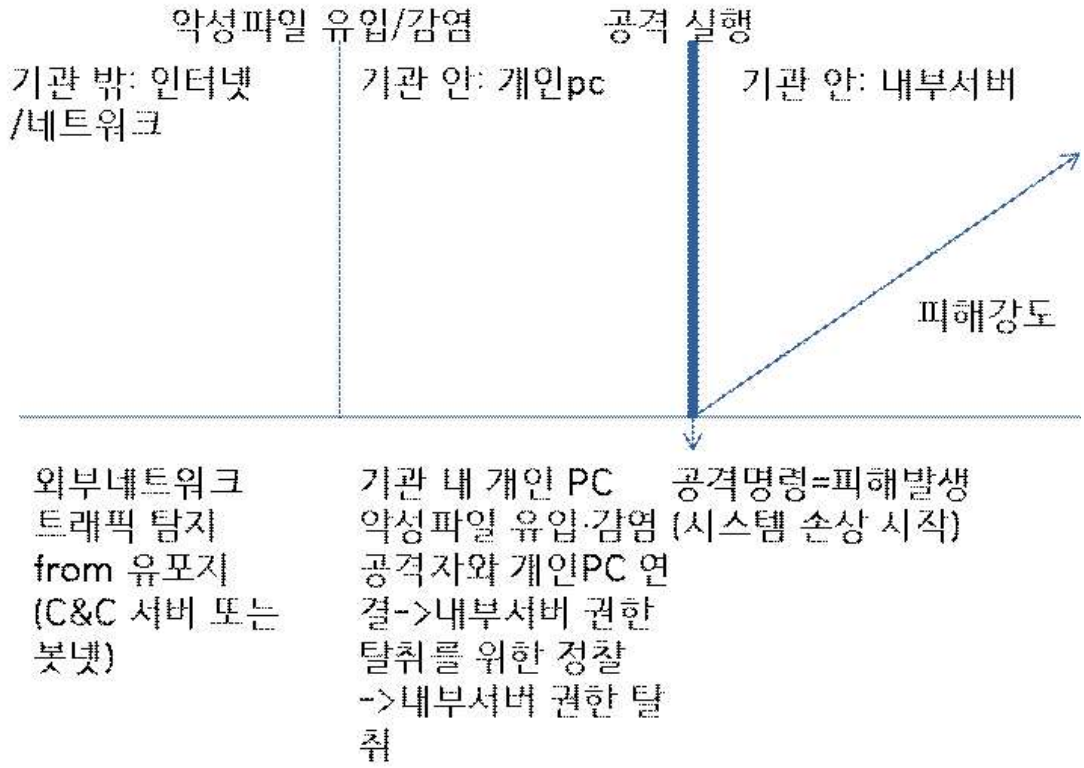
실행할 수 있는 것은 아니다. 앞의 사전 작업을 통해 내부서버에 접근할 수 있게 되면 공격자는 시스템 조작을 위한 내부정찰 작업을 하게 되고, 마침내 공격명령을 통해 시스템 운영에 이상이 발생하기 시작하는 것이다. 다음은 이 과정을 그림으로 표현한 것이다.

그림 2. APT 전개과정[55)]



55) 안철수연구소, “APT 공격의 비밀을 파헤치다”, Oct. 4, 2011, 해당보고서는 APT 공격의 진행과정과 원리를 단계별로 상세히 분석하고 있다. <http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?cmd=print&seq=18487&menu_dist=2> (2018.1.1.최종방문).

그림 3. 단면으로 나타낸 APT 전개과정



따라서 앞에서 도출한 사이버공격의 정의와 동일한 의미의 공격 발생 시점은 단면도의 굵은 선 부분이라고 할 수 있다. 이하에서는 그림의 굵은 선을 포함한 이후의 과정[56]을 사이버공격으로 보고, 그 전의 활동에 대해서는 사이버위협의 발생 또는 탐지라는 표현을 사용하여 분석을 진행하도록 한다.

56) 굵은 선 이후 즉, 공격명령 이후의 과정도 사이버공격에 포함시키는 이유는 APT 공격의 경우 공격의 종료 또는 탈출을 위한 추가적인 행위를 하는 경우도 있기 때문이다. 끝까지 은밀한 공격을 하기 원하는 공격자는 이 단계에서 자신의 흔적을 지우는 작업을 진행한다. 안철수 연구소(2011); DataNet, 2017년 11월 23일, “공격 처음부터 끝까지 추적해 지능형 공격 막아낸다”, <http://www.datanet.co.kr/news/articleView.html?idxno=117139> (2018.1.1.최종방문).

제2절 사이버공격의 초국가성과 국제법적 규제의 필요성

1. 초국가적 사이버공격의 위험성

오늘날 사이버공격은 국경을 초월하여 일어나고 있으며, 그로 인한 피해는 개인정보 탈취와 금전적 손해, 기업의 지적재산권 침해 수준을 넘어서 국가기반시설을 파괴하고, 일국의 정치상황에 영향력을 행사하는 정도에까지 이르고 있다. 즉, 사이버공격은 국가안보를 위협하는 수준에까지 이른 것이다. 이러한 사이버공격의 위험성 및 초국가적 성격은 사이버공격이 국제법의 차원에서 대응해야 할 문제라는 점을 말해준다. 이하에서는 사이버공격이 국가안보에 있어 갖는 위험성에 대해 살펴보고, 국제법을 통한 실효적 규제 방안을 모색하는 것이 왜 필요한지에 대해 논의 한다.

2008년 터키 동부지역에서는 카스피해부터 지중해에 이르는 구간을 관통하는 길이 1,760km의 송유관이 폭발한 사건이 발생하였다. 당시 사건의 원인으로는 기기의 오작동 또는 테러조직의 소행이 거론되었다. 그러나 오랜 시간의 조사 끝에 6년이 지난 2014년 당시 사건이 악성코드 삽입을 통한 사이버공격에 의한 것이었음이 밝혀지게 되었다. 공격의 배후로는 러시아가 지목되었다.[57] 2010년에는 이란의 나탄즈 핵시설에 스턱스넷이라는 악성코드 공격으로 인해 1,000개 이상의 원심분리기가 파괴된 사건이 발생하였다.[58] 해당 사건의 공격 배후는 명확하게 밝혀진 바 없지만 미국이 이스라엘의 이란 핵시설에 대한 무력공격을 저지하기 위해 이스라엘과 합작하여 사이버공격을 감행한 것으로 보도된 바 있다.[59] 2010년 스턱스

---

57) Bloomberg, Dec. 10, 2014, “Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar”, <https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar> (2017.4.14.최종방문).

58) David Albright, Paul Brannan, and Christina Walrond, *supra* note 2.

59) The New York Times, Jan. 15, 2011, “Israeli Test on Worm Called Crucial in Iran Nuclear Delay”, <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

넷 사건이 발생하기 전까지 사이버공격이 물리적 공간에도 파괴적인 결과를 가져올 수 있다는 이른바 Cyber Pearl Harbor에 대해서는 회의적인 시각이 대다수였다.[60] 그러나 스턱스넷 사건 발생 이후 사이버공격이 물리적 파괴를 가져올 수 있다는 것은 이미 직면한 현실로 받아들여지고 있다.

특히 2017년 5월 12일부터 발생한 워너크라이(WannaCry) 공격은 이러한 사이버공격의 파괴력을 확실하게 보여준 사건이다. 워너크라이 랜섬웨어 공격은 다양한 파일과 데이터를 암호화하여 이를 푸는 대가로 가상화폐인 비트코인을 요구하는 메시지가 창에 나타나는 방식으로 진행되었다. 보통의 랜섬웨어가 이메일의 첨부파일을 통해 유포되는 것과는 다르게 워너크라이 랜섬웨어는 인터넷에 접속만 해도 감염되는 특징으로 인해 개인 컴퓨터뿐 아니라 영국, 중국, 러시아 등 150여 개국의 정부기관 및 글로벌 기업의 컴퓨터가 감염 피해를 입었다.[61]

특히 영국의 경우 워너크라이 공격으로 국가보건서비스(NHS)망 산하의 248개 의료기관 중 48곳의 전산망이 마비되었으며, 의사들은 환자들의 정

?mcubz=3> (2017.9.13.최종방문).

60) 시간상으로는 BTC 송유관 폭발 사건이 스턱스넷 사건보다 앞서지만 BTC 사건의 원인이 사이버공격에 의한 것임이 밝혀진 것은 2014년이기 때문에 사이버공격의 물리적 영향에 관한 논의는 스턱스넷 사건 중심으로 이루어졌다; 2012년 당시 미 국방장관 Leon E. Panetta는 진주만 사건을 연상시키는 "Cyber Pearl Harbor" 라는 용어를 사용하면서 국가안보를 위협할 수 있는 대규모 사이버공격의 위험성을 경고하였다. The New York Times, Oct. 11, 2012, "Panetta Warns of Dire Threat of Cyberattack on U.S.", <http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html> (2017.10.30.최종방문).

61) Korea IT Times, 2017년 5월 15일, "150개국 20만대 감염시킨 '워너크라이' 주의보", <http://www.koreaittimes.com/story/69595/150%EA%B0%9C%EA%B5%AD-20%EB%A7%8C%EB%8C%80-%EA%B0%90%EC%97%BC%EC%8B%9C%ED%82%A8-%E2%80%98%EC%9B%8C%EB%84%88%ED%81%AC%EB%9D%BC%EC%9D%B4%E2%80%99-%EC%A3%BC%EC%9D%98%EB%B3%B4> (2017.9.14.최종방문).

보가 담긴 파일을 열람할 수 없게 되어 응급환자들을 다른 병원으로 이송시키는 사태가 벌어지기도 하였다.[62] 인도네시아에서도 대형 종합병원의 컴퓨터가 감염돼 진료가 중단되었으며, 러시아 내무부, 독일의 국영 철도회사 도이체반, 중국 최대 국영에너지기업 CNPC, 러시아의 이동통신기업 메가폰, 스페인의 통신기업 텔레포니카 등의 컴퓨터가 감염되어 운영이 중단되는 등 피해는 사기업부터 국가기반시설에 이르기까지 무차별적으로 발생하였다.[63]

이렇게 전세계에 걸쳐 막대한 피해를 양산한 워너크라이 공격을 주목해야하는 이유는 공격의 방식에 있다. 워너크라이 랜섬웨어는 "Shadow Brokers"라는 해킹 그룹이 미국가안보국(NSA)이 개발한 사이버무기, "Eternal Blue"[64]를 해킹하여 만든 것으로 알려져 있기 때문이다.[65] 그동안에도 테러조직이나 사이버 범죄조직과 같은 비국가행위자들의 국가 기반시설에 대한 사이버공격에 대한 우려가 제기된 바 있다.[66] 그러나 현재

---

62) The New York Times, May 12, 2017, "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool", <https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html> (2017.9.13.최종방문).

63) 이데일리, "사상 최대 랜섬웨어 테러…100여개국서 10만건 이상 피해", 2017년 5월 14일, <http://www.edaily.co.kr/news/NewsRead.edy?SCD=JH41&newsid=02099206615928920&DCD=A00804&OutLnkChk=Y> (2017.9.14.최종방문).

64) 이터널 블루는 윈도 취약점 중 SMB(Server Massage Block) 프로토콜을 사용하는 해킹 기법이다. SMB는 컴퓨터에서 파일을 공유하기 위한 통신프로토콜인데, 한 대의 컴퓨터가 감염되면 같은 네트워크로 연결된 컴퓨터는 파일을 내려 받지 않더라도 감염될 수 있으며, 감염된 컴퓨터는 또 다른 장치에 이를 퍼뜨려 확산시키게 된다.

65) The New York Times, May 12, 2017, "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool", <https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html> (2017.9.13.최종방문). 이에 대해 미국 정부가 공식적으로 확인한 바는 아직 없다.

66) 2000년대 초반에는 테러 조직이 목표 국가의 주요 기반시설에 대해 사이버공격을 시도한 흔적이 확인된 사례나 이에 대해 상당한 흥미를 갖고

까지 ISIS 나 알카에다와 같은 테러조직에 의한 대규모 사이버공격이 발생한 바가 없고[67], 오히려 이들의 활동 양상이 인터넷을 연락망으로 사용해 물리적 공간에서 소프트 테러를 자행하는 형태를 띠면서[68] 그러한 우

있다는 내용이 보고되면서 테러조직의 사이버공격에 대한 우려 및 이에 대한 논의가 촉발된 바 있었다. 그러한 예로 2002년 1월 미국의 National Infrastructure Protection System(NIPC)은 알카에다가 미국의 수도 및 폐수처리시설을 운영하는 SCADA 시스템에 대해 관심을 가지고 있다고 발표한 바 있다. 또 이듬해에는 미 정보기관의 관계자는 해당기관이 확보한 알카에다의 시스템에서 알카에다가 9/11테러 이후 미국의 기반시설을 정찰한 증거를 확보하였다고 밝히기도 하였다. 현재는 와해된 영국 런던 기반의 조직 Jaish al-Muhajireen wal-Ansar의 창시자 Sheikh Omar Bakri Muhammad는 2002년 영국의 주식시장에 대한 사이버공격을 경고한 일도 있었다. National Infrastructure Protection Centre, "Terrorist interest in Water Supply and SCADA Systems", Information Bulletin 02-001, Jan. 29, 2002, <http://www.mrws.org/Terror/Bulletin.html> (2018.1.4.최종방문); Cyber Warfare Frontline, Mountain View, PBS(2003), <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/clarke.html> (2018.1.4.최종방문); Verton D., "Bin Laden Cohort Warns of Cyberattacks", Computer Crime Research Center (2002), <http://www.crime-research.org/news/2002/11/Mess2002.htm> (2017.9.13.최종방문).

67) Thomas M. Chen, *Cyberterrorism after Stuxsnet* (U.S. Army War College Press, 2014), p. 20.

68) ISIS는 주로 웹사이트 및 온라인 매거진 운영과 함께 트위터, 인스타그램, 페이스 북 등 소셜미디어를 활용하여 양방향 소통 방식을 통해 자신의 구호를 전파하는 방식으로 사이버공간을 활용하고 있다. Lisa Blaker, "The Islamic State's Use of Online Social Media", The Journal of the Military Cyber Professionals Association, Vol. 1, No. 1 (2015), pp. 1-9; 한편 알카에다는 주로 정보를 전달하고 익명으로 만나는 장소로 인터넷공간을 활용하고 있다. Christina Schori Liang, "Cyber Jihad: Understanding and Countering Islamic State Propaganda", Geneva Centre for Security Policy, No. 2 (2015), p. 2. 즉, 이들 테러조직은 사이버공간 내에서 네트워크 공격을 통해 테러를 감행하지 않고, 인터넷공간을 전통적인 테러를 효과적으로 수행하기 위한 수단으로 활용하고 있다. 이와 같은 테러조직의 인터넷 사용은 사이버공격과는 구분하여 보아야 한다.

려는 점차 줄어들고 있었다.

사이버 범죄조직의 경우에도 국가를 배후에 두지 않은 경우에는 타국의 기반시설을 침투하여 공격하는 것이 쉽지 않기 때문에 단독으로 국가안보를 위협하는 수준의 공격을 감행할 가능성이 낮은 것으로 예상되고 있었다.[69] 그러나 최근의 워너크라이 랜섬웨어 공격사건은 타국의 기반시설만을 목표로 한 공격(Targeted Attack) 방식이 아니라 전 세계의 시스템에서 사용하고 있는 소프트웨어의 취약점을 이용하여[70] 불특정 다수의 컴퓨터를 무차별적으로 공격함으로써, 개인의 컴퓨터뿐 아니라 각국의 기반시설을 동시다발적으로 무력화시킬 수 있다는 것을 보여주었다.

또 한 가지 중요한 점은 여기에 사용된 공격 툴이 한 국가의 정보기관이 고도로 제작한 사이버무기를 해커조직이 해킹 했다는 것이다. 이를 종합하면 해킹 능력을 갖춘 테러조직이나 사이버 범죄조직이 국가의 지원을

---

69) 그동안 사이버 범죄조직이 연루된 것으로 알려진 2007 에스토니아 DDoS 공격사건, 2008년 그루지야 사이버공격사건 등은 러시아의 지원을 받은 정황이 상당수 드러난 바 있다. Wired, Mar. 11, 2009, “Kremlin Kids: We Launched the Estonian Cyber War”, <https://www.wired.com/2009/03/pro-kremlin-gro/> (2018.1.4. 최종방문); Jeffrey Carr, *Inside Cyber Warfare* (O’Reilly, 2010), p. 117; The Telegraph, Aug. 11, 2008, “Georgia: Russia 'conducting cyber war'”, <http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html> (2018.1.4. 최종방문); 대규모의 피해를 가져오는 사이버공격에는 정교한 기술과 상당한 비용이 필요하다는 논의는 Giampiero Giacomello, “Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism“, Studies in Conflict & Terrorism, Vol. 27 (2004), pp. 396-399; Thomas M. Chen, *supra* note 67, p. 23 참조.

70) PC World, May 15, 2017, “Microsoft blames U.S. stockpiled vulnerability after WannaCry ransomware attack”, <https://www.pcworld.com/article/3196523/security/microsoft-blames-us-stockpiled-vulnerability-for-ransomware-attack.html> (2017.10.30.최종방문).

통해 정교한 시스템을 개발하지 않고도, 해킹을 통해 획득한 사이버무기로 위협적인 사이버공격을 감행할 수 있다는 결론에 이르게 된다. 이는 국제법이 더 이상 국가를 배후에 둔 비국가행위자에게만 집중할 것이 아니라 국가와 연관되어 있지 않은 사이버 범죄조직과 같은 비국가행위자에 대한 규율 방안을 모색하는 것이 시급하다는 점을 시사한다.[71] 워너크라이 랜섬웨어 공격은 또한 사이버공격에 대응하기 위해서는 국가간 의 협조를 통한 국제공조가 필수적임을 보여준 사건이기도 하다.

한편 국가안보를 위협하는 사이버공격은 대규모로 수행되거나 물리적

---

71) 한편 미국과 영국은 2017년 12월 워너크라이 공격의 배후가 북한이라고 지목하였다. 미 당국자는 북한을 배후로 지목하는 것이 증거에 기반한 것이라고 하였으나 이에 관한 증거는 공개되지 않았다. The Guardian, Dec. 19, 2017, “Facebook action hints at western retaliation over WannaCry attack”, <https://www.theguardian.com/technology/2017/dec/19/wannacry-cyberattack-us-says-it-has-evidence-north-korea-was-directly-responsible> (2018.1.20.최종방문); 그러나 워너크라이 공격의 배후가 북한이라는 데 대해서는 전문가들의 의견이 나뉘고 있다. 미국은 소니해킹을 감행한 Lazarus 그룹이 사용한 멀웨어의 소스코드가 워너크라이 공격에 사용된 것과 유사하다는 이유로 북한을 배후로 지목한 것으로 추정되나, 현재까지 Lazarus 조직과 북한과의 연계성이 밝혀진 바 없으며, 워너크라이 공격으로 가장 피해를 본 두 국가가 북한의 우방인 중국과 러시아라는 점, 북한이 주도한 것으로 추정된 과거 사이버공격과 스타일이 완전히 다르다는 점 등을 근거로 북한을 배후로 추정하는 것은 무리가 있다고 전문가들은 보고 있다. Dailymail, May 19, 2017, “Was North Korea responsible for WannaCry? Experts say the hacks would be 'an anomaly' for the rogue nation state”, <http://www.dailymail.co.uk/sciencetech/article-4521746/Experts-question-North-Korea-role-WannaCry-cyber-attack.html> (2018.1.19.최종방문); DarkReading, Dec. 20, 2017, “Attack Attribution Tricky Say Some as US Blames North Korea for WannaCry”, <https://www.darkreading.com/attacks-breaches/attack-attribution-tricky-say-some-as-us-blames-north-korea-for-wannacry-/d/d-id/1330688?> (2018.1.20.최종방문).

영향력을 가져오는 것에만 국한되는 것은 아니다. 그러한 예로 2016년 미국의 민주당 전국위원회의 이메일 해킹 및 공개를 통한 대선개입의혹 사건[72]을 들 수 있다. 해당 사건에서의 이메일 해킹 행위는 비록 국가의 주요기반시설에 대한 물리적인 파괴나 인명의 살상을 가져오지는 않았으나, 여론조작 시도를 통해 타국의 정권교체에 영향력을 행사함으로써 국내문제 전반에 영향을 미친 경우이다. 이 사건의 배후로 지목된 러시아는 친러성향의 트럼프 당시 후보자의 당선을 위해 힐러리 클린턴의 이메일을 해킹해 공개함으로써 대선결과에 영향력을 행사했다는 의혹을 받고 있다. 정치·경제·사회 제도 및 정책에 대한 자유로운 선택은 한 국가의 주권사항이며, 사이버공격을 통한 타국 대선에의 개입은 국내문제 불간섭 의무에 대한 중대한 위반을 구성할 수 있다.[73]

이렇게 볼 때 국가안보에 위협이 되는 사이버공격은 기반시설에 대해 물리적 파괴를 가져오는 사이버공격과 물리적 영향을 미치지 않는 네트워크상의 공격 모두를 포함한다는 것을 알 수 있다. 따라서 국가에 대한 사이버공격이 국가안보에 위협이 되는 지 여부는 공격에 사용된 특정 형태의 사이버무기나 유형이 아니라 문제의 공격이 일국에 미치는 영향과 결과를 중심으로 판단해야 한다.

2. 사이버공격과 국가안보

제1절에서 사이버공격은 정보통신 기술을 사용하여 정치적·사회적·경제적 혼란을 야기할 목적으로 위해를 가하는 행위라고 정의 한 바 있다. 국

72) The New York Times, Sept. 14, 2016, “Sowing Doubt Is Seen as Prime Danger in Hacking Voting System”, <http://www.nytimes.com/2016/09/15/us/politics/sowing-doubt-is-seen-as-prime-danger-in-hacking-voting-system.html> (2017.4.28.최종방문).

73) 해당 사건에 대한 자세한 분석과 국내문제불간섭원칙 위반여부는 제3장에서 후술하기로 한다.

가들은 사이버공격이 자국의 안보에 위해를 가하기 때문에[74] 이에 대한 국제법의 규율이 필요하다고 인식하고 있다. 그 이유는 국가안보에 영향을 미치는 대부분의 사이버공격이 자국의 국경 밖에서 발생한 것이기 때문이다.[75] 사이버공격의 이러한 초국가적 특성[76] 때문에 국내의 법집행기관은 관할권의 한계로 이에 대한 대응에 제한을 받을 수밖에 없고, 각국의 사이버 범죄에 대한 규정이 달라 범죄인 인도 등의 국가 간 협조 절차도 제대로 이루어지지 않고 있다.[77]

국가들이 자국의 안보에 위협이 되는 사이버공격으로 인식하고 있는 것은 주로 주요기반시설에 대한 공격이다.[78] 한 국가의 주요기반시설은 여러 국가가 하나의 네트워크를 공유하여 운영되는 경우가 증가하고 있고,[79] 핵발전소와 같은 주요 기반시설의 건설을 타국 기업에 맡기는 경우도 많기 때문에[80] 이에 대한 타국발 사이버공격의 위험은 더욱 커질 수밖

74) National Cyber Security Center, "The Cyber Threat to UK Business-2016/2017 Report" (2017), p. 17.

75) James R. Clapper, Marcel Lettre and Michael S. Rogers, "Joint Statement for the Record to the Senate Armed Services Committee Foreign Cyber Threats to the United States" (2017); The Times, Feb. 12, 2017, "Russia steps up cyber-attacks on UK", <https://www.thetimes.co.uk/article/russia-steps-up-cyber-attacks-on-uk-rl262pnlb> (2017.9.25.최종방문).

76) 이승주, "일본의 사이버안보 전략과 외교", 서울대학교 국제문제 연구소 워킹 페이퍼 (2017), p. 2.

77) UK, "National Cyber Security Strategy 2016-2021", HM Government (2016), pp. 18, 63.

78) House of Parliament, "Cyber Security of Cyber Infrastructure", The Parliamentary Office of Science and Technology (2017), p. 1; The Senate Armed Services Committee, "Foreign Cyber Threats to the United States", Homeland Security Digital Library, Naval Postgraduate School, Center for Homeland Defense and Security (2017), p. 4.

79) Single European Sky's ATM Research, "European ATM Master Plan" (2015), p. 2.

80) UK Intelligence and Security Committee, "Foreign involvement in the Critical National Infrastructure-the Implication for National Secrity" (2013), pp. 5-12.

에 없다. 이하에서는 국제사회의 논의 및 각국가의 정책과 법령의 검토를 통해 주요기반시설의 범위와 이에 대한 사이버공격이 어떻게 국가안보에 주요한 위협이 될 수 있는지 살펴본다. 또한 주요기반시설만을 보호 대상으로 규정하는 것이 적절한 사이버안보 범위인지에 대해서도 검토한다.

사이버공격에 대한 국제사회의 논의 및 각국의 사이버안보 전략을 살펴보면 공통적으로 주요기반시설을 국가안보를 위해 보호해야 할 핵심대상으로 다루고 있음을 알 수 있다. 2004년 채택된 사이버안보에 관한 글로벌 문화 창조와 주요 정보 기반시설의 보호에 관한 UN총회 결의(Creation of a global culture of cybersecurity and the protection of critical information infrastructures)[81]는 주요정보기반시설의 보호가 사이버안보에 있어 핵심 전략임을 강조하고 있다. 2013년 유럽안보 협력기구(Organization for Security and Co-operation in Europe, OSCE)가 발간한 비핵 에너지 기반시설에 대한 사이버안보 실행 지침서(Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace)에서는 주요기반시설의 발전이 국가 경쟁력을 유지하기 위해 가장 중요한 요소이며 이의 보호가 국가안보의 핵심사항임을 밝히고 있다.[82]

국내법 규정 중에서는 대표적으로 미국의 Patriot Act를 들 수 있다. 동법 section 1016(e)에서는 주요기반시설(Critical Infrastructure)을 “미국에 중요한 물리적 또는 가상의 시스템 및 자산으로서 그러한 시스템 및 자산의 불능 또는 파괴가 안보, 국가경제, 공중 보건의 각 분야 또는 복수의 분야를 약화시키는 영향을 주는 것을 말한다”[83]고 정의하면서 주요기

81) UN Doc. A/RES/58/199(2004).
82) Action against Terrorism Unit Transnational Threats Department, “Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace”, OSCE (2013), p. 16.
83) USA Patriot Act of 2001 section 1016(e).

반시설의 보호가 국가안보와 불가분의 관계에 있음을 명시하고 있다. 이밖에도 미국[84], 콜롬비아[85], 독일[86], 일본[87], 오스트리아[88], 이탈리아[89], 노르웨이[90], 스위스[91], 터키[92], 호주[93], 사우디아라비아[94]와 같은 국가들의 사이버안보 전략에서도 주요기반시설의 보호가 국가안보의 핵심요소임을 강조하고 있다.

그렇다면 여기에서 말하는 주요기반시설은 무엇을 의미하는가? 국가기반시설의 지정과 보호를 위한 EU 지침(Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection)에서는 국가기반시설을 다음과 같이 정의하고 있다; "회원국에 위치한 자산, 시스템 또는 이의 일부로서 주요 사회 기능, 건강, 안전, 보안, 경제적 또는 사회적 안녕의 유지에 필수적이며, 이에 대한 방해나 파괴가 이들 자산, 시스템 또는 그 일부 기능 유지 실패를 초래하여 회원국에 중대한 영향을 주는 것을 말한다."[95]

---

84) United States of America, "Framework for Improving Critical Infrastructure Cybersecurity", NIST (2014), p. 37.
85) Colombia, "Policy Guidelines for Cybersecurity and Cyberdefense (Lineamientos de politica para la Ciberseguridad y Ciberdefensa)" (2011), p. 39.
86) Germany, *supra* note 28, p. 15.
87) Japan, "The First National Strategy on Information Security" (2006), p. 11.
88) Austria, *supra* note 30, p. 20.
89) Italy, "2013 National Strategic Framework for cyberspace security " (2013), p. 42.
90) Norway, Cyber Security Strategy for Norway" (2012), p. 28.
91) Switzerland, *supra* note 32, p. 6.
92) Turkey, "National Cyber Security Strategy and 2013-2014 Action Plan" (2013), p. 9.
93) Australia, "Cyber Security Strategy" (2009), p. 20.
94) Saudi Arabia, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia" (2013), p. A-1.
95) EU Directive on the identification and designation of European

2014년 사이버안보와 개인 데이터 보호에 관한 아프리카 연합 협약(African Union Convention on Cyber Security and Personal Data Protection)[96] 제1조는 "주요 사이버 또는 정보통신기술 기반시설은 공공안전, 경제적 안정, 국가안보, 국제적 안정을 위해서 또한 주요 사이버공간의 지속성 및 회복(restoration)을 위해 필수적인 서비스를 의미한다."고 사이버 기반시설을 정의하고 있다. 한편 탈린매뉴얼에서도 앞의 정의들과 유사하게 주요기반시설을 정의하고 있는데, "국가의 관할권 하에 있는 물리적 또는 가상의 시스템 및 자산으로서 그 중요성으로 인해 이를 무력화하거나 파괴하는 것이 국가안보, 경제, 공공보건 또는 안전, 또는 환경을 약화시키는 것"으로 보고 있다.[97]

국내 법규정을 보면 주요기반시설이 구체적으로 어떤 부분을 지칭하는지 좀 더 명확하게 알 수 있다. 특히 미국의 경우 주요기반시설 분야를 선정하여 명시하고 있다. 오바마 대통령은 2013년 주요기반시설 사이버안보 증진을 위한 대통령 행정명령[98]에 서명하면서 주요기반시설 보안 및 복원에 관한 대통령 정책지침 21(Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience)[99]에도 함께 서명하였다. 이 지침에서는 행정명령의 이행을 돕기 위해 16개의 주요

Critical Infrastructure and the assessment of the need to improve their protection (2008/114/EC), 제2조 a호.

96) 2014년 6월 27일 채택되었고, 현재까지 서명국은 8개국이며 아직 발효하지 않은 조약이다, <http://www.au.int/en/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf> (2018.1.4.최종방문).

97) NATO CCD COE, *supra* note 20, p. 258.

98) Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013).

99) Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience (2013), <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> (2018.1.4.최종방문).

기반시설 분야를 선정하고 있는데, 여기에는 에너지부문, 금융서비스부문, 정부시설부문, 정보통신기술부문, 상수도 시스템 부문, 교통시스템 부문, 상업 시설 부문 등이 포함되어있다.[100] 이 16개 분야의 주요기반시설은 2013년 발의된 사이버 국가안보 및 주요기반시설 보호법안(National Cybersecurity and Critical Infrastructure Protection Act of 2014)에도 그대로 포함되어 있다.[101]

한편 독일의 중앙안보국법(German Central Security Agency Act) 제2조 제10항에서는 주요기반시설에 대해 “이러한 분야의 시설 및 장치를 방해하는 것은 공공시설 또는 공공안전에 중대한 영향을 미친다. 관련 분야로는 에너지, 정보기술, 통신, 운송, 교통, 보건, 수자원, 식품, 금융 및 보험이 있다.”고 정의하고 있다.

이렇게 주요기반시설이 사이버공격과 밀접하게 연관되어 있는 이유는 대부분의 국가기반시설이 스카다(Supervisory Control and Data Acquisition (SCADA))시스템에 의해 운영되고 있기 때문이다.[102] 스카다 시스템은 산업제어시스템(Industrial Control Systems, ICS)을 기반으로 하는 작업공정을 감시·제어하는 컴퓨터 시스템을 말한다. 이 시스템의 운영원리는 다음과 같다. 우선 SCADA서버가 PLC(Programmable Logic Controller)[103], 원격 단말 장치(Remote Terminal Unit : RTU)[104]를 통

---

100) 16개 분야와 설명에 대해서는 <https://www.dhs.gov/critical-infrastructure-sectors> 참조 (2018.1.4.최종방문).

101) National Cybersecurity and Critical Infrastructure Protection Act of 2014 제227조 b호. 이 법안은 미국의 주요기반시설에 대한 사이버공격이 가장 핵심적인 국가안보 위협이 될 것이라는 국가안보 전문가들의 경고에 따라 이에 대비하기 위해 만들어진 법안으로 사이버공격에 대한 국가적 조치(제101조-제108조)와 사이버안보를 위한 민·관 협력체계(제201조-제204조)에 대해 규정하고 있었다. 그러나 해당 법안은 2014년 7월 하원을 통과하였으나 상원에서 부결되어 폐지되었다.

102) Nicholson A, Webber S, Dyer S, Patel T, Janicke H, “SCADA security in the light of Cyber-Warfare”, Computers & Security Vol. 31 (2012), pp. 419-420.

해 원격지에 위치해 있는 각종 정보를 수집하여 이를 네트워크로 연결된 정보처리 시스템으로 전송한다. 모니터링 및 제어시스템과 데이터베이스를 갖추고 있는 정보처리시스템은 전송된 자료값을 분석하고 제어하여 각종 설비를 효과적으로 운영하게 되는 것이다.[105] 스카다시스템은 우리나라의 한국전력공사, 수자원공사, 원자력 발전소 등의 국가기간산업을 운영하는 데도 사용되고 있다.[106] 이 시스템은 외부와의 네트워크 연결을 하지 않는 특징을 가지고 있어 보안이 뛰어나다고 알려졌으나 최근 다수의 현장에서 관리를 목적으로 셀 무선 통신망을 이용하고, 최종 소비자에게 데이터 전달 등의 목적으로 인터넷과 연동을 하는 사례가 많아지고 있다.[107]

이렇게 스카다 시스템과 인터넷, 사내 네트워크 간 연결이 증가하고 있는 현상은 스카다 시스템을 기반으로 하는 기반시설들이 사이버공격에 취약해진다는 것을 의미한다.[108] 또한 최근에는 인터넷에 연결되어 있지 않은 시스템에 대해서도 접근하여 폐쇄망을 우회할 수 있는 공격기술이 다수 개발되어 있는 것으로 알려지면서 그 위험성은 더욱 증가하고 있다.[109] 에어갭[110]은 더 이상 사이버공격으로부터의 안전을 보장해 주지 못하게 된 것이다. 2008년 BTC 파이프라인 사건, 2010년 스턱스넷 이란 원전시설 공격사건 모두 에어갭을 극복하고 스카다 시스템을 공격하여 일어난

---

103) 자료를 근거리통신망을 통해 중앙센터로 보내는 장치로 미리 프로그램된 순서에 따라 설비를 제어한다.

104) 원격감시를 위하여 현장에 설치하는 장치로 현장에서 취득한 정보를 모뎀을 통해 중앙센터로 보낸다. 원거리 감시제어에 사용된다.

105) Nicholson A, Webber S, Dyer S, Patel T, Janicke H, *supra* note 102, pp. 419-420.

106) 전자신문, "국가기간망 해킹, 대책마련 시급", 2017년 2월 7일, 27면.

107) SecurityFocus, Jul. 26, 2007, "SCADA system makers pushed toward security", <http://www.securityfocus.com/news/11402> (2086.1.4.최종방문).

108) *Ibid.*

109) 중앙일보, "인터넷 연결 안해도 해킹하는 방법은?", 2017년 1월 4일, <http://news.joins.com/article/21076038> (2017.4.19.최종방문).

110) 에어갭 네트워크는 외부의 인터넷과는 완전히 분리된 네트워크를 구축하고 운영되는 방식을 의미한다.

사건이었다. 이를 통해 스카다 시스템이 각국의 안보를 지키기 위한 핵심 영역으로 분류되고 있는 이유를 알 수 있다.

그러나 국제문서나 국내법 규정, 정책 전략에서 규정하고 있는 주요기반시설이 사이버공격으로부터 국가안보를 지키기 위해 필수적인 모든 분야를 포괄하고 있는 것은 아니다. 그 예로는 언론기관을 들 수 있다. 에스토니아 사건이나 그루지야 사건을 통해 볼 수 있듯이 언론기관에 대한 공격은 국가를 국제사회로부터 고립시킬 뿐 아니라 국민들을 고립과 혼란 상태에 빠지도록 만들 수 있다. 또한 2013년 연합뉴스 트위터 계정 탈취와 같이 해킹을 통해 언론 조작이 일어날 경우 사회적 혼란 및 국가경제에의 큰 타격이 발생할 수도 있다.[111] 언론기관에 대한 사이버공격은 그 강도에 따라 국가전체를 혼란에 빠뜨릴 수 있다는 점에서 국가안보에 위협이 되는 공격으로 분류할 수 있다. 한편 이 밖에도 규율이 필요한 범위 안에 명시적으로 포함시키기 어려운 부분도 분명히 존재한다. 그 대표적인 예로는 미국의 민주당 전국위원회의 이메일 해킹사건을 생각해 볼 수 있다. 결과적으로는 해킹행위가 일국의 주권사항에 영향을 미친 국제법위반행위에 해당하지만 개인의 이메일까지 규율범위에 명시적으로 포함시킬 수는 없기 때문이다.

지금까지의 논의를 종합해 보면, 국가들은 국가안보에 위협을 주는 강도의 사이버공격을 주요 국가기반시설에 대한 공격으로 보고 이에 대한 보호를 최우선순위로 설정하고 있음을 알 수 있다. 이에 주요국가기반시설과 사이버안보, 그리고 국가안보의 관련성을 살펴보았다. 그러나 안보에 위협을 주는 사이버공격이 규정에 명시된 주요기반시설에 대한 공격에만 국한

111) 해커집단 The Syrian Electronic Army (SEA)는 2013년 4월 연합통신의 트위터 계정을 탈취하여 백악관이 공격당했다는 거짓 메시지를 게재했으며, 이로 인해 다우존스 지수가 143포인트 하락하는 등 막대한 경제적 손해가 초래된 바 있다. The Guardian, April 23, 2013, “AP Twitter hack causes panic on Wall Street and sends Dow plunging”, <https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall>, (2017.9.15.최종방문).

되는 것이 아닌바, 그 외의 경우에 대한 가능성도 열어두고 국제법 및 국가차원에서 어떻게 대응할 지에 대한 논의가 필요하다.

제3장 국제법체제의 적용과 한계

제1절 국제법의 적용을 위한 기준설정과 문제점

현행 국제법이 사이버공격에 적용 가능한지 여부에 관한 논의는 어떠한 유형 및 강도의 사이버공격이 일반국제법상의 원칙에 위반되는지를 판단하는 문제와 관련이 있다. 국제법체제는 물리적 공간에서의 행위를 기반으로 형성되었기 때문에 기존의 판단 기준이 사이버공격의 경우 어떻게 적용되는지와 관련해서는 사이버공간의 특성을 반영한 검토가 필요하다. 특정강도의 사이버공격이 국제법상의 의무 중 어떤 의무의 위반에 해당하느냐에 따라 대응의 강도가 달라질 수 있기 때문에 명확한 기준설정의 문제는 특히 중요하다고 할 수 있다. 이하에서는 지금까지 적용되어 온 국제법상의무 위반의 판단기준에 대해 살펴보고, 이를 구체적인 사이버공격 사례에 대입하여 현행 국제법의 적용을 위한 기준설정 문제를 논의한다. 또한 사이버공격에 적용될 수 있는 분야의 조약과 구체적인 조항에 대해서도 검토한다. 논의의 말미에는 일반국제법상의 원칙 및 조약의 적용성에 관한 논의가 사이버공격의 규율에 있어 어떠한 함의를 가지는지를 진단하고, 현행 국제법의 적용만으로도 사이버공격의 문제가 효과적으로 규율될 수 있는지에 대해서 검토한다.

1. 일반국제법상의 원칙

1) 무력사용금지원칙

사이버공격이 전통 국제법 하의 무력사용에 해당하느냐의 문제는 국제법에서 사이버안보를 다루기 시작하면서부터 현재까지 논의의 핵심을 차

지하여 왔다.[112] 이에 관한 논의는 또한 피해국이 사이버공격에 대해 취할 수 있는 대응조치의 범위를 정하는 것과도 관련이 있기 때문에 중요한 의의가 있다. 현 국제법체제에서는 비무력적 대응조치만을 허용하고 있기 때문이다.[113] 만약 일부 사이버공격이 무력사용 또는 무력공격으로 간주될 수 있다면 사이버공격은 무력사용에 이르지 않는 행위, 무력사용에는 해당

112) Antolin-Jenkins, "Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?", Naval Law Review, Vol. 51 (2005); Jason Barkham, "Information Warfare and International Law on the Use of Force", New York University Journal of International Law & Politics, Vol. 34 (2001); Matthew Hoisington, "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense", Boston College International & Comparative Law Review, Vol. 32, No. 2 (2009); Eric Talbot Jensen, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense", Stanford Journal of International Law, Vol. 38 (2002); Jay P. Kesan and Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace", Harvard Journal of Law & Technology, Vol. 25, No. 2 (2012); Sheng Li, "When Does Internet Denial Trigger the Right of Armed Self-Defense?", The Yale Journal of International Law, Vol. 38, No. 1 (2013); Herbert S. Lin, "Offensive Cyber Operations and the Use of Force", Journal of National Security Law & Policy, Vol. 4 (2010); Marco Roscini, "World Wide Warfare - Jus ad bellum and the Use of Cyber Force", Max Planck Yearbook of United Nations Law, Vol. 14 (2010); Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", Columbia Journal of Transnational Law, Vol. 37 (1999); Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited", Villanova Law Review, Vol. 56, No. 3 (2011); Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent* (US Navy Office of the Judge Advocate General, 2009); ; Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", The Yale Journal of International Law, Vol. 36, No, 2 (2011).

113) 2001년 국제위법행위에 대한 국가책임에 관한 규정초안 제50조 제1항 a호.

하나 무력공격에는 미치지 못하는 행위, 무력공격에 이르는 행위 세 종류로 분류할 수 있다.[114]

UN헌장 제2조 제4항에 규정되어 있는 무력사용금지원칙은 모든 UN회원국이 국제관계에서 무력을 사용하거나 무력으로 위협하는 것을 금지하고 있다. 이 원칙은 1970년 UN헌장에 따른 국가 간 우호관계 및 협력에 관한 국제법원칙의 선언 등과 같은 국제문서에서 확인된바 있다.[115] 또한 ICJ는 1986년 니카라과 사건에서 무력사용금지원칙이 관습국제법으로 확립되었음을 확인한 바 있다.[116] 따라서 무력사용금지원칙은 UN회원국 뿐 아니라 비회원국에 대해서도 적용된다. 또한 제2조 제4항의 문언을 볼 때, 일국의 영토적 보전 또는 정치적 독립을 해하는 무력사용 뿐 아니라 헌장의 목적과 양립하지 않는 방식의 무력에 의한 위협 또는 무력사용을 금지하고 있으므로 모든 무력에 의한 위협 또는 무력사용의 불법성을 규정하는 것이 그 목적임을 알 수 있다.[117]

이 원칙을 적용하기 위해서는 force의 의미를 명확히 하는 것이 중요하다. 헌장에는 force의 정의가 나와 있지 않기 때문에 이의 정확한 의미에 대해서는 논쟁이 있다. 즉 여기서 말하는 force가 무력(armed force) 사용만을 의미하는지 아니면 경제적 또는 정치적 압력과 같은 다른 형태의 강제(coercion)도 포함하는 것인가에 관하여 주장이 일치하지 않는 것이다. 이는 제2조 4항에서는 어떤 수식어 없이 force를 사용하거나 force의 위협을 금지하고 있는데 따른 것이다.[118] 그러나 헌장의 전문 및 다른 규

---

114) Eric Talbot Jensen, *supra* note 112, p. 222.

115) Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations, UN Doc. A/RES/2625 (1970).

116) *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgement, I.C.J. Reports 1986*, para. 188.

117) NATO CCD COE, *supra* note 20, pp. 43-44.

118) Bruno Simma, Daniel-Erasmus Khan Gerog Nolte and Andreas Paulus (eds.), *The Charter of the United Nations: A Commentary* 3rd

정인 제41조, 제44조 및 제46조에서는 armed force라는 용어를 명시하고 있다. 개발도상국 및 구 동구권 국가들은 헌장 제2조 제4항에서 force가 armed force와 같이 특정되어 있지 않다는 이유로 헌장 제2조 제4항이 금지하고 있는 use of force에는 경제적 또는 정치적 강제도 포함되는 것이라고 반복하여 주장한 바 있다.[119]

그러나 1945년 헌장초안 작성을 위한 샌프란시스코 회의에서 force의 개념에 경제적 강제(economic measure)도 포함시키자는 브라질의 제안은 명확하게 거부된 바 있다.[120] 또한 1969년 비엔나 협약 제31조의 조약해석 원칙을 적용해 볼 때, 조약문의 문맥은 조약문에 추가하여 조약의 전문 및 부속서 등을 포함한다. 따라서 제2조 제4항은 헌장의 목적을 천명하고 있는 전문과 조화롭게 해석해야 한다. 헌장전문에서는 "공동이익을 위한 경우 이외에는 무력(armed force)을 사용하지 않는다는 것을 결의"하고 있다. 헌장의 규정들은 전문의 염원을 법적 효력이 있는 조항으로 구체화 시킨 것이라고 할 때, 결코 전문에서 의도한 바보다 그 범위가 더 클 수는 없다. 따라서 제2조 제4항의 force가 armed force 보다 더 광범위한 의미를 포함하고자 했다면 전문에서 결코 'armed' force라는 용어를 사용하지는 않았을 것이다. 또한 제41조와 제46조에서 armed force라는 용어를 사용한 것은 제2조 제4항의 force와 armed force를 구분하려는 의도가 아니다.[121] 제41조와 제46조에서 말하는 armed force는 헌장 제7장의 체제 안에서 평화에 대한 위협, 평화의 파괴 또는 침략행위에 대하여 안보리가 취할 수 있는 여러 조치 중 하나의 선택사항으로 규정되어 있는 것이다. 즉, 제41조 및 제46조에서 말하는 armed force는 문맥상 강제(coercion)조치의 연속선상에서 특정 부분을 지칭하는 것이다.[122] 반

---

ed. (Oxford Universith Press, 2012), pp. 208-209

119) *Ibid.*

120) UNCIO (Documnents of the United Nations Conference on International Organization San Francisco, 1945) Volume VI, pp. 334, 609.

121) Michael N. Schmitt, *supra* note 112, p. 905.

122) *Ibid.*

면 헌장 제2조 제4항에서는 force, 무력 자체를 금지하고 있다. 따라서 'armed'라는 수식어가 붙지 않았다고 해서 이를 armed force 이외의 경제적 또는 정치적 강제도 포함하는 것으로 보는 것은 헌장의 전체적인 문맥을 고려하지 않은 해석이라고 할 수 있다.

따라서 지금까지 헌장 제2조 제4항의 force는 경제적·정치적 강제를 포함하지 않는 개념으로 해석되어 왔다.[123] 이와 같은 이유로 탈린매뉴얼의 저자들은 경제적 타격을 주거나 정치적으로 혼란 등을 일으키는, 즉 물리적 파괴를 수반하지 않는 사이버공격은 국제법상 금지된 무력사용으로 볼 수 없다고 보았다.[124] 그러나 기존의 논의에서 언급되었던 경제적·정치적 강제와 경제적 손실을 가져오는 사이버공격을 같은 선상에 놓고 평면적으로 해석하는 것은 바람직하지 않다. 경제적 손실을 일으키는 사이버공격은 시스템의 무력화나 시스템 파괴를 동반할 수도 있고, 이는 국가의 주요 기반시성을 손상 또는 파괴시키는 행위에 해당하기 때문이다. 따라서 금수조치로 인한 국가경제의 손해와는 다른 차원에 해당한다고 볼 수 있다.

그러한 예로 사우디 석유기업 Aramco에 대한 Shamoon 바이러스 공격을 들 수 있다. 샤문 바이러스는 감염된 시스템으로부터 정보를 빼내 외부서버로 옮기고, 모든 정보를 내부시스템에서 삭제했다.[125] 이 공격으로 사우디 아람코는 컴퓨터 시스템의 4분의 3에 달하는 3만 5천여 개의 하드디스크가 완전히 손상되는 피해를 입었다.[126] 아람코는 단순히 업무중단으로 인한 경제적 피해를 입었을 뿐 아니라 더 이상 기존의 시스템 사용이

---

123) Bruno Simma, Daniel-Erasmus Khan Gerog Nolte and Andreas Paulus (eds.), *supra* note 118, p. 209.
124) NATO CCD COE, *supra* note 20, p. 46.
125) Symantec, Aug. 16, 2012, "The Shamoon Attacks", <http://www.symantec.com/connect/blogs/shamoon-attacks> (2017.1.14.최종방문).
126) CNN, Aug. 15, 2015, "The Inside Story of the Biggest Hack in History", <http://money.cnn.com/2015/08/05/technology/aramco-hack/> (2017.1.14.최종방문).

불가능해 이를 교체·복구하는 데 5개월이라는 시간이 걸렸다.[127] 물론 아람코는 이 사건으로 스턱스넷 사건에서 핵원심분리기의 작동불능이 일어난 것처럼 석유 생산의 가동이 중단되는 피해까지 입지는 않았다.[128] 그러나 기업 시설의 상당부분을 교체해야 할 정도의 하드디스크의 파괴를 단순히 전통적 개념의 경제적 강제로 분류하는 것은 문제가 있다. 한 국가에 대한 금수조치가 그 국가의 기반시설의 마비나 파괴를 가져오지는 않기 때문이다. 반면 피해의 수준만을 놓고 비교해 봤을 때 재래식 무기를 사용한 무력의 사용은 시설의 파괴로 이어지고, 이를 복구하는 데 상당한 시일이 걸린다는 점에서 국가전체의 네트워크를 마비시키는 DDoS공격, 시스템을 아예 파괴 시키는 멀웨어(malware)[129] 공격과 상당히 유사하다는 점을 알 수 있다.

Yaroslav Radziwill은 금수조치나 경제적 제재와 같은 경제적 강제는 시간과 범위에 있어 사이버공격과 차이가 있다고 지적하였다.[130] 즉,

---

127) Martha Finnemore, Duncan B. Hollis, “Constructing Norms for Global Cyber Security”, American Journal of International Law (2016), p. 3.

128) CNN, Aug. 15, 2015, “The Inside Story of the Biggest Hack in History”, <http://money.cnn.com/2015/08/05/technology/aramco-hack/> (2017.1.14.최종방문).

129) 악의적인을 뜻하는 malicious와 software가 결합된 말로 악성소프트웨어라고 부르기도 한다. 악의적인 목적을 위해 작성된 실행 가능한 악성 코드 또는 악성 프로그램. 멀웨어는 가장 광범위한 개념이며 자기 복제 능력과 감염 대상 유무에 따라 바이러스, 웜, 트로이목마, 스파이웨어 등으로 분류된다. 첨부파일을 열어 보거나, 소프트웨어를 다운받아 설치하는 기존의 통념을 벗어나 단지 검색 페이지의 링크나 이미지를 클릭하기만 해도 원치 않는 소프트웨어가 설치되거나, 시스템이 해킹 당할 수 있어 주의를 요한다. 한국정보통신기술협회 정보통신용어사전, <http://word.tta.or.kr/dictionary/dictionaryView.do?word_seq=048360-2> (2018.1.3.최종방문).

130) Yaroslav Radziwill, *Cyber-Attacks and the Exploitable Imperpections of International Law*, (Brill Nijhoff, 2015), p. 135.

1973년 중동국가에 의한 석유파동과 같은 경제적 강제는 국민들에게 직접적 영향을 미치기까지 시간이 걸리고, 국가원수나 국가기관에 대한 자산동결과 같은 제재는 국민들에게 직접 영향을 미치는 조치가 아니라는 것이다.[131] 반면, 사이버공격의 효과는 즉각적이고, 이로 인한 시스템 마비 또는 파괴는 민간에 직접적인 영향을 미친다는 점에서 차이가 있다. Schmitt도 사이버공격이 무력사용에 해당하는지를 판단하는 기준 8가지에 대해 이야기하면서 신속성(immediacy)과 직접성(directness)을 제시한 바 있다.[132] Yaroslav Radziwill는 또 모든 경제적 및 정치적 조치를 헌장 제2조 제4항의 범위에서 제외시키는 것은 사이버전에 있어 법적인 모호성을 악용하도록 용인하는 것이라고 하였다.[133] 이렇게 볼 때, 전통적인 개념의 경제적·정치적 강제와 경제적 피해를 야기하는 사이버공격의 차이점을 바탕으로 무력사용에 해당하는 사이버공격의 개념을 새롭게 정리할 필요가 있다. 사이버공격이 무력공격에 해당되는지 여부도 이를 출발점으로 판단 할 수 있을 것이다. 무력공격이 일어났는지 여부는 무력사용의 규모와 효과를 기준으로 판단하기 때문이다.

한편 ICJ는 니카라과 사건에서 미국이 *contras*를 무장 및 훈련시킨 것도 무력사용에 해당한다고 판시한 바 있는데, 이로보아 헌장 제2조 제4항에서 말하는 force가 반드시 “군대”에 의한 무력사용을 의미하는 것은 아니라고 할 수 있다.[134] 탈린매뉴얼에서는 이러한 점을 들어 조직된 집단에게 타국에 대한 사이버공격을 수행하기 위한 멀웨어 및 이를 사용하는 데 필요한 교육을 제공하는 것 또한 무력사용으로 인정될 수 있다고 보았다.[135] 그러나 여기서 주의할 점은 미국이 무장 및 훈련시킨 반군 *contras*가 실제로 내란(civil strife)에 참여 했다는 것이다. 무력사용금지원칙을 천명하고 있는 1970년 국가 간 우호관계 선언에서는 “타국의 영토

131) Yaroslav Radziwill, *supra* note 130, p. 135.
132) Michale N. Schmitt, *supra* note 112, p. 914.
133) Yaroslav Radziwill (2015), pp. 134-135.
134) *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986*, para. 228.
135) NATO CCD COE, *supra* note 20, p. 46.

를 급습(incursion)하기 위해 비정규군이나 무장조직을 결성하거나 독려하는 것",“타국 내에서 일어나는 내란활동에 참여하는 것”이 금지된 무력사용에 해당한다고 하였다.[136] ICJ는 니카라과 사건에서 우호관계선언의 해당 부분을 직접 인용하면서 미국의 활동이 무력의 위협이나 사용을 수반하는 내란행위로 이어질 때 무력사용금지원칙의 위반이 적용된다고 하였다.[137] 따라서 ICJ의 판결을 부분적으로만 보고 단순히 타국에의 사이버공격을 위한 멀웨어나 이에 대한 교육을 어떤 조직에 제공하는 것을 무력사용으로 보는 것은 주의해야 한다. 이러한 행위가 금지된 무력사용이 되기 위해서는 해당 사이버공격이 무력사용 혹은 위협에 준하는 결과로 이어져야 한다.

사이버공격이 국제법상 금지된 무력사용을 구성할 수 있는지와 관련하여 또 하나 짚고 넘어갈 부분은 UN헌장 제41조이다. 헌장 제41조에서는 제39조에 따라 평화에 대한 위협, 평화의 파괴 또는 침략행위의 존재가 결정된 경우 무력의 사용을 수반하지 않는 조치를 취할 수 있도록 하고 있다. 이 규정에서는 그러한 조치의 예로 각종 통신의 중단을 들고 있다. 이를 이유로 사이버공격도 일종의 통신의 중단 또는 방해에 해당되어 무력사용으로는 볼 수 없다는 주장이 제기될 수 있다. 그러나 제41조는 특정 국가로의 혹은 특정 국가로부터의 통신이 직접적인 침투행위 없이 중단(interruption)되는 상황을 상정한 것이다.[138] 그러나 일국의 통신 기반시설을 통제하는 컴퓨터 시스템에 대한 공격(interference)은 목표 대상국가의 네트워크에 대한 침투를 수반한다.[139] 따라서 사이버공격행위가 헌장 제41조상의 조치에 포함된다고 보고 사이버공격이 무력사용에 이를 수 없다는 주장은 잘못된 것이다.[140]

---

136) Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations, UN Doc A/RES/2625 (1970), p. 4.
137) *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986*, para. 228.
138) Johann-Christoph Woltag, *supra* note 38, para. 8.
139) *Ibid.*
140) *Ibid.*

지금까지 논의한 바를 정리하면 우선 군대의 개입여부에 관계없이 기존의 재래식 무기를 사용한 결과와 같이 물리적인 파괴를 가져오는 사이버공격이 국제법상 금지된 무력사용에 해당하는 것은 명확하다고 볼 수 있다. 그러나 시스템에 연결된 시설의 가동이 중단되거나 인명에 피해를 야기하는 결과를 수반하지 않는 시스템의 무력화 또는 파괴를 가져오는 사이버공격이 금지된 무력사용에 해당하는 지에 대해서는 좀 더 논의가 필요하다. 이를 위해서는 앞에서 검토한 바 있듯 전통적인 개념의 경제적·정치적 강제와 경제적 피해를 야기하는 사이버공격의 차이점을 인식하고, 이와 같은 강도의 사이버공격이 수반하는 시스템 마비 또는 무력화의 문제를 어떻게 해석할 지에 대한 논의가 필요하다.

2) 자위권

사이버공격에 대해 자위권을 행사하기 위해서는 사이버공격이 무력사용의 단계를 넘어 무력공격에 해당해야 한다. 자위권은 개별국가가 합법적·독자적으로 행사할 수 있는 유일한 무력사용권으로 관습국제법상의 권리이며 동시에 UN 헌장 제51조상의 권리이기도 하다. 헌장 제51조에서는 행사 요건으로 무력공격(armed attack)의 발생을 규정하고 있으나, 이에 대해 정의하고 있지는 않다. 따라서 무력공격의 의미는 관습국제법 및 이를 해석한 국제재판소의 판결을 통해 추론해 볼 수 있다.

우선 분명한 것은 무력공격은 UN헌장 제2조 제4항의 무력사용과 같은 의미가 아니라는 것이다. ICJ는 1986년 니카라과 사건에서 UN헌장 제2조 4항에 규정된 무력사용이 모두 헌장 제51조의 무력공격을 의미하는 것이 아니라고 하였다.[141] 이어서 무력공격은 “가장 중대한 형식의 무력사용(the most grave forms of the use of force)”[142]이어야 하고, 일국의 정규군뿐 아니라 정규군과 같이 중대한 무력행사를 할 수 있는 무장세력,

141) *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986*, para. 191.
142) *Ibid.*

용병 등을 타국 영토에 보내어 행하는 공격을 의미한다고 하였다. 재판소는 해당 설시가 1974년 채택된 침략의 정의에 관한 UN 총회결의 제3조[143]를 인용한 것이라고 하면서 이는 관습국제법을 반영하는 것이라고 하였다.[144] 따라서 "무력사용 중에서도 규모와 효과 면에서 정규군이 타국에 행하는 수준의 가장 중대한 형식의 무력사용"이 자위권 발동 요건을 충족하는 무력공격에 해당하는 것이다.

그렇다면 여기서 중요한 것은 이러한 무력공격의 개념을 사이버공격에도 적용할 수 있을 것인가이다. 또한 사이버공격이 무력공격으로 인정된다면 어느 수준의 사이버공격을 무력공격으로 볼 수 있는 것인지 그 기준을 정하는 것도 중요하다. 먼저 앞에서 살펴본 전통적인 무력공격은 재래식 무기(kinetic force)를 사용한다는 개념을 포함하고 있다. 그러나 이는 행위의 수단에 초점을 맞추고 있는 도구적 접근(instrumental approach)에 따른 분석으로 이러한 해석에 따르면 전통적인 형태의 파괴력이 있는 무기를 사용한 경우만을 무력공격으로 본다.[145] 이를 적용하면 해킹, 디도스 공격, 서비스 거부, 논리폭탄, 웜 바이러스 등을 사용한 사이버공격은 전통적 무기를 사용하지 않았기 때문에 무력공격에 해당하지 않게 된다.[146] 그러나 이는 무력공격의 의미를 좁게 해석한 것으로 사이버공격이 끼칠 수 있는 잠재적인 피해를 생각해 보았을 때, 무력공격 여부를 판단하는 적절한 기준이라고 할 수 없다. 비록 수단은 다를지라도 결과는 전통적인 무력공격과 같을 수 있기 때문이다.

---

143) The General Assembly Resolution 3314 (XXIX) of 1974 on the Definition of Aggression Article 3 (g).

144) *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986*, para. 195.

145) Robin Geiß & Henning Lahmann, "**F**reedom and Security in Cybersp ace: Shifting the Focus away from Military Resp onses towards Non-Forcible Countermeasures and Collective Threat-Prevention", in Katharina Ziolkowski (ed.), *Peacetime Regime For State Activiteis in Cyberspace. International Law, International Relations and Diplomacy* (NATO CCD COE Publications, 2013), p. 622.

146) *Ibid.*

ICJ는 1996년 핵무기의 위협 및 사용의 합법성에 관한 권고적 의견에서 UN헌장 제2조 제4항, 제51조 및 제42조는 무기의 형태를 특정하고 있지 않으며, 사용하는 무기에 관계없이 무력사용의 개념을 적용할 수 있다고 한 바 있다.[147] 또한 Kelsen도 유엔헌장 제2조 제4항의 무력사용이 무기를 사용하는 것과 무기를 사용하지 않고 일국이 타국에 국제법에 위반되는 행위를 하는 것 두 가지를 모두 포함하고 있다고 해석하였다.[148] 또한 Brownlie는 생물학 무기나 화학무기도 재래식 무기와 같이 폭발 효과는 일으키지는 않지만 이들 무기의 사용 목적이 인명과 재산의 파괴를 위한 것인바 UN헌장 제2조 제4항의 무력사용으로 볼 수 있다고 해석하였다.[149] 그밖에도 생물학 무기, 화학무기의 사용이 '대량살상무기'로 불리는 것도 이러한 의견을 뒷받침 한다고 볼 수 있다.[150] 탈린매뉴얼에서도 다수의 전문가 그룹이 무력공격이 발생했는지의 판단 기준은 무기를 사용했느냐가 아니라 사이버 작전의 결과가 실제 무력공격으로 발생한 결과와 비슷한지의 여부라고 하였다.[151] 이는 효과 기반 접근(effect-based approach)법을 적용한 것으로 수단이 아닌 결과에 초점을 두고 문제를 해석하는 방식이다.[152] 현재 다수의 학자들이 사이버공격에 대해서도 효과 기반 접근법을 적용하고 있다.[153] 이는 UN헌장에서도 무기를 특정하지 않

147) *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996*, para. 39.
148) Hans Kelsen, *Collective Security under International Law*, Studies of International Law Publication 49 (US Naval War College, 1954), p. 57.
149) Ian Brownlie, *International Law and the Use of Force by States* (Oxford University Press, 1963), p. 362.
150) United Nations Office for Disarmament Affairs는 nuclear, biological and chemical weapons를 weapons of mass destruction으로 분류하고 있다, <https://www.un.org/disarmament/wmd/bio/> (2018.1.5. 최종방문); 또한 안전보장이사회 결의 제1540호에서도 핵무기, 생물학 및 화학 무기를 대량살상무기로 보고 이의 확산 저지를 각 회원국에게 촉구하고 있다. UN DOC. S/RES/1540(2004), p. 1.
151) NATO CCD COE, *supra* note 20, p. 55.
152) Johann-Christoph Woltag, *supra* note 38, para. 8

고 있고, 무기의 형태도 계속해서 발전·변화하고 있다는 점을 생각할 때, 합리적인 접근이라 할 수 있다.

이러한 접근방식을 적용하면 재래식 무기를 사용한 것과 같은 결과를 가져오는 사이버공격은 무력사용으로 볼 수 있고, 규모와 효과 면에서 중대한 무력사용에 해당하는 경우에는 무력공격으로 보아 자위권을 사용할 수 있는 것으로 해석 할 수 있다. 탈린매뉴얼에서도 '규모와 효과'를 단순한 무력사용과 무력공격을 구별하는 유용한 기준이라고 하였다.[154] 그러나 규모와 효과를 처음으로 언급한 ICJ도 이를 구별할 수 있는 구체적인 기준을 언급하지 않았기 때문에 탈린매뉴얼의 작성자들은 '중대한' 무력사용에 준하는 사이버공격이 무엇을 의미하는지에 대해 검토하였다.[155] 그 결과 전문가그룹은 사람을 부상 또는 사망하게 하거나 재산을 손상 또는 파괴하는 모든 무력사용은 규모와 효과 요건을 충족하는 것이라고 하였다.[156]

탈린매뉴얼의 전문가 그룹은 먼저 실제 예로 2007년의 에스토니아에 대한 사이버 '작전'을 검토하였는데, 이 사건의 경우 당시 국제사회가 이를 무력공격으로 인정하지 않았다는 점을 밝히며 전문가 그룹도 이에 동의하였다고 하였다.[157] 다음으로 2010년 스턱스넷 사건에 대해서는 이 '작전'이 이란의 원심분리기에 미친 손해로 보아 무력공격에 해당한다고 일부 전문가들이 인정하였다.[158]

탈린매뉴얼의 작성자들은 또한 인명 피해나 재산의 파괴 이외의 부정적 효과를 가지는 행위에 대해서도 무력공격을 인정할 수 있는지 검토하였다. 그 대표적인 예가 금융기관에 대한 공격으로 시장의 붕괴를 초래하는 공격이다. 전문가들은 이러한 재정적 손실이 무력공격의 성립에 필요한 손해에 해당되지 않는다고 보았다. 반면 금융기관의 마비는 국가와 사회 전체

153) *Ibid.*
154) NATO CCD COE, *supra* note 20, pp. 45-46.
155) *Ibid*, p. 48.
156) *Ibid*, p. 55.
157) NATO CCD COE, *supra* note 20, pp. 57-58.
158) NATO CCD COE, *supra* note 20, p. 58.

에 재앙적 결과를 가져오기 때문에 이를 초래하는 사이버 작전은 무력공격으로 보아야 한다는 전문가도 있어 이 부분에 있어서는 합의가 이루어지지 않았다.[159] 그러나 국가 주요기반시설의 중요 구성요소인 시스템에 심각한 영향을 가져오는 사이버 작전은 무력공격으로 인정할 수 있다고 하였다.[160]

그러나 앞에서도 지적한 바 있듯 사이버공격으로 인해 경제적 손해가 발생했다고 해서 이를 경제적 손실을 가져온 경제적 강제로만 판단하는 것은 문제가 있다. 금융기관의 네트워크에 대한 사이버공격은 시스템 무력화 내지는 시스템 파괴를 일으키는 공격으로 경제적 손해를 수반하는 복합적 성격의 공격이다. 또한 많은 국가들이 주요기반시설에 은행과 같은 금융기관을 포함시키고 있다는 점도 이들 시설에 대한 사이버공격이 무력공격에 이를 수 있다는 것을 뒷받침한다. 즉, 시스템의 무력화 또는 파괴를 가져오는 사이버공격이 무력사용에 해당될 수 있다면, 규모와 효과면에서 중대한 같은 성격의 사이버공격도 무력공격에 해당하는 것으로 볼 수 있다. 다수의 학자들도 국가에 광범위한 경제적 또는 사회 정치적 혼란을 가져오는 사이버공격은 규모와 효과 기준을 충족시킬 수 있는 것으로 보았다.[161]

그렇다면 무력사용과 무력공격을 나누는 기준은 어떻게 설정할 것인가? 이 문제가 그렇게 간단하지 않다는 사실은 사이버공격에 대한 자위권 사

159) NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd Edition (Cambridge University Press, 2017), pp. 342-343.

160) NATO CCD COE, *supra* note 20, p. 57.

161) Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution", Journal of Conflict & Security Law, Vol. 17, No. 2 (2012), p. 231. Tsagourias는 금융기관에 대한 대규모 공격으로 인한 피해를 재래식 무기에 의한 피해와 비교하면서 폭발과 같은 물리적 피해는 아니지만 목적을 수행할 수 없게 만든 unavailability에 기초해 둘을 같은 것으로 볼 수 있다고 하였다; Walter Gray Sharp, *CyberSpace and the Use of Force*, (Aegis Reserch Corporation, 1999), p. 117; Yaroslav Radziwill, *supra* note 130, p. 144.

용에 가장 적극적인 입장을 보이는 미국의 관련 언급을 살펴보면 알 수 있다. 2012년 당시 미 국무부 차관보 Harold Hongju Koh[162] 교수는 "대체적으로 사망, 부상, 또는 상당한 파괴를 야기하는 사이버 행위는 무력사용으로 볼 수 있다."고 하였다.[163] 즉, 사이버공격의 물리적 결과가 폭탄투하나 미사일 발사의 경우와 같다면 이러한 사이버공격은 무력사용과 동일하게 보아야 한다는 것이다. Koh 교수는 특히 사이버공격을 무력사용으로 판단하는 기준으로 사건의 정황, 행위의 주체, 공격의 목표와 장소, 효과와 공격의 의도를 들었다.[164] 그러면서 사이버공격으로 인한 핵발전 원자로 노심의 용해, 주민 밀집지역에 대한 댐 개방, 항공교통의 통제불능을 야기하여 항공기를 추락시키는 것 등을 그 예로 제시하였다.[165]

Koh교수는 이어서 미국은 오랫동안 어떤 형태의 불법적 무력사용에 대해서도 자위권을 행사할 수 있다는 입장을 견지해 왔다고 하면서 무력공격과 무력사용을 구분하는 기준은 없다고 하였다.[166] 이는 실제로 미국이 오랫동안 견지해온 공식적인 입장이다.[167] 즉, 미국의 입장에서 자위권 발

---

162) Harold Hongju Koh는 2009년부터 2013년까지 오바마 행정부의 차관보급 Legal Advisor of the Department of State을 역임하였다.

163) Harold Hongju Koh, "International Law in Cyberspace", Harvard International Law Journal, Vol. 54 (a footnoted version of a sppech delivered on Sept. 18, 2012 at the USCYBERCOM Inter-Agency Legal Conference on the roles of cyber in National Defense) (2012), pp. 3-4.

164) *Ibid.*

165) *Ibid.*

166) Harold Hongju Koh, *supra* note 163 p. 7.

167) William H. Taft IV, "Self-Defense and the Oil Platforms Decision", Yale Journal of International Law, Vol. 29, No. 2 (2004), pp. 299-302; Abraham D. Sofaer, "The Sixth Annual Waldemar A. Solf Lecture in International Law: Terrorism, the Law, and the National Defense", Military Law Review, Vol. 126 (1989), pp. 93-96 미국은 ICJ 가 니카라과 사건 및 Oil Platforms 사건에서 무력공격과 무력사용을 구분하여 보는 것에 대해 국가의 자위권 사용을 지나치게 제한하는 것으로 보고 비판적인 시각을 견지해 왔다; James E. McGhee, "Hack, Attack or Whack; The Politics of Imprecision in Cyber Law", Journal of Law and Cyber Warfare, Vol. 4

동의 기준은 무력사용에 해당하는 사이버공격의 발생인 것이다. 이는 무력공격과 무력사용을 분명히 구분해 보는 ICJ 및 여타 국가들의 입장과 분명한 차이를 보이고 있어, 사이버공격에 대해 자위권을 발동할 경우 자의적인 기준 적용이 우려되는 대목이다.

이에 관한 기존의 논의를 살펴보면 그루지야에 관한 EU 보고서에서는 최소 강도 이상의 물리적 강제는 모두 무력사용에 해당한다고 하면서 최소강도 이하의 예로 무인정찰기(unmanned aerial vehicle, UAV)나 한두 명의 조종사가 탑승한 비행기의 파괴를 들었다.[168] 또한 ICJ도 배 한척에 대해 기뢰를 설치해 재산손괴 및 소수의 희생자를 야기한 것을 무력공격으로 볼 수 있을 것인지에 대해 명확한 판단을 하지 않은 바 있다.[169] 따라서 Koh 교수가 언급한 것과 같이 단순히 항공 관제시스템에 대한 사이버공격으로 항공기가 추락하는 것을 무력사용 및 무력공격에 준하는 사이버공격으로 보는 것은 자위권 발동의 범위를 지나치게 넓게 볼 위험이 있다.

이를 방지하기 위해서는 사이버공격이 야기할 수 있는 결과가 영향을 미칠 수 있는 범위에 대한 분석이 우선 필요하다. 또한 이를 바탕으로 무력사용과 무력공격을 구분 짓는 사이버공격의 한계점(threshold)에 대해 국가들의 합의가 선행되어야 한다. 이에 대한 합의 없이는 사이버공격의 국제법 규율에 관한 논의는 자위권 원칙을 사용할 수 있는지 없는지의 논의만을 반복하게 될 가능성이 높다.

사이버공격에 대해 자위권을 행사할 수 있는지 여부와 관련해서 또 하나 검토해야 할 것은 바로 누적효과이다. 즉, 누적적 무력사용이 무력공격으로 인정될 수 있는가의 문제이다. 이에 대해서는 그 자체 단독으로는 무

(2014), p. 25.

168) Heidi Tagliavini, “Report of the Independent International Fact-Finding Mission on the Conflict in Georgia Vol. II, Council of Europe (2009), p. 242, 각주 49.

169) *Oil Platforms (Islamic Republic of Iran v. United States of America), Judgement, I.C.J Reports 2003*, para. 72.

력공격의 정의에 해당하지 않는 무력사용이라도 누적되면 무력공격과 같은 것으로 보고 자위권 행사의 대상이 될 수 있다고 보는 견해가 있다.[170] 이를 "침격전술론(Nadelstichtaktik, hit-and-run pin-prik tactics)" 또는 "누적적 사건론(accumulation of events theory)"이라 한다.[171]

ICJ도 여러 판결에서 이를 인정하는 듯한 표현을 사용한 바 있다. 니카라과 사건에서는 니카라과의 행위가 온두라스와 코스타리카에 대한 무력공격을 구성하는지를 판단하면서 "singly or collectively to an armed attack"이란 표현을 사용하였다.[172] 또한 Oil Platforms 사건에서는 일련의 사건을 누적적으로 본다고 해도(Even taken cumulatively) 이를 미국에 대한 무력공격이라고 볼 수 없다고 하였다.[173] 마지막으로 Armed Activities on the Territory of the Congo사건에서 ICJ는 콩고민주공화국의 무력공격이 있었는지를 판단하면서 "even if this series of deplorable attacks could be regarded as cumulative in character"라는 문구를 통해 무력사용의 누적이 무력공격을 구성할 수도 있다는 뉘앙스의 설시를 한 바 있다.[174]

이를 두고 개개의 무력사용은 무력공격으로 인정될 수 없을지라도 계속된 무력사용을 누적적으로 보면 무력공격이 될 수도 있음을 시사하는 것이라고 해석하는 주장도 있다.[175] 특히 딘슈타인은 Oil Platforms 사건에

---

170) 김대순, 국제법론, 제18판 (삼영사, 2015), p. 1631.

171) Katharina Ziolkowski, "Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt Criteria", International Conference on Cyber Conflict for Use of Force (2012), p. 302.

172) *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986*, para. 231.

173) *Oil Platforms (Islamic Republic of Iran v. United States of America), I.C.J Reports 2003*, para. 64.

174) *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgement, I.C.J. Reports 2005*, para. 146.

175) 대한변협신문, 2009년 6월 8일 6면-김찬규, "국제법상 자위권의 현주소", <http://news.koreanbar.or.kr/news/articleView.html?idxno=3965> (2018.1.5. 최종방문).

서의 ICJ 설시가 일련의 행위가 누적적으로 평가되어 무력공격을 구성할 수도 있음을 강력히 시사하는 것이라고 평가하였다.[176] 또한 누적적 사건론이 자위권 행사 가능성에 영향을 주고 있음을 언급하면서 1967년 7월 이스라엘의 '6일전쟁(Six-Day War)이 이에 따라 정당화 된다고 주장하기도 하였다.[177]

이 이론은 사이버공격에 대해서도 중요한 시사점을 준다. 무력공격에는 이르지 못하는 일련의 사이버공격이 누적되면 무력공격으로 인정되어 자위권 행사가 가능하게 될 수 있기 때문이다. 일부 학자들은 국가들이 무력공격에 이르지 않는 산발적인 사이버공격에 대해서는 자위권 발동이 불가능하다는 점을 악용하는 것을 억제하기 위해 이 이론을 인정해야 한다고 주장한다.[178] 그러나 '누적적 사건론'은 테러행위에 대한 대응차원에서 미국이 고안한 이론일 뿐, 아직 확립된 실정국제법원칙이 아니기 때문에 이를 적용하여 자위권 행사가 가능하다고 말할 수는 없다는 주장도 있다.[179] 그러나 앞서 살펴본 ICJ의 설시와 학자들의 주장을 생각해 볼 때, 누적적 사건론의 적용 여부가 명백히 불가능하다고 결론을 내릴 수는 없다고 본다. 앞으로 국제법의 발전에 따라 사이버공격에 대해 누적적 사건론의 적용가능성은 열려 있다고 볼 수 있다.

만약 누적적 사건론이 적용가능하게 된다면, 이를 사이버공격에도 적용하기에 앞서 명확히 해야할 부분이 있다. 공격의 시작과 끝을 판단하는 기준 마련, 기간 산출, 공격 포인트에 대한 기준 등이 그것이다. 사이버공격의 특성상 어디로부터 발생한 공격을 같은 공격으로 볼 것인지, 공격의 시작을 언제로 볼 것인지 등이 명확하지 않기 때문이다. 재래식 공격의 경

176) Yoram Dinstein, *War, aggression and self-defence*, (Cambridge University Press, 2011), pp. 206-207.
177) *Ibid.*
178) Levi Grosswald, "Cyberattack Attribution Matters under Article 51 of the U.N. Charter", Brooklyn Journal of International Law, Vol. 36 (2010-2011), pp. 1176-1177.
179) 제성호, "유엔헌장상의 자위권 규정 재검토", 서울국제법연구, 제17권 제1호 (2010), p. 85.

우, 미사일을 발사하거나 지상군 공격을 하거나 그 행위가 가시적이기 때문에 누적적 사건론을 적용하기 위한 공격의 시작 시점, 공격의 발원지 등을 판단하기가 비교적 쉽다. 또한 누적적 사건론 적용을 위해서는 공격의 발원지가 같아야 하는데, 사이버공격의 경우 이를 공격 서버가 존재하는 국가로 보아야 하는지 아니면 동일한 서버만을 기준으로 해야 하는지 등이 명확하지 않은 부분이 있다. 이 또한 국가들이 개별적으로 자의적 기준을 사용할 위험이 있는 부분이다.

사이버공격은 물리적 공간에서의 공격과는 그 양상이 다르게 나타나는 점이 많다. 물리적 공간에서의 공격의 경우 상대방 국가의 기반시설을 파괴하기 위해서는 재래식 무기가 물리적으로 국경을 넘어 목표시설을 직접 파괴하고, 이에 따라 인명피해가 수반되는 경우가 대부분이었다. 그러나 사이버공격의 경우에는 한 명의 인력도 국경을 넘을 필요 없이, 또한 인명피해를 일으키지 않고도 타국의 기반시설을 무력화 또는 파괴할 수 있다.[180] 이렇게 근본적으로 개념과 성격이 다른 사이버공격을 기존의 무력사용, 무력공격을 판단하는 기준을 그대로 대입하여 적용하려는 시도는 바람직하다고 볼 수 없다. 기존 국제법 하에서 무력공격을 판단하는 기준도 명확하지 않은데, 이를 그대로 사이버공격에도 적용할 수 있다는 주장은 사이버공격의 빈도가 재래식 무기를 사용한 공격보다 훨씬 더 많다는 점을 생각할 때 더욱 위험하다고 볼 수 있다. 따라서 사이버공격의 특성을 고려한 기준설정을 위한 논의가 반드시 필요하다.

3) 주권평등원칙

주권평등의 원칙이 사이버공간의 규율에도 그대로 적용된다는 것에 대해서는 대부분의 국가들이 동의한다.[181] 그러나 주권평등 원칙의 개념 및

---

180) Yaroslav Radziwill, *supra* note 130, p. 143.

181) 제3차 UNGGE 보고서 UN Doc. A/68/98 (2013), paras. 19-20; 정보 안보에 관한 UN총회 결의 UN Doc. A/RES/68/243(2014), p. 3; 제4차

범위를 어떻게 보느냐에 따라 적용 기준이 달라질 수 있는 문제가 있다. 이하에서는 주권평등 원칙의 개념과 이를 사이버공간에 적용하는 데 있어 발생할 수 있는 문제에 대해 검토해 보기로 한다.

(1) 주권평등원칙의 기본개념

주권평등의 원칙은 국제관계에서 모든 국가가 법적으로 독립되어 있고, 평등함을 의미한다. 국제관계를 규율하는 기본 원칙들 중에서 이 원칙은 모든 국가 간에 완전한 합의가 형성되어 있는 유일의 원칙이며, 국제법의 출발점을 구성하고 있다.[182] UN 헌장 제2조 제1항은 모든 회원국의 주권평등을 기구의 기본 원칙으로 규정하고 있다. 이 원칙은 이후 1970년 국가간 우호관계선언에서의 재확인으로 모든 국가들에게 적용되게 되었다. 주권이라는 개념은 여러 가지 측면을 가지고 있으며,[183] 그동안 국제사회에서는 국가주권의 다양한 측면들을 보호하기 위해 여러 국제법원칙이 발전해 왔다.

그 중의 하나가 외부의 침입으로부터 국가의 영토를 보호하는 영토주권의 원칙이다.[184] 이는 베스트팔렌 조약(Treaty of Westphalia) 체결의 영향으로 영토 할당(apportionment of territories)에 따른 정치적 단위로서의 국가가 출현하게 되면서 국제법에서 주권개념이 등장하게 되었기 때문이다.[185] 이후 주권은 자국의 영토에 대해 배타적인 권한을 행사할 수

UNGGE 보고서 UN Doc. A/70/174 (2015), paras. 26-28.

182) 김대순, *supra* note 170, p. 438; *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986*, para. 263.

183) Robert Jennings and Adam Watts, (eds.), *Oppenheim's International Law*, 9th edn., Vol. 1 PEACE (London: Longman, 1992), p. 382.

184) *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. People's Republic of Albania), Merits, Judgment, I.C.J. Reports 1949*, p. 35.

185) Russell Buchan, "The International Legal Regulation of State-Sponsored Cyber Espionage", in Anna-Maria Osula and Henry

있는 국가의 권리로 인식되었다. 영토주권의 개념은 1949년 코르푸해협 사건에서도 확인된 바 있다. 이 사건에서 ICJ는 “독립국가간 영토주권의 존중은 국제관계의 필수적 기초”라고 판시 하였다.[186] 또한 국제법상 국가의 힘은 그 영역 및 영역 내에 있는 모든 사람, 재산, 상황에 대하여 규율하거나 이들 사항에 영향력을 행사한다는 관할권의 개념도 국가 주권의 중요한 특징이다.[187]

(2) 사이버공간에 대한 국가관할권

그렇다면 국가 영토의 경계를 넘은 사이버 행위의 국제법적 성격에 대해서 다음과 같은 근본적인 질문이 제기될 수 있다. 사이버공간 안에서도 국가가 영토주권을 소유하는가? 즉, 국가가 사이버공간에 대해 관할권을 행사할 수 있는지, 할 수 있다면 어느 범위까지 행사할 수 있는지에 관해 문제가 제기 될 수 있는 것이다. 이러한 문제가 제기되는 이유는 영토와 주권의 상호의존적인 관계 때문인데, 전통적으로 영토의 개념은 물리적 공간을 의미하였기 때문이다.[188]

반면 사이버공간은 육지 영토나 영해 또는 영공과는 달리 인위적으로 만들어진 가상공간이다. 또한 사이버공간은 유비쿼터스한 공간이어서 영토에 기반한 경계가 없고, 한 국가가 전적으로 소유할 수 없다는 특징을 가지고 있다. 전통적으로 국가안보의 대상인 국가기반시설과 이를 통제하는 시스템은 국가의 영토 내에 위치해 있었다. 그러나 오늘날에는 그러한 기반시설을 운영하는 시스템이 인터넷에 연결되어 있거나 타국의 서버에 있

Rõigas (Eds.), *International Cyber Norms-Legal, Policy & Industry Perspectives* (NATO CCD COE Publications, 2016), p. 69.

186) *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. People's Republic of Albania), I.C.J. Reports 1949* , p. 35.

187) 정인섭, 신국제법 강의, 제7판 (박영사, 2017), p. 166.

188) David Johnson and David Post, “Law and Borders: The Rise of Law in Cyberspace”, Stanford Law Review, Vol. 48 (1996), p. 1367.

는 경우가 많다. 이에 우주 또는 공해와 같이 사이버공간에 대해서는 특별한 법체제가 필요하다는 주장도 있다.[189] 그러나 이러한 기반시설은 현실세계와 연결되어 있고, 또한 우주공간 또는 공해와는 달리 정부 및 민간업체가 '소유'하고 있기 때문에 이들 시설이 사이버공간에 기반을 두고 있다는 사실 만으로 영토주권 원칙으로부터 면제될 수는 없다.[190] 그보다는 오히려 사이버공간의 이러한 특징으로 인해 사이버공간 전체가 한 국가의 주권아래 있을 수는 없다고 보는 것이 타당하다.[191]

실행을 통해서도 국가들이 이미 사이버공간에 대해서 영토주권의 개념을 적용하고 있다는 것을 확인할 수 있다.[192] 이러한 실행을 확인할 수 있는 예 중의 하나로는 사이버안보에 관한 국제규범을 연구하는 UN정부전문가그룹의 제3차 UNGGE 보고서[193]를 총의로 채택한 정보 안보에 관한 UN총회 결의를 들 수 있다.[194] 또한 제4차 UNGGE 보고서에서도 국가주권 및 주권에서 파생하는 원칙들이 국가들의 사이버활동에 적용되며, 국가들은 자신의 영토 내에 위치한 사이버 기반시설에 대해 관할권을 행사함을 명시하고 있다.[195]

---

189) PW Franzese, "Sovereignty in Cyberspace: Can It Exist?", Air Force Law Review, Vol. 64 (2009), pp. 1, 18.

190) Wolff Heintschel von Heinegg, "Legal Implications of Territorial Sovereignty in Cyberspace", in Czosseck C, Ottis R, Ziolkowski K (Eds.), *2012 4th International Conference on Cyber Conflict* (NATO CCD COE Publications, 2012), pp. 9-10.

191) *Ibid.*

192) Sean Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention", Baltic Yearbook of International Law, Vol. 14 (2014), p. 142.

193) United Nations, General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98 (2013), paras. 19-20.

194) UN Doc. A/RES/68/243 (2014), p. 3.

195) United Nations, General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications

미국도 2011년 백악관에서 발간한 '사이버공간에서의 국제전략'에서 국가들이 사이버공간을 통해 전통적인 국가의 권한을 행사하고 있음을 언급한 바 있다.[196] 러시아와 중국은 사이버공간에 대한 주권 수호에 가장 집중하고 있는 국가이다. 또한 앞서 언급한 바 있듯 각국가의 사이버안보전략에서 사이버공격으로부터 주요 국가기반시설을 보호하는 것을 국가안보의 핵심요소로 언급하고 있는 것도 각 국가들이 사이버공간에 대해 관할권을 행사하고 있음을 방증하는 예라고 할 수 있을 것이다.[197] 탈린매뉴얼 규칙 1에서도 국가는 자국의 주권 영역 내의 사이버 기반시설 및 사이버 활동에 대해 통제권을 행사할 수 있다고 규정하고 있다.[198] 이렇게 볼 때, 국가는 자국의 영역 안에 있는 사이버 기반시설에 대해서는 영토주권을 가지며 이에 대해 배타적 관할권을 가진다고 볼 수 있다. 이때, 사이버 기반시설이 정부의 소유인지 민간 기업의 소유인지는 문제가 되지 않는다.[199]

한편 타국의 영역에 소재하는 일국의 사이버 기반시설을 통제하는 서버에 사이버공격이 발생한 경우, 이에 대한 영토주권의 문제가 발생할 수 있다. 탈린매뉴얼 2.0에서는 에스토니아의 경우를 예로 들어 이 문제를 검토하였다. 에스토니아는 타국에 중요한 정부 데이터를 백업 저장하는 디지털

---

in the Context of International Security, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174 (2015), paras. 26-28.

196) The White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World" (2011), p. 9, <https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>

197) 본 논문 제2장 제2절 참조.

198) NATO CCD COE, *supra* note 20, p. 16.

199) Wolff Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace", International Law Studies, Vol. 89, No. 123 (2013), p. 129; NATO CCD COE, *supra* note 20, p. 16.

대사관을 설치할 계획을 밝힌 바 있다.[200] 탈린매뉴얼의 전문가들은 만약 타국에 위치한 디지털 대사관에 사이버공격이 발생한다면, 이는 에스토니아의 정부기능 수행에 영향을 미치게 되므로 에스토니아의 주권을 위반하는 행위가 되는 동시에 기반시설 소재 국가의 주권도 침해한 행위라고 하였다.[201] 이를 통해 탈린 매뉴얼의 저자들은 국가의 주요 기반시설을 운영하는 서버가 일국의 영토 밖에 있더라도 해당서버가 자국 내의 기반시설에 연결되어 있다는 것을 근거로 영토주권 원칙이 적용된다고 보고 있음을 알 수 있다. 즉, 국가는 자국의 주요기반시설에 대해 배타적 관할권을 가지고 있기 때문에 이를 운영하는 서버의 위치가 영토주권 원칙을 적용하는 데 영향을 미치지 않는다고 본 것이다. 이와 같은 입장은 오늘날 클라우드 컴퓨팅[202] 등 국가의 기반시설을 운영하는 서버가 자국 내에 있지 않은 경우가 많은 현실을 생각할 때, 합리적인 해석이라고 볼 수 있다.

(3) 영토주권침해를 구성하는 사이버공격

다음으로 문제가 되는 것은 어떤 종류 또는 어느 강도의 사이버 행위가 주권평등의 원칙, 즉 영토주권의 침해인가이다. 2013년 탈린매뉴얼에서는 물리적 손해를 초래하지 않는 멀웨어의 설치와 같은 사이버공격행위가 주권 침해에 해당되는지에 대해서는 합의를 보지 못했다.[203] 반면 탈린 매뉴

200) e-Estonia, Jun. 2017, “Estonia to open the world’s first data embassy in Luxembourg”, <https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/> (2017.10.30.최종방문)

201) NATO CCD COE, *supra* note 159, p. 23.

202) 클라우드 컴퓨팅(cloud computing)은 인터넷 기술을 활용하여 가상화된 정보 기술(IT) 자원을 서비스로 제공하는 것을 말한다. 사용자는 소프트웨어, 서버, 네트워크와 같은 IT 자원을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 실시간 확장성을 지원받으며, 사용한 만큼 비용을 지불하는 컴퓨팅을 말한다. 한국정보통신기술협회 정보통신용어사전, <http://word.tta.or.kr/dictionary/dictionaryView.do?word_seq=038679-1> (2018.1.4.최종방문).

얼 2.0에서는 사이버공격행위를 침해의 정도에 따라 세 가지로 분류하여 이들 행위가 각각 주권침해에 해당하는지 검토하였다.[204] 첫 번째 유형은 타국 발 사이버공격행위가 물리적 손해를 가져온 경우이고, 두 번째는 기능의 상실을 가져오는 경우, 마지막 세 번째는 기능 상실 미만의 영토보전 침해를 가져오는 공격이다.[205]

먼저 첫 번째 경우에 대해서는 스턱스넷과 같이 멀웨어의 삽입으로 원심분리기의 작동 불능을 초래한 것처럼 시설의 운영에 물리적 영향을 주는 공격행위를 예로 들면서 이는 주권침해에 해당한다고 하였다.[206] 두 번째는 물리적 피해를 야기하진 않으나 주요 기반시설의 시스템의 복구나 교체가 불가피한 강도의 사이버공격으로 이는 결과적으로 물리적 피해를 가져온 사이버공격과 유사한 것으로 볼 수 있어 영토주권 원칙의 위반에 해당한다고 하였다.[207] 마지막 세 번째 유형에 대해서는 전문가들의 합의가 이루어지지 못했는데, 사이버공격이 발생했으나 물리적 피해나 시스템의 손상과 같은 피해가 일어나지 않은 경우이다.[208] 매뉴얼에서 언급한 예로는 기반시설이나 연결된 프로그램이 다르게 작동하도록 하는 공격, 저장된 데이터를 변경하거나 지우는 것, 백도어[209]를 설치하는 것 등이 있

---

203) NATO CCD COE, *supra* note 20, p. 16.
204) NATO CCD COE, *supra* note 159, p. 20.
205) *Ibid.*
206) *Ibid.* 탈린매뉴얼의 전문가들은 이러한 행위는 또한 무력공격, 금지된 무력사용 또는 금지된 간섭에 해당될 수 있다고 하였다.
207) NATO CCD COE, *supra* note 159, p. 21.
208) *Ibid.*
209) 시스템 보안이 제거된 비밀 통로로, 서비스 기술자나 유지 보수 프로그램 작성자의 접근 편의를 위해 시스템 설계자가 고의로 만들어 놓은 시스템의 보안 구멍을 말한다. 트랩도어(trapdoor)라고도 한다. 대규모의 응용 프로그램이나 운영 체계(OS) 개발에서는 코드 도중에 백도어라는 중단 부분을 설정하여 쉽게 보수할 수 있게 한다. 최종 단계에서 삭제되어야 하는 백도어가 남아 있으면 컴퓨터 범죄에 악용되기도 한다. 한국정보통신기술협회 정보통신용어사전 , <http://word.tta.or.kr/dictionary/dictionaryView.do?word_seq=062015-2> (2018.1.4.최종방문).

다.[210] 세 번째 유형도 영토주권 원칙의 위반에 해당한다고 주장한 전문가들은 영토주권 원칙이 국가가 자국의 영토에 대한 접근 및 영토 내에서의 모든 활동을 완전히 통제하는 것을 의미하는 것으로 해석하는 입장이다.[211] 자국의 사이버공간에 대해 완전한 통제를 행사하려고 하는 러시아, 중국이 여기에 해당한다고 볼 수 있다. 반면 물리적·기능적 손해의 발생을 영토주권 원칙 위반의 요건으로 주장하는 입장은 주권 원칙을 제한적으로 해석하여 적용하는 입장이라고 볼 수 있다.

앞에서 말한 세 번째 유형의 행위는 기밀정보에 접근하여 이를 복제하거나, 해당 정보를 삭제·수정하는 사이버 간첩행위에 활용되는 경우가 많다. 영토주권 원칙을 제한적으로 해석하는 입장에 따르면 대부분의 사이버 간첩행위는 국제법위반이 아니다.[212] 탈린매뉴얼에서도 사이버 간첩행위는 외교문서 및 통신의 보호의 경우를 제외하고는 국제법상 금지되지 않는다고 보고 있다.[213]

그러나 영토주권 원칙을 넓게 보는 입장은 물리적 손해를 그 위반 요건으로 보지 않는다.[214] 이 입장에 따르면 일국의 요원이 타국가의 법을 위반하여 그 국가의 영토를 침범하여 행한 전통적인 간첩행위도 타국의 영

---

210) NATO CCD COE, *supra* note 159, p. 21.

211) Ibid.

212) 대부분의 사이버 간첩행위라고 한 것은 사이버 간첩행위를 분류하는 기준이 학자마다 다르기 때문이다. 물리적 손해를 야기했던 Stuxnet 사건이 처음 시작은 malware의 설치에서 시작했기 때문에 이를 사이버 간첩행위로 분류하는 학자들도 다수 있다; Stefan Kirchner, “Beyond Privacy Rights: Cross-Border Cyber Espionage and International Law”, John Marshall Journal of Information Technology & Privacy Law, Vol 31 (2014), p. 2; James P. Farwell & Rafal Rohozinski, “Stuxnet and the Future of Cyber War”, Survival Global Politics and Strategy, Vol. 53, No.1 (2011), pp. 26-27.

213) NATO CCD COE, *supra* note 20, pp. 30, 233.

214) Quincy Wright, “Espionage and the Doctrine of Non-intervention in Internal Affairs”, in Roland J. Stanger(ed.), *Essays on Espionage and International Law* (OHIO state university press, 1962), p. 12.

토주권과 정치적 독립을 존중할 국제법상의 의무를 위반한 것으로 본다.[215] 타국의 영공에서 정찰기를 사용하는 것도 그 국가에 대한 영토주권의 침해 행위임이 일반적으로 받아들여지고 있는 것[216]을 생각할 때에도 물리적 손해가 발생해야만 영토주권 존중 의무의 위반이 되는 것은 아니라는 것을 알 수 있다.

또한 세 번째 유형의 예처럼 상대방 국가의 시스템에 백도어를 설치하는 것은 공격 행위자가 언제든지 시스템에 접근할 수 있다는 것을 의미한다. 이는 시스템 손상이나 멀웨어의 설치와 같은 치명적 공격행위를 위한 준비작업으로도 볼 수 있기 때문에, 이를 특별한 피해를 주지 않는 사이버 공격으로 단정 지어 보는 것은 바람직하지 않다. 시스템에 대한 통제권을 획득하면 공격을 실행하는 데는 아주 짧은 시간만이 소요되는 사이버공격의 특성을 생각하면 더욱 그렇다고 볼 수 있다.

다수의 국가들도 실제로 사이버 간첩행위가 국가주권을 침해하는 행위라고 인식하고 있다.[217] 이는 최근의 사례를 통해서도 확인할 수 있다. 2013년에 미국이 브라질에 대해 계속적으로 사이버 간첩행위를 해오고 있었다는 사실이 드러난 사건이 있었다. 이 사건 이후 브라질 대통령 Dilma Rousseff는 워싱턴을 방문하여 오바마 행정부의 대표들을 만나 국제문제에 대해 토의하려고 예정되어 있던 일정을 취소하였다.[218] 대신 그녀는 UN총회에서 사이버 간첩행위가 국가주권을 침해하는 행위라며 NSA(US National Security Agency)의 행위를 비난하였다.[219]

---

215) *Ibid.*

216) 니카라과 사건에서 ICJ는 허가 받지 않은 비행기를 사용해 타국 정부의 관할 하에 있는 영공을 비행하는 것은 타국의 영토주권을 존중해야 하는 원칙의 위반을 구성한다고 설시한 바 있다; *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986*, para. 251.

217) Russell Buchan, *supra* note 185, p. 71.

218) The Guardian, September 24, 2013, “Brazilian President: US Surveillance a ‘Breach of International Law”, <https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance> (2017.11.8.최종방문).

219) *Ibid.*

Dilma Rousseff는 총회에서의 연설에서 “타국의 문제에 그런 식으로 간섭하는 행위는 국제법위반행위이다... 주권국가는 타국의 주권에 결코 손상을 가할 수 없다...정보 및 데이터를 가로채는 불법행위는 테러로부터 국가들을 보호한다는 명목으로 결코 정당화 될 수 없다”고 하였다.[220] Dilma Rousseff는 여기에서 그치지 않고 미국 측에 해당 ‘불법행위’에 대한 설명과 사과 및 재발방지를 보증할 것을 요구하였다.[221] 이를 통해 브라질이 단순한 외교적 항의가 아닌 국제법 차원에서 이 문제에 대응하고 있음을 알 수 있다.

중국도 전직 NSA 요원이었던 Edward Snowden이 가디언지를 통해 미국이 각국가의 기밀정보를 감찰해온 내용을 폭로한 사건과 이에 대한 중국 당국의 추후 조사결과를 들어 미국의 행위에 대해 의견을 표명한 바 있다. 중국은 강한 용어를 사용하여 미국의 행위를 평가하였는데, 미 국가안전보장국이 “심각하게 국제법을 위반 하였다”고 하였으며, “이러한 행위는 거부되어야 하며 전세계로부터 비난 받아 마땅하다”고 주장하였다.[222] 일련의 사건에서 비난의 대상이 된 미국도 2011년 ‘사이버공간에서의 국제전략’에서 “사이버공간 안에서의 네트워크에 대한 공격, 감청 및 평화와 안전, 시민의 자유와 프라이버시를 위협하는 여타 다른 적대적 행위는 미국의 영토주권을 침해하는 행위라고 천명”하고 있다.[223]

---

220) *Ibid.*

221) The Washington Post, Sept. 24, 2013, “Brazil’s president condemns NSA spying”, <https://www.washingtonpost.com/world/national-security/brazils-president-condemns-nsa-spying/2013/09/24/fe1f78ee-2525-11e3-b75d-5b7f66349852_story.html> ;해당페이지에서 브라질 대통령의 연설 실황을 확인할 수 있다. ; 2001년 국제위법행위에 대한 국가책임에 관한 ILC 초안 제30조에서는 국제위법행위에 책임이 있는 국가에게 위반행위의 중지와 재발방지에 관한 적절한 확보 및 보장을 할 의무가 있음을 규정하고 있다.

222) The Guardian, May 27, 2014, “China Demands Halt to ‘Unscrupulous’ US Cyber-Spying”, < https://www.theguardian.com/world/2014/may/27/china-demands-halt-unscrupulous-us-cyber-spying>

이렇게 볼 때, 일국이 자국영토의 경계를 넘어 타국의 영토 내에 있는 네트워크나 데이터에 대해 가한 사이버공격은 비록 물리적 손해를 야기하지 않더라도 타국에 대한 영토주권 침해 행위를 구성한다고 볼 수 있다. 이 때, 타국의 영토 내에 있는 네트워크나 데이터라 함은 그 국가의 영토 내에 있는 물리적 기반 시설과 연결된 네트워크 및 데이터를 의미한다.[224]

이상을 정리하면 일국이 영토적 경계를 넘어 타국 영토 내의 물리적 기반시설과 연결된 시스템 혹은 데이터를 공격하는 경우 이는 영토주권 존중 원칙의 위반을 구성한다. 이때 위반을 구성하는 사이버공격의 범위와 관련하여 물리적 피해가 초래되는 강도의 공격만이 주권존중 원칙의 위반이 되는 것이 아님을 살펴보았다. 그러나 어떤 강도 및 종류의 사이버공격이 영토주권원칙의 위반을 구성할 것인지에 대해서는 논란이 계속될 것으로 보인다.

영토주권 원칙의 개념과 범위에 대한 국가들의 입장에 차이가 있기 때문이다. 러시아와 중국은 영토주권 원칙의 개념을 넓게 해석하고 있다. 이에 가시적인 피해 발생을 기준으로 하지 않고, 자국에 대해 발생하는 넓은 범위의 사이버 행위를 위반행위로 보고 있다.[225] 이는 정보 자체를 위협으로 보는 시각 때문인데, 이로 인해 인터넷을 통한 propaganda 행위도 금지된 것으로 보고 있다. 그러나 탈린매뉴얼을 작성한 다수 전문가들은 사이버공격행위는 그로 인한 피해가 명확한 경우에만 영토주권을 위반하는 것이라고 결론 내리고 있어 국가들 사이에 적용기준에 관한 갈등이 있을 것으로 예상된다.[226] 러시아·중국 진영은 탈린 매뉴얼이 서방진영의 입장

---

223) The White House, *supra* note 196, p. 12, <https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>; "...attacks on networks, exploitation of networks, and other hostile acts in cyberspace that threaten peace and stability, civil liberties and privacy' may qualify as violations of U.S. territorial sovereignty..."

224) Russell Buchan, *supra* note 185, p. 71.

225) 2015 International Code of Conduct for Information Security UN Doc. A/69/723 (2015), (3), (6).

을 대변하는 수단이라고 보며, 이를 인정하지 않는 입장을 보이고 있다.[227]

미국은 비록 2011년 사이버 전략에서 감청행위도 영토주권을 위반하는 것이라고 명시한 바 있으나 실제로는 감청 및 도청을 가장 활발히 하고 있는 대표적인 국가이다. 앞서 살펴본 브라질 및 Snowden 사건 외에도 최근 있었던 미국의 메르켈 총리 전화 감청 사건, 멕시코 전·현직 대통령의 개인 이메일 감시행위가 드러난 사건[228] 등이 그 예이다. 또한 최근 미국과 영국은 영토주권 원칙은 국내문제불간섭원칙 등의 위반여부를 판단하기 위한 기준을 제시할 뿐, 그 자체로는 사이버공격을 방지하는 효과가 없다는 인식을 드러낸 바 있다.[229] 국가들의 영토주권 원칙에 대한 인식의 차이가 명확하게 드러나는 대목이다. 따라서 이른바 저강도(Low Intensity) 또는 그 행위가 잘 드러나지 않는 사이버공격에 대해 어떻게 반응하고, 대응할 것인가의 문제는 아직도 모호한 영역으로 남아있다고 할 수 있다. 결국 영토주권의 위반을 구성하는 사이버공격의 최소 한계를 정

---

226) 이에 따라 탈린매뉴얼 작성자들은 피해를 야기하지 않는 propaganda 행위는 기본적으로 영토주권 위반이 아니라고 보고 있다. NATO CCD COE, *supra* note 159, pp. 24, 26.

227) Lawfare, May 31, 2015, “Tallinn 2.0 and a Chinese View on the Tallinn Process”, <https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process> (2017.10.3.최종방문); Russia Beyond, May 29, 2013, “Russia warns against NATO document legitimizing cyberwars“, <https://www.rbth.com/international/2013/05/29/russia_warns_against_nato_document_legitimizing_cyberwars_26483.html> (2017.10.3.최종방문).

228) BBC NEWS, October 23, 2013, “Merkel calls Obama about 'US spying on her phone'”, <http://www.bbc.com/news/world-us-canada-24647268>

229) Asia & The Pacific Policy Society, Sept. 18, 2017, “The need for clarity in International Cyber Law”, <https://www.policyforum.net/the-need-for-clarity-in-international-cyber-law/> (2017.10.3.최종방문).

하는 문제는 앞으로 발생할 사건과 그에 대한 국가들의 대응이 축적 되어야 좀 더 명확해 질 수 있을 것이다.

4) 국내문제불간섭원칙

국내문제 불간섭의 원칙은 영토주권 원칙과 함께 주권평등원칙의 또 다른 표현이다.[230] 그러나 '국내문제' 및 '간섭'의 개념과 범위는 영토주권원칙과 불간섭 원칙 사이에 구별점이 있음을 의미한다. 이하에서는 먼저 국내문제불간섭원칙의 개념과 요건에 대해 검토해보고, 이 원칙이 구체적으로 어떻게 사이버공격의 경우에 적용되는지 알아보기로 한다.

(1) 국내문제불간섭원칙의 개념과 요건

다수의 UN 결의와 ICJ 판결은 일국의 타국에 대한 강제, 간섭, 방해 행위가 불간섭 의무 위반을 구성한다는 점을 언급하고 있다.[231] 특히 ICJ는 이들 행위 중 몇몇을 중대한 정도에 이르지 않는 무력사용으로서 헌장 제51조 상의 자위권을 발동시킬 요건은 충족시키지 못하나 국내문제 불간섭 의무 위반이라고 판시한 바 있다.[232] 국내문제불간섭원칙은 확립된 국제법 원칙으로 1933년 국가의 권리와 의무에 관한 몬테비데오 협약(1933 Montevideo Convention on the Rights and Duties of States) 제8조에서 "어떤 국가도 타국의 국내 또는 국외문제에 간섭할 권한을 가지지 않는다"는 규정을 통해 확인된바 있다. 이는 이후 1970년 UN총회에서 만장일치로 채택된 국가 간 우호관계와 협력에 관한 국제법원칙 선언에서도 "국가는 타국의 국내관할 하의 문제에 간섭하지 않을 의무가 있다"는 문

230) 정인섭, *supra* note 187, p. 166.
231) Mary Ellen O'Connell, "Cyber Security without Cyber War", (2012) 17(2) Journal of Conflict and Security Law, Vol. 17, No. 2 (2012), p. 202.
232) *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986*, paras. 187-201.

구로 확인되었다.[233] 이 선언에서는 불간섭 의무에 대해 “어떠한 국가도 자신의 주권 하에 타국을 종속시키고 그로부터 어떠한 종류의 이익을 얻기 위해 타국을 강제하여 경제적·정치적 또는 다른 어떤 형태의 조치를 사용하거나 이를 조장할 수 없다”고 천명하고 있다.[234]

이밖에도 국내문제 불간섭 의무는 다수의 조약 및 결의에서 국제법원칙으로 확인되었다.[235] ICJ도 1986년 니카라과 사건에서 국내문제 불간섭의 원칙이 관습국제법의 일부임을 확인한 바 있다.[236] 해당 판결에서 ICJ는 금지된 간섭은 각국가가 주권평등 원칙에 의해 자유롭게 결정할 수 있도록 허용된 문제에 대한 간섭을 의미한다고 하였다. 또한 그러한 문제의 예로 정치적, 경제적, 사회적, 문화적 제도와 외교 정책에 대한 선택을 들었다. 또한 간섭은 그러한 국가의 자유로운 선택에 대해 강제적 방법이 사용되었을 때 불법이 되는 것이라고 하였다.[237]

이후 *Democratic Republic of Congo v Uganda(2005)* 사건에서 ICJ는 콩고민주공화국의 영토에서 반군의 군사 활동에 관여하여 Ituri 지역을 점령하고 반군에게 군사·병참·경제 및 재정지원을 한 우간다의 행위에 대해 판단하였다. 재판소는 이러한 우간다의 행위가 콩고민주공화국의 주권 및 영토적 보전을 침해했다고 하면서 불간섭 원칙 위반에 해당한다고 판시하였다.[238] 이를 종합하면 국내문제 불간섭 의무의 위반을 구성하기 위

---

233) Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations, UN Doc A/RES/2625 (Oct. 24, 1970) para 1.

234) *Ibid.*

235) 1928 OAS Convention on the Rights and Duties of States in the Event of Civil Strife 134 LNTS 45; Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, UN Doc A/Res/2131 (1965).

236) *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986* , para. 202.

237) *Ibid.,* para. 205.

238) *Congo (Democratic Republic of the Congo v. Uganda), I.C.J. Reports 2005*, paras. 168, 227.

해서는 1) 타국의 주권적 문제에 관한 간섭행위가 있어야 하고, 2) 그러한 행위가 강제적이어야 한다.[239]

(2) 주권문제에 대한 간섭에 해당하는 사이버공격

이 두 가지 요건을 사이버공격에 적용하면 어떤 행위가 구체적으로 주권적 문제에 관한 강제적 간섭을 구성한다고 할 수 있을까? 우선 첫 번째 요건인 주권적 문제에 대한 간섭행위부터 살펴보자. 앞에서 살펴본 몬테비데오 협약, 우호관계 선언 및 ICJ의 판결을 통해 유추해보면 불간섭 의무에서 말하는 주권적 문제 또는 국내문제는 일국의 관할권 내에 있는 사항을 의미한다는 것을 알 수 있다.[240] 구체적으로는 각국가가 자유롭게 결정할 수 있는 정치적·사회적·경제적·외교적·문화적 제도 및 정책에 관한 문제라고 볼 수 있다. 따라서 사이버공격이 한 국가의 정치·경제·사회 등의 문제에 영향을 미친다면 이는 주권적 문제에 대한 간섭이라고 볼 수 있다.

탈린 매뉴얼 2.0은 국내문제에 대한 간섭이 반드시 국가의 기반시설이나 국가의 행동과 관련된 부분에 대한 사이버공격일 필요는 없다고 하였다.[241] 그보다는 문제의 사이버공격이 국내문제에 대한 국가의 권한을 손상시킬 목적으로 행해진 것이면 첫 번째 요건을 충족하는 것이라고 하였다.[242] 저자들은 그러한 예로 한 국가가 타국의 상업 은행의 웹사이트에 게재된 내용을 삭제하기 위해 사이버공격을 수행하는 것을 들었다.[243] 이러한 사이버공격이 간섭에 해당하는 이유는 온라인 게재 사항에 관한 규정을 만드는 것은 일국의 국내문제에 해당하기 때문이다.[244] 이에 따르면 '국내문제에 대한 간섭'에 해당하는 행위는 정해진 대상에 대한 공격이나

239) Russell Buchan, *supra* note 185, p. 74.
240) UN 헌장 제2조 제7항에서도 UN의 국내문제 불간섭의무에 대해 규정하고 있다.
241) NATO CCD COE, *supra* note 159, p. 315.
242) *Ibid.*
243) *Ibid.*, pp. 315-316.
244) NATO CCD COE, *supra* note 159, p. 316.

물리적이고 가시적인 피해를 요구하지 않기 때문에 그 범위가 다른 국제의무 위반의 경우보다 더 광범위할 수 있음을 알 수 있다.

그렇다면 공격의 대상이 되는 서버가 공격 대상 국가가 아닌 다른 국가의 영토에 위치해 있는 경우에도 주권적 문제에 관한 불법적 간섭이라고 볼 수 있는가.[245] 다시 말해서 국가가 직접 만들고 작성한 정보이긴 하지만 그것이 타국의 영토에 위치한 사이버 기반시설에 저장되어 있거나 타국에 위치한 사이버 기반시설을 통해서 전송되는 경우에도 국가가 주권을 행사한다고 볼 수 있느냐는 것이다.[246]

이와 관련하여 2013년 동티모르(Timor-Leste)가 호주에 위치해 있는 동티모르의 변호인측 사무실로부터 서류와 디지털 데이터를 몰수한 호주에 대해 해당 행위가 국제법위반임을 주장하며 ICJ에 잠정조치를 요청한 사건이 있었다.[247] 동티모르는 2013년 대륙붕 유전에 대한 양국 간의 석유와 가스 수입 분배문제를 규정하는 협정관련 난제에 대해 PCA에 제소하였고, 이 사건은 2017년 3월 동티모르가 2006년 조약의 파기를 호주정부에 통보하기로 합의하면서 종결되었다.[248] ICJ는 호주가 진행 중인 사건과 관련하여 동티모르와 호주에 주재하고 있는 동티모르측 변호인과의 사이의 통신에 어떠한 방법으로든 간섭해서는 안된다고 하면서 이는 유엔헌장 제2조 제1항에 반영되어 있는 국제법질서의 기본 원칙인 주권평등원칙에서 파생된 것이라고 하였다.[249] 따라서 동티모르가 주장하는 호주의 간섭 없이 중재절차 또는 교섭을 진행할 권리 및 여기에 포함된 변호인과의

---

245) 앞서 이러한 행위는 영토주권 침해 행위에 해당한다고 분석한 바 있다.
246) Russell Buchan, *supra* note 185, p. 74.
247) *Questions relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), Provisional Measures, Order of 3 March 2014, I.C.J. Reports 2014*, para. 1.
248) *Arbitration under the Timor Sea Treaty Termination Order (Timor-Leste v. Australia), PCA, Case No. 2013-16, 2017*, p. 1-3.
249) *Questions relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), Provisional Measures, Order of 3 March 2014, I.C.J. Reports 2014*, paras. 22-30.

통신에 있어서 기밀성을 보장받을 권리와 간섭받지 않을 권리는 타당성이 있다고 판단하면서 잠정조치를 명하였다.[250]

본 사건에서 비록 ICJ가 호주의 행위에 대해 명확한 국제법적 판단을 내린 것은 아니지만 재판소가 잠정조치를 내리면서 한 국제법적 해석은 상당한 중요성을 가지고 있다고 볼 수 있다. 몰수된 정보가 동티모르가 아닌 호주에 소재하고 있었음에도 그러한 정보가 동티모르의 주권 및 국제법상 금지된 간섭과 관련된 문제라고 본 것은[251] 사이버공격 대상 서버가 타국 영토에 위치하고 있는 경우에도 불간섭의무의 적용이 가능함을 시사하기 때문이다. 즉, 국가가 기밀정보를 타국에 위치한 서버에 저장하거나 그러한 기밀 정보를 타국에 위치한 사이버 기반시설을 통해 전송할 때, 그 정보는 중요한 차원의 국가 주권을 의미한다는 것이다.

정보가 국가 주권과 불가분의 관계에 있다는 주장은 상업적 거래에 관한 정보 보다는 국가의 공공 기능 행사와 관련된 정보가 차단되었을 때 특히 확실해 진다.[252] 2004년에 UN 총회 결의로 채택된 국가 및 그 재산의 관할권 면제에 관한 UN협약 제5조에서 국가는 타국 법원의 관할권으로부터 그 자신과 재산에 대하여 면제를 향유하나 제10조에서 상업적 거래에 관련된 사항에 대해서는 면제를 원용할 수 없다고 규정하고 있는 것도 이를 뒷받침 한다고 볼 수 있다. 한 연구에서도 일국의 전자 정보가 그 국가의 영토 밖에 위치하고 있는 경우, 그 국가가 소유하거나 그 국가가 배타적으로 사용하는 상업적 목적 이외의 정보는 국가 주권과 불가분의 관계이며 그 국가의 배타적인 관할 대상이라는 것이 일반 국제법원칙이라고 보았다.[253] 이로 볼 때 국가는 자국 영토 밖에 위치한 사이버 기반시설에 저장된 정보 또는 데이터에 대해서도 '국가 데이터 주권'[254]을 가지며

250) *Ibid.*
251) Russell Buchan, *supra* note 185, pp. 75-76.
252) Vineeth Narayanan, "Harnessing the Cloud: International Law Implications of Cloud-Computing", Chicago Journal of International Law, Vol. 12 (2012), p. 783.
253) Wolff Heintschel Von Heinegg, *supra* note 199, p. 130.
254) Kristina Irion, "Government Cloud Computing and National Data

이에 대한 간섭 또는 방해는 국가 주권에 대한 침해행위로 간주할 수 있다. 즉, 국내문제는 반드시 영토적 개념에 국한된 것이 아님을 알 수 있다.[255]

(3) 강제적 간섭의 의미와 사이버공격에의 적용

다음으로 사이버공격행위가 국내문제불간섭원칙 위반의 또 다른 요건인 강제성을 띨 수 있는가에 대해서 살펴보기로 한다. 1986년 니카라과 사건에서 ICJ는 주권평등의 원칙에 의해 일국이 자유로이 선택하도록 허용된 문제에 대해 타국이 강제의 방법을 사용하는 것을 불법적 간섭이라고 하였다.[256] ICJ는 또 강제의 방법 중 가장 명확한 예로 직접적 무력사용이나 체제전복적인 또는 테러집단에 대한 간접적 무력 지원을 들었다.[257] 따라서 무력사용에 해당하는 사이버공격을 직접 수행하거나 이러한 행위를 지원하는 것은 불법한 간섭에 해당하게 된다. 한편 이 판결이후 학계는 강제의 의미를 충족하기 위해서는 국가의 의사를 조종하는 명령형의 압력(imperative pressure) 부과가 요구된다는 것에 대해 동의하고 있다.[258]

오펜하임은 간섭은 실제 상황을 유지하거나 변경하려는 목적으로 타국의 문제에 독재적인 간섭(dictatorial interference)을 하는 것을 의미한다고 하였다.[259] Jamnejad 와 Wood도 일국이 타국의 정책 변화를 달성하기 위해 취한 행동을 강제가 적용된 경우로 보았다.[260]

정리하면 강제는 일국이 '자유로이 선택하고 결정해야 하는 문제'에 대

Sovereignty", Policy and Internet, Vol. 4 (2012), p. 40.

255) 정인섭, *supra* note 187, p. 167.

256) *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986*, para. 205.

257) *Ibid.*

258) Russell Buchan, *supra* note 185, p. 77.

259) Lassa Oppenheim and Hersch Lauterpacht, *International Law: A Treatise. Vol. I, Peace*, 8th edn. (London: Longman, 1955), p. 305.

260) Jamnejad and Wood, "The Principle of Non-Intervention", Leiden Journal of International Law, Vol. 22 (2009), pp. 347-348.

해 그 국가가 의도한 바대로 '선택하고 결정할 수 없을 정도의 압력'을 행사하는 것으로 단순히 영향을 미치는 것과는 구분되어야 한다. 따라서 어떠한 간섭이 불법적인 간섭인지 즉, 강제성이 있었는지를 판단하기 위해서는 피해국에게 행사된 간섭의 영향을 평가하는 것이 필요하다.[261] 때로 불간섭의무는 국가 간의 모든 상호작용을 명백히 금지한다고 비판을 받기도 하는데, 특정 강도 이상의 행위를 의미하는 강제성의 요건이 불간섭 원칙의 범위를 한정하는 역할을 해준다.[262]

탈린매뉴얼 2.0의 전문가들은 이에 대해 단순한 강제와 불간섭 의무 위반을 구성하는 강제를 구분 하면서, 후자는 목표한 국가의 문제에 강제적 행위의 결과가 나타나도록 고안된 것이어야 한다고 하였다.[263] 예를 들어 이웃 국가의 특정 종족 집단이 소유하고 있는 사이버 기반시설에 대해 사이버공격을 하는 것은 이웃 국가의 국내문제를 선택하는 데 있어 영향을 주고자 한 행위가 아니기 때문에 불간섭의무 위반에 해당하지 않는다고 하였다.[264] 그러나 해당 행위가 불법한 간섭이 아니라고 해서 적법한 행위로 인정되는 것은 아니라는 점을 유념해야 한다. 해당행위는 명백한 영토주권의무 위반이다. 또한 사이버공격행위가 피해국가의 주권문제에 강제성을 행사했는지, 그 영향을 평가하는 것은 다소 주관적인 문제이기 때문에 명확한 기준을 정하기 어렵고 사건별로 판단해야 한다는 한계가 있다.

이하에서는 강제의 방법으로 무력이 사용되지는 않았으나, 위에서 살펴본 요건을 적용하여 불간섭 의무의 위반에 해당되는 사례에 대해 검토해 보기로 한다. 가장 먼저 검토할 사례는 러시아가 공격의 배후로 추정되는 2007년 에스토니아에 대한 분산서비스 거부(DDoS) 공격 사건이다. 당시 NATO는 사이버 전문가를 파견해 에스토니아를 지원했고, 조사결과 확인

---

261) Russell Buchan, "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?", Journal of Conflict & Security Law, Vol. 17, No. 2 (2012), p. 224.
262) Jamnejad and Wood, *supra* note 260, p. 348.
263) NATO CCD COE, *supra* note 159, p. 318.
264) Ibid.

된 공격자 대부분이 러시아인이었으며, 공격 경로도 러시아로 밝혀졌다.[265] 이에 에스토니아는 러시아에 공식적으로 수사를 요청했으나, 러시아는 공격 사실을 부인하면서 수사요청을 거절하였다.[266] 이에 따라 공격의 배후가 러시아라는 사실을 명백하게 밝힐 수는 없었으나[267] 지금까지 나타난 정황에 근거해 러시아가 공격의 배후라는 점을 전제로 사건을 검토하기로 한다.

먼저 2007년 공격에 강제성이 있었는가? 다시 말해서 이 공격이 에스토니아 정부로 하여금 정책을 변화시키도록 강제하기 위해 감행된 것인가? 앞에서 살펴보았듯이 이를 판단하기 위해서는 해당 사이버공격이 에스토니아에 미친 영향을 살펴보아야 한다. 당시 에스토니아에 대한 사이버공격은 정부, 방송사 및 금융기관과 같은 민간부문에 걸쳐서 광범위하게 일어났다. 민간부분을 먼저 살펴보면, 에스토니아에서는 은행업무의 95퍼센트

---

265) Ronald J. Deibert, Rafal Rohozinski, Masashi Crete-Nishihata, "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war", Security Dialogue, Vol. 43, No. 1 (2012), p. 4; NBC News, Aug. 7, 2009, "A Look at Estonia's Cyber Attack in 2007", <http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.WCcdfdKLTIU> (2017.10.5.최종방문).

266) 국방일보, 2016년 9월 5일, "디도스 배후는 러시아?...국가대상 최초의 사이버공격",<http://kookbang.dema.mil.kr/kookbangWeb/view.do?parent_no=1&bbs_id=BBSMSTR_000000001163&ntt_writ_date=20160906> (2018.1.5. 최종방문).

267) 실제로 2009년 러시아 여당 의원 보좌관인 코스탄틴 골로스코코프는 모스크바 타임스와의 인터뷰에서 "수십 명의 IT전문가들을 규합해 사이버 테러를 주도했다"면서 그러나 나쉬 차원의 지원이나 러시아 관리들의 도움을 받지는 않았다고 밝힌 바 있다. 나쉬는 친크렘린 청년단체로 2007년의 에스토니아 사이버공격을 주도한 콘스탄틴 골로스코코프는 이 단체의 회원이다;Reuters, Mar. 13, 2009, "Kremlin loyalist says launched Estonia cyber-attack", <http://www.reuters.com/article/us-russia-estonia-cyberspace-idUSTRE52B4D820090313> (2018.1.5. 최종방문).

가 전산으로 처리되고 있었는데, 해당 DDoS 공격으로 인해 다수의 에스토니아 대규모 은행의 웹사이트가 마비되었고, 이는 에스토니아의 경제적 활동에 심각한 지장을 초래하였다. 미디어 영역에 대한 피해 또한 심각했는데, 이는 미디어에 대한 접근 경로가 대부분 인터넷을 통해 이루어지고 있었기 때문이다. 이 공격으로 인해 주요 방송사의 웹사이트가 조직적으로 공격을 당했고, 인터넷 접속이 불가능해 지면서 민간인들이 해당 사이버공격으로 인해 벌어지고 있는 상황에 대한 정보를 제공을 받을 수 없었다. 더욱 심각한 것은 DDoS 공격이 해외에서 시작됐다는 것이 밝혀지자 공격을 완화시키기 위해 담당자들이 외부와의 연결을 차단시켜 버렸고, 이로 인해 모든 국제적 웹 트래픽[268]이 차단되어 결과적으로 에스토니아는 국제사회로부터 차단되는 결과가 발생한 것이다. 공공부분에 있어서는 특히 주요 정부 사이트들이 공격의 대상이었다. 대통령 집무실, 국무총리실, 국회, 국가 감사원, 국가 정보기관 및 각 정부부처의 웹사이트가 기능을 멈췄고, 이메일 확인도 불가능해 지는 등 공격이 지속된 3주간 동안 업무마비 상태를 겪었다. 이 공격으로 인해 에스토니아는 큰 사회적 혼란과 수천만 달러의 경제적 피해를 보았다.[269]

해당 사이버공격의 규모와 기간, 에스토니아 전역에 끼친 피해를 생각해 볼 때, 이러한 사이버공격은 에스토니아의 구소련 참전 기념 청동동상 이

---

268) 전신, 전화 등의 통신 시설에서 통신의 흐름을 지칭하는 말이다. 한국정보통신기술협회, 정보통신용어사전, <http://word.tta.or.kr/dictionary/dictionaryView.do?word_seq=058388-1> (2018.1.25.최종방문).

269) New York Times, May 29, 2007, “Digital Fears Emerge After Data Siege in Estonia”, <http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=0> (2018.1.5. 최종방문).
; The gardian, May 17, 2007, “Russia accused of unleashing cyberwar to disable Estonia”, <https://www.theguardian.com/world/2007/may/17/topstories3.russia> (2018.1.5. 최종방문).

전 정책을 변경하도록 압력을 가하는 강제성 요건을 충분히 충족한다고 볼 수 있다. 다음으로 에스토니아 내에 있는 동상을 다른 지방으로 이전시키는 문제는 국가가 자유로이 결정할 수 있는 정치적 문제, 즉 국내문제임이 분명하므로 이 사건의 사이버공격은 강제성을 띠고 타국의 주권적 문제에 간섭한 행위로 불간섭의무 위반을 구성한다고 볼 수 있다.

사이버공격을 통해 공격 목표 국가의 정권교체에 영향을 미치려는 시도는 좀 더 명백하게 국내문제 불간섭 의무를 위반한 경우로 볼 수 있다. 그 첫 번째 예로 2014년 우크라이나 대선 당시 러시아가 사이버공격을 통해 선거 결과를 조작하려던 사건을 들 수 있다. 2014년 5월 25일은 우크라이나의 대선일 이었다. 그런데 대선일 사흘 전, 우크라이나 중앙선관위의 컴퓨터가 공격을 당하는 사건이 발생했다. 중앙선관위 컴퓨터 시스템에 침투한 해커는 첫날에는 저장되어 있는 중요한 파일들을 삭제했고, 투표 응답 검수 프로그램을 운영 불가 상태로 만들었다. 다음날에는 CyberBerkut이라는 해커 집단이 전날의 공격을 자신의 행위라고 주장하면서 선거에 사용되는 컴퓨터 기반시설을 파괴했다는 내용의 이메일을 보냄과 동시에 그 증거로 기타 문서를 웹사이트에 게재 했다. 우크라이나 당국은 선거 결과가 방송되기 40분 전에야 악성 바이러스를 제거할 수 있었다. 당국의 설명에 따르면 만약 중앙선관위 컴퓨터에 설치되어 있던 악성 바이러스를 제거하지 못했다면 극우 민족주의 정당의 후보 Dmytro Yarosh가 37퍼센트의 득표율로 당선된 것으로 방송이 되었을 것이라고 밝혔다. 반면 실제 당선자인 Petro Poroshenko는 29퍼센트의 득표율로 낙선한 것으로 보도되도록 조작되어 있었다. Dmytro Yarosh는 선거에서 실제로는 1퍼센트의 득표율을 기록했다. 그런데 흥미로운 사실은 같은 날 러시아의 제1채널에서 Dmytro Yarosh가 37퍼센트의 득표율을 기록하여 당선되었고, Petro Poroshenko는 29퍼센트의 득표율로 낙선했다는 내용이 방송된 것이다.[270]

---

270) Tech Week Europe, May 23, 2014, “Pro-Russian Hackers Attack Central Election Commission Of Ukraine”,

놀라운 것은 우크라이나에 대한 사이버공격이 여기에서 그치지 않았다는 것이다. 투표가 끝난 선거 다음날 새벽 개표 시스템이 DDoS 공격을 받았는데, 이로 인해 시스템이 작동하지 않아 새벽 한시에서 세시 사이에 개표작업이 지연되었고, 최종 결과 발표 또한 아침까지 미뤄지게 되었다. 또한 예정되어 있던 선거 보도자료는 다시 재검토 되는 상황이 벌어졌다. 사이버 보안 전문 기업 Arbor Networks가 해당 DDoS 공격을 추적한 결과 CyberBerkut 과의 연관되어 있음이 확인되었다. 우크라이나는 공격의 배후로 러시아를 지목하였지만 러시아는 이를 부인하였다. CyberBercut 도 러시아와의 연계성 여부에 대한 답변을 내놓지 않았다.

그러나 전문가들은 그 동안 우크라이나의 네트워크 시스템을 침입한 바이러스를 분석하면 특이한 점이 발견되는데 우선 첫 번째 특징은 바이러스가 키릴문자(Cyrillic)로 작성되었다는 것이다.[271] 또한 공격의 흐름이 모스코바와 키에프로 수렴된다는 것, 공격이 국가의 지원을 받았음을 짐작하게 하는 정교한 코딩기술이 사용되었다는 점이 그것이다.[272] 캘리포니아 공대의 정치학 교수 Peter Ordeshook는 Dmytro Yarosh가 우크라이나에서 지지율이 높지 않았기 때문에 조작된 결과가 발표되었더라도 러시아의 영향을 받은 극우주의자들의 소행으로 생각되었을 것이라고 분석했다.[273] 그러나 그는 이어서 만약 조작된 선거결과가 담긴 바이러스가 발견

<http://www.techweekeurope.co.uk/workspace/cyberberkut-hackers-attack-central-election-commission-of-ukraine-146180> (2016.11.1.최종방문).

271) The Wall Street Journal, Nov. 9, 2015, “Ukraine: Cyberwar’s Hottest Front”, <http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671> (2018.1.5.최종방문).

272) *Ibid.*

273) The Christian Science Monitor, Jun. 17, 2014, “Ukraine election narrowly avoided 'wanton destruction' from hackers”, <http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video> (2018.1.5.최종방문).

되어 처리되지 않았더라면 우크라이나 동부의 친러시아 반군 점령지인 도네츠크 주의 동요를 일으켰을 가능성이 크다고 하였다.[274] 이는 우크라이나 새정권의 신뢰도를 떨어뜨리고 우크라이나 내 러시아의 군사적 행동을 촉발 시키는 계기가 되었을 수도 있다고 보았다.[275]

2016년에는 타국의 한 대선후보의 이메일을 해킹해 이를 공개하는 방식으로 피해국가의 대선 개입을 시도하는 사이버공격이 발생하였다. 이 사건은 2016년 7월 러시아가 미국의 민주당 전국위원회의 이메일을 해킹했다는 내용의 보도를 통해 알려지게 되었다.[276] 이 사건은 폭로 전문사이트 위키리크스가 민주당의 대선후보인 Hillary Clinton의 캠프 선대본부장 John Podesta의 이메일 수천 건을 공개하면서 촉발되었다. 그런데 수사당국이 공개된 이메일이 러시아가 해킹을 통해 획득하여 위키리크스에 제공한 것이라는 증거를 확보했다는 내용을 발표하면서 러시아가 미국의 국내문제에 개입하려 한다는 비판이 일게 된 것이다. 이러한 의혹에 대해 위키리크스의 설립자 Julian Assange는 러시아와의 연계를 부인하였고, Vladimir Putin 대통령 및 러시아의 정부 고위관계자들도 이 같은 의혹을 전면 부인하였다.[277]

한편 이에 대해 국토안보부와 국가정보국(Director of National Intelligence, DNI)은 러시아가 미국의 대선에 개입하기 위해 민주당의 이메일을 해킹한 것이라는 내용의 공동성명을 발표 하였다.[278] 미국은 공동

---

274) *Ibid.*
275) *Ibid.*
276) The New York Times, Sept. 14, 2016, "Sowing Doubt Is Seen as Prime Danger in Hacking Voting System", <http://www.nytimes.com/2016/09/15/us/politics/sowing-doubt-is-seen-as-prime-danger-in-hacking-voting-system.html> (2018.1.5.최종방문).
277) CNN, Oct. 18, 2016, "US accuses Russia of trying to interfere with 2016 election", <http://edition.cnn.com/2016/10/07/politics/us-blames-russia-for-targeting-election-systems/> (2018.1.5.최종방문).
278) Department of Homeland Security, "Joint Statement from the Department Of Homeland Security and Office of the Director of

성명에서 러시아가 그동안 유럽과 유라시아에서 공작 해왔듯이 이번 이메일 해킹 및 누출 사건을 통해 여론을 동요시켜 미국 대선 절차를 방해하려고 하고 있다고 주장하였다.[279] 백악관 대변인도 해킹의 배후로 러시아를 지목하고 상응하는 대응조치를 취할 것을 발표하였다.[280] 이후 FBI가 공화당 대선후보인 Donald Trump의 캠프가 러시아로부터 재정적 지원을 받은 정황을 포착하여 수사를 시작했다는 내용이 보도되었다.[281] 또한 FBI가 트럼프 캠프의 선거대책위원장을 맡았던 Paul Manafort를 러시아와의 재정공모 혐의로 사전조사 했으며, 트럼프 캠프와 러시아 은행이 이메일을 주고받은 부분에 대해서도 조사하고 있다는 사실도 언론을 통해 보도되었다.[282]

위키리크스 사건이후 트럼프는 푸틴 대통령과의 친분을 과시한 전적과 푸틴 대통령을 최고의 지도자로 치켜세웠던 점, 시리아 내전, 나토 및 우크라이나에 대한 트럼프의 정책안이 러시아의 대외 정책과 유사한 점을

National Intelligence on Election Security", Oct. 7, 2016, <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national> (2018.1.5.최종방문).

279) *Ibid.*

280) The White House-Office of the Press Secretary, "Press Briefing by Press Secretary Josh Earnest", Oct. 12, 2016, < https://www.whitehouse.gov/the-press-office/2016/10/12/press-briefing-press-secretary-josh-earnest-10122016> (2018.1.5.최종방문); The Washington Post, Oct. 7, 2016, "U.S. government officially accuses Russia of hacking campaign to interfere with elections", <https://www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html> (2018.1.5.최종방문).

281) The New York Times, Oct. 31, 2016, "Investigating Donald Trump, F.B.I. Sees No Clear Link to Russia", <http://www.nytimes.com/2016/11/01/us/politics/fbi-russia-election-donald-trump.html> (2018.1.5.최종방문).

282) *Ibid.*

들어 러시아 정부와의 결탁 여부에 대한 의혹을 받아왔다.[283] 그러나 FBI는 아직까지 러시아와 트럼프 캠프사이의 연계성에 대해 명백한 증거를 찾지 못했다고 밝혔다. 또한 지금까지의 수사 결과로 볼 때, 확실한 점은 러시아의 주목적이 트럼프를 지지하기 위한 것이기 보다는 대선 자체에 혼란을 일으켜 미국의 정치적 독립성을 해하는 것이라고 하였다. 이는 러시아가 오바마 정부의 컴퓨터 네트워크를 계속해서 해킹해온 증거와 종합해 볼 때 명백하게 드러난다고 하였다.[284]

이상 러시아가 타국의 정권 교체에 영향을 미치기 위해 사이버공격을 통해 간섭한 두 개의 사건에 대해 살펴보았다. 첫 번째 사건은 우크라이나의 선거관리 시스템에 대한 직접적인 사이버공격으로 우크라이나 대선 개표 및 결과 발표 전 과정에 영향을 미친 사건이었다. 두 번째 사건은 미국 대선이 치러지기 전 유력한 후보 진영의 이메일을 해킹해 해당 진영에 대한 불리한 정보를 공개하면서 대선 판도에 영향력을 행사한 사건이다. 이 두 사건을 국내문제 불간섭 의무 위반여부와 관련해 살펴보면, 먼저 선거를 통해 대통령을 선출하는 문제는 대표적인 국내관할 문제이자 주권적 사항이다. 따라서 두 사건 모두 국내문제 불간섭 의무 위반의 첫 번째 요건인 타국의 주권적 문제에 대한 간섭행위에 해당한다.

한편 우크라이나 사건의 경우 해킹을 통해 설치한 멀웨어가 제거되지 않았다면 공격 측에서 설정해놓은 거짓 결과가 발표됨에 따라 엄청난 국가적 혼란이 초래되었을 것이다. 또한 이후 시스템이 복구되어 결과가 수정 발표된다고 해도 새 정부의 신뢰도는 계속해서 의심을 받을 가능성이 높다. 이는 친러시아 세력과의 갈등이 문제되고 있는 우크라이나의 국내적 상황을 고려할 때 더욱 그렇다고 볼 수 있다. 사실 멀웨어가 제거되지 않는 최악의 상황은 면했지만, 2014년 우크라이나 대선은 해당 사이버공격

283) CNN, Nov. 1, 2016, “FBI investigations into Trump-Russia ties yield little”,<http://edition.cnn.com/2016/11/01/politics/donald-trump-russia-fbi-investigations/> (2018.1.5.최종방문).
284) *Ibid.*

으로 위기를 맞았고, 국가전체에 혼란이 초래 되었던 것을 부인할 수 없다.

미국의 민주당 이메일 해킹사건의 경우에도 주요 대권주자 중 하나인 힐러리 클린턴의 지지율에 적지 않은 영향을 미쳤다. 사건 이후 실시된 여론조사 결과에서 클린턴의 지지율은 역대 최저치를 기록했다.[285] 설상가상으로 사건 발생 얼마 후 FBI가 힐러리의 이메일에 대해 재조사를 실시한다고 발표하자 클린턴과 트럼프의 지지율은 1퍼센트 포인트 차로 좁혀졌다.[286] 뿐만 아니라 미국의 선거 시스템, 나아가서는 미국의 정치제도에 러시아가 개입·간섭을 하고 있다는 의혹은 상당한 정치적 파장을 가져왔다. 이메일 스캔들로 인한 파장은 트럼프가 집권한 후에도 계속 이어져 지금까지도 트럼프 대통령의 지지율 및 정책 수행에 적지 않은 영향을 미치고 있다.[287]

각 사건에서 사이버공격이 미친 영향력을 생각해 볼 때, 각각의 사이버

---

285) The Washington Post, Aug. 31, 2016, “A record number of Americans now dislike Hillary Clinton”, <https://www.washingtonpost.com/news/the-fix/wp/2016/08/31/a-record-number-of-americans-now-dislike-hillary-clinton/> (2018.1.5.최종방문).

286) Fox News, Oct. 30, 2016, “New poll: 34 percent 'less likely' to vote for Clinton after new email revelations”, <http://www.foxnews.com/politics/2016/10/30/new-poll-34-percent-less-likely-to-vote-for-clinton-after-new-email-revelations.html> (2018.1.5.최종방문).

287) Newsweek, Jun. 10, 2017, “Trump impeachment calls surge as president faces ‘most serious scandal’ in U.S. history”, <http://www.newsweek.com/trump-impeachment-comey-testimony-president-623888> (2017.10.5.최종방문); Independent, Jul. 12, 2017, “Democrat files first articles of impeachment against Donald Trump”, <http://www.independent.co.uk/news/world/americas/us-politics/trump-impeachment-bill-obstruction-justice-democrats-file-house-russia-investigation-a7838141.html> (2017.10.5.최종방문).

공격은 니카라과 사건에서 ICJ가 설시한 주권적 사항에 대한 피해국의 '선택'과 '결정'에 간섭하는 '강제'의 범주에 충분히 해당된다고 볼 수 있다. 이는 또한 앞서 살펴본 학자들이 제시한 강제의 개념에도 모두 부합한다. 우선 우크라이나와 미국에 사이버공격을 감행한 주체는 정권교체 또는 정치적 혼란이라는 특정목적을 실현하기 위해 국가를 구성하는 국민의 의사를 조종하는 명령형의 압력을 부과한 것으로 볼 수 있다. 또한 우크라이나 정권을 친러성향의 정권으로 교체하려 한 점, 트럼프를 지지하는 것으로 알려진 러시아가 민주당 후보를 겨냥해 공격한 점은 현재 상황을 변경하려는 목적으로 타국문제에 간섭한 것으로 볼 수 있다. 이는 오펜하임이 제시한 강제의 개념에도 부합한다. 따라서 CyberBercut의 배후가 러시아인 것이 밝혀지거나, 위키리크스에 해킹한 이메일을 제공한 당사자가 러시아임이 밝혀진다면 러시아의 행위는 명백한 불간섭 원칙 위반을 구성하는 것으로 볼 수 있다.

(4) 사이버공격의 강도와 강제성 판단기준

지금까지 사이버공격의 경우 국내문제 불간섭 의무를 어떻게 적용할 수 있는지에 대해 검토해 보았다. 불간섭 의무 위반 요건은 두 가지로 나누어 살펴보았는데, 두 가지 요건 중 타국의 주권적 문제에 대한 간섭행위인지를 판단하는 것은 어려운 일이 아닌 것으로 보인다. 다만 범위가 넓어서 이를 열거할 수 없을 뿐이다. 그러나 또 다른 요건인 강제성 여부를 판단하는 데는 일정한 기준이 필요하다. 앞서 '강제'의 여부를 판단하기 위해서는 그 국가가 의도한 바대로 선택하고 결정할 수 없을 정도의 압력이 행사되어야 하는 것으로 정리한 바 있다. 또한 이를 판단하기 위해서는 타국의 행위가 피해국에 미친 영향과 결과를 평가하는 것이 필요하다고 하였다.

그런데 강제를 평가하는 세부적인 기준에 대해서는 학자들의 의견이 상충한다. 강제의 기준을 타국의 어떤 행위가 피해국에게 중요한 결과를 가

져오는 압력의 행사가 있어야만 한다는 의견과 주권적 가치를 가지는 부분에 대한 공격만으로도 강제성이 행사된 것으로 보아야 한다는 의견이 나뉘는 것이다.[288] 전자는 특히 사이버 간첩행위가 국내문제불간섭 의무 위반에 해당하지 않는다는 주장의 근거로 많이 활용된다. 타국의 서버에 침입하여 정보를 열람, 수집하기만 하는 행위는 타국에 대해 눈에 보이는 손해를 끼치거나 별다른 영향을 주지 않기 때문에 국제법상 금지되는 행위가 아니라는 것이다.

그러나 앞서 살펴본 바 있듯이 사이버 간첩행위가 단순히 타국의 네트워크에 침입하여 기밀 정보를 열람하거나 수집하는데서 그치지 않고, 시스템을 파괴하거나 제거하고, 중요한 정보를 제거하는 행위를 모두 포함한다는 점에서 전통적 의미의 간첩행위와는 차이가 있다는 점을 상기할 필요가 있다. 스턱스넷도 이란의 핵 원심분리기에 물리적 손해를 가하기 전 수개월의 잠복기를 거치며 이란의 핵시설 감시활동을 한 웜바이러스라는 사실을 잊지 말아야 한다.

한편 후자를 뒷받침 하는 견해도 다수 발견할 수 있다. Dickinson은 그의 저서에서 타국의 어떤 행위가 피해국이 만족할 만큼 제거되지 않았다면 간섭행위는 계속해서 존재하는 것이라고 하였다.[289] 이는 결국 간섭의 유무를 피해국의 판단에 맡긴다는 점에서 강제의 판단 기준을 넓게 본 후자의 의견과 맥을 같이 한다고 볼 수 있다. 또 다른 예로는 1965년 국가의 독립과 주권의 보호 및 국내문제 간섭 불허용에 관한 선언(Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty)[290]과 1970년 우호관계선언을 들 수 있는데, 두 선언 모두

---

288) Myres Smith McDougal and Florentino P. Feliciano, “International Coercion and World Public Order: The General Principles of the Law of War”, The Yale Law Journal, Vol. 67, No. 5 (1958), p. 782.

289) Edwin De Witt Dickinson, *The Equality of States in International Law* (Cambridge, Mass.: Harvard University Press, 1920), p. 260.

290) Declaration on the Inadmissibility of Intervention in the Domestic

불간섭 원칙의 범위를 설명하면서 동일한 언어를 사용하고 있다. 해당선언들에서는 어떤 국가도 타국의 주권에 간섭할 권리가 없다고 하면서 타국의 주권행사를 자신의 종속 하에 두려는 '어떠한 조치'도 '강제'에 해당한다고 하고 있다. 또한 동 의무를 설명하면서 '직접적으로나 간접적으로', '이유를 막론하고', '모든 형태의 간섭' 등의 용어를 사용하고 있는데, 이런 점들을 종합하여 해당 선언들도 불간섭 의무의 강제성 개념을 넓게 설정하고 있다고 보는 견해도 있다.[291]

뿐만 아니라 강제성의 범위를 넓게 적용한 실제 사례도 찾아볼 수 있다. 1969년대 미국이 공인되지 않은 정찰을 목적으로 우주 공간에서 인공위성을 사용한데 대한 구소련의 대응이 그것이다. 우주공간은 어떤 국가의 영토에도 속하지 않기 때문에 미국의 정찰행위가 영토주권에 대한 위반이 아니었음에도 불구하고, 소련은 미국의 행위가 자국의 정치적 보전을 침해한 행위라고 주장하였다.[292] 소련은 UN 제1위원회에서 제출한 성명에서 '주권국가의 보호 하에 있는 어떤 것에 대한 침입도 그것이 주권적 사항에 관한 것이라면' 위반행위를 구성한다고 주장하였다.[293] 소련은 더 구체적인 예를 들면서 공해상에서 무슨 일이 벌어졌는지를 단순히 관찰하는 것은 위반행위가 아니지만 그 관찰이 첩보수집을 위한 것이라면 이는 명백히 주권침해 행위라고 하였다.[294] 소련의 견해에 따르면 기밀정보 수집을 위한 타국의 사이버간첩행위는 주권적 사항에 대한 침해이다. 소련의 이러한 주장은 주권적 가치를 가지는 부분에 대한 공격만으로도 강제성이 행사된 것으로 보아야 한다는 견해와 거의 일치하는 것으로 볼 수 있다. 그

Affairs of States and the Protection of Their Independence and Sovereignty, UN Doc. A/RES/20/2131 (1965).

291) Russell Buchan, *supra* note 185, p. 78.

292) Joseph R. Soraghan, "Reconnaissance Satellites: Legal Characterization and Possible Utilization for Peacekeeping", McGILL Law Journal, Vol. 13, No. 3 (1967), pp. 470-471에서 인용된 소련의 성명을 재인용.

293) *Ibid.*, pp. 470-471.

294) *Ibid.*

러나 오늘날 거의 모든 국가가 서로에 대해 사이버 간첩행위를 수행하고 있는 것을 생각한다면 강제성의 기준에 대한 광범위한 해석은 현실적으로 적용하기가 어렵다고 볼 수 있다.

결론적으로 사이버공격의 맥락에서 불간섭 의무 위반 판단을 위한 강제성 행사 여부는 앞에 제시한 전자와 후자의 견해 사이에 있는 어느 한 지점을 기준으로 판단할 수 있다. 이론상의 견해처럼 사이버 간첩행위는 저강도의 사이버공격이므로 강제성이 행사된 경우로 볼 수 없고, 그 이상의 강도를 가지는 사이버공격에 대해서만 강제성이 행사된 것으로 볼 수 있다는 식의 기계적 적용이 불가능하기 때문이다.

따라서 강제성 여부는 사이버공격의 '유형'이 아닌 그 공격의 '내용'을 가지고 판단해야 한다. 사이버 간첩행위라도 단순한 정찰행위에서 끝났다면 이는 발견이 되더라도 피해국에 의한 외교상의 항의 정도로 끝난다고 보는 것이 현실적인 해석이 될 것이다. 이와 관련하여 독일의 메르켈 총리가 자신의 개인전화를 미국이 감청한 것에 대해 오바마 대통령에게 항의 전화를 하는 식으로 대응한 것을 생각해 볼 수 있다.[295] 한 연구에서는 사이버공격의 경우에 강제성을 판단하는데 있어서 고려할 수 있는 요소로 침해당한 주권적 가치의 중요성, 해당 공격으로 인해 영향 받은 국가이익, 공격이 미친 영향의 규모, 피해자의 수를 제시한 바 있다.[296] 이는 사이버공격의 내용을 중심으로 강제성 여부 및 불간섭 의무 위반여부를 판단하는데 참고가 될 수 있을 것이다. 그러나 불간섭의무 위반을 구성하는 사이버공격의 최소한계를 판단하는 기준의 설정은 결국 국가들의 대응 및 재판소의 판결과 같은 사례의 축적을 통해 명확해 질 수 있을 것이다.

---

295) The Guardian, Oct. 24, 2013, "Angela Merkel's call to Obama: are you bugging my mobile phone?", <https://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german> (2018.1.5.최종방문).

296) Myres Smith McDougal and Florentino P. Feliciano, *supra* note 288, p. 782.

5) 적용상의 한계

이상 일반국제법원칙의 위반을 판단하는 기준을 면밀히 검토해 보고, 이를 여러 유형의 사이버공격에 대입해 본 결과, 각 기준에 해당될 수 있는 사이버공격 강도의 경계는 여전히 모호하다는 점을 확인할 수 있었다. 이러한 모호성은 앞으로 국가들의 대응사례가 축적되면서 해소될 것을 기대할 수도 있겠지만, 지금까지 발생한 사이버공격에 대한 국가들의 대응을 보면 이러한 기대가 낙관적이지만은 않다는 것을 알 수 있다. 2007년 에스토니아 공격사건부터 2016년 미국의 민주당 이메일 해킹사건에 이르기까지 피해국이 국제법적으로 대응한 사례는 미국이 러시아 및 북한에 대응조치를 취한 경우 외에 거의 찾아보기 힘들기 때문이다. 이러한 미미한 대응의 이유는 피해는 있어도 피해를 일으킨 공격자를 명확히 알 수 없는 사이버공격의 특성에서 기인한 것도 있지만, 일반국제법상의 원칙을 적용하기에 그 기준이 명확하지 않다는 점도 중요한 한 부분을 차지한다고 볼 수 있다.

따라서 이러한 판단기준과 관련한 모호성의 문제가 지속된다면 국가들은 이점을 이용해 타국에 대한 사이버공격을 확대할 수 있고, 피해국의 입장에서도 자의적으로 기준을 해석하여 대응할 위험성이 있다. 사실 이러한 위험성은 이미 현실에서 재현되고 있음을 확인할 수 있는 사례가 꽤 있다. 푸틴 대통령이 미국 민주당 이메일 해킹의혹과 관련해 자국의 애국주의적 해킹 집단이 자발적으로 그러한 행동을 하는 것을 막을 수 없다고 한 발언이 그 한 예라고 할 수 있다.[297] 당시 이 발언은 러시아가 해킹집단을 대리자로 내세워 사이버공격을 감행하고 있다는 의혹을 인정한 것으로 해석될 수 있다는 점에서 많은 관심을 불러일으킨 바 있다. 또한 미국은 소

297) Independent, Jun. 1, 2017, “Vladimir Putin hints 'patriotic' private Russian hackers could have meddled in 2016 US election”, <http://www.independent.co.uk/news/world/americas/us-politics/vladimir-putin-russian-hackers-patriotic-private-us-election-2016-donald-trump-win-dnc-hillary-a7767436.html> (2018.1.4.최종방문).

니 해킹사건에 대해 북한의 소행임이 확실하다는 증거를 가지고 있다고 하면서 북한의 네트워크를 마비시키는 역공격을 행한 바 있다.[298] 미국은 이와 함께 북한에 대해 경제제재조치도 취한 바 있다.[299] 그러나 소니해킹 공격의 주체가 북한이라는 미국의 주장에 대해서 보안 전문가들은 가능성이 낮다고 밝힌 바 있다.[300] 또한 공격의 주체가 북한이라고 해도 미국이 취한 두 가지 조치가 비례적인 조치라고 볼 수 있는지 의문이다. 이러한 미국의 대응은 공격주체의 판단에 있어서 뿐 아니라, 공격의 강도에 대해서도 자의적인 기준이 적용될 수 있음을 보여주는 예라고 할 수 있다.

따라서 모호한 기준으로 인한 부작용이 심화되는 것을 막기 위해서는 국제법원칙이 그대로 적용가능하다고 덮어두기 보다는 국가들이 국제사회에서의 논의를 통해 명확한 기준을 마련하는 것이 필요하다.

2. 조약

국가안보에 영향을 주는 사이버공격은 일반국제법원칙을 적용해서도 규

298) BBC, Dec. 23, 2014, “Sony hack: North Korea back online after internet outage”, <http://www.bbc.com/news/world-asia-30584093> (2018.1.4.최종방문).

299) Time, Jan. 1, 2015, “U.S. Sanctions North Korea Over Sony Hack”, <http://time.com/3652479/sony-hack-north-korea-the-interview-obama-sanctions/> (2018.1.4.최종방문).

300) Dailymail, Dec. 25, 2014, “North Korea was NOT behind the Sony hack according to multiple security experts who discredit FBI findings and reveal that a studio insider named 'Lena' may be responsible”, <http://www.dailymail.co.uk/news/article-2887081/North-Korea-NOT-Sony-hack-according-multiple-security-experts-discredit-FBI-findings-reveal-insider-named-Lena-responsible.html> (2018.1.4.최종방문); CNN, Dec. 27, 2014, “Experts doubt North Korea was behind the big Sony hack“, <http://edition.cnn.com/2014/12/27/tech/north-korea-expert-doubts-about-hack/index.html> (2018.1.4.최종방문).

제할 수 있지만 기존의 조약을 통해서도 규율이 가능하다. 현재까지 사이버공격 자체를 규율하는 포괄적 다자조약은 체결된 바 없다. 그러나 다수의 테러방지 조약과 그 밖의 다자조약에서 사이버공격행위를 규제할 수 있는 내용을 포함하고 있는 것을 확인할 수 있다. 조약을 통한 사이버공격의 규제는 일반 국제법원칙을 적용하는 경우보다 그 적용 대상의 범위가 좁다는 단점이 있지만 적용 대상 행위가 구체적이고 명확하다는 점에서 장점이 있다고 할 수 있다. 이하에서는 사이버공격행위의 규제가 가능한 조약과 적용되는 내용을 구체적으로 검토한다.

1) 항공분야 관련 조약

먼저 항공기에 관한 테러방지 조약을 사이버공격에 적용할 수 있는지 여부를 검토해보기로 한다. 1970년 항공기의 불법납치 억제를 위한 협약(Convention on Offenses and Certain Other Acts Committed on Board Aircraft) 제1조에서는 항공기에 탑승한 자가 항공기를 통제 하거나, 통제를 시도하는 경우를 불법행위로 규정하고 있다.[301]

1971년 민간항공의 안전에 대한 불법적 행위의 억제를 위한 협약(The Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation)[302] 제1조 제1항에서는 운행 중인 항공기를 파괴하거나 손상시키는 경우, 그러한 손상을 줄 수 있는 장치를 장착시키는 경우를 불법행위로 규정하고 있다. 특히 제1항 d호에서는 항공기의 운항을 위한 장치를 파괴 또는 손상시키는 행위, 그러한 장치의 조작을 방해하는 행위를 불법으로 규정하고 있다. 또한 동조 제2항에서는 앞에서 언급한 행위의 시도도 불법행위로 보고 있다.

1988년 국제민간항공에 사용되는 공항에서의 불법적 폭력행위의 억제를 위한 의정서(Protocol for the Suppression of Unlawful Acts of

301) 1971년 10월 14일 발효, 당사국 수는 185개국이다.
302) 1973년 1월 26일 발효, 당사국 수는 188개국이다.

Violence at Airports Serving International Civil Aviation)[303] 제2조 제1항 b호에서는 어떤 장치, 물질 또는 무기를 사용하여 국제항공기의 운행을 담당하는 공항의 시설에 대한 파괴 또는 심각한 손상을 일으키는 행위 또는 공항의 서비스를 방해하는 행위를 앞의 1971년 민간항공의 안전에 관한 협약 제1조에서 규정하는 불법행위에 포함시킬 것을 규정하고 있다. 항공 관제시스템 또는 항공기 조작시스템에 대한 사이버공격이 감행되어 각 시스템에 대한 통제권을 탈취, 조작하는 경우, 해당행위는 앞에 열거한 각 조약상의 의무를 위반한 것으로 볼 수 있다.

2) 해상분야 관련 조약

항공분야 외에도 1988년 항해 안전에 대한 불법행위 억제를 위한 협약(Convention for the Suppression of unlawful acts against the safety of maritime navigation)[304] 제1조 및 제3조[305]에서는 군함과 정부 선박을 제외한 선박에 대해서 무력 또는 어떤 다른 형태의 위협을 행사하여 통제권을 행사하는 것을 금지하고 있다. 또한 선박에 대한 해상 통항을 위한 설비를 파괴 또는 심각하게 손상시키거나 운항을 방해하는 행위 및 그 미수행위를 금지하고 있다.

한편 1988년 대륙붕상에 소재한 고정 플랫폼의 안전에 대한 불법행위의 억제를 위한 의정서(Protocol for the Suppression of unlawful acts

303) 정식 명칭은 1971년 9월 23일 몬트리올에서 채택된 민간항공의 안전에 대한 불법적 행위의 억제를 위한 협약을 보충하는, 국제민간항공에 사용되는 공항에서의 불법적 폭력행위의 억제를 위한 의정서(Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971)로 1989년 8월 6일에 발효되었으며, 당사국은 171개국이다.

304) 1992년 3월 1일 발효, 당사국 수는 156개국이다.

305) 제3조 1항 a호, e호 및 제2항.

against the safety of Fixed Platforms Located on the Continental Shelf)[306] 제2조 제1항 및 제2항에서는 무력 또는 어떤 다른 형태의 위협을 통해 고정플랫폼을 억류·통제하는 행위, 고정플랫폼을 파괴하는 행위 및 고정플랫폼의 안전을 위협하는 각종 행위와 그 미수행위 등을 각각 범죄행위로 규정하고 있다. 앞의 항공분야와 마찬가지로 선박 또는 조약의 규율 범위에 속하는 고정 플랫폼에 대한 사이버공격으로 이들 시설에 대해 통제권을 행사하거나 물리적으로 손상을 입히는 행위를 할 경우에는 협약을 적용하여 규율할 수 있다.

3) 핵 관련 조약

핵물질 관련 테러방지 조약으로는 우선 1979년 핵물질의 방호에 관한 개정 협약(Amendment to the Convention on the Physical Protection of Nuclear Material)[307] 제7조 제1항 e호에서 핵물질을 생산, 처리, 사용, 저장하는 핵시설에 대한 행위 또는 핵시설의 운영을 방해하는 행위로 상당한 양의 방사능 또는 관련물질이 누출되어 인명 또는 재산상의 피해를 일으킬 경우 조약의 위반으로 규정하고 있다. 또한 동조 g호에서는 이와 같은 행위의 위협을 금지하고 있다.

2005년 핵 테러행위의 억제를 위한 국제협약(International Convention for the Suppression of Acts of Nuclear Terrorism)[308] 제2조 제1항 b호는 사람을 사망에 이르게 하거나 상해를 입힐 목적으로 또는 재산 또는 환경에 심각한 손해를 입힐 목적으로 또는 자연인·법인·국제기구·국가에 대해 특정행위를 하지 못하게 할 목적으로 핵시설을 사용하

306) 1992년 3월 1일 발효, 당사국 수는 144개국이다.
307) 원조 핵물질 방호협약은 1987년 발효하였고, 152개국의 당사국이 있다. 현재 개정협약은 2016년 5월 8일 발효 되었으며, 당사국은 102개국이다. 개정조항은 원조약의 해당조항을 대체하거나 해당조항에 추가되어 적용된다.
308) 2007년 7월 7일 발효, 당사국은 77개국이다.

거나 손상시켜 방사능 물질을 유출시키거나 유출시킬 위험을 초래하는 행위를 금지하고 있다. 사이버공격을 통해 핵시설 운영 시스템의 통제권을 확보하여 방사능이 유출되는 경우에 이 조약을 통해 해당행위를 규제할 수 있을 것이다. 2015년에 배후가 북한으로 추정되는 해커가 한국수력원자력의 원자력 발전소 도면을 트위터에 공개하며 원자력 시설을 폭파할 것을 경고한 사건이 있었다.[309] 실제 사고가 일어나지는 않았지만 원자력 발전소에 대한 통제권을 행사해 방사능 유출 등의 사고를 시도하거나 일으켰다면 이 두 조약을 적용할 수 있다.

4) 기타 다자조약

이밖에도 1973년 외교관 등 국제적 보호인물에 대한 범죄의 방지 및 처벌에 관한 협약(Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents)[310] 제2조 제1항 b호에서 국제적 보호인물의 신체나 자유를 위태롭게 할 수 있는 그의 공관, 사저 또는 교통수단에 대한 폭력적 공격행위, c호에서는 그러한 공격의 위협, d호에서는 그러한 공격의 미수행위, e호에서는 그러한 공격에 공범으로 가담하는 행위를 범죄행위로 규정하고 있다. 이 조약에서 말하는 국제적 보호인물이란 제1조에 따르면 국가원수, 정부수반 또는 외무부장관 및 그들과 동행하는 가족 구성원으로 이들이 외국에 체류할 경우 동 조약이 적용된다. 따라서 이들이 외국에 체류하는 동안 공관, 사저 또는 교통수단에 대해 폭력적인 사이버공격을 시도하는 경우 이는 범죄행위를 구성하게 된다.

---

309) 한국경제, 2015년 7월 9일 A33면, “한수원 원전 도면 유출' 그 해커가 돌아왔다”, <http://www.hankyung.com/news/app/newsview.php?aid=2015070892041> (2018.1.5.최종방문).

310) 1977년 2월 20일 발효, 당사국은 172개국이다.

또한 1997년 폭탄테러행위의 억제를 위한 국제협약(International Convention for the Suppression of Terrorist Bombings)[311] 제2조 제1항에서는 공공장소, 국가나 정부시설, 대중교통 시스템 또는 기반시설에 대해 폭발물 뿐 아니라 기타 장치를 통해서 사망이나 심각한 신체적 손상을 일으키려는 의도로, 앞서 언급한 장소나 시스템을 파괴하거나 중대한 경제적 손실을 일으키려는 의도로 폭발물 뿐 아니라 기타 장치를 넘겨주거나, 장착 또는 폭발시키는 등의 행위를 범죄행위로 보고 있다. 또한 같은 조 제2항 및 제3항에서는 각각 미수행위, 공모행위 등도 범죄행위로 규정하고 있다. 제1조에서는 국가 또는 정부시설을 정부 대표, 공무원 또는 정부간기구의 직원 등이 사용하는 건물을 포함하는 것으로 정의하고 있으며, 기반시설은 그 소유기관에 상관없이 상수도, 에너지, 연료 또는 통신서비스를 공급하는 시설을 의미한다고 규정하고 있다. 또한 제1조 제3항에서 인명피해나 상당한 손해를 초래할 수 있도록 고안 되었거나 그러한 능력을 가진 것을 '기타 장치'라고 정의하고 있다. 따라서 단지 폭발물이 아닌 컴퓨터 장치, 논리폭탄, malware 등을 이용한 사이버공격을 통해 국가 기반시설 등에 폭발을 일으키거나 이를 시도하는 경우에도 이 조약의 적용을 통해 규제할 수 있을 것으로 보인다.

한편 1999년 테러리즘의 자금조달 억제를 위한 국제협약(The International Convention for the Suppression of the Financing of Terrorism)[312] 제2조에서는 부속서에 언급된 조약들[313]에서 규정하고 있

311) 2001년 5월 23일 발효, 당사국은 164개국이다.
312) 2002년 4월 10일 발효, 당사국은 173개국이다.
313) 동 협약의 부속서에서는 Convention for the Suppression of Unlawful Seizure of Aircraft(1970), Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation(1971), Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents(1973), International Convention against the Taking of Hostages(1979), Convention on the Physical Protection of Nuclear Material(1980), Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving

는 위법행위에 대해 직·간접적으로 자금을 제공하거나 모금한 행위와 그 미수행위를 불법으로 규정하고 있다. 부속서에 열거되어 있는 조약들에는 앞에서 언급한 조약들이 모두 포함되어있다. 따라서 앞서 언급한 조약들에서 금지하고 있는 행위에 자금을 조달한 경우에도 적용이 가능하다.

5) 적용상의 한계

그러나 이들 조약은 행위가 아닌 행위자에 대한 처벌을 중심으로 규율하고 있어, 이를 통해 국가를 규율하는 데는 한계가 있다는 단점이 있다. 이들 조약의 당사국들이 부담하는 의무는 협약상의 범죄를 국내법상의 범죄로 규정[314]하고, 처벌 수단을 마련하는 것이다. 또한 당사국들은 협약상의 범죄행위에 대한 관할권 확립[315], 협약상의 범죄를 당사국 간 체결한

International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation(1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation(1988), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf(1988), International Convention for the Suppression of Terrorist Bombings(1997)로 총 9개의 테러방지조약을 언급하고 있다.

314) 1970년 항공기의 불법납치 억제를 위한 협약 제2조; 1971년 민간항공의 안전에 대한 불법적 행위의 억제를 위한 협약 제3조;1973년 외교관 등 국제적 보호인물에 대한 범죄의 예방 및 처벌에 관한 협약 제2조 제2항;1988년 항해 안전에 대한 불법행위 억제를 위한 협약 제5조; 1997년 폭탄테러의 억제를 위한 국제협약 제4조; 1999년 테러리즘의 자금조달 억제를 위한 국제협약 제4조; 2005년 핵테러행위의 억제를 위한 국제협약 제5조.

315) 1970년 항공기의 불법납치 억제를 위한 협약 제4조; 1971년 민간항공의 안전에 대한 불법적 행위의 억제를 위한 협약 제5조;1973년 외교관 등 국제적 보호인물에 대한 범죄의 예방 및 처벌에 관한 협약 제3조;1988년 항해 안전에 대한 불법행위 억제를 위한 협약 제6조; 1988년 대륙붕상에 소재한 고정 플랫폼의 안전에 대한 불법행위의 억제를 위한 의정서 제3조;1997년 폭탄테러의 억제를 위한 국제협약 제6조; 1999년 테러리즘의 자금조달 억제를 위한 국제협약 제7조.

범죄인인도조약상의 인도대상 범죄로 포함시킬 의무[316] 및 이러한 범죄행위를 방지하기 위해 모든 실행 가능한 조치를 취할 의무[317]를 담당한다. 즉 협약의 당사국들은 협약의 직접적인 위반 당사자가 될 수 없고, 협약에 규정된 입법조치를 하지 않았거나 범죄행위를 방지하지 못한 것에 대해서만 국가책임을 지게 되는 것이다. 따라서 협약에서 규정하고 있는 금지된 행위에 속하는 사이버공격을 수행한 테러조직이나 해커조직이 실제 규율대상이라고 할 수 있다. 때문에 국가가 직접 협약에서 규정하고 있는 사이버공격을 감행한 경우에는 이들 조약을 적용하기에는 사실상 한계가 있다는 문제점이 있다. 또한 국가가 proxy를 통해 사이버공격을 한 경우에는 해당 국가가 관련자를 처벌하거나, 범죄인 인도 조항에 따라 proxy를 인도할 가능성은 희박하다고 볼 수 있다.[318] 이는 앞서 살펴본 협약을 통해 비국가행위자 및 국가의 사이버공격을 규제하는데 한계가 있음을 보여준다. 한편 협약을 통해 국가행위에 대한 직접 책임을 추궁하기는 어렵더라도, 비국가행위자에 대한 처벌이나 인도를 요구하기 위해서는 확실한 귀속이 요구된다. 그러나 타국에서 수행된 사이버공격에 대한 귀속을 밝히기 위해서는 공격의 발생지로 추적되는 국가, 즉 비국가행위자가 소재하고 있는 국가의 협조가 필수적인 경우가 많다. 따라서 위반행위와 관련해서 협

316) 1970년 항공기의 불법납치 억제를 위한 협약 제8조 제1항; 1971년 민간항공의 안전에 대한 불법적 행위의 억제를 위한 협약 제8조 제1항;1973년 외교관 등 국제적 보호인물에 대한 범죄의 예방 및 처벌에 관한 협약 제8조 제1항;1988년 항해 안전에 대한 불법행위 억제를 위한 협약 제10조 제1항; 1997년 폭탄테러의 억제를 위한 국제협약 제8조 제1항; 1999년 테러리즘의 자금조달 억제를 위한 국제협약 제4조; 2005년 핵테러행위의 억제를 위한 국제협약 제13조 제1항.

317) 1971년 민간항공의 안전에 대한 불법적 행위의 억제를 위한 협약 제10조 제1항;1973년 외교관 등 국제적 보호인물에 대한 범죄의 예방 및 처벌에 관한 협약 제4조;1988년 항해 안전에 대한 불법행위 억제를 위한 협약 제13조 제1항; 1997년 폭탄테러의 억제를 위한 국제협약 제15조; 1999년 테러리즘의 자금조달 억제를 위한 국제협약 제18조; 2005년 핵테러행위의 억제를 위한 국제협약 제7조.

318) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 510.

조에 관한 의무를 명시하고 있지 않은 현재의 협약체제는 그 적용이 상당히 제한적이라고 할 수 있다.

제2절 사이버공간의 특성과 현 체제의 한계

1. 귀속성기준 중심 논의의 한계

지금까지 사이버공격에 대해서 일반국제법원칙과 조약을 적용하는 문제에 대해 살펴보았다. 기존의 국제법원칙을 적용하여 사이버공격을 규율할 수 있다고 해도 행위의 귀속 문제가 해결되지 않으면 그러한 원칙의 적용이 가능하다는 사실은 무의미해진다.[319] 위반행위의 당사자를 밝히지 못했다는 것은 곧 법 적용의 대상이 부재함을 의미하기 때문이다. 즉, 한 국가에 타국으로부터의 사이버공격이 발생했다고 한다면 피해국은 공격의 강도에 따라 자위권을 행사할 수도 있고, 대응조치를 취하거나 다른 국제법원칙의 위반을 들어 국가책임을 추궁할 수도 있을 것이다. 그러나 현 국제법 하에서는 '누가' 위법한 사이버공격을 감행했는지 귀속을 밝히고, 그 행위가 국가로 귀속이 되는 경우에 한해서 자위권이나 대응조치를 통해 대응을 할 수 있다.[320] 따라서 '귀속'의 문제를 다루지 않고 사이버공격에 대한 국제법원칙의 적용가능 여부를 논의하는 것은 그 의미가 퇴색될 수 밖에 없는 것이다. 그만큼 행위의 귀속을 밝히는 문제는 중요하다. 귀속의 문제는 특히 사이버공격의 경우에 더 중요하게 다루어지고 있는데, 이는 사이버공간의 특성상 물리적 공간에서 일어난 사건의 경우보다 귀속을 밝히기가 더 어렵기 때문일 것이다. 이하에서는 기존의 귀속성 판단 법리 및 기준과 사이버공간에서의 귀속성 판단의 차이 등을 검토해 보고, 현 체제의 한계에 대해 논의해보기로 한다.

---

319) Sklerov는 귀속의 문제가 사실상 국가들의 대응을 봉쇄하고 있다고 하였다. Matthew J. Sklerov, *supra* note 112, p. 8.

320) 자위권의 경우 비국가행위자로 행위자가 밝혀지더라도 원용이 가능할 수 있다. 이에 대해서는 본 절 비국가행위자의 규율에 관한 논의에서 후술하기로 한다.

1) 국가귀속성 법리적용의 한계

기존의 국가귀속성 법리를 사이버공격에도 그대로 적용할 수 있는지 여부를 알기위해서는 우선 물리적 공간에서 위법행위의 귀속을 밝히는 것과 사이버공격에 대한 귀속을 밝히는 것의 차이에 대해 살펴보는 것이 필요하다. 먼저 물리적 공간에서 국제법위반행위가 발생한 경우에는 공격의 위치와 공격의 행위자를 밝히는 것이 그리 어려운 일이 아니다. 미사일을 발사하거나 무기지원 등을 하는 경우 물리적 공간에 그 흔적이 남고, 공격자도 명확히 드러나기 때문이다.[321] 따라서 이 경우 피해국이 국가책임을 추궁할 때 쟁점이 되는 국가 귀속성의 문제는 공격 행위자와 국가의 연관성을 밝히는 것이다. 실제 사례를 통해 살펴보면 이는 더욱 명확해진다. 9.11 테러에 대해 자위권을 행사 하는데 있어 미국이 염두에 둔 것은 공격자인 알카에다를 찾는 것이 아니라, 알카에다와 알카에다의 주둔지인 아프가니스탄의 연관성이었다.[322]

ICJ에 회부된 사건 중 국가귀속성 여부가 쟁점이 되었던 대표적인 두 사건의 경우도 마찬가지다. 1986년 니카라과 사건에서는 반군의 위법한 행위가 미국에 귀속되는지가 문제 되었고, 2007년 보스니아 제노사이드 사건에서는 세르비아계 민병대가 보스니아 회교도를 집단학살한 행위가 신유고연방의 행위로 귀속되는지가 쟁점이 되었다. 이 같은 사례에서 볼 수 있듯, 물리적 공간에서는 위반행위의 당사자를 찾는 것 자체가 문제가 되는 것이 아니라 드러난 공격자와 그 배후의 연관성을 찾는 것이 문제가 된다. 그러나 사이버공격의 경우에는 공격자를 찾는 문제부터 시작해야 한

321) Kenneth Geers, Darien Kindlund, Ned Moran, Rob Rachwald, “World War C: Understanding Nation-State Motives Behind Today’s Advanced Cyber Attacks”, FireEye (2013), p. 5.

322) 알카에다의 행위가 그 주둔지인 아프가니스탄에 귀속된다면 자위권을 행사할 명분이 명확해지기 때문이다. 그렇지 않을 경우, 비국가행위자인 알카에다에 자위권을 행사할 수 있는지의 문제 및 자위권 행사과정에서 아프가니스탄의 영토주권 침해 문제가 발생하기 때문이다.

다. 따라서 물리적 공간에서는 행위의 귀속성이 공격자의 행위를 국가에 귀속시키는 한 가지 문제로 나타난다면, 사이버공격에서는 다음과 같이 여러 단계를 거쳐 귀속성이 밝혀질 수 있다. 첫 번째 단계는 현재 일어나고 있는 위험이 사이버공격에 의한 것인지 아니면 단순한 네트워크 오작동 문제인지를 파악하는 것이다.[323] 사안이 사이버공격에 의한 것이라는 것이 밝혀진 후에는 공격의 거점이 되고 있는 컴퓨터, 서버 또는 IP주소를 추적해야 한다. 또한 추적한 공격거점이 실제 위협의 유포지인지 위장된 주소인지 검증해야 하는데, 여기까지의 과정이 두 번째 단계에 해당한다.[324] 세 번째로는 추적한 컴퓨터 또는 서버를 사용한 공격 행위자를 찾아야 한다. 그리고 나서야 마지막 네 번째 단계로 공격 행위자와 국가와의 연관성을 밝히는 작업에 착수하게 된다.[325] 이렇게 총 네 단계 중 세 단계를 거치고 나서야 물리적 공간에서의 경우와 같은 선상에서 귀속성 문제를 다룰 수 있게 되는 것이다.

그런데 2001년 국제위법행위에 대한 국가책임 ILC 초안 규정 등을 보면, 귀속에 관한 법리는 물리적 공간의 경우를 중심으로 형성되어 있음을 알 수 있다. 2001년 ILC 국가책임 초안 제4조부터 제11조까지는 개인 또는 기관의 행위가 국가행위로 귀속될 수 있는 경우에 대해 규정하고 있다. 그 중에서도 행위의 실행은 사인이 하였으나 사인과 국가 사이의 특별한 관계가 의심될 때, 국가귀속성을 증명하기 어려운 문제가 종종 발생한다.

---

323) JustSecurity, Dec. 11, 2014-Kristen Eichensehr, “Cyber Attribution Problems--Not Just Who, But What”, Just Security, <https://www.justsecurity.org/18334/cyber-attribution-problems-not-who/> (2017.4.13.최종방문).

324) Chris Prosise, Kevin Mandia, *Incident Response & Computer Forensics*, 2nd ed. (Mcgraw-Hill, 2003), p. 25; Susan W. Brenner, “At Light Speed”: Attribution and Response to Cybercrime/Terrorism/Warfare, Journal of Criminal Law & CRIMINOLOGY, Vol. 97 (2007), p. 383.

325) Russell Buchan, Marco Roscini, Nicholas Tsagourias, “State Responsibility for Cyber Operations: International Law Issues, British Institute of International and Comparative Law (2014), p. 6.

따라서 이 문제를 규정하고 있는 제4조 및 제8조가 귀속여부를 판단하는 데 주로 문제가 되어왔다. 초안 제4조는 국내법에 근거가 있는 국가기관의 행위를 국가의 행위로 귀속시킬 수 있다고 규정하고 있고, 제8조는 사인이 한 행위라도 사실상 국가의 명령이나 지시 또는 통제에 따라 행동한 경우에는 국가의 행위로 귀속된다고 규정하고 있다.

그러나 ICJ는 여기에서 더 나아가 '통제'의 정도를 중심으로 국가귀속성을 판단하는 기준을 정립하여 적용해 왔다. ICJ는 제4조와 관련하여 가장 높은 통제의 수준을 의미하는 전적인 의존성(complete dependence) 기준을 적용하였다.[326] 초안 제4조는 국내법상의 근거를 요건으로 명시하고 있으나 ICJ는 비록 국내법상의 근거가 없더라도 개인이나 단체가 국가와 전적인 의존관계에 있는 경우에는 예외적인 경우로서 국가기관과 동일하다고 보았다.[327] ICJ는 니카라과 사건에서 반군이 미국의 정부 기관과 동일시되거나 이들의 행위가 미국정부를 위하여 한 행위라고 증명될 수 있을 정도의 통제가 행사된 경우에 이 기준이 충족될 수 있다고 보았다.[328] 2007년 보스니아 제노사이드 사건에서 ICJ는 전적인 의존성이 완전한 통제를 의미하며 개인이나 단체가 어떠한 자율성도 가지지 않은 국가기관의 단순한 도구로써 행동하는 것을 말한다고 설시하였다.[329]

한편 제8조에 대해서는 완전한 통제 보다는 낮은 수준의 실효적 통제 기준(effective control)을 적용하여 개인이나 집단의 행위를 국가의 행위

---

326) 니카라과 사건 당시에는 국가책임초안이 완성되지 않았었기 때문에 이 기준과 관련한 규정이 언급되지 않았으나, 2007년 보스니아 사건에서 ICJ는 전적인 의존성이 초안 제4조의 국가기관 여부를 판단하기 위한 것이라고 하였다. *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007*, paras. 397, 406.

327) *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986*, paras. 109-110; *Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), I.C.J. Reports 2007*, para. 393.

328) *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986* , para. 109.

329) *Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), I.C.J. Reports 2007*, para. 394.

로 간주할 수 있는 것으로 보았다.[330] ICJ는 니카라과 사건에서 실효적 통제의 기준을 만족시키기 위해서는 국제법에 위반되는 구체적 행위에 대한 국가의 지시 또는 강요가 있어야 한다고 보았다.[331] 이후 ICJ는 보스니아 제노사이드 사건에서도 VRS가 세르비아의 실효적 통제 하에 행동했는지를 판단하기 위해 위반행위가 일어난 각각의 작전에 대하여 통제나 지시가 이루어 졌는지를 살펴보았다.[332]

이밖에도 1997년 Tadić사건에서 구유고전범재판소(ICTY)의 상소심 재판부는 전반적 통제(overall control)의 개념을 적용하여 귀속성여부를 판단하였다. 상소심재판부는 집단에 대한 지원 뿐 아니라 해당 집단이 활동하는데 있어 전반적 계획을 조직 또는 도와주는 것을 전반적 통제로 보았다.[333] 상소심 재판부는 군대나 비정규군과 같이 조직화되고 체계화된 집단에 대해서는 니카라과 사건에서 실효적 통제여부를 판단하기 위해 요구된 '위반행위에 대한 국가의 구체적 지시'가 있었는지를 입증할 필요가 없다고 하였다. 상소심 재판부는 이 '조직화되고 체계화된 집단'의 구성원은 독립적으로 행동하지 않고, 조직의 기준에 따라 행동하며 그 조직의 장의 권위에 복종하기 때문에 그 조직 전체가 국가의 전반적 통제 하에 있다면 귀속성을 만족시키기에 충분하다고 보았다.[334]

이렇게 귀속성에 관한 ILC 초안 규정이나 ICJ 및 ICTY의 법리는 모두

---

330) Ibid., paras. 401, 413; *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986*, para. 115.

331) *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986*, para. 115; Ibid, Separate Opinion of Judge Ago, para. 16.

332) *Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), I.C.J. Reports 2007*, para. 413.

333) *Prosecutor v. Dusko Tadić, ICTY, Case IT-94-1-A, 1999*, para. 114.

334) Ibid, para. 120. 이 사건은 VRS가 민간인들을 수용소에 감금·구타·살해한 행위에 대해서 이에 참여한 Dusko Tadić의 형사책임을 다룬 것이었다. 따라서 이 사건에서 VRS가 유고연방의 사실상 기관인지 여부가 다루어진 이유는 개인의 형사책임을 추궁하기 위해 Tadić의 행위가 재판소의 관할 대상범죄를 구성하는지를 결정하기 위해서였지 국가책임이 문제가 되었던 것이 아님을 유념할 필요가 있다.

공격자가 특정된 상황에서 그 공격자와 국가와의 관계를 밝히는데 초점이 맞춰져 있다. 사이버공격의 행위자를 밝히기 위한 앞의 세 단계에 대한 내용은 규정이나 법리 모두에 있어 고려대상이 되고 있지 않은 것이다. 그런데도 현재 사이버공격의 귀속에 관한 연구는 기존 기준의 적용가능여부 또는 기준의 수정이 필요한지 여부에 초점이 맞춰져있다.[335] 이러한 연구가 필요가 없다거나 적절하지 않다는 것은 아니다. 국가들이 proxy를 이용해 사이버공격을 하는 경우가 증가하고 있기 때문에 기존의 기준 자체에 관한 논의도 반드시 필요하다. 그러나 공격자를 찾아내는 것부터가 귀속성 증명의 출발이 되는 사이버공격의 경우, 이 문제에 관한 고려 없이 공격자가 특정된 후의 경우를 상정하고 있는 기존의 기준에 관한 논의만을 하는 것은 여러 단계를 건너 뛴 논의에 불과하다.

2) 행위자확인원칙의 필요성

앞의 세 단계가 귀속의 문제와 관련해 중요하게 논의되어야 하는 이유는 다음과 같다. 우선 사이버공격의 귀속문제는 기술의 문제가 중요한 부분을 차지하기 때문이다. 이는 첫 번째 및 두 번째 단계와 관련이 있다. 먼저 첫 번째 단계와 관련하여 현재 감지된 이상 현상이 오작동에 의한

335) David E. Graham, “Cyber Threats and the Law of War”, Journal of National Security Law & Policy, Vol. 4 (2010), pp. 92-93; Luigi Condorelli, Claus Kress, “The Rules of Attribution: General Considerations”, in James Crawford, Alain Pellet, Simon Olleson (eds.), *The Law of International Responsibility* (Oxford University Press, 2010), p. 227; Russell Buchan, Marco Roscini, Nicholas Tsagourias, *supra* note 325, p. 5; Nicholas Tsagourias, *supra* note 161, p. 239; Collin S. Allan, “Attribution Issues in Cyberspace”, Chicago-Kent Journal of International and Comparative Law, Vol. 13, No. 2 (2013), pp. 73-74; Kubo Macak, “Decoding Article 8 of the International Law Commission’s Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors”, Journal of Conflict & Security Law (2016), p. 423.

것인지 사이버공격에 의한 것인지를 알기 위해서는 패킷 흐름의 분석과 같은 기술이 필요하다.[336] 이상 현상이 공격으로 판정된 다음으로는 네트워크상의 공격거점을 파악해야 한다. 이를 위해서는 digital forensic 기법을 사용해 공격의 소스를 추적한다. forensic 기법은 법정에 증거로 제시할 목적으로 증거를 수집, 분석, 처리하는 것을 의미한다.[337] digital forensic은 컴퓨터, 휴대전화, 폐쇄회로(CC)TV 등의 정보기기에 남아 있는 디지털 자료를 법적 증거로 사용하기 위해 이를 수집하여 과학적으로 분석하고 탐색하는 절차를 의미한다.[338]

사이버공격의 경우, 삭제된 이메일을 복구하여 증거를 수집하거나 네트워크 분석을 통해 IP주소 등을 역추적하여 악성코드나 공격의 거점을 알아내는 방법을 주로 사용하게 된다. 그러나 forensic 기법을 통해서는 공격 컴퓨터나 공격의 위치를 찾아내는 데 도움을 얻을 수는 있지만 그 결과가 완벽할 수 없다는데 함정이 있다.[339] 인터넷은 본래 사용자를 추적하

---

336) 이란정부는 스턱스넷 사건 발생 초반에 원심분리기에 일어난 피해가 기술문제나 시스템 운영 문제로 인해 일어난 것으로 보았다. The New York Times, Jun. 1, 2012, “Obama Order Sped Up Wave of Cyberattacks Against Iran”, <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0> (2017.4.18.최종방문); 2008년 BTC 송유관 폭발 당시에도 폭발의 원인이 사이버공격 때문이라는 것을 파악하지 못했으나, 전문가들의 조사 후에 해커들이 시스템 취약점을 이용해 네트워크에 침투하여 악성코드를 삽입하여 일어난 사건임을 알아낼 수 있었다. Homeland Security News Wire (Dec. 17, 2014), <http://www.homelandsecuritynewswire.com/dr20141217-2008-turkish-oil-pipeline-explosion-may-have-been-stuxnet-precursor> (2017.4.14.최종방문).

337) 양대일, 정보보안개론, (한빛아카데미, 2013), p. 253.

338) 한국정보통신기술협회, "정보보호기술용어", 한국정보통신기술협회 (2013), p. 24.

339) Lipson, H.F., *supra note* 10, pp. 13-14; Scott J. Shackelford, *supra* note 10, p. 200.

기 위한 의도로 만들어진 것이 아니고,[340] 해커들은 tunneling[341] 및 데이터 로그를 파괴하는 것과 같이 추적을 어렵게 만드는 다양한 기술을 보유하고 있다. 이는 사이버공격 후에는 이러한 기술을 이용하여 공격의 흔적을 지워버릴 수 있음을 의미한다. 따라서 추적 기술은 신속성과 결합된 경우에 그 효과를 볼 수 있다.

한편 세 번째 단계인 추적한 공격 서버의 사용자인 실제 공격자를 찾는 데는 기술 외의 요소가 필요하다. 트래킹 기술을 통해 공격의 거점을 알아냈다고 해도, 이것이 실제 공격이 이루어지고 있는 지정학적 위치를 나타내는 것은 아닐 수 있기 때문이다.[342] 오늘날 인터넷 사용자들은 암호화(encryption), 이미지 및 오디오 파일과 같은 디지털 매체를 통해 메시지를 숨겨 전송하는 steganography, 익명의 이메일 계정, 보낸 사람을 숨기거나 위장할 수 있는 fake mail, IP 소스 도용 등 사이버공간에서 실제 사용자를 위장할 수 있는 기술에 점점 능숙해지고 있다.[343] 실제로 전문가들은 러시아가 공격의 근원지를 아시아인 것처럼 위장하여 사이버공격을 실행한 사례들을 확인했다고 밝힌 바 있다.[344] 때문에 패킷[345]이 발생하는

---

340) Lipson, H.F., *supra note* 10, pp. 13-15.

341) 데이터 스트림을 인터넷 상에서 가상의 파이프를 통해 전달시키는 기술로 패킷 내에 터널링할 대상을 캡슐화시켜 목적지까지 전송한다. 대부분 보안 채널의 역할을 하므로, 암호화 기법 적용이 필요하고, 엄격하게 계층화된 프로토콜들을 뒤집어 감싸서 만들 수도 있다. 터널링에는 여러 가지 종류가 있는데, 그 중 SSH 터널링은 방화벽에 터널을 뚫어 오리지널 패킷을 직접 연결시키는 기법이다. 즉, 암호화된 패킷을 직접 전달하는 것이기 때문에 악성코드 탐지에 걸리지 않는다.

342) Russell Buchan, Marco Roscini, Nicholas Tsagourias, *supra* note 325, p. 2; Levi Grosswald, *supra* note 178, p. 1167; Susan W. Brenner, *supra* note 324, pp. 409-410.

343) Chris Prosise and Kevin Mandia, *supra* note 324, p. 25; 공격자는 사이버공간상에서 공격자와는 전혀 무관한 위치에 있는 시스템을 장악할 수 있고, 이들 시스템을 좀비로 활용하여 공격을 감행할 수도 있다 Mary Ellen O'Connell, *supra* note 231, p. 202.

344) Kenneth Geers, Darien Kindlund, Ned Moran, Rob Rachwald, *supra* note 321, p. 13.

지점을 밝혀냈다고 해서 이것이 곧 공격행위자를 찾았다는 것을 의미하는 것은 아니다. 이는 단지 지금 현재 공격 흐름을 유포하고 있는 공격의 수단을 의미하는 것이다. 때문에 네트워크 또는 서버가 위치한 곳에서 공격자가 사이버공격을 하고 있는지를 알기 위해서는 공격 서버가 있는 곳으로 탐지된 현지와의 협력을 통한 확인 작업이 필요한 것이다. 이는 사이버공격의 행위자를 밝히기 위해서는 공격의 흐름이 탐지된 국가의 협조가 반드시 필요하다는 것을 의미한다.

한 연구에서는 사이버공격사건 문제를 해결하는 데 있어 가장 중요하다고 할 수 있는 공격자 파악을 위해서는 forensic 기법뿐 아니라 다른 국가들의 전략 및 지정학적 목표에 대한 심층적 이해가 뒷받침 되어야 한다는 점을 지적하고 있다.[346] 따라서 사이버공격의 경우에도 국가귀속성을 밝히기 위해서는 digital forensic 기법 외에도 국가정보기관이 제공하는 정보, 국가와 해킹조직 간의 연계성에 관한 정보나 정황 및 이에 대한 분석 등이 함께 필요하다.[347]

사이버공격의 귀속을 밝히는 문제는 이와 같이 각 단계가 긴밀히 연결되어 있는 종합적인 과정이다. 따라서 공격자를 밝히는 과정이 생략된 기존의 귀속성 법리를 사이버공격에 그대로 적용하는 것은 적절하지 않다. 사이버공격의 귀속을 밝히는 것은 국가책임 추궁의 차원을 넘어서 효과적인 대응을 위한 핵심요소이기 때문이다. 따라서 이러한 대응을 위한 출발

345) 패킷(packet)은 데이터 전송에서 사용되는 데이터의 묶음을 말한다. 패킷 전송은 두 지점 사이에 데이터를 연속적으로 전송하지 않고, 전송할 데이터를 적당한 크기로 나누어 패킷의 형태로 구성한 다음 패킷들을 하나씩 보내는 방법을 쓴다. 각각의 패킷은 일정한 크기의 데이터뿐만 아니라 데이터 수신처, 주소 또는 제어 부호 등의 제어 정보까지 담고 있다. 한국정보통신기술협회 정보통신용어사전, <http://word.tta.or.kr/dictionary/dictionaryView.do?word_seq=061960-2> (2018.1.25.최종방문).

346) Kenneth Geers, Darien Kindlund, Ned Moran, Rob Rachwald, *supra* note 321, p. 5.

347) Russell Buchan, Marco Roscini, Nicholas Tsagourias, *supra* note 325, p. 2.

점이 되는 행위자 확인에 관한 법리 및 절차적 공백의 해결이 국가귀속성 기준의 문제보다 우선적으로 논의되어야 한다.

2. 비국가행위자 규율방안의 부재

1) 주요행위자 또는 대리자로서의 비국가행위자

사이버공격을 규율하는 데 있어 현 국제법체제에 존재하는 또 하나의 한계점은 바로 비국가행위자를 규제할 규범과 체제가 부재하다는 점이다. 이 문제가 사이버공격에 있어 특히 중요한 이유는 사이버공간의 특성과 관련이 있다. 사이버공격을 위한 기술획득이 비교적 용이하고 상대적으로 적은 비용이 요구되는 사이버공간의 특징은 비국가행위자가 악의적인 사이버공격의 주요행위자로 활동할 수 있는 충분한 여건을 제공해 준다.[348] 뿐만 아니라 기본적으로 익명성이 보장되고[349], 장소적 한계를 뛰어넘을 수 있다는 점도 테러조직과 같은 비국가행위자가 활발히 활동할 수 있는 환경을 만들어주고 있다.[350]

중요한 것은 이러한 점이 단지 우려사항이 아니라 지금 현재에 일어나고 있다는 점이다.[351] 2017년 전 세계를 강타한 워너크라이 사건[352]은 사

348) Russell Buchan, Marco Roscini, Nicholas Tsagourias, *supra* note 325, p. 4.

349) Mary Ellen O'Connell, *supra* note 231, p. 202.

350) Russell Buchan, "Cyberspace, Non-State Actors and the obligation to Prevent Transboundary Harm", Journal of Conflict & Security Law, Vol. 21, No. 3 (2016), p. 429.

351) 최근 국가주요기반시설에 대한 사이버공격에 대한 테러조직들의 관심이 증가하고 있으며, 이들이 사이버공격 기술을 보유한 전문가들을 고용하고 있다는 사실이 보도된 바 있다. Meduza, Jul. 20, 2017, "Moscow's cyber-defense How the Russian government plans to protect the country from the coming cyberwar", <https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense> (2017.10.9.최종방문).

이버무기를 해킹할 수 있는 기술이 얼마나 가공할 만한 위력을 발휘할 수 있는지를 보여준 예다. 이밖에도 2003년 알카에다가 미국의 기반시설을 정찰한 증거를 확보했다는 미 정보기관의 발표[353] 이후, 주로 인터넷공간을 테러조직원 모집이나 propaganda의 도구로만 사용하는 것으로 인식되어 오던 테러조직들이 최근 몇 년간 언론사나 정부기관 등에 대한 사이버공격을 감행하면서[354] 테러조직의 사이버공격에 대한 우려가 다시 나타나고 있다. 한 예로 ISIL은 2015년 프랑스 공영방송국 TV5Monde의 네트워크를 공격해 11개의 채널 및 웹사이트와 소셜미디어 개정을 장악하고, 해킹을 통해 획득한 프랑스 군인들에 대한 정보를 공개하는 등의 사건이 있었다.[355]

가장 심각한 문제는 비국가행위자가 국가의 지원을 받아 타국에 대한 사이버공격을 하는 빈도가 증가하고 있다는 점이다.[356] 2014년 미국의 통

---

352) 사건에 관한 자세한 설명은 본 논문 제2장 제2절 참조.

353) Cyber Warfare Frontline, Mountain View, PBS (2003), <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/clarke.html> (2018.1.5.최종방문).

354) Nicholas Tsagourias, "Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts", Journal of Conflict & Security Law, Vol. 21, No. 3 (2016), p. 456.

355) The Telegraph, Apr. 9, 2015, "Isil hackers seize control of France's TV5Monde network in 'unprecedented' attack", <http://www.telegraph.co.uk/news/worldnews/europe/france/11525016/Isil-hackers-seize-control-of-Frances-TV5Monde-network-in-unprecedented-attack.html> (2017.10.9.최종방문).

356) Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012), p. 53; Financial Times, Sept. 5, 2015, "Cyber crime: states use hackers to do digital dirty work", <https://www.ft.com/content/78c46db4-52da-11e5-b029-b9d50a74fd14#axzz3l9Zncob9> (2017.4.17.최종방문); The Express Tribune, Jan. 19, 2017, "NATO sees sharp rise in state-backed cyber attacks: Stoltenberg", <https://tribune.com.pk/story/1300700/nato-sees-sharp-rise-state-backed-cyber-attacks-stoltenberg/> (2017.4.17.최종방문);

신기업 Verizon의 데이터 침입에 관한 조사 보고서(Data Breach Investigations Report)는 국가가 연계된 조직에 의한 사이버 간첩행위가 증가추세에 있으며, 2013년 총 사례 중 87퍼센트에 달하는 511건이 동아시아(49%) 또는 동유럽(21%)에서 기인한 국가가 연계된 해커조직에 의한 것이라고 밝혔다.[357] 특히 러시아와 중국은 '민족주의 해커집단(nationalistic hackers)'을 통해 사이버공격을 수행해 왔다는 의혹을 받아왔지만 그때마다 단호하게 이를 부인해 왔다.[358] 그러한 의혹은 공격의 거점과 공격 수행자의 신원을 밝히는 등 상당히 신빙성 있는 자료들로 뒷받침 되었으나 그때마다 중국과 러시아는 이들과의 연루성을 일축하는 것으로 공격의 배후를 밝히는 문제는 흐지부지 되었다.[359]

Nashi[360]와 RBN[361]은 러시아가 배후에 있는 것으로 추정되는 대표적

ABC News, Sept. 23, 2016, "Concerns over rise in state sponsored cyber attacks", <http://www.abc.net.au/news/2016-09-23/concerns-over-rise-in-state-sponsored-cyber-attacks/7872182> (2017.4.17.최종방문); SC Media, Sept. 29, 2015, "The rise of state-sponsored cyber attacks", <https://www.scmagazineuk.com/the-rise-of-state-sponsored-cyber-attacks/article/534793/> (2017.4.17.최종방문); Securityweek, Aug. 23, 2016, "Rise in State-sponsored Cyber Espionage: The Tipping Point of Cyber Warfare?", <http://www.securityweek.com/rise-state-sponsored-cyber-espionage-tipping-point-cyber-warfare> (2017.4.17.최종방문).

357) Patryk Pawlak and Gergana Petkova, "State-sponsored hackers: hybrid armies?", Issue Alert in European Union Institute for Security Studies (2015), p. 2.

358) Stewart Baker, Shaun Waterma, George Ivanov, "In the Crossfire-Critical Infrastructure in the Age of Cyber War", McAfee (2010), p. 31.

359) *Ibid.*

360) 친 푸틴 청년단체로 러시아 및 러시아 정부의 정책에 반대하는 세력에 대항하는 활동을 국내외적으로 펼치고 있다. Jeffrey Carr, *supra* note 69, p. 115.

361) Russian Business Network, 러시아의 상트 페테르부르그에 기반을 둔 사이버 범죄조직.

인 해커조직 및 사이버 범죄 집단이다. 2009년 Nashi의 일원이 한 언론사와의 인터뷰에서 자신 및 몇 명의 관련자들이 2007년 사이버공격 및 2008년 그루지야에 대한 사이버공격을 주도했다는 사실과 자신의 조직이 여러 해킹 작업에 대해 러시아 정부의 재정적 지원을 받았다는 점을 폭로하면서 러시아의 배후설에 대한 의혹이 불거진 바 있다.[362] 또한 2008년 그루지야 공격 당시 공격의 거점으로 추적된 C&C서버가 RBN이 통제하고 있는 서버에서 비롯된 점, 해당 서버가 러시아 정부의 영향력 아래에 있는 것이었다는 점 등으로 RBN이 러시아의 지원을 받았다는 의혹이 강하게 제기된 바 있다.[363] 그러나 러시아는 두 경우 모두 연루 의혹을 부인했으며, 더 이상의 조사가 이루어 질 수 없어 러시아가 배후에 있다는 직접적 증거는 발견할 수 없었다.[364] 이와 같이 비국가행위자들이 단독으로 또는

362) Wired, Mar. 11, 2009, “Kremlin Kids: We Launched the Estonian Cyber War”, <https://www.wired.com/2009/03/pro-kremlin-gro/> (2018.1.5. 최종방문); Jeffrey Carr, *supra* note 69, p. 117; Lenta.ru, Jan. 17, 2012, “Пока не загорятся здания”, <https://lenta.ru/articles/2012/01/17/jakemenko/?> (2018.1.5.최종방문).

363) 전문가들은 2008년 그루지야 사이버공격이 진행된 과정 및 방식이 광범위하고, 정교한 것을 볼 때, 해당 공격이 국가의 지원이 없이는 불가능한 것이라고 지적한 바 있다. US Cyber Consequences Unit, “Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008”, US-CCU Special Report (2009), p. 4; New York Times, Aug. 12, 2008, “Before the Gunfire, Cyberattacks”, <http://www.nytimes.com/2008/08/13/technology/13cyber.html> (2018.1.5.최종방문); The Telegraph, Aug. 11, 2008, “Georgia: Russia 'conducting cyber war'”, <http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html> (2018.1.5. 최종방문).

364) 이 밖에도 국가의 지원을 받아 타국에 대한 사이버공격을 감행하고 있는 대표적인 민족주의 해커집단으로는 The Syrian Electronic Army (SEA), SEA는 시리아의 대통령 Bassar al-Assad와 연계되어 있는 것으로 알려진 해커 집단으로 뉴욕 타임즈, 워싱턴 포스트, 르몽드, 가디언지 등 주로 서구의 주요 언론사와 트위터, 페이스 북과 같은 소셜 네트워크 등에 대한 사이버공격을 수행한 바 있다. 이 조직은 시리아 대통령 아사드가 운영하는

국가와 연계하여 초국경적 성격의-특히 국가에 대한- 사이버공격을 감행하고 있다는 사실은 이들에 대한 국제법 규율의 필요성과 현 국제법의 한계를 동시에 나타내고 있다.

2) 비국가행위자 규율에 있어서의 한계

현재 비국가행위자의 사이버공격을 규제하는 데 있어서의 한계는 구체적으로 두 가지로 요약할 수 있다. 첫째는 비국가행위자는 기존 국제법원칙 위반의 주체가 될 수 없다는 점이다. 앞에서 논의한 주권평등의 원칙, 국내문제불간섭의 원칙, 무력사용 금지의 원칙 위반의 주체는 국가이다.[365] 앞서 살펴본 테러 조약 등에서도 비국가행위자의 처벌에 대해 규정하고는 있지만 그러한 의무의 주체는 국가이기 때문에 비국가행위자가 위반의 직접적 주체가 될 수는 없다. 대응조치 또한 국가를 상대로만 취할 수 있다. 2001년 ILC초안 제49조 제1항에서는 피해국이 유책국에 대해서 대응조치를 취할 수 있다고 규정하고 있고, ICJ도 정당한 대응조치에 관해 설시하면서 이는 국제법위반행위를 한 국가를 대상으로 취해져야 한다고

기관의 도메인을 사용하며, 이들의 활동은 아사드의 사촌의 지원을 받고 있는 것으로 밝혀진 바 있다. Brandon Valeriano and Ryan C. Maness, “Cyber Conflict and Non-State Actors- Weapons of Fear”, in *Cyber War versus Cyber Realities-Cyber Conflict in the International System*, (Oxford University Press, 2015), p. 165; The Guardian, April 30, 2013, “Syrian Electronic Army: Assad's cyber warriors”, <https://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background> (2018.1.5.최종방문);

365) UN 헌장 제2조 제4항, 탈린매뉴얼 2.0에서도 주권존중 원칙, 불간섭 의무, 무력사용금지원칙의 위반 주체는 오직 국가만이 될 수 있다는 점을 지적하고 있다. NATO CCD COE, *supra* note 159, pp. 18, 175; ICJ도 2010년 코소보 독립선언의 합법성에 관한 권고적 의견에서 영토적 일체성 존중에 관한 원칙은 국가들 사이에만 국한되어 적용되는 것이라고 하였다. *Accordance with International Law of the Unilateral Declaration of Independence In Respect of Kosovo, Advisory Opinion, I.C.J. Reports 2010*, para. 80.

하였다.[366] 탈린매뉴얼 2.0에서도 대응조치는 비국가행위자를 상대로 취해질 수 없다고 하였다.[367] 비국가행위자는 앞서 살펴본 국제법의무의 위반주체가 될 수 없기 때문에 이는 당연한 논리적 귀결이라고 할 수 있다. 따라서 비국가행위자의 행위가 국가로 귀속되지 않는 경우, 사실상 피해국은 이에 대해 국제법에 따른 어떠한 대응도 할 수 없게 되는 것이다.

다만 예외적으로 자위권은 국가가 아닌 무력공격의 주체에게도 행사될 수 있는 것으로 인정되고 있다.[368] 자위권을 규정하고 있는 유엔 헌장 제51조는 무력공격을 당하는 대상으로 국가를 언급하고 있지 무력공격의 주체에 대해서는 침묵하고 있다. 학자들은 이를 비국가행위자가 무력공격을 할 수 있는 주체로 인정되는 것으로 해석하고 있다.[369] 국가들 또한 이제는 비국가행위자에 대해 자위권을 행사할 수 있는 것으로 인식하고 있다.[370]

대표적인 예로 2001년 9.11테러에 대한 미국의 대응을 들 수 있다. 미국은 공격의 주체인 테러조직 알카에다에게 자위권을 행사하였고, 이에 대한 국가 및 국제사회의 반응을 통해 비국가행위자에 대한 자위권 행사가

---

366) *Gabčíkovo-Nagymaros Project (Hungary/Slovakia), Judgement, I.C.J. Reports 1997*, paras. 82-83.

367) NATO CCD COE, *supra* note 159, p. 175.

368) 그러나 이 견해가 아직까지 보편적으로 받아들여지고 있는 것은 아니다. 학자들은 전통적으로 자위권은 국가들을 상대로만 원용해 왔다는 점, UN 헌장이 국가 간의 무력충돌을 규율하기 위해 작성 되었다는 점을 이유로 든다. Antonio Cassese, “Terrorism is also Disrupting Some Crucial Categories of International Law”, European Journal of International Law, Vol. 12, No. 5 (2001), pp. 996-998. 또한 헌장 제1장은 국가의 행동을 규율함으로써 국제평화와 안전을 유지하는 것을 그 목적으로 제시하고 있다.

369) Yoram Dinstein, *supra* note 176, p. 225; Michael N. schmitt, “Preemptive Strategies in International Law”, Michigan Journal of International Law, Vol. 24 (2003), pp. 536-540; Matthew J. Sklerov, *supra* note 112, pp. 49-50.

370) Matthew J. Sklerov, *supra* note 112, p. 50; Michael N. schmitt, *supra* note 369, p. 539.

가능하다는 해석이 널리 받아들여지고 있음을 알 수 있다. 사건 발생 후 안보리는 결의 제1368호, 제1373호를 차례대로 각각 채택하면서 9.11테러를 '국제평화 및 안전에 대한 위협'으로 규정하고, 헌장에 따른 개별적 또는 집단적 자위권의 고유한 권리를 재확인 하였다.[371] NATO, 미주기구(OAS)도 헌장 제51조에 근거하여 집단적 자위권을 원용하며 지지의사를 표명하였다.[372] 또한 미국의 자위권 행사에 대해 극소수의 국가[373]를 제외하고는 다수의 국가가 개별적으로 지지의사를 표명하거나 아프가니스탄 공습에 직접 참가하였다.[374] 이렇게 볼 때, 국가들 간 및 학자들 간 이견은 있으나 비국가행위자에 대해 자위권에 근거한 무력대응을 할 수 있다는 사실은 다수에 의해 지지되고 있는 것으로 볼 수 있다. 따라서 무력공격에 달하는 사이버공격을 감행한 비국가행위자에 대해서도 자위권을 행사할 수 있다는 데 대해서는 해석상 무리가 없을 것으로 보인다.

한편 Simma 재판관은 2003년 Oil Platforms 사건에서 개별의견을 통해 일국이 타국에 대해 무력공격에는 이르지 않지만 무력을 사용한 공격

---

371) UN Doc. S/Res/1368(2001); UN Doc. S/Res/1373(2001).

372) NATO는 헌장 제51조에 근거하여 워싱턴 조약 제5조에 규정된 집단적 자위권을 원용하였으며, OAS는 결의를 통해 리오 조약의 집단적 자위권을 원용하였다(OAS Res RC23/Res1/01).

373) 이라크, 수단, 북한은 미국의 작전에 대해 테러를 이유로 아프가니스탄의 국민들을 공격하는 것은 정당화 될 수 없다고 주장하였다. 또한 이란, 말레이시아, 쿠바도 미국의 행위를 비난하였다: Steven R Ratner, "Jus ad Bellum and Jus in Bello After September 11", American Journal of International Law, Vol. 96, No. 4 (2001), p. 910.

374) 중국, 러시아, 이집트와 같은 국가들은 미국의 작전을 지지하였고, 영국은 작전에 직접 참여하였다. 이밖에 독일, 프랑스, 이탈리아, 네덜란드 등의 NATO 동맹국들은 병력 지원의사를 밝혔으며 그루지야, 오만, 파키스탄 등의 중앙아시아 국가들은 미국이 공습할 수 있도록 영공이용을 허가 하였다; CNN, "Operation Enduring Freedom Fast Facts", Oct. 5, 2016, <http://edition.cnn.com/2013/10/28/world/operation-enduring-freedom-fast-facts/> (2017.3.8.최종방문); Sean D. Murphy, "Terrorism and the Concept of 'Armed Attack' in Article 51 of the UN Charter", Harvard International Law Journal, Vol. 43 (2001), p. 49.

을 감행한 경우, 피해국은 무력공격에 이르지 않는, 공격에 비례한 대응조치를 통해 자신을 방어할 권리가 있다고 한 바 있다.[375] Simma 재판관은 또한 2005년 콩고영토에서의 무력 활동에 관한 사건에서 “일국의 영토 전체 또는 일부에 정부 당국이 부재한 경우, 그러한 국가의 영토에서 비정규 세력이 이웃국가에 대한 무력공격을 수행한다면 그 행위가 해당 영토국가로 귀속될 수 없다고 해도 이는 여전히 무력공격에 해당한다. 또한 그 행위가 영토국가로 귀속되지 않는다고 해서 피해국이 자위권을 행사할 수 없다면 이는 합리적인 것으로 볼 수 없다”고 한[376] Kooijmans 재판관의 개별의견을 자신의 개별의견에 인용하면서 전적으로 동의를 표시하였다.[377] 이를 연결지어 생각하면 국가로 귀속되지 않는 무력공격에 이르지 않는 비국가행위자의 공격에 대해서도 비례적인 무력사용을 통한 대응조치가 허용될 수 있다는 주장이 제기될 수 있다. 즉, 비국가행위자에 대해서도 행위의 국가귀속 여부와 상관없이 자위권 이하의 대응조치가 가능하다는 주장이 제기될 수 있는 것이다. 이는 또 국가로 그 행위가 귀속되지 않는 비국가행위자의 사이버공격에도 적용될 수 있는 것이 아닌가 하는 질문으로 이어질 수 있을 것이다.

그러나 우선 2003년 Oil Platforms사건에서 Simma 재판관의 의견은 무력공격에 이르지 않는 강도의 국가의 공격에 대한 무력적 대응조치의 허용성 여부를 검토한 것으로 행위자에 중점을 둔 것이 아니다. 또한 2005년 콩고 사건에서 국가로 귀속되지 않은 비국가행위자의 행위에 대한 언급은 비국가행위자의 공격도 규모와 효과에 따라 유엔 헌장 제51조상의 무력공격으로 인정될 수 있다는 점을 강조하기 위한 것이었음을 주목할 필요가 있다.[378] 따라서 이를 무력을 사용했으나 무력공격에는 이르지 못

375) *Oil Platforms (Islamic Republic of Iran v. United States of America), I.C.J Reports 2003,* Separate Opinon of Judge Simma, paras. 12-13.
376) *Congo (Democratic Republic of the Congo v. Uganda), I.C.J. Reports 2005,* Separate Opinion of Judge Kooijmans, para. 30.
377) Ibid., Separate Opinion of Judge Simma, para. 12.
378) Ibid., Separate Opinon of Judge Simma, para. 11.

한 비국가행위자의 행위에 대해서도 국가귀속성을 따지지 않고 무력을 사용한 대응조치가 가능하다고 확대해석 하는 것은 적절하지 않다.[379]

무엇보다도 사이버공격의 경우에는 공격의 흐름이 탐지된 국가가 문제된 공격을 실행한 비국가행위자가 실제 위치한 장소라고 확신할 수 없다는 점에 있어서 Simma 재판관 및 Kooijmans 재판관이 언급한 경우와 구별되어야 한다. 개별의견에 언급된 경우는 비국가행위자의 공격이 국가로 귀속될 수는 없더라도, 그 행위의 발생이 해당국가라는 점과 그 행위의 주체가 밝히 드러난 경우이다. 그러나 사이버공격의 경우에는 이 두 가지 모두가 불분명하다. 공격의 흐름이 탐지된 국가에 실효적 정부가 건재하는 경우에도 이는 마찬가지라고 할 수 있다. 한 국가의 영토에서 무력을 사용한 공격이 발생하는 경우, 국가가 이를 파악하지 못할 가능성은 매우 낮다. 따라서 비국가행위자에 의해 무력을 사용한 공격이 발생한 경우, 비록 이를 공격이 발생한 영토국가에 귀속시킬 수는 없더라도 이에 대한 피해국의 대응조치는 어느 정도 정당성이 인정될 수 있을 것이다. 징후가 분명한 비국가행위자의 공격을 방지하지 못한 영토국가에게도 그 책임이 인정될 수 있기 때문이다. 그러나 사이버공격의 경우에는 자국의 관할권 내에 있는 서버에 대해 해당국가의 정부가 완벽한 감시를 하는 것은 사실상 불가능하기 때문에, 공격의 흐름을 탐지하지 못했다거나 그 공격을 방지하지 못한 것에 대해 책임을 묻는 것이 용이하지 않다. 따라서 두 경우는 유사해보이지만 실제로는 차이가 있다.

또한 사이버공격의 경우에는 그 강도가 무력공격에 미치지 못하는 중대한 무력사용에 이르지 못하더라도 국가안보에 영향을 미칠 수 있는 방식

379) 사실 국가에 대해서도 무력적 대응조치가 가능하다는 Simma 재판관의 개별의견은 국제법적으로 확립되었다기 보다는 공격의 강도를 판단하는 데 있어 국제법상 법리적 불확실성이 존재한다는 점을 나타내주고 있다고 해석하는 것이 적절하다. Cameron S. D. Brown, “Cyber-Attacks, Retaliation and Risk: Legal and Technical Implications for Nation-States and Private Entities”, in Jean-Loup Richet(ed.), *Cybersecurity Policies and Strategies for Cyberwarfare Prevention* (IGI Global, 2015), p. 173.

으로 진행되는 경우가 더 많은 비중을 차지한다. 때문에 이러한 논리가 적용될 수 있다고 하더라도 실제 비국가행위자의 사이버공격에 대응하는 데 실효성이 있을지는 의문이다. 결론적으로 현 국제법체제 내에는 무력공격에 이르지 않는 사이버공격의 귀속이 비국가행위자로 밝혀지더라도 그 행위가 국가로 귀속되지 않는 경우 이를 규율할 수 있는 방법이 여전히 부재하다고 보는 것이 적절한 해석이라고 할 수 있다.

이를 정리하면 현재의 국제법체제를 통해 비국가행위자를 규율할 수 있는 경우는 비국가행위자의 행위가 국가로 귀속되는 경우, 비국가행위자가 무력공격에 이르는 사이버공격을 감행한 경우, 조약상 당사국 내의 비국가행위자를 당사국의 국내법을 통해 처벌하거나 피해국으로 인도하는 경우 세 가지에 국한됨을 알 수 있다. 이 중 직접적으로 비국가행위자를 규율할 수 있는 경우는 자위권을 원용하는 것뿐이다. 그러나 귀속의 증명이 어려운 사이버공격의 특성상 무력공격에 이르는 사이버공격이 발생했다고 해도 추적된 소스를 통해 비국가행위자가 실제 공격자라는 것을 밝히기가 어렵다. 무엇보다도 민족주의 해커집단의 예에서도 살펴본 바와 같이 사이버공격이 특정 집단의 행위인 것으로 추적된다고 해도 이에 대한 국가귀속성을 증명하는 직접적 증거를 찾기는 현재 상황에서 불가능 하다고 볼 수 있다. 이에 더해 피해국의 요청에 대한 국가들의 협조마저 이루어지지 않고 있는 현실을 생각할 때, 위 세 경우를 통한 비국가행위자의 규율도 사실상 불가능한 것이라고 볼 수 있다. 따라서 비국가행위자는 일반국제법상의 원칙 및 조약 등의 규율에서 제외된 상태라고 볼 수 있다.[380]

이러한 상황에서 현재 비국가행위자에 대한 규율은 각국의 국내형법에 맡겨져 있다.[381] 이 점이 바로 두 번째 한계에 해당한다. 사이버공격을 국

---

380) 일부 학자들은 전쟁범죄, 국제형사법, 국제 인권법 규정이 비국가행위자에게 직접 적용될 수 있다고 언급하기도 한다. 그러나 이들도 사이버공격에 대해 앞의 규범들이 실제로 적용되기는 어렵다고 보고 있다. Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 510; NATO CCD COE, *supra* note 159, pp. 174-175.

381) Sean M. Condron, "Getting It Right: Protecting American Critical

내 형법상의 문제로 다루는 것은 피해국이 수동적 방어 및 공격 발생국 형법 규정에 국한해서만 행동할 수 있도록 대응의 범위를 제한한다.[382]

우선 비국가행위자를 각국의 국내형법에 따라 규율하는 것이 피해국이 취할 수 있는 조치를 수동적 방어로 국한시키는 이유는 국내 형법상 사이버공격이 금지되어 있기 때문이다. 컴퓨터 보안이라고 흔히 부르는 수동적 방어는 방어벽이나 안티바이러스 소프트웨어 등을 설치하는 것을 의미한다. 이는 상대방의 공격시도를 사전에 차단하는 성격의 조치이다.[383] 그러나 어떠한 정교한 컴퓨터 보안시스템도 국가의 주요 기반시설을 사이버공격으로부터 완벽하게 방어할 수 없다는 사실은 이미 증명된 바 있다.[384] 특히 수동적 방어조치는 최근 사이버공격에 많이 이용되고 있는 제로데이 취약점 공격[385]에 대해서는 어떤 방어도 할 수 없다는 점이 지적된다.[386] 제로데이 취약점 공격은 공격대상 소프트웨어의 취약점[387]에 대한 패치가 보급되지 않은 상황에서 이루어지는 것이기 때문이다.

Infrastructure In Cyberspace", Harvard Journal of Law & Technology, Vol. 20, No. 2 (2007), pp. 414-415.

382) Matthew J. Sklerov , *supra* note 112, p. 7.

383) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 474.

384) Andrew M. Colarik, Cyber Terrorism: Political and Economic Implications, (Idea Group Publishing, 2006), p. 38; David E. Graham, *supra* note 335, p. 92.

385) 보안 취약점이 발견되었을 때 그 문제의 존재 자체가 널리 공표되기도 전에 해당 취약점을 악용하여 이루어 지는 보안 공격. 공격의 신속성을 의미하는 것으로, 일반적으로 컴퓨터에서 취약점이 발견되면 제작자나 개발자가 취약점을 보완하는 패치를 배포하고 사용자가 이를 내려받아 대처하는 것이 관례이나, 제로 데이 공격은 대응책이 공표되기도 전에 공격이 이루어 지기 때문에 대처 방법이 없다. 한국정보통신기술협회, 정보통신용어사전, <http://word.tta.or.kr/dictionary/dictionaryView.do?word_seq=060566-1> (2018.1.25.최종방문).

386) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 474.

387) 취약점(vulnerability)은 기능명세, 설계 또는 구현단계의 오류나 시동, 설치 또는 운용상의 문제점으로 인하여 정보 시스템이나 네트워크가 내포하고 있는 취약한 부분을 의미하는 것으로 보안의 위협 대상이 된다. 한국정보통신기술협회, "정보보호기술용어", 한국정보통신기술협회(2013), p. 57.

한편 국내 형법을 통해 사이버공격을 효과적으로 억지하기 위해서는 해당 행위가 공격이 발생한 국가의 형법에도 위반되는 행위로 규정되어 있어야 하고, 이에 따른 처벌이 명확해야 한다.[388] 그러나 공격이 발생한 국가가 사이버공격에 관한 규정을 잘 마련하고 있다고 해도 문제의 사이버공격이 소위 라이벌 국가 또는 적국을 향해 발생한 경우, 공격 발생국가는 의도적으로 공격 행위자에 대한 처벌을 하지 않을 수 있다.

이러한 사례는 이미 여러 차례 발생한 바 있다. 중국은 자국 내의 국제적 해커들을 엄중히 단속할 것을 천명한 바 있으나[389], 현재까지 초국가적 사이버공격을 한 해커가 국내법에 따라 처벌된 사례는 없다.[390] 보안 전문가들은 중국이 해커들로부터 정보를 사고, 타국에 대한 간첩행위를 위해 이들을 활용하는 등 오히려 의도적으로 해커들의 형법 위반행위를 용인하고 있다고 하였다.[391] 또한 2016년 미국 대선개입 해킹 의혹에 대한 푸틴 대통령의 최근 발언에서, 러시아도 타국에 대한 자국 해커들의 사이버공격을 용인하고 있음을 추론해 볼 수 있다.[392] 이는 공격 발생국의 형법상 규제가 국제적 사이버공격을 억지하는 데 효과적이지 않다는 점을 보여주는 예라고 할 수 있다.

---

388) Andrew M. Colarik, *supra* note 384, p. 39.

389) 중국정부는 중국의 해커들이 독일의 주요 정부기관의 컴퓨터 시스템을 공격해왔다는 보도가 독일에서 나오자 이에 대한 반응으로 독일정부와의 협력하에 이들 해커에 대한 강력한 조치를 취할 것을 천명한 바 있다. Financial Times, “Beijing pledges crackdown on hackers”, Aug. 28, 2007, <https://www.ft.com/content/a625db16-54c4-11dc-890c-0000779fd2ac> (2017.10.10. 최종방문).

390) Matthew J. Sklerov, *supra* note 112, p. 9.

391) Schneier on Security, Jul. 14, 2008, “Chinese Cyber Attacks”, <https://www.schneier.com/blog/archives/2008/07/chinese_cyber_a.html> (2017.10.10. 최종방문).

392) CNN, Jun. 2, 2017, “Putin: 'Patriotic' Russian hackers may have targeted US election”, <http://edition.cnn.com/2017/06/01/politics/russia-putin-hackers-election/index.html> (2017.10.10.최종방문).

한편 피해국의 국내형법도 타국에서 발생한 비국가행위자의 사이버공격을 억지하는데 효과적이지 않기는 마찬가지다. 2014년 미국은 기업의 지적재산 탈취행위 혐의로 중국 인민해방군(People's Liberation Army)[393] 소속 다섯 명을 기소한 바 있다.[394] 그러나 기소대상 다섯 명이 미국의 영토에 들어오지 않는 한 그 이상의 조치는 할 수 없다. 이러한 관할권의 한계는 기본적으로 초국경적 성격을 가진 비국가행위자의 사이버공격을 국내법을 통해 규제한다는 것이 얼마나 비효율적인지를 보여주는 것이라 하겠다.[395] 물론 피해국은 공격이 발생한 것으로 추적된 국가에게 외교적 노력을 통해 처벌할 것을 촉구하거나 범죄인 인도 조약을 통해 해당 범죄인의 인도를 요구할 수도 있다. 그러나 앞서 검토한 바 있듯 국가가 연계된 비국가행위자의 사이버공격이 증가하고 있다는 조사결과와 예로 든 중국 및 러시아의 행동 등으로 미루어 볼 때, 각국가가 이에 응할 가능성은 낮다고 볼 수 있다.

3) 상당한 주의 의무의 적용가능성

이러한 한계와 관련하여 상당한 주의 의무(duty of Due diligence)[396]

393) 중국 인민 해방군 내에는 61398부대, 61486부대와 78020부대로 구성된 사이버부대가 있다. 기소된 다섯 명의 장교는 61398부대 소속인 것으로 알려져 있다.

394) U.S. Attorney's Office Western District of Pennsylvania, "U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations And A Labor Organization For Commercial Advantage", United States Department of Justice, May 19, 2014, <https://www.justice.gov/usao-wdpa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and> (2017.4.18.최종방문).

395) Ruperto P. Majuca and Jay P. Kesan, "Hacking Back: Optimal Use of Self-Defense in Cyberspace", Illinois Public Law and Legal Theory Papers Series (2009), Research Papers Series No. 08-20, pp. 19-20.

396) due diligence 원칙은 주권평등원칙에서 파생된 것으로 팔마스도 중재판정

의 적용을 통해 비국가행위자의 규율 문제를 해결할 수 있다는 주장도 있다.[397] 국가는 자국의 영토가 다른 국가에 피해를 주는 방식으로 사용되는 것을 방지할 일반적 의무, 이른바 상당한 주의 의무를 부담한다.[398] 이에 따라 국가는 자국의 영토 내에서 비국가행위자가 타국에 영향을 주는 사이버공격을 감행하는 것을 방지할 의무가 있다는 것이다. 이를 적용하면 국가는 자국 내의 비국가행위자가 타국에 대한 사이버공격을 감행하는 것을 적절히 방지하지 못했을 경우, 상당한 주의 의무 위반에 대한 간접책임을 지게 된다. 그러나 사이버공격의 특성상, 사건 발생 전에 이를 탐지하기는 상당히 어렵다.[399] 또한 이를 탐지했더라도 국가가 보유하고 있는 기술 수준에 따라 공격을 차단하지 못할 가능성도 있다. 즉, 국가마다 보유하고 있는 사이버기술 및 역량이 다르다는 점은 방지의무를 적용하는 데 있어 중요하게 검토되어야 할 부분이다. 탈린매뉴얼에서도 이 점이 지적된 바 있고, 결국 전문가들은 구체적 적용 기준에 대한 합의를 보지 못하고,

---

에서 중재인 Max Huber는 영토주권이 자국의 영토 내에서 다른 국가의 권리를 보호하는 의무를 포함하는 것이라고 하였다; *Island of Palmas case (Netherlands/USA)*, Report of International Arbitral Awards, 1928, United Nations, Vol. II, p. 839; 이후 상당한 주의 의무는 여러 사건에서 재확인되고 발전하였다. 상당한 주의 의무의 자세한 발전과정에 대해서는 Karine Bannelier-Christakis, “Cyber Diligence: A Low-Intensity Due Diligence Principle for Low Intensity Cyber Operations?”, Baltic Yearbook of International Law, Vol. 14 (2014), pp. 24-27.

397) Kriangsak Kittichaisaree, *Public International Law of Cyberspace*, (Springer, 2017), pp. 40-41; Michael N. Schmitt, “In Defense of Due Diligence in Cyberspace,” Yale Law Journal Forum, Vol. 125 (2015), p. 70; Karine Bannelier-Christakis, *supra* note 396, p. 27; NATO CCD COE, *supra* note 20, p. 27.

398) *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. People's Republic of Albania), I.C.J. Reports 1949*, p. 22

399) eWeek, Apr. 8, 2008, “Chertoff Describes 'Manhattan Project' for Cyber-defenses”, <http://www.eweek.com/security/chertoff-describes-manhattan-project-for-cyber-defenses> (2017.10.10.최종방문).

각국의 사이버역량에 비추어 합리적으로 기대할 수 있는 조치를 취해야 한다는 모호한 결론을 낸 바 있다.[400]

물론 방지의무가 위반행위를 완전히 방지할 것을 의무화하고 있는 것은 아니기 때문에 공격이 발생했다고 해서 상당한 주의 의무의 위반이 되는 것은 아니다. 그렇다고 하더라도 사이버공격을 방지하기 위해 어느 정도까지의 노력을 국가가 해야 하는지에 대해서 명확하게 합의되거나 국가관행이 확립된 바가 없다.[401] 이에 대해 피해국가가 공격 흐름을 유포하는 서버가 제3국에 있음을 확인하고 제3국에 조사협조를 구한 경우, 제3국이 협조를 거절하고 동시에 공격에 연루되었다는 점도 부인한다면 이는 제3국 스스로가 사이버공격 방지의무를 할 의사가 없다는 점을 증명하는 것이라는 주장도 제기된 바 있다.[402] 그러나 조사협조를 거부하는 것이 방지의무 위반에 해당하는지에 대해서는 검토가 필요하다. 조사협조를 의무화하는 조약이나 일반 국제법원칙이 확립된 바 없기 때문이다. 2007년 에스토니아 공격에 대해 러시아는 조사협조를 거부한 바 있으나 이에 대한 상당한 주의 의무 위반문제가 제기되지는 않았다.

한편 사전에 위반행위를 탐지하기 어렵다는 사이버공격의 특성상 '사전방지'가 아닌 이미 발생한 행위의 중단이나 처벌에 방점을 두고 상당한 주의 의무를 적용해야 한다는 주장도 있다.[403] Sklerov는 애초 9.11테러에서처럼 테러조직이 한 국가의 영토 내에 은닉하면서 타국에 대해 무력공격을 하는 것과 같이 비국가행위자가 무력공격에 이르는 사이버공격을 감행하였을 때를 상정하고 전가책임(Imputed State Responsibility)[404] 개

400) NATO CCD COE, *supra* note 20, p. 27; Michael N. Schmitt, *supra* note 397, Yale Law Journal Forum, Vol. 125 (2015), pp. 70-71.
401) Kriangsak Kittichaisaree, *Public International Law of Cyberspace*, (Springer, 2017), p. 40.
402) Jeffrey Carr, *supra* note 69, p. 67.
403) Matthew J. Sklerov, *supra* note 112, pp.14-15.
404) 1970년 초기까지 국제법 위원회는 행위의 국가귀속을 의미하는 용어로 attribution이 아닌 imputation을 사용하였다. 그러나 이에 대한 토의과정에서 국가책임에서의 귀속은 일반적인 행위가 국가로 귀속되는지를 먼저 검토하

념을 제안하였다.[405] 이는 사이버공격과 관련한 방지의무의 적용범위를 확대·구체화 시킨 것이다. Graham에 따르면 전가책임에는 자국영토 내에서 일어난 국제적 사이버공격행위를 형법상 범죄로 규정할 의무, 그러한 공격에 대한 면밀한 조사를 시행할 의무, 공격에 연루된 자들을 기소할 의무, 공격혐의자들에 대한 피해국가의 자체 조사 및 기소에 대해 협력할 의무가 포함되어 있다.[406] Sklerov는 무력공격에 준하는 사이버공격이 발생한 국가가 이 같은 조치를 시행하지 않을 경우, 피해국은 전가책임에 근거하여 공격발생국에 대해 자위권을 행사할 수 있다고 주장한다. 이 개념을 적용하면 피해국이 굳이 공격행위자와 공격발생국 간의 귀속성을 증명할 필요가 없다.[407]

Graham은 이러한 의무들이 도출되는 근거로 부다페스트협약, 국가들의 관행을 들고 있는데 그 타당성에 대해서는 살펴볼 필요가 있다.[408] 먼저 부다페스트협약은 당사국이 50개국에도 미치지 못하기 때문에 이를 근거로 위의 의무들을 도출하려는 시도는 설득력이 떨어진다. 또한 국가들의

는 데 반해, imputation은 국내형법에서 '위법한' 행위에 대한 '책임'의 귀속을 의미하는 것으로 사용되고 있다는 점이 지적되었다. 이에 따라 이후로는 행위의 위법성을 전제로 하지 않는 attribution을 사용하게 되었다. *Yearbook of the International Law Commission*, 1970, Vol. I, pp. 48-49, paras. 32-35; 법률영어 사전에서는 "Imputed"를 '대신해서 부담하는, 귀속되는'으로 번역하고 있으며, Imputed liability 이라는 법률용어를 전위책임으로 번역하고 있다. 이태희·임홍근, 법률영어사전, (법문사, 2007), p. 964; 한편 중국의 한 논문에서는 Imputed Responsibility를 轉嫁轉嫁으로 번역하여 사용하고 있다. 黄志雄, "论网络攻击在国际法上的归因", 环球法律评论, 第5期 (2014), <http://article.chinalawinfo.com/ArticleFullText.aspx?ArticleId=91372> (2018.1.3.최종방문). Graham과 Sklerov는 행위의 귀속여부와는 관계없이 일국에서 발생한 위법행위에 대한 책임을 그 행위가 발생한 국가에 전가시킨다는 의미로 해당 개념을 제시하고 있다고 볼 수 있다. 이에 본 논문에서는 "Imputed Responsibility"를 전가책임으로 번역하여 사용하기로 한다.

405) *Ibid.*

406) David E. Graham, *supra* note 335, pp. 93-94.

407) Matthew J. Sklerov, *supra* note 112, p.14.

408) *supra* note 335 , pp. 93-94.

관행으로는 범죄 방지와 행위자 처벌에 관한 UN총회 결의 및 정보기술의 범죄적 악용에 관한 총회결의 등[409]을 근거로 제시하고 있는데 이 또한 구속력 있는 국제규범이 아니다.

이보다는 제1절에서 살펴본 테러에 관한 조약을 근거로 당사국들에게 위의 의무들을 적용할 수 있을 것으로 보인다. 그러나 이 경우에도 테러조약들이 구체적으로 어떤 사이버공격행위를 국내법상의 범죄로 규정할 것을 요구하고 있는지에 대해서는 별도의 논의가 필요하다. 무엇보다도 이들 조약이 비국가행위자가 수행하는 사이버공격행위를 모두 포괄하고 있다고 볼 수 없기 때문에 그 적용범위도 제한적일 수밖에 없다. 또한 이들 조약에 언급된 정보교환 및 협력의무는 각국의 국내법에 따라 적절한 조치를 취할 것과 같은 일반적인 용어를 사용하고 있다는 점도 문제다.[410] '적절한(appropriate)' 조치가 무엇을 의미하는지에 대해서는 다양한 해석이 가능하기 때문이다. 한편 사이버공격에서 가장 중요하다고 할 수 있는 조사협조에 관한 의무는 이들 조약 중 핵테러행위의 억제를 위한 국제협약 제10조에서 유일하게 규정하고 있다. 그런데 이마저도 공격의 탐지에 대한 정보가 아니라 행위자에 대한 정보를 제공하는 경우에 조사에 대한 원조를 제공하도록 규정되어 있어 또다시 실제 공격행위자를 밝혀야 한다는 한계에 직면하게 된다.[411] 따라서 위의 조약들을 근거로 전가책임을 적용하기 위해서는 구체적인 논의를 통해 적용기준을 명확히 하는 작업이 선행되어야 한다.

또한 전가책임은 무력공격에 해당하는 사이버공격에의 적용을 상정하고 만들어진 개념이기 때문에, 그러한 수준에 미치지 못하는 사이버공격에 대해서는 적용할 수 없다. 결국 전가책임 개념의 적용을 통해 귀속의 문제를

409) UN Doc. A/Res/45/121(1990), UN Doc. A/Res/55/63(2001).

410) 1988년 항해 안전에 대한 불법행위 억제를 위한 협약 제13조 제1항 b호; 1999년 테러리즘의 자금조달 억제를 위한 국제협약 제9조 제1호, 제2호; 핵물질 관련 테러방지 조약으로는 우선 1979년 핵물질의 방호에 관한 개정 협약 제7조 제2호.

411) 핵테러행위의 억제를 위한 국제협약 제7조.

해결하더라도 비국가행위자에 의한 무력공격에 미치지 못하는 사이버공격에 대해 피해국이 취할 수 있는 대응조치가 없다는 한계는 그대로 남아있게 되는 것이다. 따라서 상당한 주의 의무의 적용과 관련된 주장은 동 의무의 적용을 위해 구체화 되어야 할 또 다른 과제를 보여줄 뿐 비국가행위자의 사이버공격을 규율하는 데 있어 해결책을 제시해 주는 것은 아니라고 할 수 있다.

4) 새로운 대안의 필요성

지금까지 살펴본 것과 같이 비국가행위자의 사이버공격행위를 규제할 마땅한 국제법적 수단이 없고, 이를 국내형법의 문제로 다루는 것도 한계가 있다는 사실은 결국 이 문제에 대한 대응에 있어 공백이 존재한다는 것을 의미한다. 게다가 이러한 한계는 국가가 비국가행위자를 proxy로 활용할 경우 직접적인 책임을 회피할 수 있다는 점 때문에 국가들에게는 상당한 매력으로 작용할 위험을 내포하고 있다.[412] 이러한 한계가 심화되면 비국가행위자의 사이버공격을 규제할 수 있는 길은 점점 요원해 질 것이다.

사이버공간에서의 활동에 대한 법적책임의 영역을 공백으로 남겨두는 것은 국제법 질서에 심각한 위협이 될 수 있다.[413] 이에 비국가행위자의

412) Andrew F. Krepinevich, "Cyber Warfare: A 'Nuclear Option?'", Center for Strategic and Budgetary Assessments (2012), pp. 49-50; Erica D. Borghard and Shawn W. Lonergan, "Can States Calculate the Risks of Using Cyber Proxies?", Orbis, Vol. 60 (2016), No. 3, p. 3; US Department of Defense, "The DoD Cyber Strategy" (2015), p. 9; Cyber Security Intelligence, Sept. 24, 2015, "Proxies and their Plausible Deniability: Challenging Conventional Wisdom", <https://www.cybersecurityintelligence.com/blog/state-proxies-and-plausible-deniability-challenging-conventional-wisdom-644.html> (2017.4.17.최종방문).

413) Nicholas Tsagourias, *supra* note 354, p. 466.

사이버공격에 대한 국제법적 대응방안을 강구하는데 있어서는 행위자 확인원칙의 마련과 국가간 협조체제 구축을 통해 사이버공격 행위자를 처벌 제재하기 어려운 현재의 구조를 개선하는 것이 필요하다. 그러나 공격과 결과발생 간의 시간차가 거의 존재하지 않는 사이버공격의 특성을 생각할 때, 사건 발생 후 책임을 묻는 체제를 확립한다고 해서 사이버공격에 대한 효과적인 대응체계가 완성되었다고 볼 수는 없다. 국제법이 사이버공격의 행위자에 대해 사후에 책임을 추궁하는 체제를 마련하는 것 외에 공격을 실시간으로 억지하기 위한 대응책을 제시하지 않는다면 국가들은 효과적인 대응을 위해 법 밖의 조치를 강구하게 될 가능성이 높다.

사이버공격에 대한 실시간 대응의 문제는 기존체제 그대로의 적용과 같은 논의만을 통해서는 해결하기 어렵다. 실시간으로 사이버공격을 억지하기 위해서는 사전에 이를 탐지하는 조치가 필요하다. 그러나 피해국이 위반행위의 발생과 귀속의 증명을 전제로 대응할 수 있게 되어있는 현행 국제법 체제 내에서 이러한 사전조치가 허용되는지에 대해서는 검토가 필요하다. 더욱이 사이버공격을 사전에 탐지하기 위해서는 사이버공간과 사이버공격만이 가지는 특성이 고려되어야 한다. 이는 결국 사이버공격에 대한 효과적인 대응책을 마련하기 위해서는 기존 체제의 적용 가능성 여부를 뛰어 넘는 차원의 논의가 필요하다는 것을 보여준다.

제4장 사이버공격의 국제법적 규율에 관한 논의와 실행

제1절 국제법 차원의 논의

국가들은 사이버공격에 대해 국제법상의 규율이 필요하다는 데 대해서는 대부분 의견이 일치한다.[414] 그러나 규율 방법에 대해서는 크게 두 가지로 의견이 나뉘어 대립하고 있다. 사이버공격의 규율은 기존의 국제법체제 안에서 충분히 가능하다는 의견과 사이버공격만을 규율하는 새로운 규제체제가 필요하다는 의견이 그것이다.

이러한 의견대립은 정보를 바라보는 기본적인 인식의 차이에서 기인한 것이다. 새로운 체제의 성립을 주장하는 러시아·중국 진영은 네트워크상의 정보 자체를 위협이자 무기로 본다.[415] 반면 현행 국제법의 적용을 주장하는 서방 진영은 정보 자체를 위협으로 인식하지 않기 때문에 정보의 자유로운 흐름을 지지한다.[416] 이러한 기본 인식의 차이는 결국 사이버공간 상에서 국가의 주권적 행위의 경계를 어디까지로 볼 것인지에 대한 갈등으로 나타나게 된다.[417] 이하에서는 대립되는 두 입장을 살펴보고, 각 입장이 사이버공격의 국제법적 규율에 있어 갖는 함의에 대해 분석해 보기로 한다.

---

414) Martha Finnemore, Duncan B. Hollis, *supra* note 127, p. 1.

415) UN Doc. A/54/213 (1999); pp. 8-10, UN Doc. A/56/164/Add.1 (2001), pp. 2-3; UN Doc. A/64/129 (2009), pp. 4-7; UN Doc. A/65/154 (2010), pp. 2-5.

416) Prakash, Rahul and Darshana M. Baruah, “The UN and Cyberspace Governance.” ORF Issue Brief, No. 68 (2014), p. 2.

417) James Andrew Lewis, “Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms”, Center for Strategic & International Studies (2014), p. 7.

1. 러시아·중국 진영의 입장

러시아는 인터넷공간에서 정보의 자유로운 이동과 표현의 자유를 주장하는 서방국가들의 입장에 반대하는 대표적인 국가이다.[418] 러시아는 미국과 달리 사이버공간에서 최강대국의 위치를 선점하지 못한 후발주자로서 사이버 강대국들이 사이버공간에서 지배적 위치를 차지하는 것에 반감을 가지고 있다.[419] 사이버공간이 이런 식으로 재편되면 결국 후발주자들은 선발주자들이 세워놓은 기준을 따라야만 하고, 기술적으로도 선발주자들에게 의존해야 하는 상황이 발생하게 된다는 것이다.[420] 또한 러시아는 사이버공간에서 유통되는 정보가 위협이라는 기본적인 인식을 바탕으로 사이버공간의 규율이라는 문제에 접근하고 있다.[421]

이러한 시각은 크게 두 가지 주장으로 나타나는데, 그 첫 번째가 국가중심의 사이버공간 통제이다. 러시아는 기본적으로는 정보의 자유로운 이동에 동의하지만 필요한 경우에는 검열과 통제가 필요한데, 그 주체가 국가여야 한다는 입장이다.[422] 러시아는 여기에서 더 나아가 민간에게 정보

---

418) Nikolay Bordyuzha, Written Contribution by Mr. Nikolay Bordyuzha, Secretary General of the Collective Security Treaty Organization, to the Seventeenth OSCE Ministeral Council, OSCE MC.DEL/16/09 (2009), p. 3; Keir Giles, "Information Troops: A Russian Cyber Command?", in C. Czosseck, E. Tyugu, T. Wingfield (Eds.), *2011 3th International Conference on Cyber Conflict*, (NATO CCD COE Publications, 2011), p. 50.

419) Keir Giles, "Russia's Public Stance on Cyberspace Issues", in Czosseck C, Ottis R, Ziolkowski K (Eds.), *2012 4th International Conference on Cyber Conflict*, (NATO CCD COE Publications, 2012), p. 65; Forbes, Oct. 24, 2014, "In Search Of A Governance. Who Will Win The Battle For The Internet?", <https://www.forbes.com/sites/federicoguerrini/2014/10/24/in-search-of-a-good-governance-who-will-win-the-battle-for-the-future-of-the-internet/#1bade1321c1d> (2017.4.10.최종방문).

420) UN Doc. A/56/164/Add.1 (2001), p. 4.

421) Keir Giles, *supra* note 418, p. 50.

를 맡겨두는 것이 결국에는 테러조직이나 범죄조직의 파괴적인 정보사용으로 이어져 국가안보 및 국제사회의 평화와 안전에 위협이 될 수 있다고 보고 있다.[423] 또한 서방국가들이 주장하는 정보의 자유로운 흐름이 이러한 위협적 요소를 더욱 심화시킨다고 보고 있다.[424] 이에 러시아는 국가의 '인터넷주권' 개념을 강조하면서 자국의 관할권 하에 있는 모든 정보를 국가의 통제 하에 두려고 한다.[425]

이러한 입장은 2011년 9월 '안보문제에 책임이 있는 고위 인사들의 국제회의'[426]에서 러시아가 제안한 '국제정보안보에 관한 협약 초안'[427]에 그대로 드러나 있다. 이 협약 제5조 제5항에서는 "각국가는 자국의 국내법에 따라 자국의 정보 공간에 대해 독립된 규범을 제시하고 관리할 권한이 있다"고 규정하고 있다.[428]

부다페스트협약에 대한 반대입장은 인터넷 주권에 대한 러시아의 인식을 가장 잘 드러내주고 있다.[429] 러시아는 부다페스트협약 제32조를 이유로 부다페스트협약에의 가입을 거부해왔다.[430] 이 협약 제32조 b호는 일국이 법적 권한 있는 자의 합법적이고 자발적인 동의를 얻는 경우, 타당사

---

422) James Andrew Lewis, *supra* note 417, p. 3.
423) UN Doc. A/54/213 (1999), p. 8.
424) UN Doc. A/56/164/Add.1 (2001), p. 4.
425) Keir Giles, *supra* note 419, p. 65.
426) International Meeting of High-Ranking Officials Responsible for Security Matters. 본 회의는 2011년 러시아의 Ekaterinburg에서 9월 22일-23일 이틀에 걸쳐 진행되었다.
427) The Ministry of Foreign Affairs of Russia, Draft Convention on International Information Security (Sept. 9, 2011).
428) *Ibid.*, Art. 5.5.
429) Martha Finnemore, Duncan B. Hollis, *supra* note 127, p. 7; Council on Foreign Relations, Dec. 11, 2014, "Coming Soon: Another Country to Ratify the Budapest Convention", <http://blogs.cfr.org/cyber/2014/12/11/coming-soon-another-country-to-ratify-to-the-budapest-convention/> (2018.1.25.최종방문).
430) Daniel Kennedy, "Deciphering Russia: Russia's Perspectives on Internet Policy and Governance", Global Partners Digital (2013), p. 11.

국의 허가 없이도 자국의 컴퓨터 시스템을 통해 타국에 위치한 서버에 저장되어 있는 데이터에 접근하거나 데이터를 전송받을 수 있도록 하고 있다.[431] 러시아는 이 조항이 회원국 및 회원국 국민의 주권과 안전을 손상시킬 수 있다며 반대 입장을 밝혀왔다.[432]

그러나 러시아가 이 협약의 가입을 거부하는 주된 이유는 이 협약 제32조 b호의 "타 당사국의 허가 없이도", "법적 권한 있는 자의 합법적이고 자발적인 동의" 라는 문구 때문이다. 정보에 대한 통제권이 민간에게 주어지는 것을 거부하는 입장을 취하고 있는 러시아에게 해당 조항은 민간이 국가의 통제를 벗어나 타국에게 정보 또는 시스템에 대한 이용권을 주는 것으로 해석되기 때문이다. 러시아는 또한 타국발 정보가 무분별하게 자국에 유통되는 것에 대해서도 극도로 경계하는 입장을 드러낸 바 있다.[433] 따라서 러시아는 국가의 인터넷주권을 우회하는 듯한 해당 조항이 포함된 부다페스트협약에 대해 가입거부 입장을 고수하고 있다. 러시아는 이처럼 밖에서 들어오는 정보에 대한 통제 뿐 아니라 자국의 관할 하에 있는 정보가 국경 밖으로 나가는 것에 대한 통제권도 인터넷주권의 범위 안에 포함시키고 있다.

러시아의 주된 입장 두 번째는 사이버공간을 규율하기 위한 새로운 국제법체제가 필요하다는 것이다. 여기에는 물론 부다페스트협약 이외의, 즉 국가의 정보에 대한 주권을 명시한 새로운 규제체제가 필요하다는 내용이

---

431) Council of Europe, Convention on Cybercrime, 32.b.
access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

432) Cybercrime Convention Committee (T-CY), "Report on the 2nd Multilateral Consultation of the Parties Strasbourg, 13 and 14 June 2007", Council of Europe, Jul. 20, 2007, <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d52a1> (2018.1.5.최종방문).

433) UN Doc. A/54/213 (1999), p. 9

중요한 한 부분을 차지한다.

그러나 또 한 가지 중요한 축을 이루는 부분은 사이버무기 군축을 위한 다자조약의 체결이다. UN 등 국제기구에 제출한 문서를 검토하면 러시아가 정보를 위협으로 보는 시각에서 더 나아가 무기로 보고 있음을 알 수 있다. 러시아는 정보통신분야에서의 기술발전이 정보무기의 창출을 통해 군비확장경쟁을 촉발할 수 있다고 하면서 정보무기 사용의 결과가 대량살상무기를 사용한 결과에 비견할만한 것이라고 강조하였다.[434] 러시아는 또한 사이버기술이 범죄조직에 의해서 적대적 행위를 위한 수단으로 또는 군사적 무기로 사용될 가능성을 제기하였다. 러시아는 각국이 자국의 국내법을 통해 불법적인 정보사용을 규제하고 있기는 하지만 국가마다 규제의 기준과 범위가 다른 것도 문제점으로 지적하였다. 특히 이러한 정보무기가 테러조직이나 범죄조직에 의해 사용될 경우, 정보공격의 규모와 성격은 필연적으로 국경을 초월하는 국제적인 차원에서 이루어지게 될 것이라고 보았다. 따라서 사이버공간에 대한 각국의 법령을 조화시키는 것이 필요하고, 궁극적으로는 이를 규율하기 위한 국제법체제가 필요하다는 것이다.[435]

주목할만한 것은 정보전 및 정보전투 수단의 역할이 증가하는 현 상황에서 국가주권의 '위협'에 대한 전통국제법의 정의에 대해 재고할 필요가 있다고 주장한 부분이다. 러시아는 정보 및 경제적 파워의 조합이 군사적 무력의 사용을 의미하는, 전통국제법에서 금지하고 있는 '강제'를 우회하여 무력을 사용한 것과 같은 결과를 가능하게 한다고 지적하였다. 즉, 무력사용금지원칙을 주축으로 하는 현 국제법체제 내에서는 러시아가 국가안보나 국제평화에 대한 중대한 위협으로 여기는 심각한 경제적 타격 또는 사회적·정치적 혼란을 가져오는 사이버공격이 국제법상 금지된 강제의 범위에 포함되지 않는다는 것이다.[436]

---

434) UN Doc. A/54/213 (1999), p. 8.
435) UN Doc. A/56/164/Add.1 (2001), pp. 3-4.
436) *Ibid.*, p. 5

러시아는 여기에서도 정보기술 선진국들이 정보무기의 사용이 무력사용 금지원칙에 의해 제한되지 않는다는 이를 사용하여 타국에 대한 사이버공격을 감행하는 것이 용인되는 상황을 경계하고 있다. 따라서 '정보의 자유로운 흐름'이라는 모토 아래 정보의 위협적인 사용이 국제법 하에서 용인되는 상황을 막기 위해 명확한 기준을 도입하여 정보사용을 규제하는 체제의 성립이 필요하다고 주장하고 있는 것이다. 러시아는 사이버무기를 제한하는 다자체제가 구축되지 않으면, 결국 냉전시기와 같은 상황이 벌어지게 될 것이라고 하면서 사이버무기 군축조약의 필요성을 역설하였다. 러시아는 제네바 군축회의의 틀 내에서 이 문제를 논의해야 한다고 제안하기도 하였다.[437]

이러한 주장을 면밀히 살펴보면 러시아는 사이버공간에 대해 기존의 국제법원칙을 적용하는 것에 반대를 하는 것은 아니라는 것을 알 수 있다. 오히려 러시아는 국가주권평등의 원칙, 국내문제불간섭원칙, 무력사용금지원칙 등의 국제법원칙을 사이버공간에도 적용하기 위해서는 정보의 위협적인 영향력을 제한할 수 있는 기준을 새로운 체제의 도입을 통해 마련해야 한다고 보고 있다. 러시아는 특히 중국과 함께 무력사용금지원칙이 사이버공간에 대해서도 엄격하게 지켜져야 한다고 주장하고 있다. 이는 사이버공간에서 일어난 악의적인 활동에 대해서 무력을 사용한 대응을 해서는 안된다는 것이다.[438] 이러한 입장은 UNGGE보고서 채택과정에서도 확인할 수 있다. 러시아와 중국은 2015년 UNGGE보고서 채택 당시, 인터넷 통신기술의 사용에 대한 국제법에 합치하는 조치에 자위권을 명시하는 데 반대하였다.[439] 이에 보고서에는 자위권, UN헌장 제51조 라는 문구 대신

437) *supra* note 434, pp. 8-9.
438) Lawfare, Jul. 4, 2017, "The UN GGE Failed. Is International Law in Cyberspace Doomed As Well?", <https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well> (2017.9.19.최종방문).
439) The Diplomat, Jul. 31, 2017, "UN GGE on Cybersecurity: The End of Era?", <http://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china

“inherent right in the Charter”라는 표현으로 대체되었다.[440]

이와 같은 입장은 2017년 UNGGE회의에서도 계속되었다. 2017년 UNGGE 최종 세션에서 국가들의 정보통신기술 사용에 적용가능한 특정 국제법과 관련하여 자위권, 국제인도법, 국가책임 및 대응조치 원칙이 최종 초안 제34항에 포함되었다. 쿠바는 이에 대해 반대선언서를 내며 명시적으로 반대의사를 밝혔다. 선언서에서 쿠바는 이러한 원칙의 명기는 사이버공간을 군사활동의 장으로 만들고, 특정 정보통신기술 사용의 피해자라고 주장하는 국가가 군사적 조치를 포함한 처벌적 대응조치를 합법화하는 것이라며 이에 대한 심각한 우려를 표명하였다.[441] 비록 쿠바만 공식적인 선언을 통해 반대의사를 표명했으나, 여기에는 러시아와 중국도 GGE 논의 과정에서 이와 입장을 같이 한 것으로 보도되고 있다.[442] 러시아와 중국이 자위권을 명기하는 데 이토록 민감한 반응을 보이는 이유는 자위권 개념 자체에 반대하기 때문이 아니다. 그보다는 서방국가들이 자국에 대해 발생한 사이버활동의 강도를 자의적으로 판단하여 이에 무력으로 대응할 가능성이 높다고 판단하기 때문이다.[443]

-and-russia-just-made-cyberspace-less-safe/> (2017.9.19. 최종방문).

440) UN Doc. A/70/174 (2015), para. 28 (c).

441) Miguel Rodriguez (Representative of Cuba), “Declaration at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”, Jun. 23, 2017, p. 1, <https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf>

442) The Diplomat, Jul. 31, 2017, “UN GGE on Cybersecurity: The End of Era?”, <http://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/> (2017.9.19. 최종방문); The Guardian, Aug. 23, 2017, “Dispute along cold war lines led to collapse of UN cyberwarfare talks“, <https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges> (2017.9.19.최종방문).

443) Asia & Pacific Policy Society, Sept. 18, 2017, “The need for clarity

러시아는 또한 중국 및 쿠바와 함께 적대적 사이버공격에 대한 대응조치에 대해서도 부정적인 입장을 밝힌 것으로 알려졌다. 이들 국가는 악의적 사이버공격에 대해 피공격국이 자국의 사이버역량을 사용하여 역해킹과 같은 대응조치를 하는 것에 대해 우려를 나타냈다고 보도 되고 있다.[444] 구체적으로는 이러한 조치가 공격자의 행동을 중단시키기 위한 것이라고 해도 조치의 시기 및 강도를 어떻게 해야 하는 지를 판단하기 어렵다는 이유로 반대의사를 낸 것이다.[445]

지금까지의 내용을 정리하면 러시아가 주장하는 새로운 체제에는 국가의 인터넷주권, 사이버무기 군축, 사이버공간에서의 활동에 대한 무력대응 금지가 반드시 포함되어야 한다. 러시아는 이러한 입장을 중국, 우즈베키스탄 등의 국가와 함께 UN 차원의 다자조약 체결을 통한 새로운 사이버 규제체제의 성립을 주장하면서 구체화시키고 있다.[446]

2011년 9월 러시아는 중국, 우즈베키스탄 및 타지키스탄과 함께 '정보안보에 관한 국제적 행동수칙'이라는 명칭으로 UN총회 결의안을 제출하였다.[447] 이 결의안 b호에서는 국가가 적대행위나 침략행위를 수행하거나 국제평화와 안전에 위협을 주기 위해 또는 정보무기나 관련 기술을 확산하기 위해 정보통신기술을 사용하지 않아야 한다는 점을 강조하고 있다.[448] 또한 c호는 국가가 테러리즘, 분리주의, 또는 과격주의를 선동하거

---

in international cyber law", <https://www.policyforum.net/the-need-for-clarity-in-international-cyber-law/> (2017.9.19.최종방문).

444) *Ibid.*

445) *Ibid.*

446) Keir Giles, *supra* note 418, p. 50; The Cybersecurity Source Magazine US, Apr. 23, 2010, "Global Cybercrime treaty rejected at U.N.", <https://www.scmagazine.com/global-cybercrime-treaty-rejected-at-un/article/557657/> (2018.1.5.최종방문).

447) International Code of Conduct for Information Security, UN Doc. A/66/359 (2011). 이는 러시아가 앞서 말한 '국제정보안보에 관한 협약 초안'을 제안한 직후에 UN에 제출한 것이다.

나 다른 국가의 정치·경제와 사회적 안정 및 정신적 및 문화적 환경을 해치는 정보의 전파를 억제하는데 협력해야 한다고 촉구하고 있다.[449] 제출된 결의안의 내용에서 러시아가 주장해오던 내용이 그대로 반영된 것을 확인할 수 있다. 해당 결의안은 주요기반시설을 운용하는 컴퓨터네트워크의 보호와 정보의 자유로운 이동을 지지하는 서방국가들의 거센 반발을 샀다.[450]

이후 2015년 러시아와 중국, 우즈베키스탄, 키르키즈스탄, 카자흐스탄 다섯 개 국가는 서방국가들의 반발을 고려하여 개정된 결의안을 UN총회에 제출하였다.[451] 개정된 결의안에서는 2011년 결의안 b호의 “hostile”, “acts of aggression”, “proliferate information weapons or related technologies” 등의 문구가 삭제되었다. 대신 국제평화와 안전의 유지에 반하는 활동을 수행하기 위해 정보통신 기술 및 네트워크를 사용해서는 안된다는 일반적인 내용의 수정된 문구를 담았다.[452] 그러나 제5항에서 국가가 “특히 정보기술 분야에서 자신의 지배적 지위를 이용하지 않도록” 이라는 문구가, 제7항에서는 “오프라인 환경에서의 개인의 권리는 온라인 환경에서도 보호되어야 한다” 는 문구가 추가되었다.[453] 결국 2011년 결의안에서의 다소 과격한 표현을 삭제하는 대신 추가한 문구를 통해 여전

448) 러시아는 1998년 유엔 총회에 정보무기통제에 관한 조약 체결을 제안하는 결의 초안을 보냈으나 서방국가들로부터 지지를 받지 못한 바 있다. UN Doc. A/Res. 53/70 (1999); UN Doc. A/54/213 (1999), pp. 8-10; UN Doc. A/C.1/53/3 (1998), pp. 3-4.

449) International Code of Conduct for Information Security, UN Doc. A/66/359 (2011).

450) CCD COE Incyder News, Feb. 10, 2015, “An Updated Draft of the Code of Conduct Distributed in the United Nations – What’s New?”, <https://CCD COE.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html#footnoteref6_kjqqss0> (2017.4.10.최종방문).

451) International code of conduct for information security, UN Doc. A/69/723 (2015).

452) *Ibid,* Code of Conduct 2(2).

453) *Ibid,* Code of Conduce 2(5), 2(7).

히 서방의 지배를 제한하고, 사이버공간에 대한 통제를 주장하는 기존 논지를 고수하고 있다. 무엇보다도 2013년 UN총회에서 총의로 채택된 제3차 UNGGE보고서[454]의 사이버공간에 대한 기존 국제법의 적용을 명시하지 않음으로써 사이버공간을 규율하는 새로운 국제법체제 마련에 대한 기존의 입장에 변화가 없음을 보여주었다.

한편 중국은 사이버안보에 대한 국제법적 규율에 대해 러시아와 같은 입장을 취하는 대표적인 국가로 사이버공간에서의 정보 흐름에 관한 기본적 시각을 공유하고 있다. 중국은 러시아와 마찬가지로 인터넷 선발주자인 선진국들이 사이버공간에서 지배적인 위치를 차지하는 것에 반감을 가지고 있으며,[455] 사이버무기 규제[456]와 사이버공간에서의 자위권 사용[457], 인터넷 주권에 대해서도 러시아와 입장을 같이하고 있다.

---

454) United Nations, General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98 (2013).

455) Milton L. Mueller, "China and Global Internet Governance: A Tiger by the Tail," in Ronald Deibert, John Palfrey, Rafal Rohozinski and Jonathan Zittrain (eds.), *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (Cambridge, MIT Press, 2011), p. 182.

456) 사이버무기 규제에 대한 중국의 입장은 2009년에 상하이 협력기구의 회원국간에 체결한 국제정보안보 보장을 위한 협력에 관한 협약(Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, 이하 SCO협약)에서 잘 드러난다. 이 협약 제2조는 정보무기의 개발 및 사용, 타국의 이익과 안보에 손상을 주는 방식으로 정보공간에서의 지배적 위치를 사용하는 것, 타국의 경제·사회·문화적 환경에 해를 끼치는 정보의 유통 등을 주요 위협으로 규정하고 있다.

457) 중국은 그동안 무력사용금지원칙이 규정되어 있는 UN헌장에 대한 엄격한 해석을 고수해 왔으며, 사이버공간에 대해서도 이러한 입장을 일관되게 보이고 있다. 대표적으로 중국은 미국이 사이버공간에서 자위권적 조치를 사용하는 것을 국제법위반으로 보고 있다. Julian Ku, "How China's Views on the Law of Jus ad Bellum Will Shape Its Legal Approach to Cyberwarfare", Hoover Institution (2017), p. 1.

2. 미국 및 서방진영의 입장

사이버 문제에 대해 새로운 체제가 필요하다고 주장하는 러시아 및 중국의 입장과는 달리 미국을 비롯한 서방국가들은 현행 국제법이 사이버공간에도 그대로 적용가능하다고 주장한다.[458] 새로운 체제 형성에 반대하는 진영의 입장을 간단하게 정리하면 기본적으로 사이버공간에서 정보의 자유로운 이동과 표현의 자유 보장을 지지하되,[459] 위협이 되는 활동에 대해서는 현행 국제법을 적용하여 대응한다는 것이다. 기본적으로 정보를 위협으로 보고 이의 통제에 방점을 두는 러시아 및 중국과는 대조적인 인식을 가지고 문제에 접근하고 있다는 점을 알 수 있다. 이러한 인식의 차이는 우선 사이버공간의 주요 행위자를 파악하는 데 있어 다중이해자 접근 방식 대 사이버공간에 대한 국가주권의 강조로 나타나고 있다.

이러한 서방국가들의 입장은 2011년 개최된 사이버공간에 관한 '런던 국제회의'(London International Conference on Cyberspace)나 '경제협력개발기구'(Organisation for Economic Cooperation and Development, OECD)의 '인터넷 정책입안 원칙에 관한 권고'[460]와 같은 국제문서에서 확인할 수 있다. 런던회의에서 의장을 맡았던 영국의 외무장관 William Hague는 성명에서 안전한 디지털 환경은 각국 정부의 노력만으로는 이루어질 수 없음을 분명히 하면서 시민사회, 다양한 산업분야가 함께 참여하는 다중이해관계자 접근 방식의 중요성을 강조하였다.[461]

---

458) Developments in the field of information and telecommunications in the context of international security, UN Doc. A/59/116/Add.1 (2004), pp. 3-6.

459) Prakash, Rahul and Darshana M. Baruah, *supra* note 416, p. 2.

460) OECD, "OECD Council Recommendation on Principles for Internet Policy Making", (2011), pp. 3-8.

461) UK Foreign & Commonwealth Office, "London Conference on Cyberspace: Chair's statement" (2011), <https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement> (2018.1.5.최종방문).

이후 사이버공간에 대한 자율성 및 다중이해자 접근 방식을 지지하는 이러한 입장은 같은 해 12월에 발표된 OCED 권고[462], 2012년 국제전기통신회의[463], 미래 인터넷 거버넌스에 관한 글로벌 다중이해관계자 회의[464] 등에서도 확인된 바 있다. 미국을 비롯한 서방국가들의 다중이해자 접근방식에 대한 지지는 이후 2013년 제3차 UN GGE보고서, 2015년 제4차 UN GGE보고서에도 반영되어 사이버공간에서 국제안보와 평화를 달성하기 위해 민간부문과 시민사회의 참여가 필요하다는 문구가 명시되었다.[465]

다중이해관계자 접근 방식은 사이버공간에서의 국가주권을 중시하는 러

462) OECD, *supra* note 460, pp. 3-8.

463) World Conference on International Telecommunications. 해당회의에서 미국을 비롯한 영국, 캐나다, 프랑스, 포르투갈, 스웨덴 등의 국가들은 국가의 검열이 지나치게 확대될 수 있다는 이유로 정부의 인터넷공간에 대한 통제권한 확대에 관한 안을 국제전기통신규약에 포함하는 것에 반대하였다. International Telecommunication Union, "Signatories of the Final Acts: 89", <http://www.itu.int/osg/wcit-12/highlights/signatories.html> (2018.1.5.최종방문); Jonathan Clough, "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization", Monash University Law Review, Vol. 40, No. 3 (2014), p. 729; BBC News, Dec. 14, 2012, "US and UK Refuse to Sign UN's Communications Treaty" *BBC News*, <http://www.bbc.com/news/technology-20717774> (2018.1.5.최종방문).

464) Global Multistakeholder Meeting on the Future of Internet Governance. 이 회의의 결과물로 다중이해관계자 체제를 지지하는 성명(NETmundial Multistakeholder Statement)이 채택되기도 하였으며, 러시아, 중국 및 이란과 같은 국가들은 정부 관리 중심의 체제를 옹호하며 이에 반대의사를 표명한 바 있다. Global Multistakeholder Meeting on the Future of Internet Governance, Apr. 23, 24, 2014, <http://netmundial.br/netmundial-multistakeholder-statement/> (2017.4.11.최종방문); Stuart N. Brotman, "Multistakeholder Internet governance: A pathway completed, the road ahead", Center for Technology Innovation (2015), p. 3.

465) UN Doc. A/68/98 (2013), paras. 12, 24, 25; UN Doc. A/70/174 (2015), paras. 21(g), 23, 31.

시아와 중국의 입장과 극명하게 대조를 이루는 모습을 보여주고 있다.[466] 다중이해관계자 모델에서 국가는 민간부문, 시민사회 등 여러 행위자 가운데 하나일 뿐이다.[467] 이들 행위자는 사이버공간에서 공유하는 원칙, 규범, 의사결정 절차에서 각자의 역할이 있다.[468] 이러한 다원적 형식의 절차는 국가중심의 규제체제와는 현저하게 대조를 이루는 것이다.[469] 따라서 사이버공간의 국제적 규율과 관련하여 러시아·중국 진영과 미국 등 서방진영을 나누는 또 하나의 구도는 국가 행위자 중심의 다자체제(Multilateral) 대 다중이해자 중심체제(Multistakeholder) 라고 할 수 있다.[470]

정보에 대한 인식의 차이는 사이버공간을 규율하는 국제법체제에 대한 입장의 차이로도 나타나고 있다. 앞서 살펴본 러시아와 중국은 정보를 규율하는 새로운 국제법체제가 마련되어야 한다는 입장이고, 서방국가들은 현행 국제법이 적용가능하다는 입장이다. 서방국가들이 말하는 기존의 국제법에는 2001년 부다페스트협약이 포함되어 있다. 이는 러시아와 중국이 부다페스트협약을 종종 기존의 협약 또는 기존의 국제법이라고 지칭하면서 새로운 국제법체제가 필요하다고 주장하는 데 따른 것이다.

2010년 제12차 UN 범죄방지 및 형사사법위원회(The Twelfth United Nations Congress on Crime Prevention and Criminal Justice)에서 중국과 러시아는 사이버 범죄에 대한 범세계적인 협약이 필요하며 이에 대한 협상절차가 시작되어야 한다고 주장하였다.[471] 이들은 기존의 부다페

---

466) Tim Maurer, “Cyber Norm Emergence at the United Nations- An Analysis of the Activities at the UN Regarding Cyber-Security”, Belfer Center (2011), P. 25.
467) Martha Finnemore, Duncan B. Hollis, *supra* note 127, p. 21.
468) Tim Maurer, *supra* note 466, P. 25.
469) Martha Finnemore, Duncan B. Hollis, *supra* note 127, P. 21.
470) Tim Maurer, *supra* note 466, P. 25.
471) Report of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, UN Doc A/CONF.213/18 (2010), p. 56, para. 202; SC Magazine, Apr. 23, 2010, “Global Cybercrime Treaty Rejected at UN”, <https://www.scmagazine.com/global-cybercrime-treaty-rejected-at-un

스트협약을 포함한 사이버 범죄조약이 주로 양자 간에 체결된 것이거나 지역적인 것이기 때문에 전 국제사회를 아우르지 못한다면서 UN차원의 사이버 범죄 협약의 필요성을 역설하였다.[472]

이에 대해 미국, 영국 및 유럽연합은 사이버 범죄의 국제적 규제는 기존의 2001년 부다페스트협약으로도 충분하다는 의견을 제시하였다.[473] 또한 이들은 새로운 협약에 관한 논의는 시기상조라고 하면서 새로운 협약의 초점과 범위가 먼저 명확하게 설정되어야 한다고 하였다. 새로운 협약의 협상과정에서 이견이 있을 것으로 예상되는 주제로는 역외관할권 및 이로 인한 국가주권 문제, 프라이버시와 국가안보, 정부 간 협상 과정에서 민간부문의 참여 여부에 관한 문제가 지적되었다.[474]

서방국가가 말하는 현행 국제법은 또한 UN헌장에 규정된 무력사용금지원칙, 주권평등의 원칙, 국내문제불간섭원칙, 자위권의 원용, 국제인도법 원칙, 국가책임원칙을 의미한다. 2013년 제3차 UNGGE보고서, 2015년 제4차 UNGGE보고서에서는 기존의 국제법원칙이 사이버공간의 규율에도 그대로 적용된다고 하면서 그러한 원칙의 예로 주권평등의 원칙, 무력사용금지원칙, 불간섭원칙, 분쟁의 평화적 해결 원칙 정도가 담겨 있었다.[475] 사이버공간에서 국가들이 취할 수 있는 조치도 앞서 살펴본 것처럼 자위권

/article/557657/> (2017.4.11.최종방문); Jonathan Clough, *supra* note 463, p. 727.

472) UN Doc A/CONF.213/18 (2010), p. 56, para. 202.

473) Jonathan Clough (2014), p. 727; UN Doc A/CONF.213/18 (2010), p. 56, para. 203.

474) *Ibid.*, p. 57, para. 204.

475) United Nations, General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98 (2013), paras. 16, 19-20, 23; United Nations, General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174 (2015), paras. 11, 24-27.

이 아닌 inherent right으로 표현되었다.[476] 국가책임, 대응조치, 자위권, 국제인도법 원칙은 2017년 UNGGE에서 사이버공간에 적용가능한 국제법 원칙을 구체화하자는 논의를 통해 언급된 것이다.[477] 열거된 국제법원칙들을 보면 적대적인 사이버공격 발생 시의 대응에 대해 방점을 두고 있음을 알 수 있다. 즉, 서방국가들의 시각이 다분히 반영되어 있는 것이다.

이번 2017년 UNGGE의 논의 과정을 면밀히 살펴보면 서방국가와 반대 진영의 주장이 특정 기존 국제법원칙에 대한 해석에 있어 대척점에 서 있다는 것을 알 수 있다. 미국은 무력사용금지원칙을 사이버공간의 규율에 적용함에 있어 재래식 무기를 사용한 것만을 무력의 사용으로 보지 않는다.[478] 따라서 일정 강도 이상의 사이버공격을 무력공격으로 보고, 이에 대해서는 자위권을 통한 대응이 가능하다고 주장하는 것이다.

그러나 이에 반대하는 진영은 무력사용금지원칙을 엄격하게 해석하기 때문에 사이버공간에서 일어난 일에 대해 물리적 공간에서의 무력사용으로 대응하는 것에 대해 우려를 표현하고 있다.[479] 이는 2017년 UNGGE 최종세션에서 정보통신기술의 악의적인 사용을 무력공격으로 볼 수 있어 자위권을 사용한 대응이 가능하다는 내용이 담긴 초안에 대해 강하게 반대의사를 밝힌 쿠바의 선언에서 잘 나타난다.[480] 대응조치와 관련해서도

---

476) UN Doc. A/70/174 (2015), para. 28(c).

477) Just Security, Jun. 30, 2017 - Michael Schmitt and Liis Vihul, "International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms", <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/> (2017.9.22.최종방문).

478) Julian Ku, *supra* note 457, p. 1;

479) Geneva Digital Watch, Jun. 30, 2017, "UN GGE: Quo Vadis?", <https://dig.watch/DWnewsletter22> (2017.9.22.최종방문); Lawfare, Aug. 25, 2017, "Forcing China to Accept that International Law Restricts Cyber Warfare May Not Actually Benefit the U.S.", <https://lawfareblog.com/forcing-china-accept-international-law-restricts-cyber-warfare-may-not-actually-benefit-us> (2017.9.22.최종방문).

480) Miguel Rodriguez (Representative of Cuba), "Declaration at the

서방국가는 무력공격에 이르지 못하는 사이버공격에 대해서는 역해킹과 같은 조치를 대응조치의 범위에 포함시켜 기존의 국제법을 그대로 적용하려고 한다.[481]

미 국무부의 사이버 문제 담당자인 Christopher Painter는 이를 'Internet connectivity' sanctions라고 하였다.[482] 반대진영은 이에 대해서도 조치의 시기 및 강도를 어떻게 해야 하는 지를 판단하기 어렵다는 이유로 이에 반대하였다. 이들은 서방진영이 자의적인 기준을 적용하여 자위권을 원용하여 무력대응을 하거나 역해킹과 같은 대응조치를 취하는 것을 우려하고 있다. 자위권은 우선적으로 피해국이 발동여부를 판단하게 되어 있기 때문이다. 즉, 자위권 및 대응조치가 필요하다고 판단되는 선공격의 강도, 성격, 조치 시기 등의 기준이 명확히 마련되지 않은 상황에서 이들 원칙을 보고서에 명시하는 것에 반대하고 있는 것이다.

이에 대해 미국 측 대표 Michele G. Markoff는 반대국가들이 적용가능한 원칙의 도입을 막는 것을 통해 사이버공간 안에서 제한 없이 악의적 사이버활동을 하며 자신들의 정치적 목적을 달성하려 한다고 비판하였다.[483] 중국 및 러시아 진영의 주장을 사이버활동에 적용가능한 국제법에

Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (2017), p. 2, <https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf>

481) Asia & The Pacific Policy Society, Sept. 18, 2017, "The need for clarity in international cyber law", <https://www.policyforum.net/the-need-for-clarity-in-international-cyber-law/> (2017.9.22.최종방문).

482) Geneva Digital Watch, Jun. 30, 2017, "UN GGE: Quo Vadis?", <https://dig.watch/DWnewsletter22> (2017.9.22.최종방문).

483) Michele G. Markoff, "Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security", US Department of State, Jun, 23, 2017,

있어서 유용한 수준의 모호성을 유지하려는 의도로 보는 시각도 있다. 이는 그러한 모호성을 유지하는 것이 사이버공간 내에서의 활동에 전략적 유연함을 제공해 주기 때문이다.[484]

미국을 비롯한 서방국가들은 사이버공간에서 일어나는 행위를 가능한 한 물리적 공간에서의 상황에 대응시켜 현행 국제법을 그대로 적용하려고 한다. 따라서 사이버공간 내에서의 활동도 금지된 부분에 대해서만 대응을 하려는 입장을 보이고 있는 것이다. 2013년 제3차 UNGGE 보고서에서부터 2015년 제4차 UNGGE보고서까지 유지되어 왔던 이러한 주장은 2017년 UNGGE 보고서 채택에 실패하면서 향후 과제로 남겨지게 되었다.

3. 소결

이상으로 사이버공간의 규율과 관련하여 의견이 나뉘는 대표적인 두 진영의 입장을 각각 살펴보았다. 이 두 진영의 입장을 정리하면 사이버공간에 대한 국제법 규율에 대해 중요한 시사점을 도출할 수 있다. 이는 특히 두 진영이 서로를 비판하는 내용에서 찾을 수 있다. 이들이 서로를 비판하는 내용을 한 단어로 요약하면 바로 '법적 모호성'(legal ambiguity)이다. 러시아와 중국은 서방국가들이 자위권, 대응조치와 같은 현행 국제법원칙을 '그대로' 적용가능하다는 주장을 통해 '자의적 기준'을 사용하여 사이버공간을 전장으로 만들려고 한다고 비판한다. 반면 서방국가들은 러시아·중국을 필두로 한 국가들이 적용 가능한 국제법원칙의 명시를 저지하고, 이로 인한 법적 공백을 활용하려 한다고 비판하고 있다.

양 진영의 비판에서 언급된 법적인 모호성은 사이버공간을 법적으로 규

<https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm> (2017.9.20.최종방문).

484) Asia & The Pacific Policy Society, Sept. 18, 2017, "The need for clarity in international cyber law", <https://www.policyforum.net/the-need-for-clarity-in-international-cyber-law/> (2017.9.20.최종방문).

율하는 데 꼭 해결되어야 할 문제들이다. 우선 현재 일어나고 있는 사이버공격의 빈도를 생각할 때, 자위권 원용이나 대응조치를 위한 사이버공격의 강도에 대한 명확한 기준설정은 꼭 필요한 작업이다. 서방국가들은 사이버공간에 대해서도 현행 국제법원칙이 그대로 적용된다고 주장하면서 사이버공격을 강도별로 유형화하여 기존 국제법원칙에 끼워 넣는데 집중하고 있다.

그런데 그 과정에서 기존의 원칙을 적용하기에는 그 경계가 모호한 강도와 효과를 가지는 유형의 사이버공격이 명확한 적용 영역이 정해지지 않은 채로 남겨지는 현상이 나타나고 있다. 이는 러시아와 중국이 제기한 자의적 대응에 대한 우려가 전혀 근거 없는 주장이 아님을 보여주는 것이라고 볼 수 있다. 러시아와 중국의 사이버공간 규율에 대한 주장이 다소 국가중심적이고 폐쇄적인 면이 있는 것은 사실이지만 이를 서방국들의 기술적 지배를 경계하기 위한 것으로만 치부하는 것이 적절하지 않은 이유가 여기에 있다. 명확한 기준마련과 관련된 문제는 적용 가능한 국제법원칙의 명시를 위해 선행적으로 요구되는 사항이다.

한편 새로운 규제체제의 성립이 필요하다면서도 구체적 대안에 대해서는 침묵하고 있는 러시아와 중국은 법적인 공백을 메울 수 있는 실질적인 규제방안을 제시해야 한다. 인터넷주권, 사이버무기 군축조약, 사이버공격에 대한 무력대응 금지로 대변되는 이들의 주장은 구체적으로 어떤 규칙과 기준을 통해 사이버공간이 규율되어야 하는지 실체가 없다는 것이 가장 큰 문제점이다. 사이버무기 군축조약에 대해서도 조약의 성안을 제안했을 뿐이다.

인터넷주권과 관련한 주장에서도 이러한 문제점을 발견할 수 있다. 러시아와 중국은 주권을 침해할 가능성이 있다는 이유로 부다페스트협약에의 가입을 거부하고 있다. 그러나 이들이 문제삼고 있는 부다페스트협약 제32조 b호는 이들의 우려만큼 주권을 제약하는 조항이 아니라는 해석이 지배적이다.[485] 협약의 해설서에서는 제32조 b호에서 말하는 데이터를 공개

485) Jonathan Clough, *supra* note 463, pp. 719-723.

할 법적으로 권한 있는 자(lawfully authorised)가 누구를 의미하는 지는 상황 및 준거법에 따라 다양하게 해석될 수 있다고 하면서 명확한 정의를 내리지 않고 있다.[486] 또한 이와 관련된 구체적인 실행이 축적되지 않았기 때문에 협약의 성안자들이 이 분야를 포괄적으로 규율하기는 불가능하다는 결론을 내렸다고도 이야기하고 있다.[487] 이렇게 볼 때, 부다페스트협약 제32조 b항은 그 적용에 있어 해석의 여지가 많고, 상황에 따라 국가들 간에 합의가 이루어져야 할 부분이 많은 조항이라고 할 수 있다. 이는 해당 조항이 국가의 인터넷주권을 심각하게 해한다는 중국 및 러시아의 우려가 현실적이지 않다는 점을 보여준다.

반면 부다페스트협약에 관한 논란은 오히려 사이버공간의 규율에 있어 협조체제의 중요성을 부각시켜 주었다고 볼 수 있다. 국경의 제한이나 경계가 없는 사이버공간의 특성상 자국 영역 밖에서 발생한 사이버공격에 대해 조사하기 위해서는 국가 간의 협조가 필수적이기 때문이다. 2007년 에스토니아 DDoS 공격사건에서 러시아의 협조거부로 인해 조사가 더 이상 진행되지 못하고, 공격자를 밝히지 못한 채 사건이 일단락 된 사실은 이러한 해석을 뒷받침해준다.[488] 국가 간의 협조 부재는 사이버공격의 경우 명확한 출처를 규명하기 어렵다는 점을 사이버공간의 특성으로 인식하게 하는데 기여한다. 그러나 이러한 인식의 고착화는 proxies를 이용한 국가들의 사이버공격을 용인하는 결과를 낳을 수 있고,[489] 현행 국제법원칙을 적용하는 데도 걸림돌로 작용한다. 이는 역설적으로 협조체계의 구축이 사이버공간의 규율에 있어 얼마나 중요한 과제인지를 보여준다.

---

486) *Ibid.*
487) *Ibid.*, p. 52, para. 293.
488) Wired Magazine, August 21, 2007 - Davis Joshua, “Hackers Take Down the Most Wired Country in Europe”, <https://www.wired.com/2007/08/ff-estonia/#>.
489) Just Security, Dec. 11, 2014 - Kristen Eichensehr, “Cyber Attribution Problems--Not Just Who, But What”, < https://www.justsecurity.org/18334/cyber-attribution-problems-not-who/> (2017.4.13.최종방문).

이상 양 진영의 논의를 종합할 때 사이버공격에 대한 대응과 관련하여 중요한 부분이 빠져있다는 것을 알 수 있다. 사이버공격은 과정이 진행됨에 따라 저강도 수준에서 고강도의 수준으로 급격하게 전환된 수 있는 특징을 가지고 있다. 즉, 목표한 시스템을 장악하기까지는 이를 위한 사전작업으로 기관 내 개인 컴퓨터를 감염시키기 위해 바이러스를 유포하거나, 감염된 컴퓨터를 정찰하는 등의 불법적인 접근에 머무르지만 일단 내부시스템을 장악한 후 공격이 실행되면 빠른 시간 내에 치명적인 결과를 야기하게 되는 것이다. 따라서 사이버공격에 효과적으로 대응하기 위해서는 저강도 위협 수준에서 이를 탐지하여 사전에 공격을 차단하는 조치가 반드시 필요하다. 양 진영의 논의에는 이러한 근본적인 문제에 대한 고려가 결여되어 있는 것이다.

이는 양 진영이 합의를 통해 현행 국제법이 적용되는 명확한 기준을 마련한다고 해도 해결하기 어려운 문제이다. 그러한 기준을 적용한다는 것은 이미 위반행위가 발생했다는 것을 의미하기 때문이다. 또한 협조체계의 구축을 통해서 공격자를 밝힐 수 있게 된다 하더라도 이는 시간이 걸리는 과정이기 때문에 이 역시 사후적인 대응으로 귀결될 수밖에 없다. 사후적인 대응은 책임 추궁과 제제를 통해 향후 공격발생을 억지하기 위해 꼭 필요한 절차이지만 사후적 대응체제의 확립만으로 사이버공격에 대한 법적규율이 완성되었다고 볼 수는 없다. 따라서 사이버공격의 규율과 관련해서는 공격의 사전탐지 및 대응에 대한 국제법 차원의 논의가 별도로 필요하다.

제2절 각국의 대응전략

국가들은 국제법 차원의 논의와는 별개로 국내적으로 사이버공격에 대한 대응전략을 마련하고 있다. 이는 개별 국가가 실제로 직면하고 있는 사이버공격에 대응하기 위한 것이기 때문에 적용되는 원칙과 같이 이론적인 논의 차원을 넘어서 좀 더 실제적인 면을 가지고 있다. 즉, 국가들의 대응 및 대응전략은 곧 사이버공격에 대처하는 국가들의 실행을 보여주는 것이다. 적용되지 않는 법은 의미가 없듯이 국제법이 사이버공간을 규율하는 적절한 방안을 찾기 위해서는 국가들의 실행을 파악하는 것이 반드시 필요하다. 이를 통해 국제법이 놓치고 있거나 뒤쳐져 있는 부분이 있다면 그러한 부분을 반영해야 사이버공간에 대해서도 실효성 있는 국제법이 될 수 있다. 또한 이들 중 용인할 수 없는 부분이 발견된다면 국가들의 실행이 고착화되기 전에 이를 규제하기 위한 국제법적 규제방안을 마련하는 것이 필요하다. 이하에서는 주요 국가들의 대응전략 및 실행에 대해 검토해 보고 앞에서 살펴본 국제적 차원의 논의와 종합하여 현 상황을 진단해 보기로 한다.

1. 미국

미국은 부시 대통령 임기 중인 2003년, “The National Strategy to Secure Cyberspace”[490]와 같은 사이버안보 관련 보고서를 발표하는 등 일찍부터 사이버안보에 관심을 보여왔다. 그러나 보다 적극적인 사이버안보전략을 마련하게 된 것은 오바마 대통령 취임 이후라고 할 수 있다. 오바마 대통령은 사이버안보를 국가안보의 주요 이슈로 상정하고 2009년 사이버안보 보좌관 직위를 신설, 하워드 슈미트(Howard A. Schmidt)를 임명하였다. 또한 2010년에는 전략 사령부 (U.S. Strategic Command,

490) The White House, “The National Strategy to Secure Cyberspace” (2003).

USSTRATCOM)하에 사이버 사령부(U.S. Cyber Command, USCYBERCOM)를 신설하였다. 사이버 사령부는 미 국방부의 정보네트워크를 방어하고, 미국 및 동맹국의 사이버공간을 적국의 사이버공격으로부터 보호하기 위한 군사적 차원의 사이버 작전을 수행하는 역할을 담당하고 있다.[491]

미국은 이 당시만 해도 사이버안보에 있어 적극적인 억지 보다는 방어에 초점을 두고 있었다. 2011년 백악관이 발간한 사이버 전략 보고서를 보면 미국은 사이버공간에서의 자신의 역할을 국방, 외교, 개발의 세 영역으로 나누어 설명하고 있다. 우선 국방분야에서는 파괴력을 가지는 사이버공격을 최대한 신속히 파악하여 억제하고, 완화시켜 피해를 최소화 하는 방어전략을 취할 것을 먼저 언급하고 있다. 또한 당시에도 사이버공격에 대해 자위권 행사가 가능하다고 하고 있으나 구체적으로 어떤 경우에 어떤 수단을 사용하여 사이버공격에 대한 자위권을 행사할 수 있는지에 대해서는 언급하지 않고 있다. 이밖에도 국제법상 적용가능한 모든 외교·군사·경제적 조치를 취할 수 있다고 하는데 이 역시 구체적인 조치에 대해서는 언급하지 않고 있다. 마지막으로 개발 영역에서는 사이버공격을 방어할 수 있는 기술 개발과 이에 대한 보급 및 교육이 무엇보다 중요하다고 하면서 이러한 기술을 이용하여 사이버공격에 대비한 정부·민간의 합동 훈련이 효과적인 사이버안보 전략임을 강조하고 있다.[492]

같은 해 국방부가 발간한 사이버공간에서의 방위전략(Department of Defense Strategy for Operating in Cyberspace)에서도 백악관이 발간한 보고서와 마찬가지로 방어에 초점을 두고 있음을 알 수 있다. 방위전략에서 언급하고 있는 다섯 가지 전략적 이니셔티브 중 첫 번째 전략적 이니셔티브는 국방부가 사이버공간을 조직하고, 훈련시키며 사이버공격에 대비한 장비를 갖추도록 하는 것이다.[493] 두 번째 전략적 이니셔티브는 국방

491)http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/ (2017.1.9.최종방문).

492) The White House, *supra* note 196, pp. 13-14, 21.

493) US Department of Defence, “Department of Defense Strategy for

부의 네트워크와 시스템을 보호하기 위해 보안에 방점을 두고 있는데, 특기할 점은 이 부분에서 국방부가 적극적 방어 개념을 사이버안보에도 도입할 것을 이야기 하고 있다는 점이다. 그러나 이에 관한 설명을 보면 실시간으로 위협을 탐지하는 데 초점이 맞춰져 있어 전략기조는 여전히 방어에 중점이 있음을 알 수 있다.[494] 세 번째 전략적 이니셔티브에서는 정부부처와 정보기관 및 민간부분의 공조를, 네 번째 전략적 이니셔티브에서는 동맹국들과의 협력을 통한 집단 사이버안보 구축을, 마지막 다섯 번째 이니셔티브에서는 뛰어난 사이버 인력과 기술혁신을 통해 국가의 사이버 능력을 배양한다는 내용을 담고 있다.[495]

이렇게 백악관 보고서와 방위전략 곳곳에서 자위권, 방어기술 개발, 군용 사이버전 시뮬레이션 프로그램의 개발 등 공격적인 대응을 의미하는 용어를 발견할 수 있으나, 구체적 설명 없이 원론적인 언급에 그치고 있는 것을 볼 때, 당시까지 사이버안보에 대한 인식은 방어에 그 초점이 맞춰져 있었음을 짐작할 수 있다.

그러나 2015년에 발간된 "국방부 사이버 전략(The Department of Defence Cyber Strategy)"의 내용을 살펴보면 2011년의 전략과 비교하여 보다 더 공세적인 태도를 취하고 있음을 발견할 수 있다. 먼저 시작부분에서 미국의 가치를 위협한 사이버공격의 예로 북한의 소니픽쳐스사 공격[496]을 언급하면서 이와 같은 파괴적 사이버공격이 미국의 핵심 기반시설에도 일어날 수 있음을 경고하고 있다. 국방부는 이러한 사이버공격으로부터 미국의 가치를 보호하기 위해 국내법 및 국제법에 따라 필요한 조치

Operating in Cyberspace" (2011), pp. 5-6.

494) *Ibid.,* pp. 6-7. 본 전략에 소개된 적극적 사이버방어(Active Cyber Defence)는 공격에 직접 대응하는 조치를 취하기보다는 실시간으로 발생하는 위협을 탐지하는 센서 등 첨단 기술의 활용에 초점을 맞추고 있어 이 당시, 적극적 방어 개념이 다양한 공격적인 조치의 활용과 관련해서는 구체화되지 않은 것으로 보인다.

495) *Ibid.,* pp. 8-12.

496) US Department of Defence, "The Department of Defence Cyber Strategy" (2015), p. 2.

를 취할 것이라는 점을 먼저 언급하면서 취할 수 있는 조치가 아니라 현재 취하고 있는 군사적·외교적·경제적·정보적·법적 조치에 대해 구체적으로 소개하고 있다.[497] 언급된 구체적 조치로는 먼저 군 차원에서 사이버공격 대응훈련을 하고 있다는 점과 네트워크가 연결되지 않은 상황을 대비하여 통신시스템에 접속되지 않은 상황에서 작전을 수행하는 훈련이 있다.

또한 군은 대통령이나 국방장관의 명령에 따라 임박한 또는 진행되고 있는 사이버공격에 대응한 사이버 작전을 수행할 수 있다고 하였는데,[498] 이는 지금까지 발간된 보고서 중 처음으로 언급된 것이다. 이러한 사이버 작전의 예로는 사이버공격을 방해하는 것을 들고 있는데, 이는 네트워크를 교란시키거나 공격자에게 직접적으로 대응 사이버공격을 하는 것을 의미하는 것으로 보인다. 또한 이러한 대응 공격은 상대방의 국방네트워크만을 대상으로 하지 않고 상대국의 핵심 기반시설이 될 수도 있다고 설명하고 있다.[499] 이는 임박했거나 현재 진행되고 있는 공격을 완화(mitigate)시키는 수준을 넘어, 공격의 소스를 추적하여 직접 타격하는 역타격 또는 역해킹을 의미하는 것으로 미국의 대응전략이 소극적 방어에서 적극적 방어 혹은 적극적 억지로 전환되었음을 파악할 수 있는 대목이다.

특히 뒤이어 효과적인 억지를 위해 가장 중요하고 근본적인 부분이 바로 귀속의 문제임을 강조하면서 귀속의 문제를 해결하기 위해 국방부와 미 정보기관이 상당한 투자를 해왔다는 점을 언급하고 있다.[500] 국방부 전략이 말하는 귀속에 관한 설명에서는 추적을 통해 귀속을 밝히게 되면 공격에 사용된 기법·기술 및 공격의 절차까지 파악할 수 있고, 사이버공격 발생 시 즉각 이에 반응하고 거부 공격을 하는데 도움이 된다는 내용을 담고 있다. 나아가 귀속을 밝힘으로 인해 공격이 발생한 근원지를 공격하여 공격 행위자를 무력화 시킬 수 있다고 언급하고 있는 것[501]으로 보아

497) US Department of Defence, *supra* note 496, p. 2.
498) *Ibid.*, pp. 4-5.
499) *Ibid.*, p. 5.
500) *Ibid.*, pp. 11-12.
501) *Ibid.*

여기서 말한 귀속은 공격이 발생한 네트워크 추적이지 행위자를 찾아내는 단계까지를 의미하는 것은 아니라고 할 수 있다.

국방부 사이버전략은 이밖에도 사이버공격에 대해 취할 수 있는 외교적 행동, 법적 조치, 경제제재의 예로 미국이 중국의 경제적 사이버 간첩행위에 대해 취한 조치를 들고 있다. 미국은 여러 차례 중국에 대해 미국 기업의 지적 재산 탈취행위와 그로 인한 경제적 피해에 대해 우려를 표명한 바 있다. 그러나 이후에도 그러한 행위가 계속 되었고, 이는 명백한 미국법 위반임을 들어 미 법무부가 2014년 중국 인민 해방군(People's Liberation Army) 소속 다섯 명을 기소한 사건이 있었다.[502] 보고서는 이 사건을 예로 들면서 이는 미국 법을 위반한 데 대한 정당한 조치였을 뿐만 아니라 향후 중국의 사이버 간첩행위를 억지하기 위한 조치였다고 밝히고 있다.[503] 이는 위에 언급한 조치 중 법적인 조치에 해당한다고 할 수 있다.

미국이 방어적 대응 보다는 적극적이고 공격적인 방어로 대응태세를 전환 했다는 사실은 위 전략에 언급되지 않은 사례 및 법령 제정 시도에서도 확인할 수 있다. 2016년 12월 29일 미 국무부는 35명의 러시아 외교관에 대해 persona non grata 를 선언하고 72시간 내에 미국을 떠날 것을 명령하였다. 또한 러시아 정부가 소유한 미국 내의 2개 시설을 폐쇄하는 제재안도 발표하였다.[504] 오바마 대통령은 2015년 4월 21일 타국 발

---

502) U.S. Attorney's Office Western District of Pennsylvania, "U.S. Charges Five Chinese Military Hackers For Cyber Espionage Against U.S. Corporations And A Labor Organization For Commercial Advantage", United States Department of Justice, May 19, 2014, <https://www.justice.gov/usao-wdpa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and> (2017.4.18.최종방문).

503) US Department of Defence, *supra* note 496, p. 12.

504) The White House, "Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment", Dec. 29, 2016, <https://www.whitehouse.gov/the-press-office/2016/12/29/statement-p

사이버위협행위에 대해 미국 내에 있는 자산을 동결하는 행정명령을 발한 바 있는데, 이번 시설 폐쇄조치는 동 행정명령에 따른 것이다.[505] 이에 따라 조치가 발표된 다음날인 30일부터 모든 러시아 관계자들의 해당 시설에 대한 접근이 차단되었다. 미 국무부는 이번 조치가 사이버공격을 통한 러시아의 미 대선개입에 따른 것이라고 밝혔다.[506]

오바마 대통령은 러시아의 민주당전국위원회(Democratic National Committee, DNC) 해킹에 대한 대응은 여기에 그치지 않을 것이라고 하면서 추가제재조치를 취할 수 있음을 시사했다. 이후 오바마 대통령이 미 국가안보국(NSA)에 러시아의 기반시설에 파괴력이 있는 사이버무기를 침투시킬 것을 지시했다는 내용이 보도된 바 있다.[507] 해당 사이버무기는 침투한 채로 머물러 있다가 필요할 때 실행하면 러시아의 시설을 무력화 시킬 수 있는 "the digital equivalent of bombs"인 것으로 알려지고 있다.[508]

---

resident-actions-response-russian-malicious-cyber-activity> (2017.1.16.최종방문).

505) The White House, "Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities", Apr. 1, 2015, <https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m> (2017.1.16.최종방문).

506) Mark C. Toner, "Department of State Actions in Response to Russian Harassment", Press Statement, Dec. 29, 2016. <https://www.state.gov/r/pa/prs/ps/2016/12/266145.htm> (2017.1.10.최종방문).

507) The Washington Post, Jun. 23, 2017, "Obama's secret struggle to punish Russia for Putin's election assult", <https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.48639dccadb9> (2017.9.21.최종방문).

508) Meduza, Jul. 20, 2017, "Moscow's cyber-defense How the Russian Government plans to protect the country from coming cyberwar", <https://meduza.io/en/feature/2017/07/19/moscow-s-cyber-defense>

한편 공화당 하원의원 Tom Graves는 2017년 3월 Active Cyber Defense Certainty Act(ACDC)를 제안하였다.[509] 논의 초안(Discussion Draft) 상태인 이 법안이 통과되면 허가 받지 않은 접근을 금지하는 Computer Fraud and Abuse Act(CFAA)에 대한 개정이 불가피하게 된다.[510] 현재 CFAA는 타인의 컴퓨터에 대한 허가받지 않은 접근을 컴퓨터 범죄로 규정하고 있다.[511] 그러나 ACDC는 해킹 피해자가 공격에 대한 방어조치로서 공격자의 컴퓨터에 허가 없이 접근한 경우에는 CFAA 위반에 해당하지 않는다는 내용을 담고 있다.[512] 법안에서 언급하고 있는 적극적 방어조치로는 법 집행기관과의 공유를 목적으로 공격자[513]의 컴퓨터에 허가 없이 접근하여 범죄행위를 추적하는 것, 피해자의 네트워크에 계속되는 공격 행위를 방해하는 것을 예시로 들고 있다.[514] 다음 항에서는 제한되는 행위에 대해서도 규정하고 있는데, 공격자의 컴퓨터가 아닌 제3자의 컴퓨터에 저장된 정보의 파괴, 제3자에 대한 물리적 침해 등이 그것이다.[515] 이 법안은 국가기관이 아닌 민간에게 적극적 사이버방어조치를 가능하게 하고, 공격자의 네트워크에 한해서는 역해킹도 허용된다는 점에서 상당히

(2017.9.21.최종방문).

509) The Atlantic, Jul. 14, 2017, “When Companies Get Hacked, Should They Be Allowed to Hack Back?”, <https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/> (2017.9.21.최종방문).

510) Lawfare, Mar. 7, 2017, “Legislative Hackback: Notes on the Active Cyber Defense Certainty Act discussion draft”, <https://www.lawfareblog.com/legislative-hackback-notes-active-cyber-defense-certainty-act-discussion-draft> (2017.9.21.최종방문).

511) CFAA Section 1030 of title 18.

512) Tom Graves, “Discussion Draft”, Mar. 3, 2017, <https://tomgraves.house.gov/uploadedfiles/discussion_draft_ac-dc_act.pdf> (2017.9.21.최종방문).

513) *Ibid.,* 초안에서는 공격자를 피해자의 컴퓨터에 허가 없이 지속적으로 침입한 공격 소스의 당사자인 개인 또는 단체를 의미하는 것으로 정의하고 있다.

514) *Ibid.*

515) *Ibid.*

파격적인 내용을 담고 있다.

미국정부가 이러한 적극적 방어조치를 실제로 감행하여 공격자로 추정되는 네트워크에 타격을 입힌 사례도 있다. 2014년 12월 21과 22일 10시간 동안 북한의 인터넷이 먹통이 되는 사건이 있었는데, 미국토안보위원회 의장인 Michael McCaul 하원의원은 이것이 소니픽쳐스 해킹에 대한 보복의 일환으로 취해진 조치라고 밝힌 바 있다.[516] 미국은 이밖에도 대통령 행정명령을 통해 소니 해킹에 대한 보복조치의 일환으로 북한 정부기관과 고위관료들에 대한 경제 제재를 부과 하였다.[517]

이상 사이버공격에 대한 최근 미국의 대응을 보면 경제제재 및 외교적 조치, 보복 공격, 사이버무기의 활용으로 공세적인 입장을 취하고 있음을 확인할 수 있다. 미국의 대응은 특히 민간에까지 적극적 방어를 허용하려는 움직임을 보일 만큼 적극적이고 공격적이다. 이러한 미국의 대응이 국제법에 부합하는 지에 대해서는 분석이 필요하겠지만 적극적 방어조치가 현실화 되고 있다는 것은 부인할 수 없는 사실이다.

2. 영국

영국은 사이버안보를 위해 공격적인 사이버 능력을 개발하고 있다고 공개적으로 밝힌 첫 번째 국가다.[518] 2013년 9월 당시 영국의 국방장관 Philip Hammond는 사이버안보 개혁에 대해 발표하는 성명에서 국방부가

---

516) Dallas News, Mar. 17, 2015, “North Korea Web outage was retaliation for Sony hack, lawmaker says”, <https://www.dallasnews.com/business/technology/2015/03/17/north-korea-web-outage-was-retaliation-for-sony-hack-lawmaker-says> (2017.9.21.최종방문).

517) The Guardian, Jan. 2, 2015, “Obama imposes new sanctions against North Korea in response to Sony hack”, <https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview> (2017.9.21.최종방문).

518) Kubo Macˇak, *supra* note 335, p. 408.

사이버방어의 최전선에서 영국의 안보를 위해 일할 수백 명 규모의 컴퓨터 전문가들을 사이버 예비군으로 고용할 계획이라고 밝혔다. Philip Hammond 장관은 이러한 계획의 주목적은 사이버공간상에서 대응공격, 필요한 경우에는 공격의 근원지를 타격할 수 있는 능력을 갖추기 위함이라고 설명하였다.[519] 그는 송전선이나 항공관제시스템을 무력화 시키는 사이버공격에 대응할 능력을 갖추지 못한다면 이는 불가피하게 군사적 대응으로 이어지게 된다고 하면서 적극적 방어 전략의 중요성을 역설하였다.[520] 또한 이러한 최첨단의 역량을 갖추기 위해 사이버·정보기관·정찰 분야에 막대한 투자를 하고 있다고 하였다.[521]

영국은 2011년 사이버공간에 대한 런던회의를 개최할 정도로 사이버안보 분야에서 리더임을 자처하고 있는 국가다. 2010년 영국의 국가안보 보고서에서는 사이버공격을 테러공격과 함께 첫 번째 우선순위(Tier I)에 두고 있을 만큼 이에 대한 관심도 지대하다.[522] 그러나 위 성명을 발표하기 전 영국이 주창한 사이버안보 정책 기조는 공격적이기 보다는 사이버공격을 현실적인 위협으로 인식하고, 이를 방어하기 위한 프로그램 개발에 힘써야 한다는 등의 일반적 성향을 띠고 있었다.[523]

이는 2011년 영국정부가 발간한 사이버안보 전략에서도 확인할 수 있

519) UK, Sep. 29, 2013, “New cyber reserve unit created”, <https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit> (2017.1.11.최종방문).

520) The Guardian, Nov. 1, 2016, “Philip Hammond to spend extra £1.9bn fighting cyber-attacks”, <https://www.theguardian.com/technology/2016/nov/01/philp-hammond-to-spend-extra-19bn-fighting-cyber-attacks?CMP=oth_b-aplnews_d-2> (2017.9.25.최종방문).

521) UK, “New cyber reserve unit created”, Sep. 29, 2013, <https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit> (2017.1.11.최종방문).

522) UK, “A Strong Britain in an Age of Uncertainty: The National Security Strategy”, HM Government (2011), p. 27.

523) *Ibid.*, p. 34.

다. 보고서는 주요 목표에서 사이버공격에 대한 적극적 대응을 강조하기 보다는 사이버공간을 자유롭고 안전하게 사용하기 위한 방어에 초점을 맞추고 있다. 보고서에서 영국이 계획하고 있는 대응전략은 사이버위협을 '감지'하고 이러한 사이버위협으로부터 네트워크를 '보호' 및 '방어'하는 것으로 나타나 있다. 대응과 관련하여 가장 많이 사용된 용어는 'detection', 'defend', 'prevent' 이며, 앞서 언급한 2013년 국방장관의 성명에서 사용된 counter attack이나 strike 등의 용어는 찾아볼 수 없다.[524]

2011년 사이버 전략과 2013년 Philip Hammond 장관의 성명을 비교할 때, 2011년 전략이 발간 된지 불과 2년 만에 전략 기조가 사이버 대응공격으로 바뀐 것은 사이버위협에 대한 영국의 인식 변화를 짐작케 한다. 2016년 영국 정부가 발간한 '2016년부터 2021년까지의 국가 사이버안보 전략'에서도 이러한 인식변화가 계속 이어지고 있음을 확인할 수 있다. 우선 영국은 2015년 우크라이나 송전망에 대한 사이버공격, 2016년 방글라데시 은행시스템에 대한 사이버공격 등의 사례연구와 함께 국가 및 국가지원의 사이버공격과 사이버 간첩행위를 주요 위협으로 설명하고 있다.[525] 무엇보다 대응전략을 '적극적 사이버방어'로 명명한 부분에서 이를 명확히 확인할 수 있다.

구체적 전략으로는 공격의 거점을 찾아내고, 사이버공격을 교란·거부하며 공격적인 사이버역량을 사용하여 군사작전을 시행하는 것을 그 내용으로 하고 있다.[526] 이는 네트워크상의 공격거점을 파악하여, 밀려드는 트래픽을 밀어내는 역디도스 공격, 진행되는 공격이 다른 서버로 우회하도록 하는 방향변경, 공격의 거점으로 사용되고 있는 C&C 서버를 무력화하는 역타격 등의 적극적 사이버방어 기법을 그대로 설명하고 있는 것이다. 이에 대해 영국 정보통신본부(Government Communications

524) UK, "The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world" (2011), pp. 8, 26-33.
525) UK, *supra* note 77, pp. 20-21.
526) *Ibid.,* pp. 33, 49-51.

Headquarters, GCHQ) 산하의 국립사이버안보센터(National Cyber Security Center)는 DNS[527] 필터링, 봇넷 테이크다운, DMARC[528] 등과 같은 기법을 구체적인 예로 설명하고 있다.[529]

영국이 사이버공격에 대한 대응전략을 적극적 방어로 전환했다는 사실은 최근의 입법을 통해 가장 확실하게 알 수 있다. 2015년 11월 당시 내무장관이었던 Theresa May는 영국의 안보를 위해 'Investigatory Powers Bill'이라는 법안을 발의하였고, 이 법안은 의회의 통과를 거쳐 2016년 11월 29일 모든 절차를 마치고 같은 해 12월 30일에 발효하였다.[530] 이 법안은 인터넷 서비스 업체와 통신업체로 하여금 이용자의 사이

527) DNS(Domain Name System)는 TCP/IP 애플리케이션에서, www._____.com과 같은 컴퓨터의 도메인 네임을 '164.124.101.2'와 같은 IP 주소로 변환하고 라우팅 정보를 제공하는 분산형 데이터베이스 시스템이다. 한국정보통신기술협회 정보통신용어사전, <http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=041788-2> (2017.10.30.최종방문).

528) Domain-based Message Authentication, Reporting and Conformance는 도메인 기반 이메일 인증방식으로 SPF라는 메일 서버 등록제와 DKIM이라는 키 인증 서명 기술을 활용하여 발신인이 진짜인지 가짜인지를 구분해내서 이메일 스푸핑을 찾아내는 기법.

529) National Cyber Security Center, "Active Cyber Defence - tackling cyber attacks on the UK", Nov. 1, 2016, <https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk> (2017.9.22.최종방문); National Cyber Security Center, "Cyber UK in Practice Track 3: Proactive Defence", Mar. 13, 2017, <https://www.ncsc.gov.uk/blog-post/cyberuk-practice-track-3-proactive-defence> (2017.9.22.최종방문).

530) UK Parliament, <https://services.parliament.uk/bills/2015-16/investigatorypowers.html> (2018.1.22.최종방문); Independent, Dec. 31, 2016, "Investigatory Powers Act Goes Into Force, Putting UK Citizens Under Intense New Spying Regime", <https://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-act-bill-snoopers-charter-spying-law-powers-theresa-may-a7503616.html> (2018.1.22.최종방문).

트 방문 기록 등을 12개월 동안 보관하도록 하고, 정부부처, 보안당국, 경찰 등이 해당 정보에 접근할 수 있도록 하는 것을 주 내용으로 하고 있어 국민의 프라이버시 침해 논란으로 거센 반발을 불러일으켰다.[531]

그러나 이 법의 세부 규정을 보면 사이버공격에의 대응과 관련하여 역해킹을 허용하는 조항을 발견할 수 있다. 법안 제5부에 따르면 보안당국은 컴퓨터, 네트워크, 모바일 장치, 서버 등을 해킹할 수 있다고 규정되어 있다.[532] 또한 실행 초안(a draft code of conduct)에서는 이 때, 장치나 네트워크에 대한 통제권을 획득하기 위해 소프트웨어의 취약점을 이용할 수 있다고 설명하고 있다.[533] 특히 법안은 국외에서 발생했더라도 악의적인 활동이라고 판단되면 보안당국에 의한 해킹이 허용된다고 하고 있으며, 제6부 제3장에서는 Bulk Equipment Interference라고 하여 광범위한 해킹을 허용하는 내용을 담고 있다.[534] 실행 초안에서는 테러활동이 의심되는 경우를 구체적인 예로 제시하고 있다.[535] 이와 같이 영국은 미국처럼 민간에까지 적극적인 방어를 허용하는 정도까지는 아니지만 정부차원에서 적극적으로 사이버공격에 대응하는 전략을 마련하고, 실행할 준비를 마쳤음을 확인할 수 있다.

---

531) 법안이 발의된 2015년부터 2017년 현재까지 법안폐지를 위한 온라인 청원은 21만건을 넘어선 상태이다. UK Government and Parliament Petitions: <https://petition.parliament.uk/archived/petitions/173199> (2017.9.25. 최종방문); 2016년 법안이 통과된 직후 유럽사법재판소(European Court of Justice, ECJ)도 정부가 이메일 및 전자통신 기록을 일반적이고 무차별한 보유하도록 한 해당법안이 EU법 위반이라고 판결 하였다. Court of Justice of the European Union Press Release No. 145/16 (2016).

532) Investigatory Power Bill Part 5 Equipment Interference 제100조-제108조.

533) UK Home Office, "Equipment Interference Draft Code of Practice", (2016), p. 8.

534) Investigatory Power Bill Part 6, Chapter 1, Chapter 3 Bulk Equipment Interference 제137조, 제177조-제179조.

535) UK Home Office, "Security and Intelligence Agencies' retention and use of bulk personal datasets", (2016) p. 45.

3. 중국

중국은 지금까지 사이버안보전략을 발간하지 않은 몇 안 되는 국가들 중 하나이다. 그런 중국 정부가 2016년 12월 27일 국가 사이버안보 전략을 발간했다고 밝혔다. 약 15장 분량의 해당 전략 보고서는 시진핑 국가주석과 리커장 총리가 각각 조장과 부조장을 맡고 있는 중앙인터넷안전·정보화영도소조의 승인을 받은 것으로 알려졌다.[536] 인터넷정보판공실 대변인에 따르면 해당 전략은 사이버공간에서 국가의 주권·안보·발전이익을 실제적으로 보호하는 강령성 문건이라고 하였다. 보고서는 1)사이버 주권 수호, 2)국가안보 수호, 3)핵심 정보 기반시설 보호, 4)사이버 문화 건설 5) 사이버 테러와 사이버 범죄 단속 6)사이버 통제, 7)사이버 보안 기초 확립, 8)사이버방어 능력 향상 9)국제협력 강화의 9개 목록을 도전과제로 명시하고 있다.

주요내용은 우선 사이버위협을 인식하는 항목에서 인터넷 보급을 가장 처음에 언급하고 있는데, 이는 여타 국가의 사이버위협 인식에서는 볼 수 없던 특이한 점이다. 그 뒤로는 사이버공격의 위험성, 사이버 테러, 사이

---

536) 사이버안보전략 중국어 전문은:
<http://www.cac.gov.cn/2016-12/27/m_1120195926.htm>에서 확인가능하며,
다음 블로그에서 중국이 발간한 사이버안보전략의 중국어 요약본과 영문 번역본을 확인할 수 있다: China Copy Right and Media, Dec. 27, 2016, “National Cyberspace Security Strategy”, <https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/> (2017.1.12.최종방문);
CCTV.com, Dec. 28, 2016, “China releases cyberspace security strategy”, <http://english.cctv.com/2016/12/28/VIDEpR0U7vk86TR140BZVklk161228.shtml> (2017.1.12.최종방문);
보안뉴스, 2017년 1월 3일, “中 ‘국가 사이버 보안 전략’ 발표...배경과 주요 내용”, <http://www.boannews.com/media/view.asp?idx=52930&kind=4> (2017.1.12.최종방문).

버 범죄 등을 차례로 위협으로 언급하고 있다. 이에 대한 대응전략으로는 사이버안보를 위한 국내법을 완비하여 기술과 장비에 대한 통제를 실시하고, 중국 영토 내의 온라인 활동을 관리하며 유해정보가 인터넷상에 확산되는 것을 방어·억지하고 이에 연루된 행위자를 법에 따라 처벌하는 것을 들고 있다.

또한 데이터 보호를 위해 위험을 감지하고 조기경보시스템을 마련하여 사이버위협에 대처하며 사이버 보안 심사제도를 실시할 것을 밝히고 있다. 이 외에도 사이버공격 방어 능력을 강화하고, 보안 기술을 개발하며 국제 협력을 강화한다는 내용이 담겨 있으나 이에 대해서는 구체적인 방안은 제시되어 있지 않고 일반적인 서술에 그치고 있다.[537] 다만 사이버공간의 평화적인 사용을 언급하면서, 모든 국가들은 사이버공간 내에서도 UN 헌장에 규정된 무력사용금지원칙을 준수해야 하며, 국제 평화와 안전을 해하는 정보기술의 사용을 금해야 한다는 것을 강조하고 있다.[538]

중국의 사이버위협에 대한 대응전략을 한마디로 요약하면 국가주권의 사이버공간으로의 확장과 중국 국내법에 따른 사이버공간 통제라고 할 수 있다. 전략보고서에서 중국은 정보의 자유로운 흐름과 인터넷 상의 원활한 소통을 목표로 이야기 하고 있으나 핵심은 이 목표를 달성하기 위해 정부의 통제가 필요하다는 것이다. 이는 2016년 11월 7일 통과된 사이버 보안

---

537) *Ibid.*;
China Daily, Dec. 27, 2016, "China announces cyber security strategy", <http://www.chinadaily.com.cn/china/2016-12/27/content_27788200.htm> (2017.1.12.최종방문);
Global Times, Dec. 27, 2016, "China announces cybersecurity strategy", <http://www.globaltimes.cn/content/1026015.shtml> (2017.1.12.최종방문).

538) Rogier Creemers, Dec. 27, 2016, "Chinese National Cyberspace Security Strategy(English Translation)", <https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/> (2017.9.25.최종방문).

법(網絡安全法)[539]의 내용과 일맥상통하는 것이다.

2017년 6월 1일부터 시행된 이 법의 내용은 다음과 같다. 먼저 사이버 범죄나 국가안보에 영향을 미치는 사이버공격이 일어났을 때, 인터넷 서비스 제공자는 조사에 협조해야 하며, 컴퓨터 장비에 대한 시험 및 인증 절차에 반드시 응해야 한다. 중국 내의 기업들도 마찬가지로 의혹이 있을 경우에는 중국정부에 자신의 기업 데이터에 대한 완전한 접근을 허용해야 한다.[540] 여기에서 말하는 인증절차는 보안기술 기업들이 조사를 이유로 기술에 사용된 원시코드(source code), 암호정보 또는 기타 중요한 지적재산을 중국정부로부터 요구받을 수 있음을 의미한다. 또한 중국 내의 모든 기업은 데이터를 중국 내의 서버에만 저장해야 하며, 여기에는 '안전'하다고 검증된 기술만을 사용해야 한다.[541]

법 적용의 대상이 중국 내의 모든 기업이기 때문에 중국에 진출한 외국기업의 경우에도 이를 준수해야 한다. 한편 기업들이 중국 국민들에 관해 획득한 정보 및 데이터도 모두 국내 서버에 저장해야 하며 정부의 허가 없이는 외국으로 전송할 수 없다.[542] 이는 앞에서 살펴본 중국의 사이버안보 전략의 내용이 구체화 되어있는 것이라고 볼 수 있다. 시기상 법안의 통과가 먼저였으나 이 두 가지 모두 시진핑 국가주석이 주창하는 "사이버 국가 주권" 기조를 잘 나타내 주고 있다.

이를 종합해보면 중국의 사이버위협에 대한 대응은 철저한 사이버공간 통제라고 할 수 있다. 사이버 보안법의 초안이 발표되자 40개가 넘는 미국, 유럽, 일본과 같은 국가의 기업들이 리커장 총리에게 동 법안이 외국

539) 中华人民共和国网络安全法 원문은: <http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm> (2018.1.25.최종방문);
다음 사이트에서 사이버보안법의 영문 번역을 확인할 수 있다; <http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en> (2018.1.25.최종방문).

540) 제26조, 제28조, 제35조.

541) 제23조.

542) 제37조.

기업의 투자유치를 방해하고, 중국 자국의 발전에도 해가 될 것이라는 내용의 탄원서를 낸 바 있다.[543]

중국 정부가 사이버안보에 대해 이와 같이 거센 반발을 일으키는 공격적인 정책을 추진하기 시작한 데에는 2013년 스노든(Edward Snowden)의 중국에 대한 미 정부의 사이버 간첩행위 폭로가 계기가 됐다고 알려져 있다.[544] 중국은 이제 막 자국의 사이버안보 전략을 대외적으로 공개하기 시작했고, 법안과 정책 또한 시행을 이제 막 시작했기 때문에 향후 이러한 공격적인 행보는 계속될 것으로 보인다.[545]

4. 러시아

러시아의 사이버안보 전략과 실행은 자국의 인터넷공간에 대한 주권행사와 방어에 초점을 둔 중국의 대응과는 달리 다소 복잡한 양상을 띠고 있다. 앞서 러시아와 중국의 사이버공격의 규율에 대한 입장은 사이버공간에 대한 국가주권 강화와 사이버무기 규제, 사이버공간의 군사화 방지임을 살펴본 바 있다. 중국이 국제사회에서의 주장과 일관된 정책을 펴고 있다

---

543) Financial Times, Aug. 11, 2016, “Chinese laws prompt global business backlash”, <https://www.ft.com/content/8103baa0-5f9c-11e6-ae3f-77baadeb1c93> (2017.1.17.최종방문).

544) Bloomberg, Nov. 7, 2016, “China Adopts Cybersecurity Law Despite Foreign Opposition”, <https://www.bloomberg.com/news/articles/2016-11-07/china-passes-cybersecurity-law-despite-strong-foreign-opposition> (2018.1.25.최종방문).

545) 중국의 관영통신 및 언론보도에 따르면 중국공산당중앙인터넷안전·정보화영도소조는 사이버 보안법 시행을 위해 개인정보 수집 규범 표준을 만들고 있는 것으로 전해졌다; 보안뉴스, 2016년 12월 5일, “中 “개인정보 수집 규범 표준 제정”...사이버 보안법 후속조치“, <http://www.boannews.com/media/view.asp?idx=52603&kind=4> (2017.1.12.최종방문).

면 러시아는 기본적으로는 사이버공간에 대한 국가의 관리를 확대하고, 타국의 영향력을 차단하기 위해 정보통제를 강화하면서 타국 발 사이버공격에 대해서는 적극적인 방어태세를 갖추는 정책을 동시에 시행하고 있는 것이다.

우선 모니터링을 위한 소프트웨어의 개발에 대한 투자가 집중적으로 이루어지고 있는 것[546]과 지역적 차원의 인터넷 관리 기술 개발 및 국내 이메일 시스템 개발, Windows[547]에 대한 의존도를 줄이기 위한 노력 등을 통해 인터넷주권을 강화하려는 러시아 정부의 노력을 짐작할 수 있다.[548] 2015년 6월 29일 푸틴 대통령은 정부가 사용하는 제품에 있어 외국 소프트웨어 및 데이터베이스의 조달을 제한하는 법안에 서명하였고, 이는 2016년 1월 1일에 발효하였다.[549] 이에 따라 Unified Register의 리스트에 등록된 러시아산 컴퓨터 프로그램 및 데이터 베이스 제품만이 정부에 조달될 수 있게 된다.[550]

---

546) 신범식, "러시아의 사이버안보의 전략과 외교", 서울대학교 국제문제 연구소 워킹페이퍼 (2017), p. 7; Bloomberg Tecnology, Sept. 27, 2016, "Moscow Drops Microsoft on Putin's Call for Self-Sufficiency", <https://www.bloomberg.com/news/articles/2016-09-27/moscow-drops-microsoft-outlook-as-putin-urges-self-sufficiency> (2017.9.27.최종방문).

547) Microsoft 사가 제공하는 PC 운영체제

548) 러시아 기업 New Cloud Technology사는 Windows를 대체할 My Office를 개발하여 보급하고 있다. CNNtech, Sept. 28, 2016, "Moscow's government ditches Microsoft for Russian software", <http://money.cnn.com/2016/09/28/technology/moscow-russia-microsoft-software-email/index.html> (2017.9.27.최종방문).

549) Ernst & Young, "Tax Alert: Restrictions on Foreign Software for State Procurements", (2015), p. 1.

550) Federal Law No. 188-FZ "Concerning the Introduction of Amendments to the Federal Law "Concerning Information, Information Technologies and Information Protection, Article 14 of the Federal Law "Concerning the Contract System for Procurements of Goods, Work and Services to Meet State and Municipal Needs".

푸틴 대통령은 최근에도 안보를 이유로 러시아의 IT 기업들에게 국내에서 개발한 소프트웨어를 사용할 것을 주문하였다. 푸틴 대통령은 "러시아 밖의 누군가가 누르는 버튼에 의해 국가 전체가 마비될 수 있기 때문에" 국내개발 소프트웨어를 사용하지 않는 IT 기업의 제품을 러시아 정부에서 사용할 수 없다고 하면서 사실상 권고가 아닌 의무를 부과하는 발언을 하였다.[551] 특이한 점은 인터넷주권 강화 전략에서도 중국과 차이를 보인다는 점이다. 중국은 트위터나 페이스북을 차단하는 등 적극적인 검열 정책을 실시하고 있으나, 러시아는 공식적으로 이를 차단하는 등의 정책 보다는 감시에 집중하고 있다는 점이다.[552] 여기까지는 국가가 중심이 되는 인터넷 거버넌스체제의 성립을 추구하는 국제사회에서의 주장과 대내적 정책이 일치한다고 볼 수 있다.

문제는 나머지 국내정책 및 실행이 국제사회에서의 주장과는 정 반대의 모습으로 나타나고 있다는 점이다. 즉, 서방국가의 사이버공격에 대한 자위권 행사, 적극적 사이버방어와 같은 대응조치에는 반대하면서 정책상 사이버 군대의 창설을 통해서 사이버공간의 군사화를 추진하고, 대응타격 능력을 갖추며, 사이버무기의 개발에 적극적으로 투자하고 있는 것이다. 러시아는 미국의 사이버 부대 창설을 놓고 인터넷을 군사화 하는 조치라고 비판하였으나 결국 자신도 2014년 5월 사이버전 전담부대의 창설을 결정한 것으로 알려졌다.[553] 러시아의 세르게이 쇼이구 국방장관은 2013년 사

551) Russia Feed, Sept. 8, 2017, "Vladimir Putin urges Russian IT companies to switch to DOMESTIC software", <http://russiafeed.com/vladimir-putin-urges-russian-it-companies-to-switch-to-domestic-software/> (2017.9.27.최종방문).

552) 신범식, *supra* note 546, pp. 6, 15.

553) 러시아는 공식적으로는 사이버 부대의 존재에 대해 부인하고 있으나, 약 1천명 규모의 사이버 부대를 운용하고 있는 것으로 알려져 있다. 이는 당국자들의 모호한 답변을 통해서도 추측할 수 있다. 연합뉴스, 2017년 1월 10일, "러시아 1천명 규모 사이버 부대 운용…美는 9천명", <http://www.yonhapnews.co.kr/bulletin/2017/01/10/0200000000AKR20170110199000080.HTML> (2017.9.26.최종방문); 신범식, *supra* note 546, p. 11.

이버안보의 중요성을 강조하면서 사이버 사령부가 방어 뿐 아니라 필요한 경우 대응타격능력까지 갖춰야 한다고 밝힌 바 있다.[554] 또한 2015년 2월 쇼이구 국방장관은 “2020 러시아군 정보통신기술 발전 구상”을 발표하였는데, 여기에는 암호학, 프로그래밍, 수학, 통신 및 전자전 분야의 전문가들이 사이버 부대에 참여하게 된다는 내용이 포함되어 있다.[555] 이어서 같은 해 3월에는 로고진 러시아 부총리가 모스크바대학에서 열린 사이버 회의를 통해 향후 고도의 기술이 집약된 스마트 무기를 생산할 것과 러시아의 사이버안보체제가 이 무기에 기초하여 구축될 것이라고 밝혔다.[556]

러시아는 또한 2015년 말 크림반도에 독립적인 사이버 부대를 창설하겠다고 발표한 바 있다. 이 사이버 부대의 역할에는 잠재적 적국의 군 체계 교란을 위해 적국의 정보네트워크를 공격하는 것이 포함된 것으로 보도되었다.[557] 이를 종합하면 러시아의 사이버 사령부는 단지 수동적 방어만이 아닌 대응타격과 같은 적극적 사이버방어를 담당하는 기관임을 알 수 있다.[558] 결정적으로 러시아는 2016년 공격적 사이버역량을 갖추기 위해 핵무기에 버금가는 사이버 억지력을 개발할 계획을 발표하였다.[559] 러시아는 이를 위해 연간 약 2억 5천만 달러를 투자할 것으로 알려졌으며, 여기에

---

554) 신범식, *supra* note 546, p. 11.
555) JTBC, 2015년 6월 26일, “RUSSIA 포커스-세계는 사이버 전쟁 중...러, 스마트 무기기반 준비태세 강화”,<http://news.jtbc.joins.com/article/ArticlePrint.aspx?news_id=NB10940956> (2017.9.26.최종방문).
556) *Ibid.*
557) *Ibid.*
558) Reuters, Feb. 22, 2017, “Russia sets up information warfare units - defence minister”, <http://www.reuters.com/article/russia-military-propaganda/russia-sets-up-information-warfare-units-defence-minister-idUSL8N1G753J> (2017.9.26.최종방문).
559) SC Media, Feb. 4, 2016, “Russia to spend $250m strengthening cyber-offensive capabilities”, <https://www.scmagazineuk.com/russia-to-spend-250m-strengthening-cyber-offensive-capabilities/article/531418/> (2017.9.26.최종방문).

는 적국 군부대의 C&C 서버 및 은행·송전망·공항 등 적국의 주요기반시설을 파괴할 수 있는 악성프로그램의 개발이 포함되어 있는 것으로 보도되었다.[560] 즉, 러시아는 UN GGE와 같은 국제사회에서 기준의 자의적 판단에 대한 우려를 들어 사이버무기를 사용한 대응조치 및 사이버공격에 대한 자위권 원용에 적극적으로 반대를 표명한 자신의 입장과 정 반대의 국내정책을 시행하고 있는 것이다. 이러한 모순된 행위는 앞서 살펴본 2007년 에스토니아 DDoS 공격, 2014년 우크라이나 중앙선관위 컴퓨터 공격, 2015년 우크라이나 전선망에 대한 사이버공격, 2016년 민주당 이메일 해킹사건까지 러시아가 배후로 추정되는 실제 사건을 통해서도 확인할 수 있다.

이와 같은 러시아의 대외적 주장과 대내적 정책 및 실행의 불일치는 언뜻 보면 논리적이지 않다고 볼 수 있다. 그러나 사이버기술면에서도 앞서 있는 미국을 견제하려는 행위로 본다면 러시아 행위의 맥락은 하나다. 즉, 우선은 국내적 통제를 통해 밀려드는 서방의 영향으로부터 자국의 체제를 지키고, 이를 국제법에도 투영하여 국가가 중심이 되는 인터넷 거버넌스를 구축한다. 또한 무기 군축 조약 및 사이버역량을 사용한 대응조치에 반대하는 것을 통해 서방국의 선진기술을 견제하고, 사이버활동에 대한 자위권 차원의 대응을 반대하면서 미국의 군사적 우위도 견제하려는 것이다. 주목할 것은 러시아의 경우 해커조직이나 범죄조직과 같은 대리자를 통해 사이버공격을 수행한다는 것이다. 사이버공격의 경우 귀속을 밝히기 어렵다는 것에 더해 대리자를 활용함으로써 plausible denibility를 더욱 효과적으로 사용하고 있는 것이다.

푸틴 대통령은 2016년 힐러리 클린턴 이메일 해킹 사건과 관련해 자국의 사이버 조직이 애국적 차원에서 자발적으로 그러한 공격을 감행했을 수 있다며, 이에 대해 간접적으로 인정한 바 있다.[561] 즉, 표면적으로는

560) *Ibid.*

561) The New York Times, Jun. 1, 2017, “Maybe Private Russian Hackers Meddled in Election, Putin Says”, <

타국의 사이버 행위에 의한 내정간섭 및 파괴적인 사이버무기사용에 반대하고, 국가들의 이러한 행위에 대한 규제를 주장하면서 자국은 대리자 뒤에 숨어 타국에 대한 주권침해 및 국내문제간섭행위를 자행하고 있는 것으로 보인다. 대리자를 통해 전략적 이익은 취하나 위험은 공유하지 않는 이 같은 방식[562]은 '국가'를 중심으로 한 인터넷 거버넌스 체제의 창설을 주창하는 러시아의 주장과 맞물려 중요한 시사점을 주는 대목이라고 할 수 있다. 러시아는 비국가행위자의 초국가적인 사이버공격행위를 규제할 수 없다는 현 국제법체제의 한계와 행위 귀속의 추적이 용이하지 않은 사이버공간의 특성을 법적 모호성의 범위 안에서 국내적 및 국제적으로 잘 활용하고 있다고 볼 수 있다.

5. 기타 국가들

이밖에도 주요 국가들의 사이버안보 정책 및 법령을 간단히 살펴보면 상당수의 국가들이 중국을 제외한 앞의 세 국가와 마찬가지로 적극적 사이버방어전략을 선택하고 있음을 알 수 있다. 여기에는 영국을 제외한 유럽연합 국가들이 다수 포함된다. 먼저 프랑스는 2013년 국방백서에서 사이버공격을 국가안보에 있어 세 번째로 중요한 위협으로 상정하고 공격적인 사이버역량 개발 계획을 밝혔다.[563]

사이버안보는 주로 2009년에 설치된 French Network and Information Security Agency (ANSSI)가 위험 감지 및 공격에 대한 대응을 담당하고 있으며, 프랑스 군 내에도 사이버전을 담당하는 부대가 설치되어 있다.[564] 국방백서에서 프랑스는 사이버공격에 대한 대응으로 일

---

https://www.nytimes.com/2017/06/01/world/europe/vladimir-putin-donald-trump-hacking.html?mcubz=3> (2017.9.26.최종방문).

562) 신범식, *supra* note 546, p. 13.

563) French Republic, "French White Paper on Defence and National Security", (2013), p. 71.

564) Carmen Cristina Cirlig, "Cyber Defence in the EU-Preparing for

차적으로는 외교적 채널을 중시하고, 경찰 등 집행기관의 수사를 중요시한다고 하였다.[565] 그러나 군차원의 공세적 대응도 배제하지 않는다고 하면서 공격에 비례한 사이버역량의 사용을 통해 대응하게 될 것이라고 밝히고 있다.[566]

이어 2016년에 당시 프랑스 국방장관은 공격적인 사이버역량 사용을 더 이상 예외적인 경우로 두지 않겠다고 하였고 하면서 새로운 사이버 대응원칙의 핵심 개념 두 가지-riposte(retaliation)과 neutralization-를 공표하였다.[567] riposte는 국민의 생명과 연결된 주요국가기반시설에 대한 공격이 임박했을 때, 해당 공격을 타격하는 것을 의미하고, neutralization는 공공의 안전을 위해 사이버공격을 늦추는 기술의 사용을 포함하는 것이다.[568] 프랑스는 영국과 함께 사이버 대응전략으로 적극적 방어를 선택하고 있음을 대외적으로 어필하는 대표적인 유럽국가이다.

독일은 2011년 National Cyber Security Council 과 National Cyber Response Centre를 창설하여 운영해 왔으며, 군내에 설치된 Strategic Reconnaissance Unit은 공격적인 사이버 대응에 특화된 것으로 알려져 왔다.[569] 독일은 비교적 최근까지도 공개적으로 적극적 사이버방어전략에 대한 입장을 밝히지 않았는데, 2016년을 기점으로 확실하게 태세를 적극적 방어로 선회한 것으로 보인다. 이는 독일에 대한 러시아의 해킹사례가 빈번하고, 2017년 독일 총선에 러시아가 사이버공격을 통해 개입을 시도할 것에 대비하기 위한 것이 주된 이유로 보인다.[570] 이같은 방향 선회는

---

cyber warfare?", European Parliamentary Research Service (2014), p. 7.

565) French Republic, *supra* note 563, p. 101.

566) *Ibid.*

567) Philippe Baumard, *Cybersecurity in France* (Springer, 2017), pp. 36, 37.

568) *Ibid.*, p. 38.

569) Carmen Cristina Cirlig, *supra* note 564, p. 7.

570) Independent, May 4, 2017, "German spy chief warns Russia cyber attacks aiming to influence elections", <http://www.independent.co.uk/news/world/europe/germany-spy-chief

2016년 4월 독일의 국방장관 Ursula von der Leyen이 Bundeswehr(독일 연방군) 안에 새로운 사이버 사령부를 설치할 계획을 발표한 것을 통해서도 알 수 있다.[571] 동 계획은 타국 영역에도 파괴적인 사이버공격을 함으로 인해 사이버 전쟁으로 이어질 수 있다는 비판에 부딪쳤지만 국방장관은 2017년 4월까지 사령부 신설을 완료할 것임을 재차 강조하였다.[572] 2017년 이 계획은 실행되어 4월 5일 사이버 사령부가 새로이 창설되었고, 7월까지 13,500명 규모를 갖추게 되었으며, 신설된 사령부의 역할은 공격적 사이버방어 작전 수행인 것으로 보도되었다.[573]

이 밖에 EU 국가들 중 적극적 사이버방어 전략을 선택하고 있는 국가로는 덴마크와 네덜란드가 있다. 덴마크는 Danish Defence Agreement 2013-2017을 통해 국방부 산하에 설치된 사이버안보센터가 사이버공간 내에서 공격적인 작전을 실행할 수 있도록 역량을 강화하기 위해 연간 2천 5백만 크로네를 투입하기로 하였다.[574] 네덜란드는 2012년 사이버방어 전략에서 공격적인 사이버역량의 개발을 여섯 개의 최우선 과제 중 하나로 상정하였다.[575] 이후 2014년에 합동 사이버방어 사령부(Defence Cyber Command)를 군 내에 설치하여 사이버역량 개발의 역할을 담당케 하고 있다.[576] 해당 전략에서 네덜란드는 사이버공격을 방지하거나 진행되

-russian-cyber-attacks-russia-elections-influence-angela-merkel-putin-hans-georg-a7718006.html> (2017.9.29.최종방문).

571) ORF, Oct. 20, 2016, "Bundeswehr: Cyber security, the German way', <http://www.orfonline.org/expert-speaks/bundeswehr-cyber-security-the-german-way/#_edn5> (2017.9.28.최종방문).

572) *Ibid.*

573) Euractiv, Apr. 6, 2017, "Germany rolls out new cyber defence team", <https://www.euractiv.com/section/cybersecurity/news/germany-rolls-out-new-cyber-defence-team/> (2017.9.28.최종방문).

574) Forsvarsministeriet (Ministry of Defence), "Danish Defence Agreement 2013-2017" (2012), p. 16.

575) Ministry of Defence, "The Defence Cyber Strategy" (2012), pp. 5-8.

576) Carmen Cristina Cirlig, *supra* note 564, p. 7.

는 공격을 중단시키기 위해 공격적인 사이버역량을 사용하는 것이 사령부의 역할임을 밝히면서, 자국의 사이버 전략이 적극적 사이버방어임을 명백히 하였다.[577]

유럽연합 이외 국가들의 사이버 전략을 살펴보면 먼저 일본은 사이버공격에 대한 정부의 대응조치가 가능하도록 법을 개정하는 작업을 진행하고 있다. 일본총무성(The Internal Affairs and Communications Ministry)이 주도하는 개정 법안에는 일본의 주요 기반시설이 사이버공격을 당할 때, 이에 반격하는 화이트해커부대를 설치하는 내용이 포함되어 있다.[578] 일본의 부정엑세스금지법에 따르면 해킹과 같은 시스템 침입행위는 모든 대상에게 금지되어 있지만[579] 법 개정을 통해 정부에게만 예외적으로 적극적 사이버방어 행위를 허용하려는 것이다.[580] 이를 위해 13개의 주요국가기반시설을 지정[581]하고, 피해의 심각도를 판단하는 기준을 마련하고 있다. 일본정부는 피해의 정도를 5단계로 나누어 원전시설 파괴와 같이 5단계에 해당하는 사이버공격의 경우, 사이버 반격을 발동한다는 계획이다.[582] 국내적으로는 이러한 조치가 방어차원의 공격, 즉 전수방위를 규정

---

577) Ministry of Defence, *supra* note 575, p. 11

578) The Daily Yomiuri, Sept. 4, 2016, "Plan to Foster 'White-Hat Hackers'", <https://www.questia.com/newspaper/1P3-4169362171/plan-to-foster-white-hat-hackers> (2017.9.27.최종방문).

579) 부정엑세스금지법 제3조, 제4조.

580) 연합뉴스, May 17, 2017, "日정부, 사이버공격 반격할 '화이트해커 부대' 설치 추진", <http://www.yonhapnews.co.kr/bulletin/2017/05/17/0200000000AKR20170517072900009.HTML?input=1195m> (2017.9.27.최종방문).

581) 13개 분야로는 정보통신, 금융, 항공, 철도, 송전선망, 가스, 정부 행정기관, 의료서비스, 수자원, 화학산업, 신용카드, 석유산업, 운송분야가 있다. NEC Global, "Commercial facilities as targets: New Threats to critical infrastructure" (2017), p. 4.

582) 연합뉴스, 2017년 5월 17일, "日정부, 사이버공격 반격할 '화이트해커 부대' 설치 추진", <http://www.yonhapnews.co.kr/bulletin/2017/05/17/0200000000AKR201

하고 있는 일본헌법 제9조에 위배된다는 논란이 있지만 일본정부는 이를 강행하겠다는 입장을 밝히고 있다.[583] 이 같은 일본의 움직임은 미국과의 균형을 맞추기 위해 일본에게 공격적인 방어능력을 갖추는 것이 요구되기 때문이다.[584]

미국과 일본은 1997년 합의한 미일방위지침(Guidelines for U.S.-Japan Defense Cooperation)을 2015년에 개정하였는데, 개정 이유 중 하나가 사이버안보와 관련하여 일본의 군사안보전략에 변화가 필요했기 때문이었다.[585] 또한 미일 상호방위협력 및 안보조약 제5조는 일본 영토 내 어느 한 국가에 대한 무력 공격이 발생할 경우, 이에 대처하기 위한 조치를 취할 것을 규정하고 있어 사이버공격 발생 시 미국의 적극적 사이버방어 기술이 투입될 가능성도 높다고 할 수 있다.[586]

한편 이스라엘은 미국과 함께 공격적인 사이버방어조치를 실행하고 있는 대표적인 국가이다.[587] 미국이 주로 러시아나 중국을 상대로 하고 있다면 이스라엘은 이란 등의 중동국가와 하마스, 헤즈볼라와 같은 이슬람 무장 저항단체, 어나니머스와 같은 핵티비스트 등의 공격에 주로 대응한다. 이스라엘은 2014년 9월 National Authority for Cyber Defence를 창설[588], 사이버공격으로부터 국민을 보호하는 업무를 관장하도록 하고 있

70517072900009.HTML?input=1195m> (2017.9.27.최종방문).

583) *Ibid.*

584) James Andrew Lewis, "US-Japan Cooperation in Cybersecurity", Center for Strategic & International Studies (2015), p. 2.

585) Robin Sakoda, "The 2015 U.S.-Japan Defense Guidelines: End of the New Beginning", Center for Strategic & International Studies, Apr. 30, 2015, < https://amti.csis.org/the-2015-u-s-japan-defense-guidelines-end-of-a-new-beginning/> (2017.9.29.최종방문).

586) Treaty of Mutual Cooperation and Security between Japan and the United States of America, Jan. 19, 1960.

587) Matthew S. Cohen, Charles D. Freilich, Gabi Siboni, "Israel and Cyberspace: Unique Threat and Response", International Studies Perspectives, Vol. 17, No. 3 (2016), p. 1.

588) *Ibid.,* 이스라엘이 사이버 관련기관을 창설한 것은 이번이 처음이 아니다.

다.[589]

한편 Israel Security Agency (ISA 또는 Shin Bet)는 조직 내에 별도의 엘리트 사이버방어부대를 설치하여 운영하고 있다.[590] S-74라는 코드네임으로 활동하는 Shin Bet unit은 실시간 모니터링 작업을 통해 의심되는 네트워크 흐름을 추적하여 공격이 일어나기 전 먼저 타격하는 일을 하고 있다. 반 이스라엘 세력들이 수 천 개에 달하는 이스라엘 웹사이트를 공격한 OpIsrael 사건 당시, 상대가 공격에 성공하지 못했음을 확인할 수 있을 때까지 사이버 상의 반격을 반복해서 실행하였다.[591] 한편 Israel Defense Forces도 필요한 경우 군은 사이버무기를 사용할 것이라고 공식 사이트를 통해 밝힌 바 있다.[592] 이스라엘은 방어차원에서 뿐 아니라 자국의 정치적 목적을 위해서 공격적으로 사이버역량을 사용하는 것으로도 유명하다. 2010년 이란 핵시설을 마비시킨 스턱스넷 바이러스는 이스라엘이 미국과의 협력하에 개발한 사이버무기로 알려져 있다.[593] 이스라엘은 이보다 앞서 2007년 시리아의 원자로 공습 전 미리 사이버공격을 통해 시리아

1997년 세계 최초의 정부 산하 사이버안보기관 중 하나인 Tehila를 설치한 이래 Israel Defense Forces 산하의 Unit 8200 부대를 운영하는 등 사이버안보를 담당하는 기관을 꾸준히 증강해오고 있다.

589) Carmen Cristina Cirlig, *supra* note 564, p. 5.

590) *Ibid.*; Arutz Sheva Israel National News, Sept. 21, 2014, “Israel Launches National Cyber-Defense Authority”, <http://www.israelnationalnews.com/News/News.aspx/185349#.VEUT_W3DVgg> (2017.9.28.최종방문).

591) Arutz Sheva Israel National News, Apr. 25, 2014, “Secret Shin Bet Unit at The Front Lines of Israel's Cyber-War”, <http://www.israelnationalnews.com/News/News.aspx/179925> (2017.9.28.최종방문).

592) Ynet News, Apr. 6, 2012, “IDF says 'defined essence of cyber warfare'”, <https://www.ynetnews.com/articles/0,7340,L-4238156,00.html> (2017.9.28.최종방문).

593) David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, (Broadway Paperbacks, 2012), pp. 191-196.

의 레이더 시스템이 작동하지 못하도록 한 바도 있다.[594] 이 밖에도 Unit 8200은 미국과 함께 이란에 대한 Flame 멀웨어 공격의 배후로 지목되는 등 이스라엘은 공세적인 사이버 전략을 펼치고 있다.[595]

6. 소결

사이버공간의 규율에 관한 국제법적 논의와 실제 국가들의 대응을 비교해보면 둘 사이에 상당한 괴리가 있음을 알 수 있다. 국제법적 논의는 대응조치나 자위권 적용에 대한 기준마련, 새로운 체제성립 여부 등을 놓고 교착상태에 빠져 있지만, 국가들은 국내적으로는 구체적인 전략 및 실행으로 앞으로 나아가고 있다. 특히 대부분의 국가들이 국제사회에서의 주장과는 별개로 수동적 방어보다는 적극적 방어를 대응전략으로 선택하고 있는 사실은 주목을 요한다.[596] 사이버기술을 사용한 대응조치에 대해 가장 강력하게 반발하고 있는 러시아가 실제로는 가장 활발한 적극적 사이버방어 및 공격의 주체라는 점은 더욱 의미가 깊다. 미국은 여기서 더 나아가 민간에까지 적극적 대응조치를 허용하려 하고 있다. 이는 미국이 기본적으로 공세적인 대응을 원하기 때문이 아니라 기업들이 국내법의 제한을 피해 비밀리에 역해킹과 같은 자구 조치를 실행하고 있는 행태를 더 이상 막을 수 없다고 판단했기 때문이다.[597] 사이버공격의 피해를 입은 기업들의 자

---

594) Arie Egozi, “The Secret Cyber War”, Military Technology, Vol. 35, No. 3 (2011), p. 6.

595) Wired, May 28, 2012, “Meet ‘Flame,’ The Massive Spy Malware Infiltrating Iranian Computers”, <https://www.wired.com/2012/05/flame/> (2017.9.28.최종방문).

596) 앞서 살펴본 유럽연합 국가들 외에도 10개의 국가가 표면적으로는 적극적 방어전략을 택하고 있다고 말하지 않고 있으나 군사적 관점에서 사이버 대응을 고려하고 있는 것으로 보고되고 있다. 또한 이 외에도 이란, 시리아, 터키 등의 국가가 공격적인 사이버 능력을 보유하고 있는 것으로 알려져있다. Carmen Cristina Cirlig, *supra* note 564, p. 6.

597) Reuters, Jun. 18, 2012, “Hacked companies fight back with controversial steps”,

구조치에 대해서는 후술하기로 한다. 즉, 국가들의 적극적 사이버방어 전략 및 실행은 더 이상 막을 수 없는 현실인 것이다.

이러한 상황에서 실행을 반영하지 못하고 성과 없는 논의만을 반복하고 있는 국제법의 현실은 상당히 우려스럽다. 현재 국가들이 발전시키고 있는 적극적 방어의 전략과 제한 기준은 각기 다르다. 그러나 국제사회 차원의 제한 없이 국가실행이 발전하는 것은 위험하다. 따라서 각국의 실행에 대한 면밀한 검토를 통해 국제법적으로 적법한 적극적 사이버방어조치에 관한 기준과 제한 범위를 마련하는 것이 필요하다. 이는 앞서 국제법 차원의 논의에서 정리한 자위권 및 대응조치를 위한 명확한 기준 설정, 사이버무기 규제, 협조체계의 구축과도 연관된 작업이다. 국가들이 국제사회에서 각자의 입장만을 주장하며 평행선을 달리는 사이 법적 모호성은 더욱 심화되고 있다.

<https://www.reuters.com/article/us-media-tech-summit-cyber-strikeback/hacked-companies-fight-back-with-controversial-steps-idUSBRE85G07S20120618> (2017.9.29.최종방문).

제5장 적극적 방어개념의 적용과 장기적 억지를 위한 다자체제 구축

제1절 적극적 방어개념 적용의 필요성

1. 실효적 규율 방안 도입의 필요성

1) 즉각적 억지와 장기적 억지 개념의 분리

국제법이 사이버공격을 어떻게 규율할 것인가에 대한 논의는 현재까지 활발히 진행되어 왔다. 그러나 국제사회 차원의 논의는 아직도 기존의 국제법을 사이버공간에도 그대로 적용할 수 있는지 아니면 새로운 체제가 필요한지에 대한 논쟁의 수준을 벗어나지 못하고 있다는 점은 앞서 살펴본 바 있다. 그러는 사이 다수의 국가들이 국내적으로는 적극적 방어를 사이버공격에 대한 대응전략으로 삼고 있는 현실도 확인하였다. 적극적 방어는 사후대응이 아닌 선제적 혹은 동시적 대응의 개념으로서 일국의 영토에서 발사된 탄도미사일을 상대방 국가에서 타격하는 것과 유사한 원리이다. 그러나 이러한 개념은 법의 위반이 발생하고 위반행위자의 귀속이 밝혀져야만 대응을 할 수 있는 기존 국제법의 테두리를 벗어난 것이다. 사이버공격은 미사일 발사와는 달리 공격의 발원지와 공격 행위자가 가시적으로 드러나지 않는 특징을 가지고 있기 때문이다.

그런데도 다수의 국가가 이 개념을 법적·정책적으로 선택하고 있다는 것은 국가들의 실행이 국제법 차원의 논의와 일치하지 않고 있다는 것을 보여준다. 국제법은 결국 주요행위자인 국가들에 의해서 이행이 되어야만 의미가 있다는 점에서 현재 국가들의 실행은 국제법이 사이버공격에 대한 해결책을 제시하지 못하고 있다는 것을 시사한다. 오늘날 거의 모든 통신

기반시설 및 시스템이 민간부분에 의존하고 있고, 국가의 주요 기반시설과 국방활동이 대부분 이들 시설 및 시스템의 지원을 받고 있는 현실[598]을 생각할 때, 현재 상태가 지속되는 것은 바람직하지 않다.

사이버공격에 대한 대응에 있어 가장 핵심적인 부분은 시간이라고 할 수 있다. 사이버공격의 가장 두드러진 특성 중 하나가 탐지와 공격 사이의 간격이 0이기 때문이다.[599] 즉, 탐지와 동시에 공격이 일어난다는 것인데, 이는 물리적 공간에서는 심지어 핵무기를 발사하는 경우에도 몇 분간의 대응시간이 있는 것과는 대조적이다.[600] 따라서 사후대응 패러다임은 사이버공격을 억지하는 방법으로는 적절치 않다.[601]

문제는 기존의 국제법이 이러한 사후대응을 기반으로 하고 있다는 점이다. 무력사용 금지 원칙, 자위권, 대응조치 및 이에 대한 국가책임 추궁과 같은 기존의 국제법은 모두 금지된 행위가 발생하고, 위반행위의 귀속이 밝혀져야 대응을 할 수 있게 되어 있다. 그러나 사이버공격에 대한 가장 효과적인 대응은 위협을 탐지한 즉시 이를 차단하는 것이다. 따라서 최우선적으로 요구되는 조치는 네트워크상에서의 실시간 위협처리이다.

자위권의 개념을 생각하면 그 차이점을 좀 더 쉽게 이해할 수 있다. 자위권은 무력공격 발생시 그 공격을 행한 당사자에게 행사하는 것이다. 그러나 네트워크상의 공격처리는 반드시 사이버공격을 실행하는 행위자를

598) Eugenia Georgiades, William Caelli, Sharon Christensen, W.D. Duncan, “Crisis on Impact: Responding to Cyber Attacks on Critical Information Infrastructures”, The John Marshall Journal of Information Technology & Privacy Law, Vol. 30, No. 1 (2013), pp. 31-32; Clay Wilson, “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress”, CRS Report for Congress (2008), RL32114, p. 1. 보고서에서는 미군 메시지의 상당부분이 상업적 통신채널을 통해 이루어지고 있고, 이러한 의존성이 사이버 전에서 취약점이 될 수 있다고 한 Dan Kuehl 교수의 지적을 함께 언급하고 있다.

599) Eric Talbot Jensen, *supra* note 9, p. 800; Kim Taipale, *supra* note 9, pp. 3-4.

600) Eric Talbot Jensen, *supra* note 112, p. 235.

601) Kim Taipale, *supra* note 9, pp. 3-4.

대상으로 하지 않는다. 사이버공격의 경우 공격포인트와 실제 공격자의 위치가 일치하지 않는 경우가 많기 때문이다.[602] 임박한 공격을 차단·저지하기 위해서는 네트워크상의 공격거점을 찾아내 이를 처리하는 것이 필요하다.[603] 현재 국가들의 실행은 바로 사이버공격에 대한 즉각적인 대응을 통한 억지전략으로 형성되고 있다고 해석할 수 있다.

그렇다고 해서 귀속의 문제가 사이버공격을 규율하는 데에 의미가 없다는 것은 아니다. 사이버공격의 귀속을 밝혀 행위자를 처벌하거나 제재하는 것은 이후에 재발방지를 위한 장기적 대응방안으로서의 의의가 있다고 할 수 있다.[604] 즉, 사이버공격을 효과적으로 규율하기 위해서는 '즉각적 억지'와 '재발방지를 위한 장기적 억지' 두 가지를 모두 염두에 둔 전략이 필요하다. 사이버공격의 귀속을 밝히는 것은 시간이 오래 걸린다는 점[605]에서 장기적 억지에 속한다고 볼 수 있다. 귀속의 증명을 통해서 피해국은 국가책임을 추궁하거나 같은 공격이 지속되고 있다고 판단될 경우 대응조치를 취할 수 있다. 때문에 제3장에서 살펴본 것과 같이 기존 국제법을 적용하기 위한 기준을 명확히 하는 작업은 이를 위해서 필요하다. 그러나 즉각적 억지 부분에 대한 규율을 간과하고, 장기적 억지를 의미하는 기존 국제법 적용에 관한 논의에만 집중하는 것은 바람직하지 못하다.

---

602) Lipson, H.F., *supra note* 10, pp. 31, 34, 36.

603) Jan Messerschmidt은 국제법의 본질이 물리적이기 때문에 사이버공격의 위험성이 제대로 정의되지 못하고 있다는 점을 지적하고 있다. Jan Messerschmidt, *supra* note 16, p. 295.

604) 그러나 앞에서도 지적한 바 있듯 협조의무가 부재한 현체제만으로는 귀속의 증명도 거의 불가능하다는 점을 유념할 필요가 있다.

605) Chris Prosise, Kevin Mandia, *supra* note 324, p. 25; David E. Graham, *supra* note 335, p. 91; Eric Talbot Jensen, *supra* note 112, pp. 232-235; Matthew J. Sklerov., *supra* note 112, pp. 7-8; James P. Terry "Responding to Attacks on Critical Computer Infrastructure: What Targets? What Rules of Engagement?", Naval Law Review (1999), p. 177.

2) 현재 논의에 대한 비판

사이버공격에 대한 즉각적 억지를 간과하고 있는 현재의 논의에 대한 비판은 이미 여러 연구에서 지적된 바 있다. Sklerov는 귀속의 문제가 국가들이 사이버공격에 대한 즉각적인 대응을 하지 못하도록 법적으로 제한하고 있음을 지적하였다.[606] Condron은 공격자의 신원을 요구하는 현재의 패러다임은 국가들이 국제법위반을 감행하지 않고서는 사이버공격에 효과적으로 대응할 수 없도록 국가들의 양 손을 묶고 있다고 비판하였다.[607] Jensen은 귀속의 증명 없이 네트워크상의 대응조치가 법적으로 허용되어야 한다고 주장하였다.[608] James P. Terry도 같은 맥락에서 즉각적으로 공격자를 확인하는 것이 불가능한 상황에서 피해국이 사이버상의 조치를 취할 수 없는 구조는 합리적이지 않다고 하였다.[609] 이 같은 비판은 모두 귀속의 증명을 전제로 하는 현 국제법체제가 사이버공격을 저지하는 데에는 적합하지 않음을 지적하고 있다.

또 다른 비판은 헌장체제에 관한 것으로 *jus ad bellum* 에 있어서의 모호한 적용 기준이 사이버공격에 대한 적극적 방어조치를 취하는 데 걸림돌이 된다는 것이다. 즉, 헌장을 기반으로 하는 무력사용금지의 원칙 및 무력공격의 판단기준은 기존의 물리적 공간에 대해서도 확립되지 않았는데, 현재의 모호한 기준이 사이버 맥락에 적용가능하다는 논의는 모호한 영역을 더욱 확대할 뿐이라는 비판이다.[610] 기존의 무력충돌법(LOAC) 및

606) Matthew J. Sklerov, *supra* note 112, pp. 8-9.
607) Condron, *supra* note 2007, p. 415.
608) Eric Talbot Jensen, *supra* note 112, pp. 236-237.
609) James P. Terry, *supra* note 605, p. 177.
610) Andrew C. Foltz, “Stuxnet, Schmitt Analysis, and the Cyber "Use of Force" Debate”, JFQ, Vol. 67, No. 4 (2012), p. 42; Manny Halberstam, “Hacking Back: Reevaluating the legality of retaliatory Cyberattacks”, The George Washington International Law Review, Vol. 46 (2013), pp. 229-230; Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, “The Law of

‘무력사용’과 ‘무력공격’에 초점을 맞춘 헌장의 언어를 통해 사이버공격을 기존의 국제법 틀에 맞추려는 시도가 부적절하다는 지적도 위의 비판과 맥을 같이한다.[611]

이와 같은 지적은 사이버공격이 저강도의 수준에서 순식간에 재앙적인 피해를 가져오는 고강도의 공격으로 전환될 수 있는 특성을 가지고 있는 것과 관련이 있다.[612] 이와 같이 사이버 맥락에서는 전시·평시의 이분법적 구분이 불분명한 경우가 대부분이기 때문에 전통적인 틀에 사이버공격을 끼워 맞추는 시도는 바람직하지 않다는 것이다.[613] 한편 사이버공격이 초래하는 결과가 전통적인 틀에 맞지 않는 경우가 대부분이라는 비판도 함께 제기되었다. 사이버공격이 대규모의 물리적 파괴 및 인명살상을 야기한다면 이는 명백히 무력공격에 해당하기 때문에 기존의 기준을 적용할 수 있지만, 사이버공격에서 이러한 극단적인 경우는 극히 드물다는 것이다.[614] 이는 무력공격에 미치지는 못하나 국가의 기반시설에 상당한 피해를 가져올 수 있는 사이버공격-사실상 대부분의 비중을 차지하는-에 대한 대응에 있어서의 법적인 공백을 지적한 것이라고 볼 수 있다.

현 체제의 적용을 바탕으로 한 논의에 대한 비판은 탈린매뉴얼에 대한 평가로도 이어진다. 탈린매뉴얼은 기존의 국제법이 사이버공간에도 그대로 적용가능하다는 논리를 그대로 답습하고 있기 때문이다. 탈린매뉴얼은 기존의 국제법이 사이버 맥락에도 그대로 적용가능하다는 서구 국가들의 입장에 기반한 것일 뿐, 국제사회 전체가 탈린매뉴얼의 해석을 그대로 받아들이지는 않을 것이라는 지적도 같은 맥락에서 이해할 수 있다.[615] 탈린매

Cyber-Attack", California Law Review, Vol. 100 (2012), pp. 840-842.

611) William Banks, "The Role of Counterterrorism Law in Shaping *ad bellum* Norms for Cyber Warfare", International Law Studies, Vol. 89 (2013), pp. 162-163.

612) *Ibid.,* p. 162.

613) *Ibid.* ; John Dever and James Dever, "Cyberwarfare: Attribution, Preemption, and National Self Defense", Journal of Law & Cyber Warfare, Vol. 2 (2013), p. 28.

614) William Banks, *supra* note 611, p. 162.

뉴얼은 참신함을 제공하기 보다는 오히려 기존의 국제법이 사이버공간을 규율하는 것이 역부족임을 드러내주고 있다는 비판을 받기도 하였다.[616] 실제로 탈린매뉴얼은 기존 국제법원칙을 사이버공격의 경우에 대입할 수 있는 여러 가지 가능성을 제안하고 있을 뿐, 명확한 기준을 제시하지는 못하고 있다.[617]

이러한 비판들을 종합하면 현재의 논의는 귀속의 한계성을 건너뛰고 모호한 적용기준을 기반으로 하여 발전하고 있다고 볼 수 있다. 이를 반대로 해석하면 현재의 논의에는 사이버공격에 대한 대응을 위해 가장 요구되는 공격의 즉각 차단 및 저지를 위한 조치에 관한 논의가 빠져 있다는 결론에 이르게 된다. 국제법이 마땅한 대응책을 제공해주지 못하는 상황이 지속된다면 국가들이 국제법 밖의 영역에서 자구책을 찾는 현상은 계속될 것이고, 국제법은 실효성을 회복하기 힘든 상태가 될 가능성이 높다. 법의 보호가 부적절한 경우, 국가들은 불법적인 방법을 통해서라도 자국의 안보를 지킬 수단을 강구할 것이기 때문이다.[618]

문제는 적극적 방어조치가 법 밖의 영역에서 이루어지기 때문에 비밀리에 진행된다는 점이다.[619] 국제법의 규율 범위 밖에서 국가들의 적극적 사이버방어조치가 만연하게 될 때, 그로 인해 발생하는 피해와 혼란은 굳이 서술하지 않아도 알 수 있을 것이다. 이러한 상황을 방지하기 위해서는 사

---

615) Yaroslav Radziwill, *supra* note 130, p. 21.
616) James E. McGhee, "Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy", Journal of Law & Cyber Warfare, Vol. 2 (2013), p. 66.
617) James E. McGhee, *supra* note 167, p. 24.
618) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 478; Matthew J. Sklerov, *supra* note 112, p. 11; Neal K. Katyal, "Community SelfHelp", Journal of Law, Economics and Policy, Vol. 1 (2005), p. 40.
619) Linkedin, May 31, 2017 - Brian Coventry, "Hack back & Counterstrike", <https://www.linkedin.com/pulse/hack-back-counter-strike-brian-coventry> (2017.10.16.최종방문).

이버공격이 효과적으로 다루어지고 통제될 수 있는 법적 수단이 있다는 사실을 확실히 인식시키는 것이 중요하다.[620] 법적인 수단을 통해 문제를 해결할 수 있다면 국가들은 훨씬 더 예측 가능한 방향으로 행동하게 될 것이기 때문이다.[621]

3) 민간기업들의 자구조치 규제

사이버공격에 대한 마땅한 대응책의 부재로 법 밖의 영역에서 자구책을 찾는 현상은 국가들에게만 국한된 것이 아니다. 사이버공격의 피해를 입은 민간기업들도 국내법이 실효적 대응책을 제시하지 못함에 따라 자구책으로 적극적 방어조치를 취하고 있기 때문이다.[622]

2012년 Black Hat USA 보안컨퍼런스에서 사이버 보안기업 nCircle이 조사한 결과 응답자 중 36퍼센트가 보복성 해킹을 한 바 있다고 답하였다.[623] 한편 최근에는 많은 기업들이 자국 내 또는 해외 업체에 적극적 방어조치를 위탁하는 경향도 생겨나고 있다.[624] 2013년 미 연방조사국이 미국의 금융기관들을 상대로 이란이 자신의 기업들을 공격할 때 사용한 서

620) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 478
621) Sean Murphy, "The Doctrine of Preemptive Self-Defense", Villanova Law Review, Vol. 50, No. 3 (2005), pp. 704-705; Matthew J. Sklerov, *supra* note 112, p. 12.
622) Cameron S. D. Brown, *supra* note 379, p. 168; Wyatt Hoffman and Ariel E. Levite, *supra* note 17, pp. 1, 4, 15; SecurityWeek, Nov. 13, 2015, "Hacking Back: Industry Reactions to Offensive Security Research", <http://www.securityweek.com/hacking-back-industry-reactions-offensive-security-research> (2017.10.21.최종방문).
623) The Washington Post, Oct. 9, 2014, "Cyberattacks trigger talk of 'hacking back'", <https://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html?utm_term=.f9c01f3b1a44> (2017.10.20.최종방문).
624) Wyatt Hoffman and Ariel E. Levite, *supra* note 17, p. 15.

버를 무력화하기 위해 해커들을 고용한 혐의에 대해 조사한 것은 이러한 사실을 방증하는 것이라 할 수 있다.[625]

이는 국내형법상 피해를 당한 기업이 취할 수 있는 조치는 주로 수동적 방어에 국한되고, 초국경적인 사이버공격의 특성상 공격행위자의 처벌은 기대하기 어렵기 때문이다.[626] 또한 사실상 처벌이 가능하더라도 시간이 많이 소요되기 때문에 기업이 기대하는 피해 방지의 효과는 없다는 것도 문제다.[627] 예를 들어 Sapphire/Slammer Worm은 8.5초마다 크기가 두 배로 커지면서 10분 내에 취약한 시스템의 90% 이상을 감염시키는 멀웨어인데[628], 사건을 보고하고 수사를 의뢰하는 기존의 법집행 절차를 통해서는 이와 같은 특성을 가진 웜 공격에 대한 실질적인 대응이 불가능한 것이다.[629]

2015년 다보스포럼에서 글로벌 은행의 고위관계자들이 사이버공격에 대해 자신들이 직접 대응할 수 있도록 해달라고 로비한 사실은 사이버공격에 노출된 사기업들이 실효적인 법제도적 구제책의 부재에 좌절하고 있는 현실을 그대로 보여준다.[630] 당시 한 은행의 시스템 책임자는 관할권 문제

---

625) Bloomberg, Dec. 30, 2014, "FBI Probes if Banks Hacked Back as Firms Mull Offensives", <https://www.bloomberg.com/news/articles/2014-12-30/fbi-probes-if-banks-hacked-back-as-firms-mull-offensives> (2017.10.20.최종방문).

626) Ruperto P. Majuca and Jay P. Kesan, *supra* note 395, p. 7; Jan Messerschmidt, *supra* note 16, p. 291.

627) Jan Messerschmidt, *supra* note 16, p. 293; Neal K. Katyal, *supra* note 618, p. 60.

628) SANS Institute, "MS SQL Slammer/Sapphire Worm", GIAC Certifications (2003), p. 1.

629) Jan Messerschmidt, *supra* note 16, p. 293; Ruperto P. Majuca and Jay P. Kesan, *supra* note 395, p. 7.

630) Financial Times, Jan. 22, 2015, "Davos 2015: Banks call for free rein to fight cyber crime", <https://www.ft.com/davos?emailid=575988c90b860d0300a2bcea&ftcamp=crm%2Femail%2F%2Fnbe%2FfintechFT%2Fproduct&page=8> (2017.10.20.최종방문).

로 초국경적 사이버공격의 행위자를 처벌할 수 없는 국내법집행기구의 한계를 기업이 직접 공격에 사용된 서버를 찾아 무력화 시키는 조치를 통해 극복하고 스스로를 보호할 수 있는 권리를 보장해 주어야 한다고 주장하였다.[631]

문제는 이렇게 사이버공격을 당한 기업이 현재 법의 테두리 안에서 취할 수 있는 조치는 지극히 제한적인데 반해 이들 기업이 감수해야 할 피해는 크다는 데에 있다. 즉, 해킹 또는 사이버공격을 당한 기업은 공격자체로 인한 손해뿐 아니라 이 사실이 공개됨으로 인한 주가하락, 기업의 신뢰도 하락 등의 2차적 피해까지 고스란히 감내해야만 한다.[632] 또한 기업들은 자신이 대규모 사이버공격을 당했다는 사실이 공개되면 기업의 취약점이 드러나고 경쟁사가 이를 악용할 가능성이 있기 때문에 더욱 공개를 꺼리는 것으로 알려졌다.[633] 이러한 이유로 기업들은 대규모 사이버공격을 당하더라도 이를 숨기는 경향이 있고[634], 법집행기관에 의존하기 보다는 자체적으로 역해킹 등의 조치를 취하고 있는 것이다.

기업들의 적극적 방어조치는 대부분의 국가에서 형법상 금지되어 있기 때문에 주로 비밀로 수행된다는 점을 생각할 때, 민간기업의 적극적 방어조치를 통한 대응은 현재 알려진 것보다 훨씬 더 빈번하게 이루어지고 있을 것으로 예상된다.[635] 특히 주요국가기반시설의 상당부분이 사기업에 의

---

631) *Ibid.*

632) Jan Messerschmidt, *supra* note 16, pp. 293-294; The Guardian, Mar. 9, 2015, "Should we hack the hackers?", <https://www.theguardian.com/technology/2015/mar/09/cybercrime-should-we-hack-the-hackers> (2017.10.21.최종방문).

633) Jan Messerschmidt, *supra* note 16, pp. 293-294; Bruce P. Smith, "Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help", Journal of Law, Econimics and Policy, Vol. 1 (2005), pp. 172-172.

634) Amos N. Guiora, *Cybersecurity: Geopolitics, law and policy*, (Routledge, 2017), p. 101.

635) Linkedin, May 31, 2017 - Brian Coventry, "Hack back & Counterstrike",

해 운영되고 있다는 점을 생각하면 국가의 통제를 벗어난 이 같은 사기업들의 관행은 단순히 국내법집행의 실효성 문제를 넘어 국가안보 및 국가의 국제관계에 있어서도 크게 우려할 만한 사항이다.[636] 적극적 방어조치는 어떠한 강도의 조치를 선택하느냐에 따라 타국의 안보에 파괴적인 영향을 미칠 수 있기 때문이다.[637]

또한 적극적 방어조치 실행에는 정확한 공격거점 파악의 실패로 제3자에게 피해를 줄 위험이 항상 존재한다.[638] 예를 들어 공격을 탐지하고 악성코드를 상대의 서버에 보내는 역해킹을 시도할 때, 위장된 소스를 공격거점으로 파악한 경우 그 위장된 소스가 타국의 병원 시스템일 수도 있는 것이다.[639] 이 경우 공격에 대한 방어를 위해 시행한 조치가 타국의 주요기반시설에 파괴적인 영향을 주고, 국가 간의 갈등을 촉발하는 상황을 야기할 수 있다. 적극적 방어조치를 취할 수 있는 기술은 이미 상당히 발달된 상태이나 완벽하다고 할 수는 없기 때문에, 이러한 위험성은 항상 존재한다고 할 수 있다.[640] 이는 비밀리에 법 영역 밖에서 시행하는 기업들의

<https://www.linkedin.com/pulse/hack-back-counter-strike-brian-coventry> (2017.10.21.최종방문); Gus P. Coldebella and Brian M. White, "Foundational Questions Regarding the Federal Role in Cybersecurity', Journal of National Security Law and Policy, Vol. 4 (2010), p. 240.

636) Ibid., 미국의 경우 국가주요기반시설의 85%가 민간 부문에 의해 운영되고 있다.

637) Jan Kallberg, *supra* note 17, p. 32; The Washington Post, Oct. 9, 2014, "Cyberattacks trigger talk of 'hacking back'", <https://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html?utm_term=.ee279845487c> (2017.10.24.최종방문).

638) Michael N. Schmitt and M. Christopher Pitts, "Cyber Countermeasures and Effects on Third Parties: The International Legal Regime", Baltic Yearbook of International Law, Vol. 14 (2014), p. 2; Ruperto P. Majuca and Jay P. Kesan, *supra* note 395, pp. 7, 22.

639) *Ibid.*, p. 7.

640) Jay P. Kesan and Carol M. Hayes, *supra* note 112, pp. 481, 483; SecurityWeek, Nov. 13, 2015, "Hacking Back: Industry Reactions to Offensive Security Research",

자구조치가 얼마나 위험할 수 있는지를 보여준다. 기업의 자구조치가 초국경적인 파급력을 가진다는 사실과 그러한 파급력이 내포하는 위험성은 이 문제가 단순히 국내문제가 아니라 국제법의 규율이 필요한 사안임을 보여준다.

적극적 방어조치를 통한 대응이 더욱 확산되고 있는 상황에 적절히 대처하기 위해서는 우선 국가가 피해기업에게 실효적 구제책을 마련해 주면서 기업들의 자구조치를 규율하는 것이 필요하다.[641] 만일 정부가 어떤 실효적 구제책을 제시하지 않고 기업들의 적극적 방어조치 관행을 전면적으로 규제하려고 시도한다면 이는 현실을 제대로 파악하지 못한 효과 없는 조치가 될 것이다.[642] 국가가 기업의 자구조치를 규제하는데 우선적으로 걸림돌이 되는 것은 기업들이 형법 위반을 우려하여 비밀리에 적극적 방어조치를 실행하고 있다는 사실이기 때문이다. 적극적 방어조치의 제도적 보장만이 음지에 있는 기업의 활동을 양지로 나오게 할 수 있다.[643] 국가는 대부분의 주요기반시설을 운영하고 있는 기업 및 기타 기업에 대한 사이버공격에 대해 적극적 방어조치를 취할 수 있는 자원이 충분치 않고,[644] 그 외의 실효성 없는 사법적 조치의 제안은 기업들이 받아들이지 않을 것이기 때문이다. 기업이 취할 수 있는 조치의 강도조절은 제도적 보장을 논의하는 장으로 나온 기업들의 조치실행에 관한 정확한 사실파악을 통해 규제방안이 마련되어야 한다.

국제법은 국가들의 실행을 규율하지 못하고, 국가들은 민간의 초국경적 활동을 규율하지 못하는 현 상황을 극복하기 위해서는 제도 안에 실행을 포용하는 것이 필요하다. 이를 위해서는 적극적 방어 개념을 국제법을 통

<http://www.securityweek.com/hacking-back-industry-reactions-offensive-security-research> (2017.10.21.최종방문).

641) Wyatt Hoffman and Ariel E. Levite, *supra* note 17, pp. 33-34.

642) *Ibid.*, p. 14.

643) Dennis C. Blair et al. *supra* note 17, pp. 5-6.

644) Kim-Kwang Raymond Choo, "The cyber threat landscape: Challenges and future research directions", Computers & Security, Vol. 30 (2011), p. 726.

해 규율하는 방안을 마련하고, 여기에서 마련된 규율사항을 국가들이 국내적으로 이행하도록 하는 체제가 확립되어야 한다.

2. 적극적 방어의 개념과 특성

1) 적극적 방어의 정의

'적극적 방어'는 원래 적의 위협이 아군 지역에 도달하기 전에 이를 제거하여 부대의 전투력을 보존하는 전략을 뜻하는 군사용어로 적의 미사일 발사 징후 포착 시 위협의 근원지를 선제 타격하는 활동을 포함한다.[645] 미 국방부는 접전지에서 적에 대해 공격의 여지를 허용하지 않기 위해 제한된 공격적 활동 또는 반격을 하는 것을 적극적 방어라고 정의하고 있다.[646] 국가들이 사이버안보전략으로 도입하고 있는 적극적 방어는 이러한 원래의 개념을 사이버공간에 접목시킨 것이다.[647]

그러나 아직까지 사이버공간에서의 적극적 방어에 대한 명확한 정의는 확립된 바 없다. 이에 적극적 방어에 대해 서술하고 있는 연구나 보고서에서는 각각 나름의 정의를 내리고 있는데, 그 의미와 범위에 있어서는 차이가 있다. 사이버공간에서의 적극적 방어의 정의와 범주를 명확히 하는 것은 사이버안보의 복잡한 이슈에 대한 법적 및 정치적 해결책의 마련을 위해 선행되어야 할 작업이다.[648] 즉, 적극적 방어에 대한 개념정립은 적법한 실행 기준을 세우기 위한 요건과 제한사항을 정립하기 위한 출발점이

---

645) 국방과학기술용어사전 (2011), p. 742.

646) "The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy."- DoD Dictionary of Military and Associated Terms, (Department of Defense, 2017), p. 5.

647) Dennis C. Blair et al., *supra* note 17, p. 6.

648) Robert S. Dewar, "The Triptych of Cyber Security: A Classification of Active Cyber Defence", in P.Brangetto, M.Maybaum, J.Stinissen (Eds.), 6th International Conference on Cyber Conflict (NATO CCD COE Publications, 2014), p. 19.

되는 것이다.[649] 이에 이하에서는 적극적 방어의 개념을 정의해 보고, 정의한 개념에 기초하여 범주를 명확히 해보도록 한다.

미 국방부는 사이버공간에 대한 적극적 방어개념의 도입 초기에 “사이버위협 및 취약성을 발견, 탐지, 분석, 완화할 수 있는 국방부의 동시적, 실시간 대응역량”을 적극적 사이버방어라고 정의하였다.[650] 미 국방부의 정의 및 부연설명을 보면 오늘날 국가들의 적극적 방어가 공격적인 역량 사용에 초점을 맞추고 있는 것에 비해 위협의 사전 탐지를 위한 기술사용에 역점을 두고 있다는 것을 알 수 있다[651]. 따라서 적극적 방어조치에 대한 일반적 정의로 보기에는 무리가 있다. 그러나 미 국방부의 정의에서 언급된 “동시적, 실시간 대응역량”이라는 문구는 주목할 만하다. 해당 문구는 적극적 방어의 대표적인 성격을 잘 드러내주고 있기 때문이다. 특히 “실시간(in real-time)"[652]이라는 문구는 사이버 상의 적극적 방어를 정의함에 있어서 거의 항상 언급되는 단어이다.[653] 사전적 조치의 개념을 내포

649) Wyatt Hoffman and Ariel E. Levite, *supra* note 17, p. 45.
650) US Department of Defence (2011), p. 7.
651) 국방부 전략은 적극적 방어 개념 정의를 부연설명 하면서 사이버위협의 탐지를 위한 센서나 소프트웨어 등을 사용하는 것이라고 하고 있다. US Department of Defence (2011), p. 7.
652) 실시간(real-time)은 짧게는 몇 초에서 길게는 몇 분이 걸리는 사이버공격의 게시 단계, 즉 데이터 침입 시부터 목표 네트워크에 상주하며 공격을 실행하는 시기 까지를 의미한다. 이 실시간은 cyber relevant time이라고 표현되기도 하는데, 사이버공격의 경우 물리적 공간에서의 공격보다 훨씬 더 침투시간이 빠르다는 점 때문에 보다 대응시간이 단축되어야 한다는 의미로 cyber relevant time이라는 용어를 사용하는 것이다. 원래 시스템 장악을 위해 필요한 순수한 cyber relevant time은 10억분의 1초에서 100만분의 1초이나 마우스 클릭이나 키 누르는 시간 등 담당자의 인지과정을 고려할 때, 몇 초에서 몇 분에 이른다고 설명하고 있다. MJ Herring, KD Willett, “Active Cyber Defense: A Vision for Real-Time Cyber Defense”, Journal of Information Warfare, Vol. 13, No. 2 (2014), p. 1.
653) Robert S. Dewar, *supra* note 648, pp. 9, 18 ; Robert M. Lee, “The Sliding Scale of Cyber Security”, SANS Institute (2015), p. 10; MJ Herring, KD Willett, *supra* note 652, pp. 1-2; Dennis C. Blair et al., *supra* note 17, p. 7; Paul Rosenzweig, *supra* note 17, p. 105.

하고 있는 원래 용어의 의미에서도 짐작할 수 있듯이, 사이버 맥락에서의 적극적 방어는 실시간으로 일어나는 공격에 대한 대응이 목표이자 시간적 범위이다.

한편 사이버 맥락에서의 적극적 방어의 정의에 꼭 포함되어야 할 또 하나의 요소는 “사이버 상”의 조치라는 문구다. 일부 학자들은 사이버 맥락의 적극적 방어조치에 공격자에 대한 처벌이나 국가에 대한 무역제재와 같은 물리적 공간에서의 조치를 포함시키기도 하나,[654] 이러한 조치들은 공격 사후에 이루어지는 것으로서 사전적 조치의(proactive) 성격을 가지고 있는 적극적 방어의 범주를 넘어서는 것이다.[655] 또한 실시간 대응이라는 목적 및 익명성과 신속성이라는 사이버공간의 특성을 생각할 때, 사이버 맥락의 적극적 방어조치는 “사이버 상”의 또는 “네트워크 내에서의” 조치에 국한되는 것이 적절하다. 실제로 극히 일부를 제외하고는 대부분의 적극적 방어에 대한 정의에서는 “네트워크상의” 또는 “사이버공간”을 통한 조치라는 점을 명시하고 있다.[656]

이 두 가지 특성을 포함하여 정의를 내려 보면 사이버 맥락에서의 적극적 방어는 현재 발생하고 있는 위협이나 공격의 흐름을 탐지하여 공격의 경로와 흐름을 파악하고, 이를 차단시키거나 공격명령 서버(C&C 서버) 혹은 봇넷 을 직접 셧다운시키는 등의 사이버역량을 사용하여 공격에 실시간으로 대응하는 사이버공간 상의 조치를 말한다.[657] 따라서 적극적 방어

---

654) Dennis C. Blair et al., *supra* note 17, p. 9.

655) MJ Herring, KD Willett, *supra* note 652, pp. 2-3. 본 논문에서는 이미 축적된 데이터 분석을 통해 추적하고 이를 바탕으로 미래의 공격을 예측하는 작업은 실시간 대응에 해당하지 않는 것(non-real time)으로, 적극적 방어의 범주 밖에 있는 사이버방어전략이라는 점을 지적하고 있다.

656) Robert M. Lee, *supra* note 653, p. 10; Robert S. Dewar, *supra* note 648, p. 18 ; Eric Jensesn (2002), pp. 230-231; Wyatt Hoffman and Ariel E. Levite, *supra* note 17, p. 7.

657) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 461; Eric Talbot Jensesn, *supra* note 112, pp. 230-231; Robert S. Dewar, *supra* note 648, p. 19.

조치는 위협탐지에서 시작하여 이상 흐름의 발생지를 추적하고, 추적된 소스에 대해 공격적인 사이버역량을 사용하는 세 단계의 과정으로 전개된다고 할 수 있다.[658] 이하에서는 '사이버 맥락의 적극적 방어'를 '적극적 방어'라는 일반적 용어로 표현하기로 한다.

2) 사이버공격 억지효과

적극적 방어 기술은 사이버공격의 모든 단계에서 공격자의 행위를 방해하는 효과가 있다.[659] 점점 더 많은 국가 및 민간기업이 적극적 방어를 사이버공격에 대한 대응방법으로 선택하고 있는 이유는 실제적인 공격 억지효과 때문이다. 이하에서는 여러 가지 측면에서 적극적 방어가 가지는 억지효과에 대해 살펴보기로 한다.

첫째로 적극적 방어조치는 공격의 비용을 공격자에게 전가시킨다. 적극적 방어조치의 실행은 공격네트워크 손상 또는 파괴와 같이 공격자가 사용하는 공격수단에 직접 영향을 미치기 때문에 궁극적으로는 공격자에게 공격의 비용을 전가하는 측면이 있다.[660] 사이버공격자들이 공격 여부를 놓고 고려하는 요소가 탐지 가능성, 귀속의 가능성, 처벌의 강도와 공격실행의 비용[661]인 것을 감안하면 적극적 방어조치는 탐지 및 공격비용 전가의 최소 두 가지 요소를 충족하여 사이버공격 억지효과를 거둘 수 있다. 적극적 방어는 조치 과정에서 탐지된 단계에서의 공격행위를 방해·지연시키거나 공격에 사용되는 서버까지 추적해 공격자의 정보나 공격자가 사용

658) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 461.
659) Dennis C. Blair et al., *supra* note 17, p. 13; Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 475.
660) Dennis C. Blair et al., *supra* note 17, p. 15.
661) Jennifer E. Sims and Burton Gerber (eds.), *Transforming US Intelligence*, (Georgetown University Press, 2005), p. 107; Jeffrey Hunker, Bob Hutchinson, Jonathan Margulies, "Role and Challenges for Sufficient Cyber-Attack Attribution", Institute for Information Infrastructure Protection (2008), p. 8.

한 기술을 파악하는 등 귀속을 밝히는 데도 도움을 주기 때문에 공격에 대한 위험비용이 증가하게 되는 측면도 있다.[662]

두 번째로는 기술적 측면에서의 억지효과이다. 적극적 방어가 절실하게 요구되는 이유는 수동적 방어조치의 기술적 한계와 관련이 있기 때문이다. 수동적 방어를 의미하는 네트워크 보안기술은 방화벽, 안티바이러스 솔루션, IDS[663], IPS[664], UTM[665] 등 네트워크 영역에서의 고도화 정보보호 기술로 발전되어 왔다. 그러나 이와 같이 지역적 수준에서 작동하는 경계망 보안장비기술로는 지능형 지속공격(APT)과 같은 융·복합적인 사이버공격[666] 또는 여러 지역에서 다수의 봇넷을 사용하여 복합적인 목표 시스템

662) Wyatt Hoffman and Ariel E. Levite, *supra* note 17, p. 10; Dennis C. Blair et al., *supra* note 17, p. 13; William A. Owens, Kenneth W. Dam, and Herbert S. Lin (eds)., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, The National Academies Press (2009), p. 13.

663) 침입탐지시스템 (Intrusion Detection System, IDS)은 컴퓨터 시스템의 비정상적인 사용을 실시간으로 탐지하는 시스템이다. 한국정보통신기술협회 정보통신용어사전, <http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=046744-1> (2017.10.17.최종방문).

664) 침입방지시스템(Intrusion Prevention System, IPS)은 방화벽과 같은 네트워크 기반의 차단 솔루션을 논리적으로 결합한 시스템으로 비정상적인 트래픽을 능동적으로 차단하고 격리하는 것과 같은 방어조치를 취하는 보안 솔루션이다. 한국정보통신기술협회 정보통신용어사전, <http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=046745-1> (2017.10.17.최종방문).

665) 통합위협관리(Unified Threat Management, UTM)는 가상사설망, 침입차단시스템 등의 다양한 보안솔루션 기능을 하나로 통합한 보안 솔루션으로 이를 통해 각각의 보안솔루션 운용방법을 익히기 위해 들였던 시간과 비용을 절감하고, 복합적인 위협요소를 효율적으로 방어할 수 있다. 한국정보통신기술협회 정보통신용어사전, <http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=059042-3> (2017.10.17.최종방문).

666) 강정호, “빅 데이터를 이용한 선제적 사이버전 강화 방안 연구”, 보안공학연구논문지, Vol. 13, No. 3 (2016), p. 196.

을 향해 수행되는 DDoS 공격에 대처할 수 없다.[667] 현재의 보안기술로는 제로데이 취약점을 이용한 사이버공격에 대한 대응이 불가능하다는 점은 이미 언급한 바 있다.[668] 즉, 특정 시스템을 목표로 하는 이른바 표적 공격에는 진화된 기술을 이용한 복합적이고 정교한 해킹 기법이 사용되기 때문에 운용 환경 내의 취약요소를 식별하고 이에 대한 보안패치[669]를 설치하는 방법은 애초부터 한계를 내포하고 있는 것이다.[670]

가장 최근에 개발된 Anti-virus(AV) 소프트웨어의 경우에 새로 개발된 멀웨어의 10% 미만을 탐지할 수 있었다는 실험결과는 보안에 초점을 맞춘 대응의 무용성을 잘 보여준다.[671] 대부분의 멀웨어 제작자들은 AV회사의 보안 제품을 확인하고 멀웨어를 개발하기 때문에 보안회사의 제품이 등장하는 멀웨어보다 한 걸음씩 뒤지는 것은 어떻게 보면 당연한 일이라고 할 수 있다.[672] 이에 사이버공격의 피해자 및 AV회사들은 사이버공격을 막기 위해서는 공격적 수단을 통해 직접 탐지된 위협에 조치를 취하는 것이 가장 효과적인 대응방법임을 인식하게 된 것이다.[673] 즉, 방화벽이나

667) Christian Czosseck, Gabriel Klein, Felix Leder, *supra* note 43, p. 114.

668) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 474.

669) 운영 체계(OS)나 응용 프로그램에 내재된 보안 취약점을 보완하는 소프트웨어. 보안 패치를 할 경우 취약점을 악용하는 악성 코드 감염을 방지하고, 각종 개인용 컴퓨터(PC) 오류의 원인을 제거해 준다. 한국정보통신기술협회 정보통신용어사전, <http://word.tta.or.kr/dictionary/searchList.do> (2018.1.25.최종방문).

670) 김영환, 이수진, "공세적 통합 사이버작전을 위한 사이버 킬체인 전략", 보안공학연구논문지, Vol. 13, No. 5 (2016), 328; The Commission on the Theft of American Intellectual Property, *IP Commission Report*, (The National Bureau of Asian Research, 2013), p. 79; Jan Messerschmidt, *supra* note 16, p. 291.

671) Shadowserver, "60-day Virus-Stats", <https://www.shadowserver.org/wiki/pmwiki.php/Stats/Virus60-DayStats> (2017.10.18.최종방문); Christian Czosseck, Gabriel Klein, Felix Leder , *supra* note 43 p. 108.

672) Christian Czosseck, Gabriel Klein, Felix Leder, *supra* note 43, p. 108.

IDS 등의 보안기술에 근거한 수동적 방어 수준의 대응만을 허용하는 현재의 법체제는 이러한 사이버기술의 급속한 발전과 사이버환경의 변화를 반영해야하는 도전에 직면해 있는 것이다 .[674]

적극적 방어는 기존에 발생한 공격에 대한 대응이 아니라 사전탐지 및 발생 전 저지를 목표로 두기 때문에 발생한 위협을 추적(track & trace)하면서 공격자의 행동을 미리 예측하여 대응하는 형태로 진행된다. 즉, 방화벽을 설치하는 등 피해자의 홈 네트워크에 대한 조치에 집중하는 것과는 다른 차원의 기술이 사용되는 것이다.[675]

이러한 원리는 적극적 방어전략 중 하나인 사이버 킬체인의 작동방식을 보면 쉽게 이해할 수 있다. 사이버킬체인은 타격순환체계라는 뜻을 가진 Kill Chain이라는 군사용어를 사이버에 접목한 것으로 APT공격의 방어를 목적으로 미국의 군수업체인 록히드마틴사가 처음으로 제안하였다.[676] 록히드마틴사는 시스템 침입(Intrusion Kill Chain)을 정찰(Reconnaissance), 공격코드제작(Weaponization), 전달(Delivery), 취약점공격(Exploitation), 설치(Installation), 명령 및 제어(Command and

---

673) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 474; Christian Czosseck, Gabriel Klein, Felix Leder, *supra* note 43, p. 108.

674) Amanda N. Craig, Scott J. Shackelford and Janine S. Hiller, "Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis", American Business Law Journal, Vol. 52 (2015), p. 25

675) Irving Lachow, *supra* note 17, p. 3; 적극적 방어 기술은 침입을 탐지하는데 그치지 않고, 침입의 근원까지 이를 추적하는 기능을 포함하고 있다. Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 475; Dennis C. Blair et al., *supra* note 17, p. 11. 그러한 기술로는 대표적으로 beacons을 들 수 있는데, 이는 사용자의 파일에 숨겨진 형태로 존재하는 소프트웨어 또는 링크를 의미한다. 사용자의 컴퓨터에서 허가 없이 해당 파일이 삭제되면 이는 사용자의 컴퓨터와 침입자의 네트워크를 연결하여 침입자 시스템의 구조와 위치 등의 세부정보를 사용자에게 전달한다.

676) 보안뉴스, 2017년 2월 23일, "'공격이 최선의 방어' 국방부의 사이버 킬체인 전략은?", <http://www.boannews.com/media/view.asp?idx=53569&kind=2> (2017.10.18.최종방문).

Control), 목표시스템장악(Actions on objectives)의 7단계로 나누고 있다.[677] 이는 사이버공격이 계획된 절차에 따라 진행된다는 인식을 바탕으로 고안된 전략으로 탐지된 위협이 심화되기 전에 다음 단계의 대응조치를 취하여 방어를 하는 원리이다.[678] 위의 7단계 중 실제 공격은 마지막 단계인 목표시스템 장악단계에서 이루어진다.[679] 따라서 최종 목표는 공격에 해당하는 7단계에 이르기 전에 탐지(detect), 거부(deny), 방해(disrupt), 시스템 저하(degrade), 속임(deceive), 파괴(destroy) 등의 수단을 사용하여 체인을 끊어내는 것이다.[680]

세 번째는 위의 기술을 이용한 접근법 전환을 통해 거두는 억지효과이다. 최근의 워너크라이 랜섬웨어 사건은 적극적 방어기술의 도입을 통해 공격자의 입장에서 행동을 예측하고 대응하는 접근법이 얼마나 성공적인지를 보여주는 사례이다. Malware Tech라는 블로그명을 사용하는 22세의 영국소년은 워너크라이 랜섬웨어가 등록되어 있지 않은 특정 도메인 이름에 접속을 시도하는 행동패턴을 발견하였다.[681] 소년은 도메인을 8파운드에 구입하여 이를 다른 서버에 방향변경(redirection)[682]하는 방식으

677) Eric M. Hunchuns, Michael J. Cloppert, Rohan M. Amin, "Intelligence-Driven Compupter Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Lockheed Martin Corporation (2011), pp. 4-5.

678) IT Daily, 2017년 9월 29일, "사이버킬체인 모델을 통한 SIEM의 활용", <http://www.itdaily.kr/news/articleView.html?idxno=85294> (2017.10.18. 최종방문).

679) 김영환, 이수진, *supra* note 670, p. 329.

680) Eric M. Hunchuns, Michael J. Cloppert, Rohan M. Amin, *supra* note 677, p. 5.

681) USA TODAY, May 13, 2017, "How a 22-year-old inadvertently stopped a worldwide cyberattack", <https://www.usatoday.com/story/tech/news/2017/05/13/22-year-old-wannacry-ransomware-malwaretech-analyst-stopped/101637152/> (2017.10.18.최종방문).

682) 표준입력의 입력선, 표준출력의 출력선, 또는 표준 오류 출력선을 변경하는 것. 보통 이들의 입출력선은 단말장치로 되어 있으나 셸(shell)에 대해서 커맨드 시동을 지시할 때 희망하는 것을 지시할 수 있다. 방향 지정을 나타내는 기

로 킬 스위치를 작동시켜 워너크라이 공격[683]은 중단될 수 있었다.[684] 방향변경은 적극적 방어조치 중 수동적 사이버반격으로 분류되는 기법이다. 이후 Marcus Hutchins로 이름이 밝혀진 이 소년은 해킹 테크닉을 독학으로 공부한 것으로 알려졌으며, 현재 영국정부의 사이버보안센터와 함께 일하고 있는 것으로 보도 되었다.[685]

이와 같이 이른바 선의의 해커(ethical hacker)[686]를 활용한 사이버공격 방어전략이 침입테스트와 같은 기법에 의존하는 것보다 효과적이라는 점은 이미 여러 연구를 통해 증명되고 있다.[687] 선의의 해커가 주목을 받는 이유는 피해가 일어나길 기다리는 정보기관의 요원들보다 공격적인 마인드로 사고할 수 있다는 점 때문이다.[688] 이들은 실제 해커들과 같이 사고할 수 있기 때문에 시스템의 취약점을 발견하고, 공격자들의 침입시도를 추적해 이를 완화시키거나 파괴하는 효과적인 조치를 제시한다.[689] 호주

호는 보통 네 종류가 있으며 "<", "< >"은 표준 입력선의 변경, ">"과 "> >"은 표준 출력선의 변경을 나타낸다. ">"는 파일의 선두로부터의 출력을 나타내고 "> >"는 파일에의 추가를 나타낸다. 한국정보통신기술협회 정보통신 용어사전, <http://terms.tta.or.kr/dictionary/dictionaryView.do> (2017.12.21. 최종방문).

683) 사건에 대한 자세한 설명은 제2장 제2절 참조.

684) The Telegraph, May 15, 2017, "IT expert who saved the world from ransomware virus is working with GCHQ to prevent repeat", <http://www.telegraph.co.uk/news/2017/05/14/revealed-22-year-old-expert-saved-world-ransomware-virus-lives/> (2017.10.18.최종방문).

685) *Ibid.*

686) 선의의 해커라고도 번역되며 시스템을 공격하여 알아낸 취약성을 악의적 목적으로 이용하지 않고, 문제점을 알려주기 위해 보안 컴퓨터나 네트워크의 시스템을 공격하는 해커 전문가이다. 한국정보통신기술협회 정보통신 용어사전, <http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=042905-1> (2017.11.9.최종방문).

687) Tracey Caldwell, "Ethical hackers: putting on the white hat", Network Security (2011), pp. 10-11.

688) Tim Watson, "Offensive defence: thinking like a blackhat", Computer Fraud & Security (2009), pp. 5-7.

689) 689) Linkedin, May 31, 2017 - Brian Coventry, "Hack back &

정부 및 다른 정부기관들이 이 점을 인식하고 선의의 해커를 고용하여 함께 일하고 있다는 사실은 이를 방증해 주는 것이라 할 수 있다.[690]

3) 국제법적 문제점

국가들 및 민간기업들이 적극적 방어를 도입하는 것이 문제가 되는 이유는 적극적 방어조치가 여러 측면에서 기존의 법테두리 밖에 위치하기 때문이다. 이 사이버 맥락에서 적극적 방어를 도입하는 것에 대해서 법적 고려가 부족하다는 점은 여러 학자들에 의해 지적되고 있다. 이는 적극적 방어의 도입이 사이버공간에서 허용되어야 하는지에 대해서 법적으로 검토된 바가 없다는 점[691], 적극적 방어조치 도입을 위해서는 여러 가지 국제법적 문제가 고려되어야 한다는 것[692], 기존 법체계를 통해서는 적용이 불가능하기 때문에[693] 새로운 국제법규범의 창설을 통해 법체계 안에서 이를 규율하는 것이 필요하다는 주장[694] 등 다양한 양태로 지적되고 있다.

Counterstrike", <https://www.linkedin.com/pulse/hack-back-counter-strike-brian-coventry> (2017.10.16.최종방문)

690) The Australian, Apr. 24, 2015, "We want people who think like hackers: security head", <http://www.theaustralian.com.au/national-affairs/defence/we-want-people-who-think-like-hackers-security-head/news-story/1b9d3c2eec7a7e8778bd43dabfb4aa5d> (2017.10.18.최종방문); TechRepublic, Jun. 20, 2016, "Ethical hackers: How hiring white hats can help defend your organisation against the bad guys", <http://www.techrepublic.com/article/ethical-hackers-how-hiring-white-hats-can-help-defend-your-organisation-against-the-bad-guys/> (2017.10.18.최종방문).

691) Ruperto P. Majuca and Jay P. Kesan, *supra* note 395, p. 6.

692) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 463; Wyatt Hoffman and Ariel E. Levite, *supra* note 17, p. 34.

693) Ruperto P. Majuca and Jay P. Kesan, *supra* note 395, p. 7.

694) Manny Halberstam, *supra* note 610, p. 207; Dennis C. Blair et al., *supra* note 17, pp. 37-38.

적극적 방어가 내포하고 있는 문제점은 조치의 성격 또는 범위와 관계가 있다. 수동적 방어조치는 공격을 받는 네트워크 내에서만 이루어지기 때문에 국제법 및 국내법적으로 문제가 되지 않는다. 그러나 적극적 방어는 피해자의 홈 네트워크를 벗어나 공격 네트워크에 직접 영향을 미치는 조치를 포함하고 있다.[695]

표2.[696] 적극적 방어조치

강도	조치	내용	범위[697]
Less Aggressive	Honeynets or Honey Pots	의도적으로 취약점을 노출하여 해커를 세그먼트화된 서버로 유인하여 다른 구역으로의 접근을 막는 기술.	Internal Network
	Sandboxes or Tarpits	위협으로 의심되는 밀려드는 트래픽을 늦추거나 멈추는 장벽을 설치하여 정보를 수집, 검증하는 것	Internal Network
	Deception	목표를 위장하기 위해 거짓 데이터를 심거나 유인 네트워크를 만들어 공격흐름의 접근에 혼란을 주는 것	Internal Network
More Aggresive	Sinkholing	악의적인 트래픽을 방어자의 통제 하에 있는 네트워크로 재전송 시키는 것. 공격자가 봇넷을 업데이트하는 것을 막기 위해 가짜 봇넷 클라이언트를 설치하여 감염된 봇들이 방어자가 설치한 네트워크로만	Internal or External Network

695) *Ibid.*, p. 9.

696) Wyatt Hoffman and Ariel E. Levite, *supra* note 17, pp. 8-9; Dennis C. Blair et al., *supra* note 17, pp. 10-11.

		접속하도록 하는 것.[698]	
	Patching(Patch)	공격에 사용하기 위해 감염된 제 3자의 컴퓨터의 취약점에 프로그램의 목적 코드를 변경 하는 등의 임시적인 조치를 취하는 것[699]	External Network
	Beacons	파일에 숨겨진 작은 단위의 소프트웨어 링크로 시스템에 대한 허가 받지 않은 접근으로 해당 파일이 삭제되면 침입한 컴퓨터 시스템과 연결되어 공격 시스템의 구조와 위치 등의 세부사항에 대한 정보를 방어자의 시스템에 전송하는 것	Internal or External Network
	Botnet Takedowns	감염된 C&C 서버 또는 네트워크로부터 멀웨어에 감염된 수많은 컴퓨터들의 연결을 끊는 것.	Internal or External Network
	White-hat Ransomeware	공격자가 이용하는 시스템으로 훔친 정보를 수송하는 제3자 컴퓨터 시스템에 파일을 암호화 하기 위한 목적으로 멀웨어를 침투시키는 것	External Network
	Rescue Missions to Recover Assets	해킹툴을 사용하여 공격자가 사용하는 시스템에 침투하는 것으로 빼앗긴 정보를 고립화하고, 이용불가능하게 만든 뒤 궁극적으로는 다시 회복 시키는 것	External Network
Most Aggressive	Hack Backs	공격자가 공격의 수단으로 사용하는 시스템에 침투하	External Network

		여 도난당한 정보를 회수, 변경, 또는 삭제하는 조치부터 다시 공격에 이용하지 못하도록 해당 시스템이나 네트워크를 손상시키거나 파괴하는 것	

사이버공간이 하나로 연결된 네트워크임을 생각할 때, 적극적 방어조치가 피해자의 네트워크가 위치한 국가의 경계를 넘어가게 되면 해당 조치의 법적 정당성에 대한 의문은 더욱 커지게 된다.[700] 특히 적극적 방어조치가 실제 공격자가 아닌 네트워크상의 공격수단에 대해 취해지는 조치임을 생각할 때, 이는 공격과는 전혀 상관없는 제3국의 네트워크를 허가 없이 접근하는 결과를 초래할 가능성이 크다.[701]

또한 이러한 초국경적 적극적 방어조치의 영향은 단순한 네트워크나 대상 컴퓨터와 공격에 사용되는 서버와의 연결 차단에서부터 서버파괴 또는 바이러스 침투와 같은 역공격까지 다양하게 나타날 수 있다.[702] 이는 실행

---

697) 각 방어조치에 대한 영향 범위는 기본적인 기능을 바탕으로 단순화 한 것이다. 이들 조치의 강도와 영향 범위는 사용하는 방법과 각 기술들의 결합 방식에 따라 다르게 나타날 수 있다. 예를 들어 Honeypot도 그 방법에 따라 공격자의 네트워크에 영향을 미치는 방식으로 사용될 수 있다. Wyatt Hoffman and Ariel E. Levite, *supra* note 17, p. 9.

698) IT World, 2011년 3월 29일, "두번째 켈리호스 봇넷 진압 작전 성공…싱크홀 기법으로 무력화", <http://www.itworld.co.kr/news/74978> (2017.12.4. 최종방문).

699) 한국정보통신기술협회 정보통신용어사전, <http://terms.tta.or.kr/dictionary/searchList.do> (2017.12.4.최종방문).

700) Robert S. Dewar, *supra* note 648, p. 10; Ronald J Deibert, "The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace", in A. Chadwick and P. N. Howard eds., *Routeledge Handbook of Internet Politics*, (London: Routledge, 2009), p. 334.

701) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 463.

702) 이란의 핵시설을 무력화한 스턱스넷 바이러스가 malware 였음을 생각한다면, 역해킹을 통해 공격 근원에 malware를 침투시키는 조치는 공격 근원이

된 방어조치가 조치의 대상에 미치는 강도에 따라 작게는 주권침해에서 크게는 무력사용금지원칙의 위반까지 다양한 국제법 위반문제가 나타날 수 있다는 점을 나타낸다. 특히 추후 공격의 귀속을 밝히는 과정에서 조치의 대상이 제3국이었음이 밝혀지게 되는 경우에는 피해국의 심각한 국제법 위반문제가 발생할 수 있다. 만약 적극적 방어조치가 제3국의 네트워크에 심각한 피해를 야기하지 않은 경우 또는 공격의 심각성이 충분이 입증되는 경우에는 제3국으로부터 문제가 제기되지 않을 수 있으나, 제3국에 중대한 피해를 초래하였을 경우에 역외적 방어조치를 취한 피해국은 이에 대한 국제법상의 책임을 피할 수 없게 된다.

또한 추후 귀속 증명을 통해 적극적 방어조치가 취해진 네트워크와 공격자의 위치가 일치하는 경우에도 공격행위가 국가로 귀속되는지, 조치의 강도에 따라 적법한 대응조치로 정당화될 수 있는지 등의 문제가 제기될 수 있다. 이밖에도 조치가 필요성 및 비례성 원칙을 준수했는지 여부를 알기 위해서는 당시 발생한 공격의 강도와 심각성을 증명해야 하는 복잡한 문제가 발생할 수도 있다. 그러나 공격시 방대한 양의 트래픽이 발생하는 DDoS 공격의 경우에는 공격의 강도와 성격을 파악하는 것이 가능하지만 APT공격의 경우에는 소량의 패킷이 연관되기 때문에 탐지 단계에서 공격의 강도와 성격을 파악하는 것이 쉽지 않아[703] 조치 실행 후 이를 입증하는 것도 결코 쉽지 않다.

무엇보다도 현 국제법체제 내에서는 사이버공격에 대한 정확한 귀속을 밝히기 어렵다는 점을 생각할 때, 추후 귀속의 증명이 불가능한 경우에도 적극적 방어조치가 국제법적으로 또는 정치·외교적으로 문제되지 않고 실행되기 위해서는 이에 대한 적법한 근거를 마련하는 작업이 우선적으로 필요하다.

위치한 공격 탐지국의 다른 네트워크에도 심각한 피해를 초래할 수 있다. Dennis C. Blair et al., *supra* note 17, p. 9.

703) Jeffrey Hunker, Bob Hutchinson, Jonathan Margulies, *supra* note 661, p. 7.

3. 국제법개념과의 비교

‘적극적 방어’ 개념을 새롭게 국제법에 도입해야 하는지 여부를 알기 위해서는 적극적 방어조치가 기존 국제법개념에 포섭되는지, 국제법위반 가능성이 있는 조치들이 국제법상의 위법성 조각사유에 의해 정당화 될 수 있는지에 대한 검토가 필요하다. 이하에서는 각국제법개념에 적극적 방어조치를 대입시켜 보고, 두 개념의 유사점 및 차이점 분석을 통해 적극적 방어조치를 국제법의 규율 하에 두기 위해 필요한 점을 도출해보기로 한다.

1) 공격거점의 추적과 귀속의 차이

적극적 방어개념과 기존 국제법개념의 중요한 차이점은 바로 귀속의 개념이다. 기존 국제법체제 하에서는 위반행위가 국가에게 귀속될 때 이에 대한 대응을 할 수 있다. 자위권의 경우 비국가행위자에게도 행사할 수 있는 것으로 해석되고 있지만[704] 일반국제법 상 영토주권존중의무, 국내문제 불간섭의무, 무력사용 금지의무의 위반주체는 국가만이 될 수 있으며, 이에 따른 대응조치는 행위가 국가에게로 ‘귀속’되어야만 취할 수 있다. 그러나 적극적 방어조치의 실행에는 이러한 귀속의 개념이 적용되지 않는다. 적극적 방어는 사이버공간 상에서 발생한 위협적 흐름 또는 추적된 공격거점에 대해 대응하는 조치이기 때문이다. 적극적 방어가 적이 아닌 공격능력에 대한 조치를 의미한다는 한 연구에서의 정의는 귀속개념과 네트워크상의 공격 포인트와의 차이점을 잘 지적하고 있다.[705] 즉, 적극적 방어조치를 위해 필요한 것은 네트워크상의 공격경로 추적을 통한 공격수단의 파악이지 공격자나 공격자의 물리적 위치 파악이 아니다.[706] 따라서 적극

704) 본 논문 제4장 제2절 2. 비국가행위자 참조.
705) Dennis C. Blair et al., *supra* note 17, p. 10.
706) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 480; William

적 방어의 경우에는 조치를 위해 공격의 실행자를 찾거나 공격행위자의 행위가 국가로 귀속되는지를 밝히는 것이 요구되지 않는다. 때문에 국가만이 조치의 대상이 될 수 있는가 혹은 비국가행위자도 조치의 대상에 포함이 되는가와 같은 문제는 발생하지 않는다.

실제 공격자를 찾아 귀속을 밝히기 위해서는 기술적 부분 외에도 국가정보기관이 제공하는 정보, 추후 조사 및 국가 간 협력이 요구되지만[707], 적극적 방어조치를 취하기 위해 공격에 이용되는 수단을 파악하는 것에는 위협탐지 및 추적을 위한 기술이 요구되는 측면이 강하다. 물론 적극적 방어의 탐지기술을 이용한 공격 흐름의 추적이 사이버공격의 귀속을 밝히는 것과 아무런 관련이 없는 것은 아니다. 제4장에서도 살펴본 바 있지만 이 작업은 사이버공격의 국가귀속성을 밝히기 위한 네 단계 중 두 번째 단계에 속한다. 적극적 방어의 개념을 설명하고 있는 연구들에서도 귀속을 밝히는 데 도움이 된다는 사실을 적극적 방어의 기능 중 하나로 소개하고 있다.[708] 그러나 네트워크상의 공격거점을 파악하는 것이 곧 귀속을 의미

A. Owens, Kenneth W. Dam, and Herbert S. Lin (eds)., *supra* note 662, p. 141; Cameron S. D. Brown, *supra* note 379, pp. 167-168; Dorothy E. Denning and Bradley J. Strawser, "Active Cyber Defense: Applying Air Defense to the Cyber Domain", George Perkovich and Ariel E. Levite Eds, *Understanding Cyber Conflict: Fourteen Analogies* (Georgetown University Press, 2017), p. 193; The New York Times, Jan. 14, 2010, "After Google's Stand on China, U.S. Treads Lightly", <http://www.nytimes.com/2010/01/15/world/asia/15diplo.html> (2017.10.19.최종방문);

707) Kenneth Geers, Darien Kindlund, Ned Moran, Rob Rachwald, *supra* note 321, p. 5; Russell Buchan, Marco Roscini, Nicholas Tsagourias, *supra* note 325, p. 2.

708) Wyatt Hoffman and Ariel E. Levite, *supra* note 17, pp. 10-11; Shane McGee, Randy V. Sabett, Anand Shah, "Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense", Journal of Business & Technology Law, Vol. 8, No. 1 (2013), p. 29; Jeffrey Hunker, Bob Hutchinson, Jonathan Margulies, *supra* note 661, pp. 10-11.

하는 것은 아닌 것이다. 귀속개념과 사이버공간상의 공격거점 파악의 차이를 아는 것은 국제법과 적극적 방어를 개념적으로 비교하는 데 있어 출발점 역할을 한다.

2) 대응 시기와 조치실행 판단기준의 차이

적극적 방어조치가 기존의 국제법개념에 포함되지 못하는 이유는 바로 지금껏 강조한 사전적(proactive) 성격과 관련이 있다. 앞서 검토한 바 있듯 기존 국제법은 기본적으로 위반행위 및 그로 인한 피해가 발생한 후에 대응을 하는 구조로 되어 있다.[709] 책임을 추궁하거나 위반에 대한 조치를 취하기 위해서 국가로의 행위귀속을 입증하는 것도 이러한 구조 안에서 사건이 발생한 후에 이루어지는 작업이다. 반면 적극적 방어조치의 경우, 위협의 탐지 단계에서 또는 목표시스템을 장악 또는 타격하는 공격이 실행되기 전에 실행하는 것을 목표로 하기 때문에 조치의 시기에 있어 차이가 있다.

기존 국제법원칙 하에서는 위반행위 발생 후에 피해국이 위반된 의무에 비례하는 대응을 한다. 즉, 어떤 행위가 발생하면 그 행위가 특정 의무의 위반요건을 충족하는지를 판단하고, 그에 비례하는 조치를 취하게 되는 것이다. 예를 들어 국내문제불간섭의무의 위반여부를 결정하기 위해서는 발생한 행위가 피해국의 주권적 문제에 관한 간섭행위이며, 그 행위가 강제성을 띤다는 요건이 충족되어야 한다. 이에 따르면 발생한 피해를 놓고 위반여부를 판단하게 되므로 공격발생 전 대응을 목적으로 하는 적극적 방어의 개념과는 논리적으로 부합하지 않는다.

적극적 방어조치의 결정은 탐지된 사이버 상의 흐름이 악의적인 성격의 것인지 아닌지(characterizing)를 판단기준으로 하며,[710] 조치시 탐지된

709) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 518.
710) Eric Talbot Jensen, *supra* note 112, pp. 235-236; Kesan and Hayes(2012), pp. 478-479; Y. Xiang, Y. Lin, W.L. Lei and S.J. Huang,

위협이 국제법위반을 구성하는지, 국제법상의 어떤 의무위반에 해당하는 강도인지는 고려대상이 아니다.[711] 사이버 상의 흐름 자체는 중립적인 성격을 띠고 있기 때문에[712] 탐지된 이상흐름의 악의적 성격을 파악하는 것을 넘어 위협이 미칠 최종 강도를 예측하는 것은 적극적 방어단계에서 해야 할 작업이 아니다. 적극적 방어조치의 목적은 탐지한 위협의 즉각적인 차단·저지임을 생각할 때, 홈 네트워크에 멀웨어가 탐지된 경우 적극적 방어단계에서 우선 위협을 제거하고 멀웨어의 기능을 분석하는 작업은 조치 후에 이루어지는 것이 타당하다. 멀웨어의 기능을 분석하는 데는 시간이 소요되기 때문이다.

한편 적극적 방어가 탐지된 위협이나 공격의 실행을 억지하는 것이고, 국제법상의 대응조치나 자위권도 원칙적으로 위반행위 종료 전에 취해져야 한다는 점을 생각할 때, 기존 국제법에 근거한 대응과 적극적 방어에 의한 대응에 있어 조치의 시기가 겹칠 수도 있다. 그러나 이 경우에도 적극적 방어조치의 판단기준은 탐지된 위협의 공격성이며, 공격이 탐지된 단계가 대응조치 또는 자위권 발동 시기와 겹치는 것일 뿐이다. 즉, 적극적 방어는 앞서 제3장 1절에서 검토한 것과 같이 사이버공격이 미친 영향과 피해의 규모로 국제법위반 여부를 판단하여[713] 대응하는 것과는 별개의 조치인 것이다.

"Detecting DDOS attack based on network self-similarity", IEE Proc.-Commun., Vol. 151, No. 3 (2004), p. 292; William A. Owens, Kenneth W. Dam, and Herbert S. Lin (eds)., *supra* note 662, pp. 134-135.

711) 오늘날 대부분의 정교한 사이버공격은 APT 유형으로 진행되기 때문에 위협 탐지시기에 공격의 강도를 예측하는 것은 쉽지 않은 일이다. Jeffrey Hunker, Bob Hutchinson, Jonathan Margulies, *supra* note 661, p. 7.

712) Eric Talbot Jensen, *supra* note 112, p. 235.

713) 본 논문 제3장 제2절 참조.

3) 자위권

적극적 방어는 우선 무력사용에 이르지 않는 다양한 조치들을 아우른다는 점에서 무력대응을 의미하는 자위권과는 차이가 있는 개념이다. 또한 조치의 실행여부도 탐지된 사이버위협이 무력공격에 해당하는지에 따라 결정되지 않는다는 점도 자위권과는 다르다. 그러나 여기에서는 조치의 대상과 관련한 두 개념 간의 차이에 초점을 맞추어 검토하기로 한다.

적극적 방어가 사이버공간 상의 공격거점에 대한 조치라는 점은 발생한 무력공격의 귀속이 명확해야만 원용될 수 있는 자위권 개념과 구별되는 점이라고 할 수 있다. 유엔헌장 제51조에 규정된 자위권은 원용의 주체를 국가로 명시하고 있으나 발생한 무력공격의 주체에 대해서는 명시하지 않고 있다. 이 때문에 무력공격을 행한 비국가행위자에 대해서도 자위권을 행사할 수 있다는 논의가 계속되어 왔는데, 이 논의는 특별히 2001년 알카에다에 의한 9.11 테러를 계기로 더욱 활발하게 이루어졌다.[714] 그러나 이 경우에는 비국가행위자가 주둔하고 있는 국가의 영토주권 침해문제가 제기될 수 있다. 무력공격을 행한 비국가행위자의 주둔 자체만으로 주둔국가가 해당 무력공격에 대한 직접책임을 진다고 볼 수 없기 때문이다.[715] 따라서 이 경우에 자위권 원용국가는 비국가행위자에 대한 자위권 행사와 관련하여 주둔국가의 영토주권 침해문제를 정당화할 수 있는 적법한 근거가 필요하게 된다.

미국은 2001년 당시 국가가 직접 국제테러행위를 하지 않더라도 테러조직을 자국의 영토에 숨겨주거나(habouring) 이들 조직에게 은신처를 제공하는 경우에는 이들 조직의 테러행위가 국가에 귀속된다는 논리로 자위권 행사를 정당화하였다.[716] 미국은 이후에도 2014년 8월 시리아 내의 ISIL에 대한 공습을 실시하면서 시리아가 ISIL에 대해 스스로 효과적으로 대

714) 이에 대해서는 본 논문 제3장 제2절의 2. 비국가행위자 규율방안의 부재 참조.
715) ILC 국가책임 초안 제8조.
716) Kubo Mac̆ak, *supra* note 335, pp. 145-146.

응할 능력도 의사도 없다는(unwilling or unable) 이유로 집단적 자위권을 원용한 바 있다.[717] 미국은 '은닉(harbouring)' 또는 '의사나 능력이 없는'을 비국가행위자 행위자의 무력공격에 대해 주둔국에 직접적으로 책임을 귀속시키는 기준으로 사용하고 있다.[718] 그러나 학자들은 이를 테러 공격에 대해서는 사인의 행위를 국가로 귀속시키는 기준을 낮추어서 국가책임의 범위를 확장시키는 것으로 보거나[719] 자국의 영토가 다른 국가에 피해를 주는 방식으로 사용되는 것을 방지할 일반적 의무, 이른바 상당한 주의 의무[720]에 기한 간접책임에 근거하는 것으로 해석한다. 중요한 것은 비국가행위자에 대한 자위권의 행사가 자위권 행사의 일반적인 요건을 만족시키는 방식으로 적법하게 행사된다면 이 때 발생하는 주둔국가에 대한

717) Letter dated 23 September 2014 from the Permanent Representative of the United States of America to the United Nations addressed to the Secretary-General, UN Doc. S/2014/695 (2014); unwilling or unable doctrine은 미국 외에도 이스라엘, 터키, 러시아 등 여러국가들이 비국가행위자에 대한 자위권 행사를 정당화하는 근거로 사용한 바 있다. 도경옥, "시리아 내 ISIL 공습에 대한 국제법적 분석", 국제법학회 논총(2016), 제1권 제1호, p. 117; UN Security Council, Letter dated 11 September 2002 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, UN Doc. S/2002/1012(2001).

718) UN Security Council, Letter Dated 7 October 2001 From the Permanent Representative of the United States of America to the United Nations Addressed to the President of the Security Council, UN Doc. S/2001/946 (2001).

719) Derek Jinks, "State Responsibility for the Acts of Private Armed Groups", Chicago Journal of International Law, Vol. 83, No. 4 (2003), p. 83; Bruno Simma, Daniel-Erasmus Khan Gerog Nolte and Andreas Paulus (eds.), *supra* note 118, pp. 1418-1419; Michael N. Schmitt, "*Bellum Americanum* Revisited: US Security Strategy and the *Jus Ad Bellum*", Military Law Review, Vol. 176 (2003), p. 400.

720) *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. People's Republic of Albania), I.C.J. Reports 1949*, p. 22: "every State has the obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States".

영토주권의 침해는 용인되는 것으로 해석되고 있다는 것이다.[721]

사이버공격에 대해서도 위와 같은 논리를 적용하여 비국가행위자의 사이버공격행위를 은닉하거나 또는 의사나 능력이 없는 국가에 직접적으로 책임을 귀속시켜 자위권을 행사하거나 이를 방지하지 못한 것에 대해 간접적 책임을 물어 자위권을 행사할 수 있다는 주장이 있다.[722] 이에 따르면 행위의 국가귀속이 증명되지 않더라도 공격이 탐지된 국가에 대해 자위권을 행사할 수 있으므로 귀속이 아닌 공격의 거점에 대해 취하는 적극적 방어조치가 이에 포함된다는 주장이 제기될 수 있다. 즉, 적극적 방어조치의 대상인 공격거점과 타국에 은닉하고 있는 공격주체인 비국가행위자를 같은 선상에 놓고 보는 것이다. 그러나 이와 같은 논리의 적용은 다음과 같은 점에서 타당하지 않다.

첫째, 적극적 방어조치의 대상이 되는 공격의 거점은 대부분 공격주체의 위치를 반영하지 않는다.[723] 따라서 공격에 이용되는 서버나 네트워크를 공격의 주체인 비국가행위자와 같은 선상에 놓고 비교하는 것은 적절하지 않다. 둘째, 앞의 경우 자위권 행사의 대상이 되는 비국가행위자와 주둔국 간의 관련성이 명확하나 사이버공격의 경우에는 대부분 공격의 거점을 구성하는 서버가 공격의 주체와 전혀 무관한 국가에 있기 때문에 서버 위치국과 공격주체의 관련성이 성립되지 않는다. 그럼에도 불구하고, 공격의 해당서버가 위치한 국가에서 공격이 발생한 것은 사실이므로 상당한 주의의무를 적용하여 자위권을 행사할 수 있다고 주장한다면 이는 물리적 공간과 사이버공간의 차이를 이해하지 못한 주장이라고 할 수 있다.

물리적 공간에서 비국가행위자가 미사일을 발사하거나 테러행위를 위한

721) 도경옥, *supra* note 717, p. 115; 도경옥, 비국가행위자의 테러행위에 대한 무력대응, (경인문화사, 2011), pp. 130-153. 해당부분에서는 국가들이 타국의 영토에 주둔하며 테러행위를 자행하는 비국가행위자에 대해 자위권을 행사해 온 국가관행에 대해 검토하고 있다.

722) David E. Graham, *supra* note 335, p. 93; Matthew J. Sklerov, *supra* note 112, pp. 46-48.

723) 사이버공격을 감행하는 대부분의 행위자들은 자신의 위치를 드러내지 않기 위해 다른 지역의 서버를 이용해 공격을 시도한다.

훈련 등을 하는 경우에는 그러한 징후가 드러나기 때문에, 이에 대해서 비국가행위자가 주둔하고 있는 국가가 이에 대해 원조 또는 방조했다고 보는 것은 논리적으로 타당하다고 할 수 있다. 그러나 사이버공간에서는 공격을 위한 비국가행위자의 활동이 명확히 드러나지 않기 때문에, 자국 내의 네트워크에서 공격징후를 포착하는 것이 거의 불가능하다. 감시와 제보가 가능한 영토와 네트워크는 전혀 다른 차원의 공간이다. 따라서 단지 일국의 영토 내 서버나 네트워크에서 사이버공격이 탐지되었다고 해서 해당 국가에 방지의무 위반을 적용하거나 은신처를 제공 혹은 '의사나 능력이 없는'의 기준을 적용하여 자위권을 행사하기에는 정당성이 부족하다. 이는 비국가행위자에 대한 자위권 행사가 비국가행위자의 행위에 대해 소재국의 관여 정도가 클수록 또한 그러한 사실이 국제사회에 광범위하게 인정될수록 영토주권 침해가 용인되는 경향을 통해서도 알 수 있다.[724] 안보리 결의 제1368호는 테러행위자를 원조, 지원 또는 숨겨주는(harbouring) 세력도 책임을 부담한다고 하였으며, 결의 제1373호도 모든 회원국에게 테러조직에게 은신처를 제공하지 않을 의무를 부과하고 있다.[725]

따라서 귀속의 여부를 따지지 않고 우선 파악된 공격거점에 대해 네트워크상의 조치를 취하는 적극적 방어를 자위권 행사로 보는 것은 타당하지 않다. 사이버공격의 경우에 자위권을 행사하기 위해서는 국가로의 행위귀속까지 증명할 필요는 없더라도 적어도 공격주체의 지정학적 위치 파악이 필요하며, 자위권은 공격주체가 위치한 국가의 비국가행위자에 국한해서 행사되어야 한다.[726] 그러나 이 경우에도 공격주체를 찾는 귀속의 문제

---

724) 도경옥, *supra* note 717, p. 115.

725) UN Doc. S/Res/1368(2001); UN Doc. S/RES/1373(2001).

726) 터키는 자위권을 원용하여 이라크내 쿠르드노동당(PKK)에 대해 군사작전을 감행하였으며 공습이 진행된 곳은 이라크 북부 산악지대의 PKK 주둔지에 국한되었다. RUDAW, Aug. 1, 2015, "UN describes Turkish airstrikes against PKK as self-defense", <http://www.rudaw.net/english/middleeast/turkey/01082015> (2017.12.2.최종방문); 미국은 자위권을 원용하여 파키스탄 내의 알카에다 관련자들이 활동하는 지역을 공습하였다. Idaho Statesman, Sept. 27, 2010, "

는 시간이 걸리기 때문에[727], 즉각대응을 의미하는 적극적 방어와 비국가행위자에 대한 자위권 행사의 범위가 겹칠 가능성은 희박하다. 이밖에도 공격주체가 위치한 국가의 협조 없이는 실제 공격자를 찾는 문제부터 쉽지 않다는 점, 실제 공격자의 활동에 대해 국가가 알고 있었는지를 파악해야 하는 문제가 남아있다는 점, 공격이 종료되지 않은 경우에 한해서 자위권을 원용할 수 있다는 점 등 비국가행위자에 대해 자위권을 행사하기 위해서는 물리적 공간에 비해 훨씬 더 복잡한 고려사항들이 존재한다.

4) 예방적 자위권

한편 적극적 방어조치의 사전적(proactive) 성격으로 인해 이를 예방적 자위권(anticipatory self-defense)이 적용된 것으로 보아야 한다는 주장이 있다.[728] 예방적 자위권을 지지하는 입장에서 그 근거로 주장하는 Webster 미 국무장관이 제시한 자위권사용의 정당성 기준에는 급박성의 개념이 포함되어 있다. Webster 장관은 자위권에 대한 necessity는 급박하고, 압도적이고, 다른 수단을 선택할 여지가 없으며 숙고할 시간이 없는 경우에 인정될 수 있고 또한 그 행사가 비합리적이거나 과도하지 않아야 한다고 하였다.[729] 예방적 자위권의 행사가 가능하다고 주장하는 자들은

U.S. defends Pakistan incursion as 'self-defense'", <http://www.idahostatesman.com/news/article40716912.html> (2017.12.2. 최종방문); 러시아는 그루지야 내에서 활동하는 체첸 게릴라들에 대하여 자위권을 원용하여 이들의 주둔지를 공격하였다. UN Doc. S/2002/1012 (2001).

727) Chris Prosise, Kevin Mandia, *supra* note 324, p. 25; David E. Graham, *supra* note 335, p. 91; Eric Talbot Jensen, *supra* note 112, pp. 232-235.

728) Jay P. Kesan and Carol M. Hayes, *supra* note 112, pp. 513-515; Matthew Hoisington, *supra* note 112, p. 451; Walter Gray Sharp, *supra* note 161, p. 130; Eric Talbot Jensen, *supra* note 112, pp. 208-209.

729) Daniel Webster, "A Letter to Lord Ashburton", Department of State, Aug. 6, 1842, 편지 원문은

헌장 제51조에 규정된 자위권은 관습국제법상의 자위권을 성문화한 것에 불과하다고 본다.[730] 따라서 자위권의 관습국제법적 표현으로 널리 받아들여지고 있는 웹스터장관의 기준에 예방적 자위권 개념이 내재되어 있다고 보고, 이를 국제법상 허용되는 권리라고 주장하는 것이다.[731]

적극적 방어를 예방적 자위권의 개념 안에 포섭하는 주장은 바로 이 임박성 기준과 적극적 방어조치의 실행을 연결시켜 해석한다. 사이버공격행위가 전반적으로 무력공격에 이를 것으로 예상되고, 그러한 공격이 임박한 상태에 이르러 피할 수 없는 것으로 판단되는 상황에서 해당 공격을 대항하기 위해 취해진 조치는 예방적 자위권의 행사로 정당화된다는 주장이 이에 해당한다.[732] 또한 한번 실행된 무력공격에 해당하는 사이버공격이 계속적인 성격을 가지고 있다고 판단될 경우에는 이를 가까운 미래에 공격이 "임박한" 것으로 보고, 이에 대한 역공격이 예방적 자위권에 의해 정당화 된다고 해석하는 입장도 있다.[733]

그러나 우선 적극적 방어조치는 임박한 무력공격에 국한하여 취하는 조치가 아니다. 또한 적극적 방어는 앞서 살펴본 바와 같이 어떤 단계에서든 위협이 탐지된 즉시 실행되기 때문에 위협이 어느 단계에 '임박'하기를 기다리지 않는다. 무엇보다도 사이버공격은 미사일 발사와 달리 위협이 탐지된 시점에서 공격의 강도를 예측하기가 거의 불가능하다. 따라서 위의 주장에 따른 "무력공격의 임박성"을 기준으로 적극적 방어조치를 예방적 자위권의 행사로 보기에는 무리가 따른다고 할 수 있다. 앞서 살펴본 바와 같이 적극적 방어조치의 실행 기준은 탐지된 흐름의 위협성 여부이다.

<http://avalon.law.yale.edu/19th_century/br-1842d.asp#web2>에서 확인 가능하다.

730) Condron, *supra* note 381, pp. 412-413; Jay P. Kesan and Carol M. Hayes, supra note 112, p. 514.

731) Malcolm N. Shaw, *International Law*, 7th ed., (Cambridge University Press, 2014), pp. 820, 826; Jason Barkham, *supra* note 112, p. 75.

732) Michael N. Schmitt, *supra* note 112, pp. 932-933.

733) Matthew J. Sklerov, *supra* note 112, p. 36; Jay P. Kesan and Carol M. Hayes, *supra* note 112, pp. 514-515.

이밖에도 예방적 자위권의 행사기준과 관련하여 일부학자는 국가의 주요기반시설 시스템의 침투는 모두 무력사용으로 간주할 수 있기 때문에 이러한 시설에 대한 침투가 감지되는 즉시 예방적 자위권에 기한 조치를 취할 수 있다고 주장하였다.[734] 또 다른 주장으로는 사이버공격에 예방적 자위권을 적용하기 위한 전제조건을 임박한 무력공격이 아닌 국가의 본질적 이익 보호로 확대할 수 있다는 의견이 있다.[735] 그러나 ICJ는 2005년 판결에서 안보이익의 보호를 위한 무력사용은 자위권 행사로 정당화되지 않는다는 점을 분명히 한 바 있다.[736]

또한 예방적 자위권에 대해서는 학자들 간 의견이 분분하고,[737] 국가들의 실행도 일치하지 않기 때문에[738] 아직 이 개념의 인정여부에 대해서 국제사회의 보편적 합의가 이루어 졌다고 볼 수 없다. 따라서 국제법상 확립되지 않은 개념을 사이버공간에 적용하기 위해 더 확대 해석하고 수정된 기준을 제시하는 것은 바람직하지 않다고 본다. 무엇보다도 적극적 방어의 범위와 강도는 공격자에 대한 무력대응에 준하는 조치에 국한되어 있지 않으며, 국가의 주요기반시설에 대한 공격에만 대응하는 개념이 아니

---

734) Eric Talbot Jensen, *supra* note 112, pp. 208-209; Matthew Hoisington, *supra* note 112, pp. 451-453; Daniel M. Creekman, "A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China", American University International Law Review, Vol. 17, No. 3 (2002), pp. 654-655.

735) Walter Gray Sharp, *supra* note 161, p. 130.

736) *Congo (Democratic Republic of the Congo v. Uganda), I.C.J. Reports 2005*, para. 148.

737) Yoram Dinstein, *supra* note 176, p. 203; Matthew C. Waxman, "The Use of Force against States that Might Have Weapons of Mass Destruction", Michigan Journal of International Law, Vol. 31 (2009), pp. 6-7.

738) Eric Talbot Jensen, *supra* note 112, p. 220; The New York Times, Apr. 15, 1986, "Transcript of Address by Reagan on Libya", <http://www.nytimes.com/1986/04/15/world/transcript-of-address-by-reagan-on-libya.html> (2017.10.19.최종방문).

다.[739] 적극적 방어조치를 예방적 자위권의 적용이라고 주장하는 학자들은 적극적 방어조치의 범위와 강도를 사이버공간에서 취할 수 있는 가장 강력한 조치만을 의미하는 것으로 혼동하고 있는 것으로 보인다.

5) 대응조치

국가들이나 학자들은 적극적 방어조치에 관해 이야기하면서 이를 "사이버 상의 공격적 대응조치(offensive cyber countermeasures)"라고 주장하는 것을 종종 볼 수 있다.[740] 우선 적극적 방어조치가 현존하는 사이버 공격의 즉각적인 저지를 위한 것이라는 점에서 위반행위의 중지를 위해 취하는 대응조치[741]와 그 목적 면에서 상통하는 부분이 있다. 또한 적극적 방어조치가 현존하는 위협에 대한 실시간 대응이라는 점에서 위법행위 종료 전에 취해야 하는 대응조치와 시기면에서도 유사한 부분이 있다.

그러나 국제법상의 대응조치는 발생한 위법행위의 심각성과 입은 피해를 고려하여 비례적으로 취하는 조치[742]로 "일국"의 위반행위가 선행된 경우에만 취할 수 있는 조치이다. ILC는 코멘터리에서 국제법위반행위의 존재를 대응조치를 취하기 위한 전제조건이라고 하였다.[743] ICJ도 가브치코보 나지마로스(Gabčíkovo-Nagymaros) 사건에 대한 판결에서 위반행

739) 앞서도 살펴본 바 있듯, 적극적 방어조치는 공격근원을 타격하는 조치만을 의미하는 것이 아니라 공격을 차단하거나 완화하는 조치도 포함하는 개념이다.
740) Oona A. Hathaway, *supra* note 16, pp. 40, 48; Asia & the Pacific Policy Society, Sept. 18, 2017, "The need for clarity in international cyber law", <https://www.policyforum.net/the-need-for-clarity-in-international-cyber-law/> (2017.10.20.최종방문).
741) 2001년 국가책임초안 제49조; Commentaries on Draft articles on Responsibility of States for Internationally Wrongful Acts, in *the Yearbook of the International Law Commission* (2001) vol. II, Part Two, p. 130, para. 1.
742) 2001년 국가책임초안 제51조.
743) *supra* note 741, p. 130, para. 2.

위의 존재를 정당한 대응조치가 되기 위한 조건이라고 확인한 바 있다.[744] 2001년 국가책임초안 제52조 제2항에서는 권리보호를 위해 긴급대응조치를 취할 수 있다고 하면서 제1항에 규정된 불법행위 중단요구 또는 조치의 통고절차를 생략할 수 있도록 하고 있지만[745] 이 경우에도 여전히 국제법위반행위가 먼저 발생해야 한다는 전제조건에는 변함이 없다.

한편 사이버공격의 경우 국제법위반 유무를 공격이 미친 영향에 기해 판단한다는 점을 생각할 때, 적극적 방어조치의 실행 시기는 이보다 앞서는 경우가 많다고 볼 수 있다. 즉, 대응조치는 국제법위반행위가 발생해야 취할 수 있는 것인데 반해, 적극적 방어는 국제법위반행위의 발생을 조건으로 하지 않는다. 적극적 방어조치는 위협이 탐지된 즉시, 그 위협이 피해를 발생시키는 공격에 도달하기 전에 이를 제거하는 것을 최우선 목표로 하기 때문이다. 따라서 적극적 방어조치는 현 국제법의 기준으로 볼 때, 위반이 발생하기 전에 실행되는 경우가 많다. 공격이 실행되고 일정한 피해가 발생하여 국제법위반이 확실한 경우, 공격이 계속해서 진행된다면 이에 대해 취하는 사이버공간상의 조치는 시기상 적극적 방어조치와 사이버 대응조치의 교집합을 형성할 수 있다. 그러나 조치의 시기와 관련해서는 적극적 방어조치의 실행시기가 대응조치의 시기보다 광범위하다고 볼 수 있다.

대응조치는 또한 위법행위가 국가로 귀속되는 경우에 해당 유책국에게만 취할 수 있다.[746] ILC는 코멘터리에서 대응조치의 대상이 국제법을 위반한 “국가”라는 점이 대응조치에 있어 두 번째로 중요한 요소라고 설명하고 있다.[747] 이는 가브치코보 나지마로스 사건에서 ICJ에 의해서도 확인된 바 있다.[748] 대응조치의 대상이 국제법을 위반한 ‘국가’에 국한되는 데

744) *Gabčíkovo-Nagymaros Project (Hungary/Slovakia), I.C.J. Reports 1997*, para. 83.
745) NATO CCD COE, *supra* note 20, p. 37. 탈린매뉴얼에서도 국가책임초안 제52조 제1항의 요건이 절대적인 것은 아니라고 하였다.
746) 2001년 국가책임초안 제22조, 제49조.
747) *supra* note 741, p. 130, para. 4.
748) *Gabčíkovo-Nagymaros Project (Hungary/Slovakia), I.C.J. Reports*

반해, 적극적 방어조치의 대상은 공격 흐름이 포착된 서버나 네트워크 즉, 사이버공간이다. 따라서 대응조치와 적극적 방어는 그 대상에 있어서도 차이가 있는 개념이라고 할 수 있다.

예를 들어 A국이 자국에 대한 사이버공격의 위협을 탐지하여 추적한 결과 위협이 B국 및 C국의 네트워크에서 발생하는 것을 밝혀 해당 네트워크에 대한 적극적 방어조치를 취했다고 하자. 조치를 취하는 과정에서 A국은 공격을 실행한 B국 및 C국의 네트워크가 거대한 봇넷이었음을 알게 되었고, 이후 조사과정에서 실제 공격을 실행한 국가는 D국이었음이 드러났다. 이 때, A국이 B국 및 C국의 봇넷에 대한 테이크다운 조치를 통해 위협을 저지한 것은 적극적 방어조치이다. 만약 A국이 국제법상의 대응조치를 취하려면 그 대상은 D국이어야 한다. 이 경우에는 봇넷 테이크다운 조치 이후에도 D국에 의한 공격이 계속되고 있어야 대응조치를 취할 수 있다.

앞의 시기 부분에서 살펴본 것과 마찬가지로 일정한 피해가 발생한 후에 사이버공격이 탐지되었을 경우, 공격의 흐름이 유포된 봇넷에 대해서 조치를 취할 때, 그 네트워크가 실제 공격 실행국가임이 밝혀진다면 이는 적극적 방어조치와 사이버 대응조치가 일치하는 지점이라고 할 수 있다. 그러나 적극적 방어 단계에서 국가귀속성 여부를 밝히는 것은 어렵다는 것을 생각할 때, 이러한 일이 발생할 가능성은 극히 드물다고 할 수 있다.

또한 국제법상 대응조치는 선행된 위반행위와 같은 의무위반으로 취해져야 한다는 제한이 없다.[749] ILC는 코멘터리에서 “reciprocal countermeasures”라는 용어에 대해 설명하면서, 이는 피해국이 대응조치로서 취하는 유책국에 대한 국제법의무 중단이 유책국이 위반한 바로 그 국제의무이거나 위반된 국제의무와 직접적으로 연관이 있는 의무인 것을 의미한다고 하였다.[750] 대응조치에의 reciprocity 개념 적용은 1985년

1997, para. 83.

749) *supra* note 741, p. 129, para. 5.

750) *Ibid.*

당시 특별보고관 William Riphagen이 제출한 초안 제8조에 관한 코멘터리에서 언급되었다.[751] ILC는 국제법상 대응조치에는 해당개념과 같은 제한이 적용되지 않는다는 점을 분명히 하였다.[752] 즉, 유책국에 대해서 대응조치를 취할 때, 해당 위반행위와 동일하지 않은 분야에서의 의무 위반으로 대응할 수 있는 것이다.[753] 그러나 적극적 방어조치는 그 대상이 지금 현존하는 사이버공간상의 위협이다. 따라서 조치의 대상범위 혹은 분야에 있어서도 두 개념 사이에는 차이가 있다는 것을 알 수 있다.

6) 긴급피난

한편 적극적 방어를 국제법상 위법성 조각사유 중 하나인 긴급피난에 포섭되는 개념으로 이해하는 해석도 있을 수 있다. 이는 긴급피난이 상대방의 위반행위를 전제하지 않으며, 원용 대상이 국가로 제한되어 있는 것도 아니기 때문이다.[754] 따라서 국제법상 위반행위가 발생하기 전에, 국가귀속성이 증명되지 않더라도 대응할 수 있는 적극적 방어 개념과 상당히 유사한 것으로 생각할 수 있다. 이에 긴급피난이 적극적 방어 개념을 포섭할 수 있는지 그 요건을 중심으로 면밀히 검토해 볼 필요가 있다.

2001년 국가책임 초안 제25조에 규정되어 있는 긴급피난의 원용요건을 보면 긴급피난 행위는 1) '중대하고 급박한 위험'으로부터 2) '국가의 본질적 이익'을 보호하기 위해 취하는 3) '유일한' 조치여야 한다.[755] 먼저 국

751) William Riphagen, "the sixth report of the Special Rapporteur on State responsibility", *Yearbook of the International Law Commission* (1985), Vol II. (Part One), pp. 10-11.
752) *supra* note 741, p. 129, para. 5.
753) James Crawford, *State Responsibility: The General Part* (Cambridge University Express, 2014), p. 685. 크로포드는 ILC 코멘터리에서도 제49조와 관련하여 상호주의적인 대응조치(reciprocal countermeasures)와 다른 조치들 간의 구분이 없다고 한 부분에 주목하였다.
754) 2001년 ILC 국가책임 초안 제25조; *supra* note 741, p. 80, para. 2. NATO CCD COE, *supra* note 159, pp. 137-138.
755) 2001년 국가책임 초안 제25조 제1항 a호.

가의 본질적 이익 요건부터 살펴보면 essential interest가 정확히 무엇을 의미하는지는 명확하지 않다.[756] ILC는 코멘터리에서 본질적 이익의 의미는 상황에 따라 달라질 수 있기 때문에 그 의미를 예단하여 규정할 수 없다고 하였다.[757] 탈린매뉴얼 2.0의 전문가들은 국가들이 지정한 주요 국가기반시설이 긴급피난에서 의미하는 국가의 본질적 이익에 해당할 수 있다고 보았다.[758] 그러나 2016년 미국의 민주당 이메일 해킹사건이 미국에 미친 영향을 생각하면 특정시설이나 기관에 대한 사이버공격을 본질적 이익에 대한 위협으로 지정하는 것은 바람직하지 않다. 그보다는 사이버공격의 경우에도 무엇이 국가의 본질적 이익을 구성하는지는 상황에 따라 달라진다고 보는 것이 적절하다.

한편 긴급피난을 원용하기 위해서는 국가의 본질적 이익이 중대하고 급박한 위험에 처해야 한다. ILC는 중대하고 급박한 위험은 단지 감지된 수준이 아니라 객관적으로 규명되어야 하는 것이라고 하였다.[759] ILC는 1980년 긴급피난에 관해 규정하고 있는 잠정초안 제33조[760]를 채택하면서 본질적 이익이 “극도로 중대(extremely grave)”해야 한다고 하였는데, 이는 그러한 위협이 실제 시간(at the actual time)의 이익에 대한 위협을 의미하는 것이라고 하였다.[761] 이렇게 볼 때, “급박한”의 의미가 현재적 의미만을 가지는 것으로 해석될 수도 있는데, ICJ는 가브치코보 나지마로스 사건에서 이에 대해 그러한 위험이 장기적인 관점에서 나타날 것으로 보이는 경우라 하더라도 관련 시점에 확실하게 실현될 것으로 규명할 수 있다면 이는 급박한(imminent) 위험으로 볼 수 있다고 설시한 바 있다.[762] 또한 긴급피난은 국가의 본질적 이익에 대한 중대하고 급박한 위험

---

756) NATO CCD COE, *supra* note 159, p. 135.
757) *supra* note 741, p. 83.
758) NATO CCD COE, *supra* note 159, pp. 135-136.
759) *supra* note 741, p. 83.
760) *Yearbook of the International Law Commission* (1980), Vol. II (Part Two), pp. 33-34.
761) *Ibid,*, p. 49, para. 33.
762) *Gabčíkovo-Nagymaros Project (Hungary/Slovakia), I.C.J. Reports*

을 보호하기 위한 유일한 방법으로서만 원용이 가능하다. 즉, 이러한 위험을 피할 다른 방법과 수단이 있다면 긴급피난 원용 요건을 충족할 수 없는 것이다.

이를 사이버공격에 대해서 적용해 보면, '중대하고 급박한'의 요건을 만족시키기 위해서는 단지 위협의 탐지만으로는 긴급피난에서 요구하는 수준의 위험이 규명된 것으로 보기 힘들 것으로 보인다. 즉, 공격성을 내포한 위협이 네트워크상에 존재한다는 이유만으로 긴급피난을 원용한 조치를 취하기는 힘들 것이라는 얘기다. 이는 긴급피난의 원용이 부정형으로 규정되어 있고, 상당히 높은 원용요건을 제시하고 있다는 점을 고려할 때, 논리적으로 타당한 해석이라고 할 수 있다. 이러한 엄격성은 다른 위법성 조각사유들의 경우 위법성이 조각된다는 표현으로 규정되고 있는데 반해, 긴급피난은 위법성을 조각하는 사유로 원용될 수 있다고 규정한 데서도 추론할 수 있다.[763] ILC 및 ICJ도 긴급피난은 매우 예외적인 경우에만, 드물게 인정될 수 있는 것으로 보았다.[764] 따라서 감지된 위협이 국가의 본질적 이익에 중대한 영향을 미칠 가능성-국가 네트워크에 침입한 바이러스가 파괴적인 성격을 가지고 있거나 심각한 기능장애를 일으키는 수준의 것[765]-을 증명할 수 있을 때 해당요건을 만족시킬 수 있을 것으로 보인다. 예를 들어 목표 네트워크에 침투하여 장기간 잠복하면서 공격을 실행하는 스턱스넷의 경우, 바이러스의 파괴적인 성격과 향후 침투한 네트워크에 미칠 영향을 증명한다면 중대하고 급박한 위험의 요건을 충족할 수 있을 것이다. 또한 이 경우에는 이미 침투한 바이러스에 대해 조치를 취하는 것 밖에는 위험을 제거할 다른 방법이 없으므로 유일한 방법의 요건도 충족하게 된다.

이제 긴급피난의 요건에 비추어 적극적 방어 개념이 이에 포섭될 수 있

1997, para. 54.

763) 2001년 국가책임초안 제20조-제25조.

764) *supra* note 741, p. 80, paras. 1, 2 ; *Gabčíkovo-Nagymaros Project (Hungary/Slovakia), I.C.J. Reports 1997*, para. 51.

765) NATO CCD COE, *supra* note 159, p. 136.

는지를 살펴보면 우선 적극적 방어조치는 국가의 본질적 이익이 중대하고 급박한 위험에 처했을 때만 취하는 조치가 아니다. 적극적 방어조치의 실행 기준은 탐지된 흐름의 위협성이지 그 위협의 중대성이 아니기 때문이다. 또한 조치의 실행 시 탐지된 위협이 국가의 본질적 이익에 해당하는지는 고려대상이 아니기 때문에 적극적 방어조치가 오히려 긴급피난의 경우보다 조치 실행을 위한 위협의 한계점(threshold)이 낮고, 광범위하다고 볼 수 있다. 물론 적극적 방어조치를 실행할 때에도 긴급피난의 경우와 같이 위협의 존재에 대한 규명이 필요하다. 그러나 이는 위협의 탐지를 증명하는 것이지 그 위협의 중대성을 증명하는 정도는 아니라는 점에서 차이가 있다.

또한 적극적 방어조치에는 탐지한 위협을 홈 네트워크에서 차단시키는 수동적 반격도 포함되어 있기 때문에 원칙적으로 국제법위반행위에 해당하지 않는 조치도 포괄한다. 그러나 긴급피난은 대상위험보다 덜 심각하고 위급한 국제의무를 불이행하는 조치이다.[766] 따라서 일부 적극적 방어조치가 긴급피난에 해당할 수는 있어도 광범위한 적극적 방어의 개념을 모두 포섭할 수는 없는 것이다.[767]

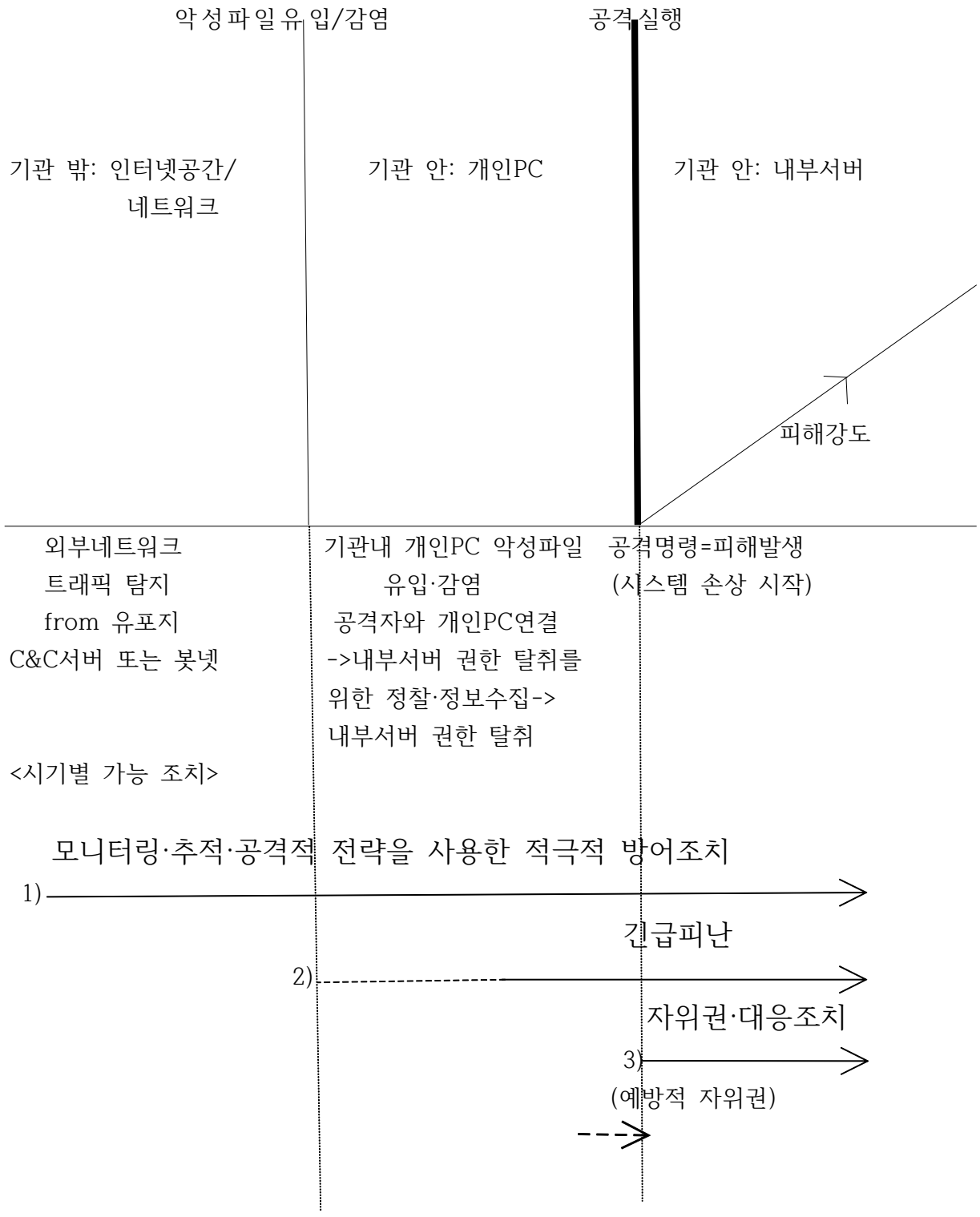
7) 적극적 방어개념의 국제법적 적용

이상과 같이 적극적 방어의 개념과 기존의 국제법개념과의 비교를 통해 두 개념이 겹치는 부분도 있으나 시기와 요건 부분에서 차이가 있다는 점을 확인하였다. 적극적 방어가 기존 국제법에 포섭될 수 없는 부분이 존재한다는 점은 적극적 방어조치가 가지는 위법성이 국제법의 틀 내에서 정당화되기 위해서는 앞서 살펴본 국제법원칙의 요건을 완화·수정하여 적용하거나 기존 국제법원칙에 대한 확장해석이 필요함을 의미한다. 이하에서

766) *supra* note 741, p. 80, para. 1.
767) Dorothy E. Denning and Bradley J. Strawser, *supra* note 706, p. 193.

는 일반적인 사이버공격 과정에 적극적 방어와 국제법개념을 직접 대입해 보면서 적극적 방어개념의 국제법적 적용에 있어 가장 효과적인 방법을 도출해보기로 한다.

그림 4. APT 공격의 예: 목표-기관 내 운영시스템 손상/공격과정:①유포지 획득 ②개인 PC내 악성파일 유입, 감염 ③공격자와 개인 PC연결 ④ 개인 PC 정찰, 정보수집=>내부서버권한 탈취 ⑤ 공격실행



(1) 자위권과 대응조치의 확대적용가능성

그림은 최근 가장 빈번하게 일어나고 있는 사이버공격의 유형인 APT공격의 과정을 단면적으로 표현한 것이다. 지능형지속형 공격의 특징은 곧바로 공격을 개시하지 않고, 공격목표를 달성하기 위해 오랜 기간 동안 정찰 및 정보수집을 한다는 것이다. APT공격은 불특정 다수의 네트워크를 목표로 한 무차별 공격이 아니라 기관 또는 기업의 시스템을 목표로 하기 때문에 목표 달성을 위해서는 내부서버의 권한 탈취가 필요하다. 내부서버에 대한 권한을 획득해야만 기관이나 기업의 시스템을 통제할 수 있고, 공격을 실행할 수 있기 때문이다. 공격자는 이를 위해 유포지, 즉 공격의 거점-C&C 서버나 봇넷-을 마련하고 이를 통해 악성파일을 유입시킴으로써 기관 내 개인 컴퓨터에 침투를 시도한다. 이때 유포지에 해당하는 C&C서버는 공격자가 공격을 위해 탈취한 서버일 수 있다. 이는 곧 C&C서버나 봇넷 모두 공격에 이용하기 위해 공격자에 의해 미리 해킹된 수단에 불과함을 의미한다.[768] 다음으로 개인 컴퓨터가 악성파일에 감염되면 공격자는 이를 이용해 내부 시스템에 침투하기 위해 개인컴퓨터를 정찰하며 정보를 수집하여 비밀번호를 대입해보는 등의 작업을 하게 된다. 마침내 비밀번호를 알아내 내부서버에 접속할 수 있게 되면 공격자가 원하는 때에 공격명령을 내리고 시스템손상 즉, 피해가 발생하기 시작하는 것이다.

국제법위반을 구성하는 사이버공격의 최소한계가 시스템에 대한 통제권 획득 후 취하는 조치임을 생각하면[769] 국제법위반에 해당하는 공격시점은 위 그림에서 굵은 선으로 표시된 부분이 된다. 기관 내 개인 컴퓨터에 대

768) Felix Leder, Tillmann Werner and Peter Martini, *supra* note 49, pp. 213, 224

769) 그러나 시스템에 대한 통제권 획득 및 백도어 설치와 같은 조치를 주권위반으로 보는 시각은 영토주권의 원칙을 상당히 넓게 해석하는 입장으로 이에 동의하는 국가들 및 학자들이 많지 않다는 점에서 이 기준이 국제법위반의 최소한계로 인정받을 가능성은 낮다고 볼 수 있다. 백도어를 설치하는 행위자체가 시스템 작동에 영향을 끼치는 것은 아니기 때문이다. 본 논문 제3장 제1절 주권평등의 원칙 참조.

한 바이러스 감염은 일상적으로 발생하는 흔한 현상이기 때문에 이를 국제법위반에 해당하는 공격으로 보기에는 무리가 있다.

따라서 시기상 탐지된 위협적 흐름에 대해 자위권이나 국제법상의 대응조치가 정당화 될 수 있는 시점은 피해발생이 시작된 시점[770]이라고 볼 수 있다. 그러나 사전적 대응[771]을 목적으로 하는 적극적 방어는 외부네트워크에서 악의적 트래픽이 탐지된 단계에서도 추적을 통해 봇넷에 침투하여 조치를 취하거나 봇넷 조사를 통해 C&C서버에 침투하여 역해킹을 시도하는 등의 조치를 취한다.[772] 이는 시기상으로 국제법이 허용하는 것보

---

770) Derek Bowett, "Reprisals Involving Recourse to Armed Force", Americal Journal of International Law, Vol. 66 (1972), p. 3; 2001년 ILC 초안 제49조.

771) 불특정다수의 웹사이트 모니터링을 통해 봇넷과 C&C서버를 탐지하는 방법, 인터넷 트래픽 스캐닝, 네트워크 접속 유형·C&C서버와의 통신 분석, 앤드포인트 로그 모니터링 등의 지능적 탐지기법 사용을 통해 그림의 1)번 및 2)번 구간에서의 조치가 가능하다. Basil AsSadhan, Jose´ M.F. Moura, "An efficient method to detect periodic behavior in botnet traffic by analyzing control plane traffic", Journal of Advanced Research, Vol. 5 (2014), pp. 435-436; Felix Leder, Tillmann Werner and Peter Martini, *supra* note 49, p. 222 ; Felix Leder, Tillmann Werner, "Know Your Enemy: Containing Conficker", Honeynet Project (2009), pp. 1, 22; 조강유·장대일·김민수·정현철·노봉남, "트래픽 프로파일링 방법을 통한 봇넷 탐지기법", 한국정보기술학회 논문지, Vol. 9, No. 9 (2011), pp. 83-93; 보안뉴스, 2008년 6월 24일, "네트워크위협의 중심 최신 봇넷의 이해와 방어", <http://www.boannews.com/media/view.asp?idx=10412> (2017.12.29.최종방문); IT Daily, 2017년 12월 1일, "APT 대응 솔루션, 통합이 답이다", <http://www.itdaily.kr/news/articleView.html?idxno=86304> (2017.12.29. 최종방문).

772) 봇넷 테이크 다운조치는 봇넷 자체에 조치를 취하는 경우와 봇넷 조사를 통해 C&C 서버를 추적해 들어가 C&C 서버 내에서 봇넷과의 연결을 끊는 조치로 나눌 수 있다. 봇넷 자체에 조치를 취하는 경우에는 악의적인 트래픽 탐지를 역추적하여 봇넷으로의 침투, 심겨진 멀웨어를 해부하고 제거하는 과정에서 내부 데이터를 수색하는 작업이 수반되며, 시스템을 무력화할 수도 있다. C&C 서버를 추적하여 침투하는 경우에는 서버에 대한 완전한 통제권을 획득하기 위해 서버의 취약점 이용, 시스템의 통신망 파괴 행위인 루트킷 설치 등이 수

다 훨씬 앞선 시점에서 조치를 취하는 것이다. 게다가 이들 조치는 그 자체로 대상 컴퓨터의 하드웨어를 파괴하거나 서버 시스템에 손상을 초래할 수 있다는 점에서 국제법위반의 문제가 발생할 수 있다.[773]

이렇게 볼 때, 그림에서 굵은 선으로 표시한 부분은 시스템에 대한 최소한의 손상이 시작되는 시점이기 때문에 공격의 강도나 위반행위 발생의 요건을 완화한다고 해도 굵은 선 앞부분에 대한 조치를 자위권이나 대응조치를 적용해 정당화하기는 어렵다고 볼 수 있다. 이는 비례성 요건을 생각할 때 더욱 분명해진다. 자위권을 원용하거나 대응조치를 취하기 위해서는 비례성 원칙의 준수가 요구된다. 먼저 자위권과 관련해서는 원용국의 무력사용이 대상국의 위반 또는 무력공격의 저지 및 격퇴라는 목적을 달성하기 위해 행사된 경우에만 비례성을 충족하는 것으로 보고 있다.[774] 또한 예방적 자위권이 허용된다고 가정하더라도 이는 무력공격이 일어나는 것을 저지하기 위해서 행사되어야 한다.[775]

즉, 자위권에 대한 비례성 원칙은 위반행위의 강도가 아니라 방어 및 저지라는 목적에 비례해야 한다는 점에 초점이 맞춰져 있고, 또한 동시에 상대방의 무력공격[776] 또는 임박한 무력공격이라는 전제조건이 포함되어 있

반되는데 이러한 과정은 역해킹에 해당한다. Christian Czosseck, Gabriel Klein, Felix Leder, *supra* note 43, pp. 115-118; 루트킷은 해커가 설치한 악성코드가 백신이나 PC 사용자에게 발각되지 않도록 숨겨주는 역할을 한다. 대부분의 루트킷은 일반 프로그램이 동작하는 계층보다 더 하위 계층, 즉 커널이라는 운영체제 핵심 부분에 숨어서 동작하여 탐지가 어렵다. 한국정보통신기술협회, “정보보호기술용어”, 한국정보통신기술협회 (2013), p. 24.

773) Dennis C. Blair et al., *supra* note 17, p. 26.

774) Christine Gray, *International Law and the Use of Force*, 3rd ed. (Oxford University Press, 2008), p. 150; Derek Bowett, *supra* note 770, p. 3; *Yearbook of the International Law Commission* (1980), Vol. II (Part One), p. 69, para. 121: Yoram Dinstein, *supra* note 176, pp. 262-263.

775) YILC, *supra* note 774, p. 69, para. 121.

776) *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986*, para. 176; *Oil Platforms (Islamic Republic of Iran v. United States of America), I.C.J Reports 2003*, para. 77; *Congo (Democratic Republic of the Congo v.*

음을 알 수 있다. 그러나 그림의 굵은 선 앞부분의 단계에서는 무력공격에 달하는 사이버공격이 발생할 가능성을 예측하는 것이 불가능하다는 점, 이에 따라 무력공격을 격퇴할 목적으로 취한 조치라는 것이 인정될 수 없다는 점에서 이 단계에서의 적극적 방어조치를 자위권 행사로 볼 수는 없는 것이다.

한편 ILC 초안 제51조에서는 대응조치가 국제위법행위의 심각성을 고려하여 입은 피해에 비례해야 한다고 규정하고 있다. 이에 위반과 피해의 판단 기준을 아주 광범위하게 확대해석하여 개인 컴퓨터의 바이러스 감염을 국제법위반 및 이로 인한 피해발생으로 본다고 해도 이 단계에서 취하는 봇넷 테이크 다운이나 역해킹은 입은 피해를 초과하는 조치가 된다. 따라서 요건을 완화하거나 확대한다고 해도 대응조치로 적극적 방어조치를 정당화하기에는 한계가 있는 것이다. 더구나 기관 밖 네트워크 단계에서 취하는 조치는 요건을 완화하는 경우에도 대응조치의 범위에 해당될 수 없다. 이는 자위권의 경우에도 마찬가지다.

또 한 가지 문제점은 귀속과 관련된 것이다. 조치의 대상인 봇넷과 C&C서버가 공격자에 의해 장악된 사이버공격의 또 다른 피해자[777]라는 점이 문제가 될 수 있는 것이다. 적극적 방어조치로 인해 피해를 입는 대상이 공격의 의도나 기여도가 없는 제3자일 가능성이 높기 때문이다. 따라서 적극적 방어조치는 많은 경우 공격자에 대한 직접적인 조치가 아니라 공격자로부터 공격 수단을 빼앗거나 공격경로를 방해하는 역할을 한다.[778] 그러나 국제법상 대응조치는 제3국을 상대로 취할 수 없고, 자위권 원용의 경우에는 해킹된 서버에 무력사용에 이르는 강도의 조치를 취할

Uganda), I.C.J. Reports 2005, para. 147.

777) Irving Lachow, *supra* note 17, pp. 4-5.

778) 공격자에 대한 직접적인 조치는 정확한 귀속증명을 통해 공격자를 찾아 처벌 등 법적 조치를 하는 것이다. Bank Info Security, Jun. 3, 2014, “Botnet Takedown: A Lasting Impact?”, <https://www.bankinfosecurity.com/malware-takedown-lasting-impact-a-6903> (2017.12.20.최종방문)

경우 더욱 심각한 문제가 발생할 수 있다.

다만 위반의 발생이 확실하고, 피해가 이미 상당히 진행된 경우에는 귀속이 확실하지 않더라도 피해국이 취한 조치의 강도에 따라 대응조치 또는 자위권을 통해 적극적 방어조치가 정당화될 수 있는 가능성을 열어두어야 한다는 주장이 제기될 수 있다. 이 경우는 그림에서 굵은 선의 뒷부분에 해당한다. 이 때 취한 적극적 방어조치가 대응조치 또는 자위권에 포함되기 위해서는 조치대상국에게 먼저 연락을 취하거나 확인을 하는 절차가 선행되어야 하고, 동 절차 후에도 위협 탐지국에서 조치를 취하지 않는 경우에는 공격국가로 간주한다는 요건을 설정하여 귀속 요건을 대체하는 방법이 제시될 수 있다.

이러한 대체요건이 받아들여지기 위해서는 기존의 귀속요건에 대한 상당한 완화 또는 수정이 필요하다는 점에서, 또한 즉각적 조치를 목적으로 하는 적극적 방어조치의 특성상 상대방에게 연락을 취하고, 기다리는 절차가 비효율적일 수 있다는 점에서 적용가능여부는 불확실하다고 볼 수 있다. 이는 위협이 탐지된 봇넷이나 C&C 서버에 조치를 취하는 데는 신속성이 요구되기 때문인데, 공격자가 적극적 방어조치를 감지하고 방어조치의 명령을 거절하도록 미리 새로운 명령을 내릴 수 있기 때문이다.[779] 이 경우에는 방어조치가 효과를 발휘할 수 없다. 또한 연락을 취한 후 조치를 취하는 시간이나 조치의 정도 등 양 국간의 입장차가 생길 수 있기 때문에 이와 같은 요건을 적용하는 데 있어 국가들의 반발이 예상된다.[780]

(2) 긴급피난의 확대적용가능성

이렇게 시기 및 조치의 대상, 그리고 선 위반행위의 발생문제를 고려해

779) Christian Czosseck, Gabriel Klein, Felix Leder, *supra* note 43, p. 115; Felix Leder, Tillmann Werner and Peter Martini, *supra* note 49, pp. 223-224.
780) Ibid., p. 224.

볼 때, 그림의 기관 밖 및 기관 안 개인컴퓨터에 대한 악성파일 감염시 유포지에 대해 취하는 조치를 정당화하기에 가장 적절한 개념은 상대방의 위반행위나 귀속을 전제로 하지 않는 긴급피난이라고 할 수 있다. 따라서 이하에서는 긴급피난의 적용요건 완화나 확대해석을 통해 적극적 방어조치가 내포하는 위법성을 정당화 할 수 있는지에 대해 검토해보기로 한다.

상대방의 위반행위를 전제로 하지 않는 긴급피난이 원용되는 경우에는 조치 시기가 좀 더 앞당겨 질 수 있다. 그림에서 실선으로 표시한 긴급피난의 원용시기를 기관 내 컴퓨터에의 악성파일 유입 중간쯤으로 잡은 것도 이러한 이유에서다. 그러나 그림에서 2)번 화살표가 시작되기 전 부분에 대해서는 긴급피난의 원래 요건을 적용해서는 원용이 인정되기 어려울 것으로 보인다. 기관 밖 외부네트워크에서 악의적 트래픽이 탐지된 단계까지 국가의 본질적 이익에 중대하고 급박한 위험이 발생한 것으로 볼 수는 없기 때문이다. 이는 그림에서 침투 전 및 공격실행 전 단계에서의 적극적 방어조치가 국제법원칙 안에서 정당화되기 위해서는 “국가의 본질적 이익에 대한 중대하고 급박한 위험 발생”의 요건이 상당히 완화되거나 수정되어야 함을 의미한다.

긴급피난의 확대적용을 위해서는 “본질적 이익에 대한 중대한 위반” 요건 외에도 여러 가지 고려되어야 할 사항이 있다. 먼저 긴급피난은 대상 위험보다 덜 심각하고 위급한 국제의무를 불이행하는 조치라는 점을 검토한 바 있다. 그림의 2)번 실선 화살표 앞부분에서의 조치는 사실 탐지된 위협에 비해 더 심각한 위반을 구성할 가능성이 높다. 이 문제는 특히 기관 내 침투 전 단계에서 발생할 가능성이 높다. 이 단계에서 취한 봇넷 테이크다운 조치가 감염된 멀웨어만을 제거하는 수준으로 진행되었다고 해도 조치과정에서 기밀정보 열람 및 데이터 삭제가 수반되거나 조치대상을 완전히 파괴할 수 있기 때문이다.[781] 이 때 봇넷 수색과정에서 발생한 기

781) Christian Czosseck, Gabriel Klein, Felix Leder, *supra* note 43, pp. 115-118; 실제로 Kraken이라는 이름의 봇넷의 네트워크에 침투하여 해당 봇넷의 통신프로토콜을 위조, 감염된 봇들이 공격자의 명령을 수행하지 못하도록

밀정보 열람이나 데이터 삭제 행위는 위협의 제거가 목적이었다는 이유로 조치대상국으로부터 양해를 받고, 피해를 보상하는 정도로 넘어갈 수도 있다. 이때는 위법성 조각사유 중 동의가 적용된 것으로 볼 수도 있다. 국가책임 초안 제45조에서는 이러한 동의가 사후에도 부여 가능한 것으로 규정되어 있다. 그러나 조치대상국이 라이벌 국가 혹은 적대적 관계의 국가일 경우에는 조치에 대한 동의보다는 오히려 조치국의 위법행위에 대한 책임문제가 발생할 가능성이 더욱 높기 때문에 문제가 되는 것이다.

또한 봇넷 조사를 통해 C&C서버에 침투하여 이로부터 봇넷과의 연결을 끊는 조치시 해당 C&C서버가 제3국의 주요기반시설 운영서버를 해킹한 경우라면 조치 자체로 심각한 국제법위반문제가 발생할 수 있다. 서버와의 연결 차단만으로도 시스템 운영에 큰 피해를 야기할 수 있기 때문이다. 이는 명백히 대상위험보다 더 심각한 국제의무의 불이행에 해당할 뿐 아니라 긴급피난 행위가 상대 국가의 본질적 이익을 심각하게 해하는 경우가 될 수 있다. ILC초안 제25조 제1항 b호에서는 이 경우 긴급피난을 원용하여 위법성을 조각시킬 수 없다고 규정하고 있다.

그러나 사이버공격의 수단으로 사용되는 봇넷 운영의 특성을 고려할 때, 예외적으로 2)번 구간에 점선으로 표시된 부분, 즉 기관내 개인 PC로의 악성코드 침투시기에 취하는 적극적 방어조치도 긴급피난으로 인정될 수 있는 경우를 생각해 볼 수 있다. 봇넷은 C&C 서버와의 통신에 암호화된 트래픽이 사용되거나 자주 업데이트 되는 등 탐지기법을 우회하는 기술의 이용 때문에 완벽한 탐지가 어렵다는 특성이 있다.[782] 이렇게 존재하는 모든 봇넷을 제거하는 것은 불가능하기 때문에 같은 유형의 봇넷이 다시 공격에 사용되는 경우가 나타날 수 있는 것이다. 이 경우 조치를 취하려는

하는 테이크다운 조치를 취할 때, 조치대상 시스템을 파괴할 가능성과 관련하여 논란이 인 바 있다. ITProProtal, Apr. 28, 2008, “Kraken Botnet Infiltration”, <https://www.itproportal.com/2008/04/28/kraken-botnet-infiltration/> (2017.12.29.최종방문).

782) Basil AsSadhan, Jose´ M.F. Moura, *supra* note 771, p. 436.

국가가 이전에 해당 봇넷의 공격에 의해 인명피해나 기반시설에 대한 중대한 시스템 손상 등의 피해를 입은 바 있다면 이에 대해 2)번의 점선 구간에서 취한 조치도 긴급피난으로 인정될 가능성이 있다. 이는 이 전의 공격 강도 및 피해에 근거하여 해당 봇넷에서 탐지된 흐름이 장기적으로 국가의 본질적 이익에 대한 중대하고 급박한 위험을 구성할 것이라는 사실을 충분히 입증할 수 있는 것으로[783] 볼 수 있기 때문이다.

실제로도 이와 유사한 경우가 발생한 바 있는데, 2009년 Conficker 바이러스를 확산하는 봇넷에 대한 테이크다운 조치가 취해진 후[784] 2016년에도 콘피커 봇넷이 직원에 대한 이메일 피싱 등을 통해 병원시스템에 대한 공격시도를 한 것이 밝혀진 것이다.[785] 2009년 당시 해당 봇넷은 병원 시스템 및 장비를 목표로 한 바 있는데, 이로 인한 인명피해는 발생하지 않았었다.[786] 비록 해당 봇넷의 공격으로 인한 중대한 피해가 발생하지는 않았었으나 병원장비에 대한 공격시도는 환자의 생명에 중대한 영향을 미칠 수 있기 때문에 이 경우에 취하는 적극적 방어조치는 비록 기관내 개인 컴퓨터 침투 단계에서 실행되더라도 긴급피난으로 인정될 가능성이 충분히 있다고 볼 수 있다.

이를 종합하면 같은 봇넷의 재공격으로 그림의 2)번 점선 구간이 긴급

---

783) *Gabčíkovo-Nagymaros Project (Hungary/Slovakia), I.C.J. Reports 1997*, para. 54. ICJ는 긴급피난 원용시 특정 위험이 당장에 발생하지 않더라도 장기적으로 실현될 것임이 확실하다는 점을 규명할 수 있다면 "급박한"의 의미를 충족하는 것으로 볼 수 있다고 설시한 바 있다.

784) Hadi Asghari, Michael Ciere, and Michel J.G. van Eeten, "Post-Mortem of a Zombie: Conficker Cleanup After Six Years", 24th USENIX Security Symposium (2015), p. 1.

785) ThreatPost, Jun. 30, 2016, "Conficker used in new wave of hospital IOT device attacks", <https://threatpost.com/conficker-used-in-new-wave-of-hospital-iot-device-attacks/118985/> (2017.12.29.최종방문).

786) Physorg, Apr. 30, 2009, "Conficker worm hits hospital devices", <https://phys.org/news/2009-04-conficker-worm-hospital-devices.html> (2017.12.29.최종방문).

피난으로 인정될 수 있는 경우를 제외하고는 2)번의 실선 화살표가 시작되는 부분부터 긴급피난이 인정된다고 볼 수 있다. 따라서 일반적인 경우 2)번의 실선 화살표 앞부분에 대한 적극적 방어조치에 긴급피난을 적용하기 위해서는 '중대하고 급박한'의 의미가 상당히 완화되어야 하고, 국가의 본질적 이익을 구성하는 대상의 범위가 확대되어야 한다. 또한 원용주체와 관련해서도 긴급피난에 한해서 국가의 행위로 귀속되는 경우의 범위를 기존의 경우보다 광범위하게 보고, 조치의 강도와 위협의 정도를 평가하는 기준도 유연하게 적용되어야 하는 등 긴급피난의 원용을 위한 요건과 제한사항의 전반적 수정이 불가피하다. 그러나 적극적 방어조치의 판단 기준이 위협의 탐지 하나임을 생각할 때, 긴급피난의 원용을 위한 많은 요건들이 이와 같은 수준으로까지 수렴될 수 있을지는 의문이다. 더구나 긴급피난이라는 개념 자체가 예외적인 경우에만 드물게 인정될 수 있는 위법성 조각사유라는 점을 생각할 때, 모든 범위의 사전적인 적극적 방어조치를 긴급피난의 개념으로 포용하기에는 한계가 있다는 것을 알 수 있다.

(3) 소결

결론적으로 국제법개념을 확대 적용하여도 그림의 1)번과 2)번 사이의 구간에서 취하는 적극적 방어조치를 어떻게 규율할 것인지의 문제가 남게 된다. 따라서 이 부분에 대한 국제법적 규율 방안에 대한 논의가 필요하다고 할 수 있다. 이에 대해 발생한 위협에 대한 대응의 시기를 위반발생 시기보다 앞당긴다는 점과 실제 행위자를 밝히지 않고 공격의 거점에 조치를 취한다는 점 때문에 적극적 방어 개념의 도입을 국제법체제에 큰 변형을 가져오는 것으로 생각할 수 있다.

그러나 국제법이 위법성 조각사유를 인정하는 이유와 방식을 고려하면 적극적 방어 개념의 도입이 국제법에 결코 큰 변화를 초래하는 것이 아님을 알 수 있다. 국제법이 자위권, 대응조치, 긴급피난 등의 위법성 조각사유를 인정하는 이유는 합법적인 행위의 범위 내에서 자국을 보호하거나

자국의 이익을 지킬 수 없는 예외적인 상황이 존재함을 인정하기 때문이다. 또한 이 경우에도 필요성 또는 비례성의 원칙과 같은 행사요건을 규정한 이유는 위법한 행위가 가지는 위험성을 제한할 필요가 있기 때문이다.

적극적 방어 개념의 도입이 필요한 이유와 규율 방식도 이와 다르지 않다. 그림의 1)번과 2)번 구간 사이의 시기에 적극적 방어조치를 취하는 것이 필요한 이유는 공격의 실행과 결과발생의 간격이 0이라는 사이버공격의 특성 때문이다. 또한 해당 조치가 우선적으로 파악된 공격거점을 대상으로 하는 이유도 실제 공격행위자를 숨기고 위협행위를 실행하는 여러 개의 공격의 수단을 둘 수 있는 사이버공간의 특성 때문이다. 한편 적극적 방어조치도 강도에 따른 위험성을 내포하고 있기 때문에 필요성과 비례성 원칙을 통한 제한이 필요하다.

이렇게 볼 때, 적극적 방어 개념의 도입은 국제법 내 위법성 조각사유의 존재와 같은 맥락에서 이해될 수 있는 것이다. 따라서 국가들이 사이버공격의 특성에 대한 이해를 바탕으로 적극적 방어조치의 필요성에 합의할 수 있다면 이 개념의 국제법 내 수용은 그리 어려운 작업이 아니다.

제2절 새로운 체제 구축을 통한 사이버공격 억지

1. 다자조약체제를 통한 규율의 필요성

사이버공격을 국제법으로 규율하는 데 있어 고려해야 할 가장 중요한 요소는 사이버공간의 특성을 반영하는 것이다. 공격과 결과발생의 간격이 0이라는 점과 공격 포인트와 공격자를 밝히는 데 있어 기술적인 면이 중요한 부분을 차지한다는 점은 사이버공간이 가지는 가장 큰 특징이며 이는 사이버공간의 규율에 반영되어야 할 점이다. 이러한 사이버공간의 특성을 반영하면 사이버공격에 대한 규율은 즉각적 억지와 재발방지를 위한 장기적 대응 두 가지 차원에서 이루어져야 한다.

앞에서는 사이버공격을 규율하는 데 있어 국제법원칙 적용의 한계와 적극적 방어 개념이 현행 국제법체제 내에 완전히 포섭되지는 못한다는 사실을 확인하였다. 그렇다면 이러한 한계와 새로운 개념을 어떤 방식으로 국제법의 규율 하에 둘 수 있는지에 대한 논의가 필요하다. 법적 구속력을 가진 대표적인 국제법의 법원에는 조약과 관습이 있다. 그러나 사이버공격을 실효적으로 규제할 수 있는 다자조약이 존재하지 않는다는 점은 이미 살펴본 바 있다. 이에 앞서 살펴본 한계들을 실효적으로 규율할 수 있는 방법으로 다자조약의 체결을 제시하기 전에 국가들의 실행을 바탕으로 사이버공격에 대한 관습국제법이 형성될 수 있는지 여부를 먼저 살펴보기로 한다.

앞서 일부 국가들은 국내입법을 통해, 다수의 국가들은 정책을 통해 사이버공격에 대한 대응수단으로 적극적 방어를 도입하고 있음을 검토한 바 있다. 이를 이유로 적극적 방어가 관습국제법으로 형성되고 있기 때문에 다자조약체제를 통한 규율 논의가 필요하지 않다는 주장이 제기될 수 있다. 관습국제법은 법으로 수락된 일반관행의 증거[787]로서 법적확신(*opinio*

787) ICJ 규정 제38조 제1항 b호.

juris)과 일반적 관행(general practice)을 성립요건으로 한다. 먼저 국가들이 정책적·법적으로 적극적 방어를 사이버안보전략으로 도입하고 있는 것이 일반적 관행을 형성하는지에 대해 살펴보기로 한다.

적극적 방어를 안보전략으로 도입하고 있는 국가들의 면면을 보면 주로 사이버역량을 갖춘 나라들임을 알 수 있다. 적극적 방어조치의 실행에는 고도의 탐지 및 추적, 공격 기술이 필요하다. 사이버역량의 구축에 따라 향후 더 많은 국가들이 적극적 방어를 전략적으로 도입할 가능성이 있지만, 현재까지의 추세만으로 국가들의 실행이 일반성을 갖추었다고 판단하기는 어려울 것으로 보인다. 무엇보다도 정책적으로 적극적 방어를 도입한 국가들이 실제로는 해당 조치를 비밀리에 실행하는 경향이 강하기 때문에[788] 국가의 실제행동을 파악하기가 쉽지 않다는 점에서 적극적 방어를 일반적 관행으로 보기에는 무리가 있다.

한편 법적 확신의 성립 여부도 실상은 국가들의 외부적인 행동으로 확인된다.[789] ICJ는 주로 국제기구의 결의나 결의가 채택되는 과정, 조약체결과정에서의 국가들의 태도 등을 통해 법적확신 여부를 확인하였다.[790] 그러나 적극적 방어 개념은 아직까지 국제기구 회의에서 논의되거나 UN 총회 결의로 채택된 사실이 없다. 사이버공간에 관한 국제법 문제를 논의하는 UNGGE에서도 현재까지 적극적 방어조치에 관한 논의는 이루어진 바 없다. 이를 종합해 볼 때, 사이버공격을 규율하는 관습국제법이 형성되

788) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 462; Joshua E. Kastenberg, "Changing the Paradigm of Internet Access from Government Information Systems: A Solution to the Need for the DOD to Take Time-Sensitive Action on the Niprnet", Air Force Law Review, Vol. 64 (2009), p. 178.

789) *North Continental Shelf (Federal Republic of Germany/Netherlands) and North Continental Shelf (Federal Republic of Germany/Denmark), I.C.J. Reports 1969*, Dissenting Opinion of Judge Tanaka, para. 176.

790) *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996*, paras. 70-71; *Nicaragua (Nicaragua v. US), I.C.J. Reports 1986*, paras. 183, 194, 186; Malcolm N. Shaw, *supra* note 731, p. 63.

기에는 상당한 시간이 걸릴 것으로 보인다. 무엇보다도 국가들이 국내적으로는 적극적 방어를 대응전략으로 도입하면서 국제적 논의에서는 이를 언급하지 않는 점, 국가들의 실제 실행이 비밀리에 이루어지는 경향이 있다는 점을 통해 이에 관한 관습국제법의 성립이 쉽지 않다는 것을 짐작할 수 있다.

따라서 관습국제법의 성립을 기다리기 보다는 현 국제법의 한계를 직시하고 다자조약체제를 통해 문제를 논의하는 것이 바람직하다. 또한 주요 사이버공격이 적대적 관계의 국가 간 또는 라이벌 국가 사이에 일어나고 있는 점을 생각하면[791] 양자조약 체결을 통한 규율은 실효성을 기대하기 힘들다. 사이버공격 기술의 발전 속도와 가속화되는 상용화 수준을 생각할 때 그 필요성은 더욱 크다고 할 수 있다. 한편 사이버공격의 규율을 위한 다자조약의 체결이 전혀 새로운 원칙을 만드는 것을 의미하는 것은 아니다. 그보다는 사이버공간의 특수성을 법체제에 반영해야 한다는 필요의식을 바탕으로 기존체제의 적용이 가능하도록 한계를 보완하고, 실효적 대응을 위한 적극적 방어 개념의 적용을 통해 현 국제법체제와 조화를 이룰 수 있도록 하는 작업으로 이해할 수 있다.

이하에서는 즉각적 억지를 위한 적극적 방어개념을 새로운 체제 안에서 어떻게 규율할 것인지 먼저 검토해 보기로 한다. 그 후에는 기존체제에 사이버공간의 특성을 반영한 장기적 대응체제 마련에 대해서도 논의해 보기로 한다.

2. 적극적 방어체제의 구축: 즉각적 억지 전략의 수립

적극적 방어 개념을 도입한 체제를 마련하기 위해서는 우선 해당조치로 인한 우려사항을 검토하는 것이 필요하다. 적극적 방어조치가 초래할 수 있는 위험요소를 통제하고 제한하는 것을 통해 효과적이고 안정적인 사이

791) 미국-러시아, 미국-중국, 미국-북한, 러시아-우크라이나, 러시아-그루지야, 러시아-독일, 러시아-에스토니아, 한국-북한의 경우가 대표적이다.

버공격 억지의 목적을 달성할 수 있기 때문이다. 적극적 방어조치에 대한 우려사항으로는 주로 조치의 강도, 제3자에 대한 피해, 방어가 아닌 보복적 성격 등이 지적된다. 적극적 방어에 대해 반대하는 입장은 특히 적극적 방어가 무고한 제3자에게 피해를 줄 수 있는 재앙적인 조치라는 것을 이유로 든다.[792] 그러나 이는 적극적 방어를 주로 역해킹과 같이 가장 공격적인 수단을 사용한 조치로만 인식한데서 비롯된 반응이다. 앞서도 지적한 바 있듯이 공격적인 수단을 사용해 악의적 흐름을 유포한 서버 또는 봇넷에 직접 타격을 가하는 hacking back은 적극적 방어조치에 포함되는 방법 중 하나이지 이것이 곧 적극적 방어조치 전체를 의미하는 것은 아니다.[793] 역해킹은 앞서 분류한 적극적 방어조치 중 현재 공격의 위험에 처해 있는 네트워크의 범위를 넘어서 공격자의 시스템에 직접적인 영향을 주는 적극적인 사이버 반격에 속하는 조치이다. Dorothy Denning은 이를 외부적 방어조치로 분류하고, 봇넷 테이크 다운, 공격 명령 및 제어(Command & Control)에 사용되는 IP주소 및 도메인 탈취 등을 그 예로 들었다.[794]

그러나 이러한 적극적 사이버 반격조치가 반드시 파괴적인 결과를 가져오는 것은 아니다. 그루지야정부는 2012년 러시아에 기반을 둔 해커가 한 달에 걸친 지속적 사이버공격을 하자 역으로 해커의 컴퓨터에 스파이웨어를 심는 조치를 취한 바 있다.[795] 그루지야 정부는 정부, 국회, 은행기관

792) 대표적인 예로 보안기업 Cigital의 기술담당 최고 책임자인 Gary McGraw는 적극적 방어조치를 무책임하며, "재앙을 초래할 방안(a recipe for disaster)"이라고 기사와 강연을 통해 여러차례 밝힌 바 있다. Synopsys, Feb. 14, 2013, "'Active defense' is irresponsible", <https://www.synopsys.com/blogs/software-security/active-defense-is-irresponsible/> (2017.10.25.최종방문).

793) Dorothy E. Denning, "Framework and principles for active cyber defense", Computers & Security, Vol. 40 (2014), p. 108.

794) *Ibid.*, p. 109.

795) Computerworld, Oct. 30, 2012, "Irked by cyberspying, Georgia outs Russia-based hacker -- with photos", <https://www.computerworld.com/article/2493051/cybercrime-hacking

및 비정부기구 사이트에 대한 악성바이러스 공격을 탐지하였고, 감염된 300-400개의 정부기관의 컴퓨터가 봇넷을 형성하여 해커가 운영하는 드롭서버로 기밀정보를 전송하고 있다는 사실을 밝혀냈다.[796] 그루지야는 우선 드롭서버와의 연결을 차단하고, 감염된 컴퓨터들을 복구하는 조치를 취하였다. 그래도 해커의 공격이 멈추지 않자 의도적으로 그루지야 정부 컴퓨터를 해커의 공격에 노출시킨 뒤, 감염된 컴퓨터에 "Georgian-Nato Agreement"라는 이름의 압축 저장파일을 심어 해커를 유인하였다. 해당 Zip Archive는 해커가 접근하여 파일을 다운로드하는 순간 해커의 시스템에 스파이웨어가 설치되도록 디자인 되어 있었다. 이로 인해 해커의 시스템이 역해킹 되었고, 해커의 웹캠을 통해 해커의 사진이 찍혀 전송되는 것은 물론 그의 시스템 데이터가 그루지야 정부로 역전송되었다.[797]

그루지야정부가 취한 조치는 결과적으로 공격자의 시스템을 역해킹하는 것이었으나, 실제 역해킹을 실행한 자는 자신이 이미 감염시킨 컴퓨터에 접속한 해커자신이었지 그루지야정부가 아니었다. 또한 공격차단조치는 파일 역전송에 그쳤을 뿐 파괴적인 결과를 야기하지는 않았다는 사실을 확인할 수 있다. 이를 통해 가장 강력한 적극적 방어 수단의 하나인 hacking back의 경우에도 어떤 방법을 선택하느냐에 따라 강도조절이 가능함을 알 수 있다. 따라서 역해킹의 위험성에 대한 우려 때문에 적극적 방어조치에서 역해킹을 완전히 배제 시키는 것은 적절하지 않다.[798] 그보다는 보복적이면서 파괴적인 방법의 역해킹을 제한하는 것이 적절하다고 볼 수 있다. Halberstam은 경제적 제재보다는 강하고 재래식 무기를 사용한 공격보다는 약한 수준의 사이버 반격을 적절한 강도의 방어조치로 제안한 바 있다.[799]

/irked-by-cyberspying—georgia-outs-russia-based-hacker----with-photos.html> (2017.10.25.최종방문).

796) Computerworld(2012).

797) Computerworld(2012).

798) Ruperto P. Majuca and Jay P. Kesan, *supra* note 395, pp. 10-11.

799) Manny Halberstam, *supra* note 610, p. 207.

그러나 공격의 수단으로 이용되는 서버를 무력화(neutralize) 시키거나 파괴하는 조치 또는 공격서버와의 완전한 차단조치 등은 반대자들이 우려하는 파괴적인 결과를 초래할 위험을 항상 가지고 있다. 사이버공격에는 주로 수백 대에서 수백만 대에 이르는 봇넷이 사용되기 때문에 공격과는 무관한 제3자가 피해를 입을 수 있으며, 공격의 거점으로 사용되는 C&C 서버는 공격과는 무관한 제3국의 기관서버를 해킹한 것일 수 있기 때문이다. 2011년 미연방수사국과 법무부는 악성코드 CoreFlood의 확산을 막기 위해 C&C 서버들을 차단하는 조치를 실행한 바 있다.[800] 미 당국은 먼저 봇넷을 컨트롤하는 다섯 개의 서버를 장악하고, 이를 봇넷 소스코드를 카피하여 만든 유인서버로 교체하여 감염된 봇에 정지명령을 내리도록 하였다.[801] 이 과정에서 당국은 정지 이외의 다른 명령을 내릴 경우 감염된 봇에 예상치 못한 피해가 갈 것을 우려하여 유인서버에 "delete yourself" 명령 설정을 하지 않았다.[802] 만약 FBI가 장악한 봇넷 서버들을 유인서버로 교체하는 대신 무력화하는 조치를 취했다면 수백만 대의 감염된 봇에 가늠할 수 없는 피해를 초래했을 것이다.[803]

따라서 적극적 방어조치를 취하는 경우에도 필요성의 원칙은 지켜져야 한다. 이는 특히 적극적 방어조치로 인해 무고한 제3자가 피해를 입을 위험이 있을 경우에 고려되어야 할 사항이다. 즉, 적극적 방어조치는 필요성의 원칙하에 탐지된 위협 및 현존하는 공격을 완화 및 방어하기 위한 목적에 한해서 취해져야 하고, 보복을 위해 사용되어서는 안된다.[804]

---

800) Wired, Apr. 13, 2011, "With Court Order, FBI Hijacks 'Coreflood' Botnet, Sends Kill Signal", <https://www.wired.com/2011/04/coreflood/> (2017.10.26.최종방문).

801) DarkReading, Apr. 14, 2011, "Coreflood Botnet An Attractive Target For Takedown For Many Reasons", <https://www.darkreading.com/risk/coreflood-botnet-an-attractive-target-for-takedown-for-many-reasons/d/d-id/1135557?piddl_msgorder=asc> (2017.10.26.최종방문).

802) *Ibid.*

803) Dorothy E. Denning, *supra* note 793, p. 111.

또한 적극적 방어조치는 비례성 원칙을 준수하여 실행해야 한다.[805] 예를 들어 은행 시스템에 대한 DoS 공격에 좀비서버(compromised server)가 이용되고 있는 경우, 해당 좀비서버가 생명에 직결된 의료기기가 연결되어 있는 병원의 서버라면 해당서버에서 나오는 트래픽을 모두 차단시키는 조치는 인명피해를 야기할 수 있다.[806] 이 경우, 경제적 피해를 막기 위해 인명피해를 야기할 수 있는 전면 blocking 기법의 사용은 비례성에 어긋나는 조치를 취하는 것이 될 수 있기 때문에 다른 기법을 선택하는 것이 필요하다. 따라서 공격의 위험에 처한 국가나 기업이 공격소스를 추적해 냈더라도 해당소스의 시스템 기능을 파악하고, 조치를 취할 경우 어떤 결과를 초래할 지를 검토하는 작업이 요구된다.[807]

한편 필요성과 비례성 원칙하에 적극적 방어조치를 취하는 데 있어 선행되어야 할 것은 위협 발생 네트워크를 정확하게 추적하는 것이다. 적극적 방어의 경우, 공격행위자를 찾아내서 배후에 국가가 있다는 사실을 밝혀야 하는 귀속의 증명이 필요한 것은 아니다. 그러나 파악한 공격거점의 정확도를 검증하는 기준은 적극적 방어조치를 취하는데도 반드시 필요하다.[808] 소스의 정확도는 조치의 성공률, 공격의 억지효과[809] 및 무고한 제

---

804) *Ibid.* ; Ruperto P. Majuca and Jay P. Kesan, *supra* note 395, pp. 11-12, 26; Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 479; William A. Owens, Kenneth W. Dam, and Herbert S. Lin (eds)., *supra* note 662, p. 64; Wyatt Hoffman and Ariel E. Levite, *supra* note 17, p. 35.

805) Ruperto P. Majuca and Jay P. Kesan, *supra* note 395, p. 40; Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 487; Eric Talbot Jensen, *supra* note 9, p. 799; Wyatt Hoffman and Ariel E. Levite, *supra* note 17, p.35.

806) 해당 좀비서버에서 나오는 트래픽 중에는 공격명령에 따른 것 뿐 아니라 기기에 연결된, 은행 시스템을 통과해야 하는 적법한 트래픽도 포함되어 있기 때문이다. Dorothy E. Denning, *supra* note 793, pp. 111-112.

807) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 527; Matthew J. Sklerov, *supra* note 112, p. 81.

808) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 484; Linkedin, May 31, 2017 - Brian Coventry, “Hack back & Counterstrike”,

3자 보호와 직결되는 문제이기 때문이다. 예를 들어 준수해야 할 탐지-추적의 절차를 마련[810]하고, 일정 수준 이상의 탐지 및 추적 기술의 사용 요건을 충족하도록 하는 기준을 설정하는 것을 생각해 볼 수 있다. 이 때, 정확도가 85% 이상 또는 추적기술의 표준 착오율이 5% 미만인지 등의 기준을 적용할 수 있을 것이다.[811] 최근 추적한 소스가 위장된(spoofed) 것일 경우를 피하기 위한 새로운 추적 기술이 많이 개발되어 소개[812]되고 있는데, 설정된 기준에 이러한 기술을 주기적으로 업데이트하여 사용하도록 하는 것도 정확도를 높이기 위한 방법이 될 수 있다.

마지막으로 검토할 우려사항은 조치의 은밀성이다. 적극적 방어조치는 사이버 공간에서 이루어지기 때문에 사이버 공격과 마찬가지로 은밀하게 진행될 수 있다. 그러나 비밀리에 수행되는 적극적 방어조치는 여러 가지 위험성을 내포하고 있다. 우선 탐지한 위협에 대해 자의적 판단을 내릴 가능성이 있다. 모니터링한 패킷의 위험성이 검증되지 않은 경우에도 적극적 방어조치를 취할 수 있다는 것이다. 현재 적극적 방어조치를 취할 수 있는 위협의 판단기준이 공식적으로 확립된 바 없기 때문에 자의적 판단의 가능성은 더욱 높다고 할 수 있다. 이는 조치를 취한 사실이 겉으로 드러나지 않기 때문에 비록 오판에 의한 조치였다고 해도 피해자가 피해에 대해 구제를 요청할 대상을 알 수 없다는 것을 의미한다.

또한 은밀한 적극적 방어조치는 그 자체로 악의적으로 활용될 위험이

<https://www.linkedin.com/pulse/hack-back-counter-strike-brian-coventry> (2017.10.26.최종방문);

809) Erik M. Mudrinich, "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem", The Air Force Law Review, Vol. 68 (2012), p. 172.

810) Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 485.

811) *Ibid.*, p. 484.

812) Abhishek Joshi & Rayan H. Goudar, "The Attack Back Mechanism: An Efficient Back-Hacking Technique", in Malay Kumar Kundu, Durga Prasad Mohapatra, Amit Konar, Aruna Chakraborty (eds.), *Advanced Computing, Networking and Informatics-Volume 2* (Springer, 2014), p. 234.

있다. 봇넷 테이크다운 조치를 위해 C&C 서버에 침투시 해당 서버가 타국의 기반시설이나 정부사이트를 해킹한 것일 경우, 조치를 취하는 과정에서 획득한 데이터나 정보를 열람하거나 해킹하여 활용할 수 있는 것이다. 이와 관련하여 실제로 미 국가안보국이 해커의 봇넷을 장악하여 자신의 스파이 행위에 활용하고 있다는 사실이 보도된 바 있다.[813] 미 국가안보국은 해커로부터 탈취한 봇넷을 라이벌 국가의 네트워크를 공격하거나 사이버 간첩행위를 하는데 사용하고 있는 것으로 드러났다.[814] 뿐만 아니라 여기에는 봇의 IP 주소가 미국으로 나타나는 경우에는 이를 피해자 구조를 위한 연방수사국으로 보내고, 봇의 IP 주소가 자국 및 다섯 개의 첩보동맹국[815]이외의 것으로 밝혀지는 경우에는 미 국가안보국이 통제하는 방식이 사용되고 있었다.[816] 이렇게 은밀히 진행되는 적극적 방어조치는 또 하나의 사이버 공격이 될 위험성을 내포하고 있다.

이상을 정리하면 적극적 방어체제의 마련에는 다음과 같은 사항 및 요건이 반드시 포함되어야 한다. 가장 우선적으로 필요한 것은 적극적 방어의 정의조항을 명시하는 것이다. 적극적 방어의 정의에 기반하여 조치의 수단 및 시기와 범위, 조치가 이루어지는 장소 등 법적규율이 필요한 부분을 확정할 수 있기 때문이다.

둘째, 적극적 방어조치를 취할 수 있는 주체를 명시해야 한다. 국가외의 주체에 대해서는 기업의 이름이나 기관명을 열거하기 보다는 국가 기반시설을 운영하거나 기타 국가안보에 위협을 주는 것으로 간주될 수 있는 산

---

813) Wired, Mar. 12, 2014, “NSA has been hijacking the botnets of other hackers”, <https://www.wired.com/2014/03/nsa-botnet/> (2018.1.2.최종방문).

814) Motherboard, Jan. 19, 2015, “How the NSA Hijacks Hacker Botnets for Spying”, <https://motherboard.vice.com/en_us/article/ypwq7g/nsa-botnets> (2018.1.2.최종방문).

815) Five Eyes는 미국, 호주, 영국, 뉴질랜드, 캐나다의 다섯 개 국가로 구성된 첩보동맹을 말한다.

816) Motherboard, *supra* note 814.

업분야를 선정하는 등의 가이드라인을 마련하는 것이 적절하다. 이후 각국가가 가이드라인에 따라 이에 해당하는 기관 및 기업을 선정하고 그 목록을 새로 마련될 다자조약의 이행기구나 UN과 같은 국제기구에 제출하는 방법이 고려될 수 있다.

셋째, 공격 발생 전 탐지된 위협 및 공격에 대해서만 취하는 적극적 방어조치의 목적상 위협 및 공격성 파악의 정확도를 확인할 수 있는 기준을 마련하는 것이 요구된다. 여기에는 위협 파악의 정확도를 증명할 수 있는 트래픽 수집기록 및 분석자료, 네트워크 모니터링을 통한 행위분석 기록, 봇넷과 C&C서버 사이의 통신 분석자료, 사용자 컴퓨터 로그 모니터링자료, 내부망 서버로그 체크 기록 등이 포함될 수 있다.

넷째, 공격거점 파악의 정확도를 판단하는 기준을 마련해야 한다. 이는 탐지된 흐름이 위협성을 가지고 있는지를 확인하는 것과는 또 다른 개념으로 조치를 취하려는 대상이 정확하게 추적된 것인지와 관련된 문제이다. 만약 조치의 대상이 되는 공격거점이 잘못 파악되는 경우, 위협저지라는 목표를 달성할 수 없을 뿐 아니라 탐지된 위협과 전혀 관련이 없는 시스템에 사이버공격을 감행한 것이 될 수 있기 때문이다. 따라서 검증된 추적기술의 사용을 요건으로 명시하고, 해당 기술사용 기록 및 표준 오차율 제시를 의무화 하는 등의 규정을 마련하는 것이 필요하다. 이를 위해서는 UN과 같은 국제기구와 소프트웨어 보안 기업의 협업을 통해 검증된 추적기술을 주기적으로 업데이트하여 목록을 공개하는 작업이 함께 이루어져야 한다.

다섯째, 필요성과 비례성 원칙의 기준을 명시해야 한다. 앞서 검토한대로 적극적 방어조치 시 필요성 원칙의 준수여부는 조치가 위협을 저지하기 위한 목적 하에 취해졌는지가 되어야 한다. 한편 비례성 원칙의 기준은 공격 결과의 예측 가능성에 따라 다르게 설정되어야 할 필요가 있다. 공격결과의 예측여부는 공격의 유형과 위협 및 공격의 탐지시기에 따라 다르게 나타날 수 있다. 우선 앞에서 예로 든 바와 같이 DDoS 공격이 이미 진행되고 있을 때 조치를 취하는 경우에는 공격의 대상이 이미 확인되었

기 때문에 공격으로 초래될 피해를 예측하는 것이 가능하다. 따라서 이 경우에는 공격으로 초래될 피해에 비례하게 조치를 취할 수 있게 된다.

그러나 APT 공격의 경우에는 내부 시스템에 대한 공격이 시작된 경우라도 공격자의 목적이 정보 유출인지 시스템 손상인지 알기 어렵기 때문에 이로 인한 피해를 예측하는 것이 쉽지 않다. 이외에도 조치를 취하는 시기가 단순히 네트워크상의 위협만이 탐지된 시점일 경우 즉, 위협이 특정기관에 침투하지 않은 경우에는 공격의 대상과 공격이 초래할 피해를 예측하는 것이 불가능하다. 그러나 한편으로 조치를 취하는 입장에서는 조치대상을 확인하는 것이 가능하고, 조치가 초래할 결과를 예측하는 것도 가능하다. 따라서 이 경우에는 조치의 강도가 공격 또는 위협의 억지를 위한 목적에 비례하게 취해졌는지를 기준으로 해야 한다.

여섯째, 적극적 조치를 실행한 당사자가 제3자에게 피해를 입혔을 경우, 이에 대한 책임을 진다는 원칙이 명시되어야 한다. 제3자는 공격 또는 위협의 발생과 관련이 없는 즉, 공격거점을 구성하지 않으나 조치의 대상에 포함된 시스템 사용자를 의미한다. 제3자 피해 책임원칙을 통해 조치실행 당사자가 불필요한 조치의 사용을 자제하고, 강도를 조절하게 하는 효과도 기대할 수 있다.[817]

일곱째, 적극적 방어조치를 실행하는 과정에서 획득한 데이터 혹은 정보 삭제의무를 명시해야 한다. 이는 봇넷 테이크다운 조치나 역해킹을 실행하는 과정에서 기밀 문서열람이나 데이터 해킹 행위가 일어날 수 있는데, 조치실행자가 이를 악용하지 못하게 하기 위함이다. 조치를 취한 국가 또는 기업이 이에 대해 부인한다면 조치 대상국 입장에서 이를 확인할 수 있는 방법은 없으나 향후 이 사실이 밝혀질 경우, 조치대상국은 조치국에게 의무 위반을 근거로 책임을 추궁할 수 있다.

여덟째, 적극적 방어조치에 대한 사후 공개의무를 명시하고 구체적인 공개절차를 마련해야 한다. 적극적 방어조치를 은밀히 실행할 경우 발생할

817) Ruperto P. Majuca and Jay P. Kesan, *supra* note 395, p. 11; Jay P. Kesan and Carol M. Hayes, *supra* note 112, p. 487.

수 있는 위험 및 부작용에 대해서는 이미 검토한 바 있다. 따라서 공개의무를 규정하는 것은 반드시 필요한 사항이다. 그러나 사전적 대응의 의미를 가지고 있는 적극적 방어조치의 목적상 이를 사전에 공개하는 것은 적절하지 않다. 조치에 대해 사전 고지할 경우, 공격자가 이를 알고 공격의 거점을 옮길 위험이 있을 뿐 아니라[818] 조치 대상국이 반발할 가능성[819]도 있기 때문에 조치의 실효성이 현저히 떨어질 수 있기 때문이다. 따라서 적극적 방어조치를 공개하는 데 있어서는 사후공개를 원칙으로 하는 것이 적절하다.

한편 조치 대상자가 자신의 시스템이 조치로 인해 어떤 영향을 받았는지 파악하고, 필요한 경우 피해보상 청구가 가능하게 하기 위해서 조치를 공개하는 절차도 반드시 필요하다. 이를 위해서는 해당절차에 조치대상의 공개와 조치 내용의 공개가 포함되어야 한다. 적극적 방어조치가 봇넷과 같은 공격거점에 취해진 경우 대부분의 조치대상은 이에 대해 알지 못할 가능성이 높기 때문이다. 또한 자신의 시스템이 조치의 대상이 되었다는 사실만으로는 조치로 인해 자신의 시스템이 어떤 영향을 받았는지 파악하기 어려울 수 있다. 이 때문에 조치내용의 공개가 함께 이루어져야 하는 것이다. 공개가 필요한 조치의 내용으로는 사용된 기술, 기술이 사용된 시스템의 위치와 기록, 부수적인 피해가 발생했는지를 파악하기 위해 필요한 확인사항 리스트 등을 예로 들 수 있다.

조치의 공개와 관련하여 또 하나 명확히 해야 할 부분은 공개 시한을 정하는 것이다. 조약 규정에 적극적 방어조치를 실행한 국가나 기업이 조치 실행 직후 그 사실을 조약기구 및 조치대상국에 통고하고, 며칠 이내에 위에서 검토한 조치의 내용, 위협탐지 정확도 평가, 공격거점의 정확도 등에 관한 보고서를 제출하는 규정을 마련해야 조약의무 이행을 확보할 수

818) Christian Czosseck, Gabriel Klein, Felix Leder, *supra* note 43, p. 115.

819) Felix Leder, Tillmann Werner and Peter Martini, *supra* note 49 p. 224.

있다.

다음은 위의 사항을 바탕으로 조약규정을 작성한 것이다.

표3 조약규정 예시

제1조 정의

이 협약의 목적상

1. “적극적 방어”란 현재 발생하고 있는 위협이나 공격의 흐름을 탐지하여 공격의 경로와 흐름을 파악하고, 이를 차단시키거나 공격명령 서버 또는 봇넷에 사이버역량을 사용한 조치를 통해 공격에 실시간으로 대응하는 사이버공간상의 조치를 말한다.
2. “위협”은 시스템에 피해를 발생시킬 수 있는 잠재적 원인으로 사이버공간상에서 정상적인 활동범위를 벗어나 악의적인 의도를 가지고 있는 통신의 흐름(traffic)을 말한다.
3. “트래픽”은 컴퓨터 시스템으로부터 발생하는 모든 스크립트들의 조합으로서 컴퓨터 시스템을 수단으로 한 통신의 발생지, 목적지, 경로, 시간, 규모, 기간, 형태를 나타내주는 통신의 흐름을 말한다.
4. “사이버공격”은 사이버공간 안에서 정보통신 기술을 사용하여 정치적·사회적·경제적 혼란을 발생시킬 목적으로 사람, 전자 및 물리적 기반시설에 대하여 위해를 가하는 행위를 말한다.

제2조 적극적 방어조치의 행사주체

1. 협약이 규정하는 적극적 방어조치를 취할 권한은 이 협약의 당사국과 협약운영위원회가 마련한 가이드라인에 근거하여 당사국이 국내적 절차를 통해 선정한 기관 또는 단체에게 부여된다.
2. 당사국은 협약의 가입일로부터 60일 이내에 국내적 절차를 통해 선정한 기관 또는 단체의 명단을 협약운영위원회에 보고한다.
3. 협약운영위원회는 각 당사국의 보고 내용을 운영위원회 홈페이지를 통해 공개한다.

제3조 필요성

적극적 방어조치는 위협이 탐지된 경우에 한해서 탐지된 위협을 저지하기 위한 목적으로 취하여야 한다.

제4조 비례성

1. 적극적 방어조치는 탐지된 위협 또는 공격으로 인한 피해를 예측할 수 있는 경우에는 예상되는 피해에 비례하게 취하여야 한다.
2. 적극적 방어조치는 탐지된 위협 또는 공격으로 인한 피해를 예측할 수 없는 경우에는 조치가 초래할 결과가 위협 또는 공격의 억지를 위한 목적에 비례하도록 취하여야 한다.

제5조 조치실행 주체의 책임

적극적 방어조치를 실행한 주체는 다음의 경우 조치의 실행으로 인한 피해에 대해 책임을 부담한다.

(a) 조치의 대상이 공격자 또는 공격에 사용된 수단이 아닌 것으로 판명된 경우

(b) 조치의 대상에 대해 필요성·비례성 원칙을 준수하지 않은 경우

제6조 공개의무

1. 적극적 방어조치를 취한 주체는 조치 실행 후 즉시 적극적 방어조치를 취한 사실을 협약운영위원회에 통고하고, 운영위원회는 이 사실을 공개해야 한다. 적극적 방어조치를 취한 주체는 조치 실행 사실의 통고와 함께 다음의 사항을 공개해야 한다.

(a) 조치 대상

(b) 조치에 사용된 기술, 그러한 기술이 사용된 시스템의 위치, 시스템에 대한 피해여부를 확인할 수 있는 리스트 등을 포함한 조치의 내용

2. 조치의 적절성 여부를 판단하기 위해 적극적 방어조치를 취한 주체는 다음의 정보를 협약운영위원회에 제출한다.

(a) 위협성 또는 공격성 여부를 판단하기 위해 사용된 트래픽 수집기록 및 분석자료

(b) 봇넷과 C&C서버 간 통신분석자료

(c) 사용자 컴퓨터 로그 또는 내부 기관망 서버로그 기록 분석자료

3. 적극적 방어조치를 취한 주체는 조치를 실행하는 과정에서 획득한 데이터, 기밀문서, 정보통신기술 등을 조치 후 모두 삭제, 폐기해야 할 의무를 부담한다.

3. 사후책임추궁체제를 통한 장기적 대응

적극적 방어 개념의 도입은 탐지된 위협이나 공격에 대한 즉각적 억지 차원의 대응을 위한 것이다. 즉, 적극적 방어는 임박한 또는 진행되고 있는 공격을 저지하여 피해발생을 최소화하는 조치로서 의미가 있는 것이지 재발방지를 확보하는 방안은 아니다. 적극적 방어는 네트워크상의 조치이기 때문에 실제 공격자에게 직접 영향을 미치지 않고, 공격행위자는 여전히 익명으로 남아 활동할 수 있기 때문이다.[820] 무엇보다도 적극적 방어조치의 대상이 되는 봇넷과 C&C서버는 공격자가 언제든 교체할 수 있는 공격수단에 불과하기 때문에 사이버공격에 대한 진정한 억지를 실현하기 위해서는 공격 행위자를 찾아내어 책임을 추궁하고, 처벌 및 제재를 하는 조치가 반드시 병행되어야 한다.

사이버공격의 귀속을 밝히는 데는 기술적인 부분 뿐 아니라 각 기관 및 국가들의 협조가 요구되어 시간이 소요되기 때문에 이는 장기적인 억지책의 성격을 띤다고 볼 수 있다. 책임추궁과 처벌 및 제재가 가능한 체제가 성립되면 그 사실만으로도 상당한 억지효과를 기대할 수 있다. 즉, 새롭게 확립된 법체제가 사이버공간의 익명성 안에 숨는 것을 더 이상 용인하지 않는다는 사실을 알게 되는 것만으로도 해커들이 공격시도를 멈추는 것을 기대할 수 있다.[821] 앞서 사이버공격의 경우 기존체제를 그대로 적용하여 공격행위자를 찾고 책임을 추궁하기에는 법적인 모호성과 한계가 존재함을 확인하였다. 따라서 새로운 체제에서는 이러한 법적 모호성 문제를 해소하고, 한계를 극복하는데 초점을 맞추어야 한다.

---

820) Kaspersky는 역해킹조치의 문제점 중 하나로 공격자가 영원히 익명으로 남아있을 수 있다(Attackers can remain anonymous forever) 는 점을 들었다. Kaspersky Daily, Sept. 16, 2015, “The Four Biggest Problems with “Hacking Back””, <https://www.kaspersky.com/blog/hacking-back-i/15101/> (2017.10.27. 최종방문).

821) Ruperto P. Majuca and Jay P. Kesan, *supra* note 395, p. 16.

우선 해결되어야 할 법적 모호성으로는 기존 국제법원칙 위반을 판단하는 기준설정의 문제가 있었다. 앞서 러시아와 중국은 자의적인 기준을 사용하여 사이버공격의 국제법위반여부를 판단하고, 자위권 또는 대응조치를 취하는 데 반대한 바 있다. 따라서 모호한 경계에 관한 논의를 통해 기준을 명확히 설정할 필요가 있다. 이를 위해서는 국가들의 논의 포커스가 적용가능한 국제법원칙의 명시에서 이를 적용하기 위한 기준의 우선적 마련으로 옮겨져야 한다. 러시아와 중국도 자의적 기준이 아닌 명확한 기준을 먼저 설정하자는 제안에 반대하기는 어려울 것이다.

한편 사이버공격에 있어 가장 문제가 될 수 있는 모호한 경계는 무력사용에 해당하는 강도의 사이버공격이 무엇인가이다. 따라서 해당논의에는 대규모 경제적 피해를 야기하는 금융기관에 대한 공격을 어떤 강도로 판단할 것인지에 관한 논의가 반드시 포함되어야 한다. 금융기관에 대한 사이버공격에 수반되는 시스템의 파괴를 경제적 피해에 포함되는 것으로 볼 수 있는지에 대해서는 현재까지 논의된 바가 없기 때문이다. 만약 금융기관에 대한 사이버공격이 무력사용으로 인정된다면 이에 대한 대응조치는 그 이하의 강도로 제한될 것이다. 또한 명확한 기준이 설정됨에 따라 동일한 수준의 사이버공격은 그 시도가 줄어들 수 있다. 중대한 무력사용은 무력공격이 될 수 있기 때문에 동일한 수준의 사이버공격은 자칫하면 상대방의 자위권 원용을 촉발시킬 수 있기 때문이다.

다음으로 이렇게 설정된 기준을 적용하기 위해서는 귀속 증명을 위한 행위자 확인원칙의 마련과 협조의무 규정에 관한 논의가 필요하다. 즉, 이미 드러난 공격자와 국가와의 관계를 밝히는 차원을 넘어서 행위자 자체를 밝히는 과정을 귀속 개념에 포함시켜야 한다.[822] 또한 여기에는 협조의무가 반드시 함께 논의되어야 한다. 국가 간 협조 없이 사이버공격의 귀속

822) 제3장에서 사이버공격의 귀속성을 밝히는 과정을 1) 탐지된 위험의 성격 파악 2) access path 추적을 통해 공격의 근원 파악 3) 추적된 공격 근원 네트워크의 실제 사용자 파악 4) 실제 행위자와 국가의 연관성 증명의 네 단계로 나누어 살펴본 바 있다. 제3장 제2절 참조.

을 밝히는 것은 불가능하다는 것은 이미 앞서 귀속의 한계를 검토하며 논증한 바 있다. 앞서 핵테러 행위의 억제를 위한 국제협약 제10조에서 국가들의 조사협조의무를 규정하고 있지만, 그 요건이 '행위자'에 대한 정보를 제공하는 경우 조사에 대한 원조를 제공하도록 하고 있어 사이버공격에 적용하기에는 어렵다는 점을 확인한 바 있다.

따라서 협조의무를 규정하는 데 있어서도 조사협조의 기준과 같이 세부적인 규정을 마련하는 것이 중요하다. 우선적으로는 조사협조의 요건을 행위자 정보제공이 아닌 위협의 탐지로 낮추는 것이 중요하다.[823] 즉, 네트워크상의 공격거점 파악 후, 공격거점이 위치한 국가는 탐지국가의 요청시에 공격실행자를 밝히기 위한 조사협조에 응하도록 해야 한다. 또한 협조의무는 정보공개, 조사협조, 범죄인 인도 등 다양한 형태로 규정될 수 있으며, 요청받은 국가의 기술력이 부족한 경우에는 주변국의 기술지원에 관한 사항도 함께 마련하여 실효적인 협조체제가 구축될 수 있도록 해야 한다.

국가 간 조사협조에 관한 합의가 사이버공격의 규율에 효과적일 수 있다는 점은 2015년 미국과 중국의 사이버위협에 관한 합의를 통해서도 확인할 수 있다. 2015년 시진핑 주석의 방미 기간에 양국은 양국으로부터의 악의적인 사이버활동과 관련하여 정보 및 협조요청에 대해 조속히 응한다는 데에 합의 했다고 발표하였다.[824] 양국은 구체적으로 양국에서 발생한 악의적 사이버활동에 대한 전자정보 수집 및 조사요청에 협력할 것에 합

---

823) 공격경로 추적을 통해 공격 근원을 파악하는 것은 행위자를 밝히는 attribution을 밝히기 이전 단계에 속하는 작업이기 때문에 attribution과 확실히 구별되어야 한다. William A. Owens, Kenneth W. Dam, and Herbert S. Lin (eds)., *supra* note 662, p. 141; Jay P. Kesan and Carol M. Hayes, *supra* note 112, 480.

824) White House, "Fact Sheet: President Xi Jinping's State Visit to the United States", Sept. 25, <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states> (2017.10.28.최종방문).

의하는 동시에 장관급 인사들로 구성된 공동 대화 매커니즘을 마련하는데 동의하였다.[825] 이 매커니즘 안에는 신속한 협조를 위한 핫라인 설치계획도 포함되었다.[826] 양국은 합의문 전체를 공개하지 않고, 주요 내용을 정부 사이트에 게재하여 자세한 규정을 확인할 수는 없으나 공개된 Fact Sheet을 통해 사이버공격에 대한 협조의무가 합의의 주 내용인 것을 알 수 있다.[827] 당시 합의의 실효성에 대해 회의적인 반응이 많았으나, 결과적으로는 중국의 해킹 빈도가 현저히 줄어든 것으로 나타났다.[828]

미국은 이보다 앞선 2013년, 러시아와도 Cyber Hotline을 설치하는 등의 내용을 포함한 합의를 한 바 있다. 합의의 주요 내용은 사이버공간에서 양국 간의 신뢰를 강화하고 양국에서 발생하는 사이버위협에 대한 이해를 공유한다는 일반적인 수준의 것이었다.[829] 그러나 주지하다시피 해당 합의는 중국과의 합의만큼 성과를 거두지 못했다. 이는 국가 간의 합의에 있어 합의의 목적을 구체적으로 명시하는 것이 얼마나 중요한 지를 보여주는 예라고 할 수 있다. 이러한 형태의 합의가 다자체제로 확대 된다면 귀속의 증명을 통한 책임 추궁 뿐 아니라 자위권 원용 및 대응조치의 적용을 통

---

825) 중국은 법무부, 공안부, 국가안전부, 인터넷 정보국을 공동대화 매커니즘에 참여하도록 지명하였으며, 미국은 국토안보부 장관과 법무장관이 FBI를 비롯한 정보기구의 참여 하에 해당 대화의 공동 의장을 맡도록 하였다. 이 공동대화 매커니즘은 양 국가에서 서로에 대한 사이버공격이 탐지되어 정보와 원조를 요청 할 경우에 신속한 대응을 하기 위한 것이다.

826) White House, Fact Sheet(2015).

827) 중국의 경우 공식 정부 사이트 http://cpc.people.com.cn/에 Fact Sheet 게재.

828) Financial Times, Apr. 13, 2016, “Chinese hacking of US companies declines”, <https://www.ft.com/content/d81e30de-00e4-11e6-99cb-83242733f755> (2017.10.28.최종방문).

829) White House, “FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security”, Jun. 17, 2013, <https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol> (2017.10.28.최종방문).

한 처벌 및 제재의 가능성이 높아져 사이버공격에 대한 장기적 억지를 기대할 수 있다.

마지막으로는 사이버무기 군축에 관한 부분이다. 앞서 러시아가 사이버무기 군축을 위한 다자조약의 체결을 제시한 바 있음을 검토하였다.[830] 러시아는 사이버무기를 대량살상 무기와 비교하면서 이에 대한 규제가 필요함을 주장하였다.[831] 한편 오바마 대통령도 2016년 중국 항저우에서 개최된 G-20 정상회의 기간 중 푸틴대통령과 가진 양자회담 자리에서 사이버무기 경쟁을 냉전시대의 핵무기 군비경쟁에 비유한 바 있다.[832] 오바마 대통령은 이에 앞서 2015년에도 핵무기 군축체제와 유사한 사이버무기 군축체제가 필요하다고 강조한 바 있다.[833] 그러나 핵무기가 오직 국가들의 통제 하에 있었던 것과는 달리 사이버무기는 개인이나 단체도 쉽게 획득할 수 있다는 점에서 핵군축 체제에 착안하여 사이버무기 군축을 시도하는 것은 적절하지 않다.[834]

또한 사이버기술은 발전 속도가 빨라 새로운 종류의 악성코드와 기술이 계속해서 업데이트되기 때문에 구체적 무기나 기술을 특정하여 규제하기 어렵다는 문제가 있다. 뿐만 아니라 사이버공격의 영향은 고도의 기술을 사용할수록 피해가 커지는 공식이 성립하지 않기 때문에 특정 기술의 사용을 제한한다고 해서 억지효과가 나타난다고 볼 수도 없다. 2016년 민주당 이메일 해킹사건이나 2008년 그루지야 사건에 사용된 사이버기술은 고

---

830) UN Doc. A/54/213(1999), p. 8; UN Doc. A/56/164/Add.1(2001), p. 3.
831) *Ibid.*
832) The Telegraph, Sept. 5, 2016, "Barack Obama warns of Cold War-style 'cyber arms race' with Russia", <http://www.telegraph.co.uk/news/2016/09/05/barack-obama-warns-of-cold-war-style-cyber-arms-race-with-russia/> (2017.10.28.최종방문).
833) White House, "Remarks by the President to the Business Roundtable", Sept. 16, 2015, <https://obamawhitehouse.archives.gov/the-press-office/2015/09/16/remarks-president-business-roundtable> (2017.10.28.최종방문).
834) Robert Litwak and Meg King, "Arms Control in Cyberspace?", Wilson Center (2015), p. 6.

도의, 정교한 기술이 아니었음에도 불구하고 그 영향력은 막강했다는 사실이 이를 뒷받침한다.[835] 따라서 사이버공간을 이용하는 모든 사람이 이용할 수 있는 사이버기술을 통제하는 사이버무기군축 체제의 형성은 다소 현실성이 떨어지는 시도라고 볼 수 있다. 사이버공격의 억지는 앞서 제안한 기존 국제법 적용을 위한 명확한 기준설정 및 협조의무가 명시된 체제의 구축을 통해서도 충분히 달성할 수 있다.

835) 전문가들은 그루지야 공격에는 정교한 해킹기술이나 비용이 많이 드는 사이버무기가 사용된 것은 아니라고 지적하였다. US Cyber Consequences Unit, *supra* note 363, pp. 4; Newsweek, "HOW RUSSIA MAY HAVE ATTACKED GEORGIA'S INTERNET", Aug. 22, 2008, <http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111> (2017.10.28.최종방문)

제6장 결론

본 논문은 사이버공간에서 수행되는 사이버공격이 국가안보에 위협이 되고 있는 현실을 확인하고, 이에 대해 국제법적 규율이 필요하다는 인식에 기초하여 사이버공격을 효과적으로 억지하는 방안에 대해 연구하였다. 지금까지 국가들 간 사이버공격의 국제법적 규율에 대한 논의는 활발하게 진행되어 왔다. 그 이유는 사이버공격에 대한 국제법적 규율은 물리적 공간과는 구별되는 사이버공간만의 특성이 반영되어야 하기 때문이다. 그러나 현 시점에 있어서의 논의는 사이버공간의 특성을 반영하기 보다는 사이버공간의 규율을 위해 새로운 체제 마련이 필요한지 기존국제법을 그대로 적용할 수 있는지 여부에 집중되어 있다는 점을 확인할 수 있었다.

사이버공간은 물리적 공간과 달리 활동의 경계나 한계가 없고 익명성을 가지고 있어 행위자를 특정하기가 어렵다는 특징을 가지고 있다. 또한 인터넷공간은 활동의 흔적을 남기기 위한 목적으로 설계되지 않았기 때문에, 기술을 활용하여 자신의 활동 흔적을 지우거나 위장할 수 있다. 이러한 일반적인 사이버공간의 특성 외에도 사이버공격이 가지는 특성으로는 공격자와 공격거점, 공격목표 간의 독특한 관계를 들 수 있다.

대부분의 경우, 공격자는 공격 목표에 대해 직접 공격을 실행하지 않고, 공격의 거점을 마련하여 이를 거쳐 공격을 실행한다. 또한 사이버공간의 특성상 공간 활용이 자유롭기 때문에 공격의 거점은 여러 개가 될 수 있고, 여러 단계를 형성할 수도 있다. 사이버공격은 이렇게 여러 단계를 거쳐 공격이 실행되기 때문에 실제 공격자를 밝히는 귀속의 입증이 더욱 어렵고, 공격의 즉각적인 중단을 위해서는 귀속의 입증보다는 우선적으로 공격거점에 대한 조치가 필요하다. 사이버공격을 규율하기 위한 국제법적 논의에는 이러한 사이버공간 자체의 특성 및 사이버공격의 특성이 반영되어야 한다.

현재 발생하고 있는 공격의 흐름을 차단시키거나 공격의 거점이 되는 서버 또는 시스템을 직접 셧다운시키는 등의 사이버공간상의 조치[836]를 의미하는 적극적 방어는 바로 이러한 사이버공격의 특성을 반영하여 마련된 대응전략이다. 이는 공격의 중단 및 피해의 최소화를 위해 취하는 조치로 귀속의 증명보다는 위협을 사전에 탐지하고 공격 수단을 처리하는 데 그 초점이 맞추어져 있다.

문제는 이러한 조치가 또 하나의 사이버공격을 구성할 수도 있고, 조치의 대상이 되는 공격의 거점이 실제 공격자와는 관련이 없는 곳에 위치할 가능성이 높다는 점이다. 즉, 공격과는 진정한 관련성이 없는 제3국의 기반시설이나 민간 시스템이 조치의 대상이 되는 경우가 대부분이기 때문에 조치의 강도 및 결과에 따라 국제법위반의 문제가 발생할 수 있는 것이다.

특히 적극적 방어는 사전적 조치의 개념을 포함하고 있다. 본 논문에서는 국제법 규율의 대상이 되는 사이버공격의 발생시점을 목표 시스템 장악 후 이를 손상시키는 명령이 실행된 시기로 보고 분석을 진행하였다. 이는 국가들의 국제적 차원의 논의 및 국제법 연구에서 문제 삼고 있는 사이버공격이 국가안보에 영향을 주는 최소한의 피해 발생을 전제로 하고 있다는 점을 반영한 것이다. 이에 따르면 시기상 탐지된 위협에 대한 국제법상의 조치가 정당화 될 수 있는 시점은 피해발생이 시작된 시점이라고 볼 수 있다.

그러나 사전적 대응을 목적으로 하는 적극적 방어개념은 목표시스템 내부에 접근하지 않은 외부 네트워크에서 탐지된 위협을 타국에 위치한 네트워크에까지 추적해 들어가 찾아낸 봇넷이나 C&C서버를 제어하거나 무력화시키는 조치를 포함하고 있다. 이는 시기상 국제법이 허용하는 것보다 훨씬 앞선 시점에서 이루어지는 조치이며, 조치 그 자체로 대상 시스템에 손상을 초래할 수 있다는 점에서 국제법위반의 문제가 발생할 수 있다.

이는 적극적 방어조치가 사이버공격의 억지를 위한 현실적 필요성에도 불구하고 엄격한 기준을 바탕으로 국제법에 의해 규율되어야 할 필요성이

836) Eric Talbot Jensen, *supra* note 112, pp. 230-231.

있음을 역설한다. 문제는 적극적 방어가 국가들이 국내적으로 마련하고 있는 안보전략차원에서 언급되고 있을 뿐, 국제사회 차원에서는 논의된 바가 없다는 점이다. 사이버공격과 관련한 국제법 연구에서도 국가들이 마련하고 있는 적극적 방어 전략이 국제법 체제 안에서 어떤 문제점을 가지는지 검토된 바가 없기는 마찬가지다.

이에 본 논문에서는 국가들이 국내적 대응전략으로 마련하고 있는 적극적 방어 개념이 국제법의 틀 내에서 충분히 규율이 가능한지에 대해 검토하였다. 이를 위해서 적극적 방어조치시 그 시기 및 대상과 관련하여 발생할 수 있는 위법성의 문제가 자위권, 대응조치, 긴급피난과 같은 국제법상의 위법성 조각사유에 의해 정당화될 수 있는지에 중점을 두고 분석하였다. 즉, 공격자가 명확하게 밝혀지지 않은 상황에서 위협적인 흐름이 발생하고 있는 공격거점에 우선적으로 조치를 취하는 것과 국제법위반에 해당하는 사이버공격이 발생하기 전에 조치를 취하는 것이 현행 국제법체제 내에서 허용될 수 있는지에 대해서 살펴보았다.

먼저 자위권과 대응조치의 대상은 공격주체와의 관련성이 성립되는 국가 내의 시스템이어야 한다는 점에서 공격의 주체와 관련성 없이 수단에 불과한 공격거점이 주로 조치의 대상이 되는 적극적 방어조치와 구별된다는 점을 살펴보았다. 시기와 관련해서는 비례성 원칙을 중심으로 목표 시스템 장악 전에 실행한 적극적 방어조치를 자위권 또는 대응조치가 행사된 것으로 볼 수 있는지 여부를 판단하였다. 즉, 자위권 또는 대응조치의 실행시기가 공격 발생 전으로 앞당겨질 수 있는가에 대해 검토하였다. 자위권은 발생한 무력공격 또는 임박한 무력공격을 방어하기 위한 목적에 비례하게 행사되어야 한다. 그러나 사이버공격의 경우, 공격이 발생하기 전 위협 탐지 단계에서는 공격의 강도를 예측할 수 없다는 점에서 이 단계에서 취한 조치를 무력공격의 격퇴를 목적으로 한 자위권의 행사로 볼 수는 없다. 한편 대응조치의 경우에는 2001년 국가책임초안에서 국제위법행위의 심각성을 고려하여 입은 피해에 비례하게 취해져야 한다고 규정하고 있다. 이 때, 국제법 위반에 해당하는 피해의 요건을 완화하여 목표시

스템이 아닌 기관 내 개인 컴퓨터에 대한 바이러스 감염을 국제법 위반에 따른 피해발생으로 본다고 해도 이 단계에서 취하는 공격거점 무력화조치는 입은 피해를 초과하는 조치가 되어 대응조치로 정당화되기는 어렵다.

이에 마지막으로 위법행위의 발생과 귀속의 증명이 요구되지 않는 긴급피난의 개념을 확대 적용할 경우, 공격 발생 전에 취한 적극적 방어조치를 모두 포섭할 수 있는지에 대해 검토하였다. 긴급피난이 상대방의 위반행위를 전제로 하지 않는다는 점을 생각할 때, 원용 시기를 어느 정도 앞당길 수는 있다. 그러나 긴급피난은 위법성조각사유 중에서도 예외적으로 인정되는 개념으로 이를 원용하기 위해서는 엄격한 요건을 충족해야 한다. 즉, 발생한 위험이 '국가의 본질적 이익에 대한 중대한 위반'을 구성하고, 긴급피난 행위가 그러한 위험으로부터 자신을 보호하기 위한 유일한 방법이어야 하며, 긴급피난 행위가 발생한 위험보다 덜 심각하고 위급한 국제의무를 불이행하는 조치여야 하는 등의 요건을 만족해야 한다. 반면 적극적 방어조치 실행을 위한 판단 기준은 탐지된 흐름의 위협성 하나뿐이다. 긴급피난의 원용을 위한 엄격한 요건이 이와 같은 수준으로 수렴될 수 있는지에 대해서는 검토가 필요하다.

이를 위해 특정기관의 내부시스템 운영정지를 목표로 하는 APT공격과정에서 취하는 적극적 방어조치를 긴급피난에 적용해보았다. 지능적 탐지기법을 통해 위협이 기관 외부의 네트워크에서 탐지된 경우, 포착한 흐름의 위협성이 확인되었기 때문에 적극적 방어조치 실행기준을 충족한다. 그러나 이 경우에 취하는 조치를 국가의 본질적 이익에 대한 중대한 위반을 구성하는 위험으로 보기는 어렵다. 이 단계에서는 탐지된 위협의 목표가 특정기관의 내부시스템인지 여부를 파악할 수 없기 때문이다. 이는 적극적 방어의 광범위한 조치시기 및 조치 실행기준을 포용하기 위해 긴급피난의 엄격한 요건을 완화·수정하는 데는 한계가 존재함을 의미한다. 따라서 긴급피난이 포용할 수 없는 범위에서 취하는 적극적 방어조치를 국제법 내에서 어떻게 규율할 것인지에 관한 논의가 필요하다.

한편 적극적 방어조치도 사이버공간상에서 이루어지는 조치이기 때문에

은밀하게 진행될 경우 국제법을 통한 규제가 어렵다. 이에 적극적 방어조치 실행시 이에 대한 사후공개절차 마련이 필요함을 강조하였다. 이밖에도 조치의 강도 및 대상의 제한, 위협의 정확도 등 적극적 방어조치를 통한 대응을 위해서는 명확히 해야 할 사항이 많다. 따라서 이러한 사항들을 기존의 국제법개념을 적극적 방어에 적용할 수 있는 것으로 해석하는 차원의 수준보다는 국제적 차원에서 국가들의 논의를 통해 명확한 기준 및 제한사항과 절차를 마련하는 것이 보다 적절하다는 결론을 제시하였다.

적극적 방어조치가 공격의 거점에 대한 대응을 통해 공격의 중단에 초점을 맞춘 것이라면 공격자에 대한 직접적인 대응은 귀속의 증명과 관계가 있다. 귀속의 입증을 통해 공격자를 찾아내야 이에 대한 처벌 및 제재가 이루어질 수 있기 때문이다. 피해국이 유포지를 탐지하여 사이버공격을 실시간으로 억지했다고 해도 공격자는 언제든 해킹을 통해 다른 유포지를 획득하여 공격을 시도할 수 있다. 따라서 공격자에 대한 직접적인 처벌이나 제재가 이루어지지 않는다면 사이버공격에 대한 진정한 억지가 이루어졌다고 볼 수 없다.

이 논문에서는 국가들 및 학계에서 귀속의 입증이 기술의 발전에 달려있다고 생각하는 경향이 있다는 점을 문제로 지적하였다. 즉, 공격행위자를 확인하는 것에서부터 위반행위의 국가귀속성을 판단하는 문제까지 추적기술의 발전에 따라 해결될 수 있다고 전제하고 기술의 발전에 귀속입증의 문제를 맡겨두고 있는 것이다.

그러나 이 논문에서는 귀속의 입증이 결코 기술의 문제만이 아님을 살펴보았고, 귀속의 입증이 어려운 결정적인 요인은 조사협조 의무의 부재라는 점을 확인하였다. 이에 귀속의 입증을 위한 조사협조의무를 확립하는 것이야말로 이 문제를 해결하는 데 적절하다는 점을 제시하였다.

이상의 논의를 종합해보면 초국경적인 사이버공격에 효과적으로 대응하면서도 공격억지를 위한 조치의 남용을 규제하기 위해서는 사이버공간의 특성을 반영한 다자조약체제의 마련이 필요하다는 결론에 이르게 된다. 적극적 방어조치를 통한 사이버공격의 즉각적 억지와 귀속의 증명을 통한

공격자에 대한 직접적 조치, 이 두 차원의 대응이 다자조약체제의 마련을 통해 균형 있게 규율된다면 사이버공격에 대한 국제법의 규범성은 강화될 수 있을 것이다.

참고문헌

1. 국내문헌

●단행본

국방기술품질원, 국방과학기술용어사전, (국방기술품질원, 2011).
김대순, 국제법론, 제18판 (삼영사, 2015).
김석현, 국제법상 국가책임 (삼영사, 2007).
도경옥, 비국가행위자의 테러행위에 대한 무력대응 (경인문화사, 2011).
대한민국, 대한민국 국방백서 (2012).
양대일, 정보보안개론 (한빛아카데미, 2013).
이태희·임홍근, 법률영어사전, (법문사, 2007)
정인섭, 신국제법 강의-이론과 사례, 제7판 (박영사, 2017).

●논문

강정호, “빅 데이터를 이용한 선제적 사이버전 강화 방안 연구”, 보안공학연구논문지, Vol. 13, No. 3 (2016).
김영환, 이수진, “공세적 통합 사이버작전을 위한 사이버 킬체인 전략”, 보안공학연구논문지, Vol. 13, No. 5 (2016).
고경민, 이희진, 장승권, “북한의 IT 딜레마와 이중전략:인터넷 정책과 소프트웨어 산업정책을 중심으로”, 정보화정책, Vol. 14, No. 4 (2007).
도경옥, “시리아 내 ISIL 공습에 대한 국제법적 분석”, 국제법학회 논총, 제1권 제1호 (2016).
박기갑, “사이버 전쟁 내지 사이버공격과 국제법”, 국제법 평론, Vol. 32, No. 2 (2010).
박노형, “미국의 사이버안전에 관한 법 제정 동향과 시사점”, 법제연구

, Vol. 46 (2014).
성봉근, “제어국가에서 해킹제어와 방식”, 토지공법연구, Vol. 77 (2017).
신범식, “러시아의 사이버안보의 전략과 외교”, 서울대학교 국제문제 연구소 워킹페이퍼 (2017).
이수강, 김성민, 김명섭, “네트워크 트래픽을 이용한 사이버공격 발생원 추적방법”, 한국통신학회 학술대회 논문집 (2016).
이정석, 이수진, “북한 사이버공격에 대한 국제법적 검토를 바탕으로 한 국방 사이버전 수행 발전 방향”, 보안공학연구논문지, Vol. 12, No. 4 (2015).
임종인, 권유중, 장규현, 백승조, “북한의 사이버 전력 현황과 한국의 국가적 대응전략”, 국방정책연구, Vol. 29, No. 4 (2013).
장노순, “사이버안보와 국제규범의 발전: 정부전문가그룹(GGE)의 활동을 중심으로”, 정치·정보연구, Vol. 19, No. 1 (2016).
조강유·장대일·김민수·정현철·노봉남, “트래픽 프로파일링 방법을 통한 봇넷 탐지기법”, 한국정보기술학회 논문지, Vol. 9, No. 9 (2011).
제성호, “유엔헌장상의 자위권 규정 재검토”, 서울국제법연구, 제17권 제1호 (2010).
한국정보통신기술협회, “정보보호기술용어”, 한국정보통신기술협회 (2013).
허재준, 이상철, “스턱스넷의 감염 경로와 대응방안”, 정보보호학회지, Vol. 21, No. 7 (2011).

2. 국외문헌

●단행본

Akhgar, Babak, and Yates, Simeon, (ed.), *Strategic Intelligence Management-National Security Imperatives and Information and Communications Technologies* (Butterworth-Heinemann, 2013).

Arquilla, John & Ronfeldt, David (Eds.), *Networks and netwars: The future of terror, crime and militancy* (RAND Corporation, 2001).

Baumard, Philippe, *Cybersecurity in France* (Springer, 2017).

Brownlie, Ian, *International Law and the Use of Force by States* (Oxford University Press, 1963).

Carr, Jeffrey, *Inside Cyber War* (O'Reilly, 2010).

Chadwick A, and P. N., Howard, eds., *Routeledge Handbook of Internet Politics* (London: Routledge, 2009).

Chen, Thomas M., *Cyberterrorism after Stuxsnet* (U.S. Army War College Press, 2014).

Clarke, Richard A. and Knake, Robert K., *Cyber War: The Next Threat to National Security and What to Do About It* (Harper Collins e-books, 2010).

Colarik, Andrew M., *Cyber Terrorism: Political and Economic Implications* (Idea Group Publishing, 2006).

Colarik, Andrew M. and Janczewski, Lech J., *Cyber Warfare and Cyber Terrorism* (Information Science Reference, 2007).

Collings, Deirdre and Rohozinski, Rafal, *Shifting Fire: Information Effects in Counterinsurgency and Stability Operations* (Center for Strategic Leadership, US Army War College and the Advanced Network Research Group, 2006).

Crawford, James, *State Responsibility: The General Part* (CUP, 2013).

Crawford, James, Pellet, Alain, Olleson, Simon (eds.), *The Law of International Responsibility* (Oxford University Press, 2010).

Czosseck, Christian and Podins, Karlis (eds.), *Conference on Cyber Conflict Proceedings* (CCD COE Publications, 2010).

Czosseck, Christian, Tyugu, E, Wingfield T (Eds.), *2011 3th International Conference on Cyber Conflict* (NATO CCD COE Publications, 2011).

Czosseck, Christian, Ottis, R., Ziolkowski, K (Eds.), *2012 4th International Conference on Cyber Conflict* (CCD COE Publications, 2012).

Czosseck, Christian, Geers, Kenneth (Eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press, 2009)

Davidoff, Sherri, Ham, Jonathan, *Network Forensics: Tracking Hackers Through Cyberspace*, (Prentice Hall, 2012).

Deibert, Ronald Palfrey, John, Rohozinski, Rafal and Zittrain, Jonathan (eds.), *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (Cambridge, MIT Press, 2011).

Dickinson, Edwin De Witt, *The Equality of States in International Law* (Cambridge, Mass.: Harvard University Press, 1920).

Dinniss, Heather Harrison, *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012).

Dinstein, Yoram, *War, aggression and self-defence* (Cambridge University Press, 2011).

Ebbesson, Jonas, Jacobsson, Marie, Klamberg, Mark, Langlet, David and Wrange, Pål (eds), *International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi* (Brill/Nijhoff, 2014).

P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2014).

Fijnaut, Cyrille, Wouters, Jan and Naert, Frederik(eds.), *Legal Instruments in the Fight against International Terrorism*: A Transatlantic Dialogue (Nijhohh, 2004).

Gray, Christine, *International Law and the Use of Force*, 3rd ed. (Oxford University Press, 2008).

Guiora, Amos N., *Cybersecurity: Geopolitics, law and policy* (Routledge, 2017).

Healey, Jason (ed.), *A fierce domain : conflict in cyberspace, 1986 to 2012* (Cyber Conflict Studies Association, 2013).

Hine, Christine(ed.), *Virtual Methods: Issues in Social Research on the Internet* (Berg Publishers, 2005).

Hoffman, Wyatt and Levite, Ariel E., *Private Sector Cyber Defense-Can Active Measures Help Stabilize Cyberspace?* (Carnegie Endowment for International Peace, 2017).

Jarvis, Lee, Macdonald, Stuart and Chen, Thomas M.(eds.), *Terrorism online: politics, law and technology* (Taylor & Francis Group, 2015).

Jennings, Robert and Watts, Adam (eds.), *Oppenheim's International Law*, 9th edn., Vol. 1 PEACE (London: Longman, 1992).

Jun, Jenny, LaFoy, Scott, Sohn, Ethan, *North Korean's Cyber Operations-Strategy and Responses*, CSIS (Rowman&Littlefield, 2015).

Kelsen, Hans, *Collective Security under International Law*, Studies of International Law Publication 49 (US Naval War College,

1954).

Kim, Zetter, *Countdown to Zero Day : Stuxnet and the launch of the world's first digital weapon* (Crown Publishers, 2014).

Kittichaisaree, Kriangsak, *Public International Law of Cyberspace* (Springer, 2017).

Kundu, Malay Kumar, Mohapatra, Durga Prasad, Konar, Amit, Chakraborty, Aruna(eds.), *Advanced Computing, Networking and Informatics-Volume 2* (Springer, 2014).

NATO Cooperative Cyber Defence Centre of Excellence, *The Tallinn Manual on International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013).

_____, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd Edition (Cambridge University Press, 2017).

Oppenheim, Lassa and Lauterpacht, Hersch, *International Law: A Treatise. Vol. I, Peace*, 8th edn. (London: Longman, 1955).

Osula, Anna-Maria and Rõigas, Henry, (Eds.), *International Cyber Norms-Legal, Policy & Industry Perspectives* (NATO CCD COE Publications, 2016).

Owens, William A., Kenneth W. Dam, and Herbert S. Lin (eds)., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (The National Academies Press, 2009).

P. Brangetto, M. Maybaum, J. Stinissen (Eds.), *6th International Conference on Cyber Conflict* (NATO CCD COE Publications, 2014).

Perkovich, George and Levite, Ariel E. Eds, *Understanding Cyber Conflict: Fourteen Analogies* (Georgetown University Press, 2017).

Prosise, Chris and Mandia, Kevin, *Incident Response & Computer Forensics*, 2nd ed. (Mcgraw-Hill, 2003).

Radziwill, Yaroslav, *Cyber-Attacks and the Exploitable Imperfections of International Law*, (Brill Nijhoff, 2015).

Reich, Pauline C. & Gelbstein, Eduardo eds., *Law, Policy and Technology: Cyber Terrorism, Information Warfare, Digital and Internet Immobilization* (IGI Global, 2010).

Richet, Jean-Loup(ed.), *Cybersecurity Policies and Strategies for Cyberwarfare Prevention* (IGI Global, 2015).

Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (Broadway Paperbacks, 2012).

Sharp, Walter Gray, *Cyberspace and the Use of Force* (Aegis Research Corporation, 1999).

Shaw, Malcolm N., *International Law*, 7th ed. (Cambridge University Press, 2014).

Simma, Bruno, Khan, Daniel-Erasmus, Nolte, Gerog and Paulus, Andreas (eds.), *The Charter of the United Nations: A Commentary* 3rd ed. (Oxford Universith Press, 2012)

Sims, Jennifer E. and Gerber, Burton L.(eds.), *Transforming US Intelligence* (Georgetown University Press, 2005).

Sklerov, Matthew J., *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent* (US Navy Office of the Judge Advocate

General, 2009).

Stanger, Roland J.(ed.), *Essays on Espionage and International Law* (OHIO state university press, 1962).

The Commission on the Theft of American Intellectual Property, *IP Commission Report* (The National Bureau of Asian Research, 2013).

Valeriano, Brandon, and Maness, Ryan C., *Cyber War versus Cyber Realities-Cyber Conflict in the International System* (Oxford University Press, 2015).

Wolfrum, Rudiger and Roben, Volker (eds), *Developments of International Law in Treaty Making* (Springer, 2005).

Wolfrum, Rudiger (ed.), *Max Planck Encyclopaedia of Public International Law* (Oxford Public International Law, 2015).

Yearbook of the International Law Commission, 1980, Vol. II, Part One (United Nations, 2001).

Yearbook of the International Law Commission Vol. II, Part Two (United Nations, 2001).

Ziolkowski, Katharina (ed.), *Peacetime Regime For State Activiteis in Cyberspace. International Law, International Relations and Diplomacy* (NATO CCD COE Publications, 2013).

●논문

Abrams, Marshall and Weiss, Joe, “Malicious Control System Cyber Security Attack Case Study-Maroochy Water Services, Australia”, The MITRE Corporation (2008).

Albright, David, Brannan, Paul, and Walrond, Christina, “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz

Enrichment Plant?", Institute for Science and International Security Report (2010).

Allan, Collin S., "Attribution Issues in Cyberspace", Chicago-Kent Journal of International and Comparative Law, Vol. 13, No. 2 (2013).

Asghari, Hadi, Ciere, Michael, and Eeten, Michel J.G. van, "Post-Mortem of a Zombie: Conficker Cleanup After Six Years", 24th USENIX Security Symposium (2015).

AsSadhan, Basil, Moura, Jose´ M.F., "An efficient method to detect periodic behavior in botnet traffic by analyzing control plane traffic", Journal of Advanced Research, Vol. 5 (2014).

Baker, Stewart, Waterma, Shaun, George Ivanov, "In the Crossfire-Critical Infrastructure in the Age of Cyber War", McAfee (2010).

Banks, William, "The Role of Counterterrorism Law in Shaping *ad bellum* Norms for Cyber Warfare", International Law Studies, Vol. 89 (2013).

Barkham, Jason, "Information Warfare and International Law on the Use of Force", New York University Journal of International Law & Politics, Vol. 34 (2001).

Blair, Dennis C. et al., "Into the Gray Zone-The Private Sector and Active Defence against Cyber Threats-", Center for Cyber & Homland Security (2016).

Borghard, Erica D. and Lonergan, Shawn W., "Can States Calculate the Risks of Using Cyber Proxies?", Orbis, Vol. 60, No. 3 (2016).

Bowett, Derek "Reprisals Involving Recourse to Armed Force",

Americal Journal of International Law, Vol. 66 (1972).
Brenner, Susan W., “At Light Speed”: Attribution and Response to Cybercrime/Terrorism/Warfare, Journal of Criminal Law & Criminology, Vol. 97 (2007).
Brotman, Stuart N., “Multistakeholder Internet governance: A pathway completed, the road ahead”, Center for Technology Innovation (2015).
Brown, Cameron S. D., “Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice“, International Journal of Cyber Criminology, Vol. 9, No. 1 (2015).
Brown, Gary and Poellet, Keira, “The Customary International Law of Cyberspace”,Strategic Studies Quarterly, Vol. 6 No. 3 (2012).
Buchan, Russell, “Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?”, Journal of Conflict & Security Law, Vol. 17, No. 2 (2012).
Buchan, Russell, Roscini, Marco, Tsagourias, Nicholas, “State Responsibility for Cyber Operations: International Law Issues, British Institute of International and Comparative Law (2014).
Bürgin, Annina & Schneider, Patricia, “Regulation of Private Maritime Security Companies in Germany and Spain: A Comparative Study”, Ocean Development & International Law, Vol. 46, No. 2 (2015).
Caldwell, Tracey, “Ethical hackers: putting on the white hat”, Network Security (2011).
Charney, Scott et el., “From Articulation to

Implementation-Enabling Progress on Cybersecurity Norms", Microsoft (2016).

Choo, Kim-Kwang Raymond, "The cyber threat landscape: Challenges and future research directions", Computers & Security, Vol. 30 (2011).

Christakis, Karine Bannelier, "Cyber Diligence: A Low-Intensity Due Diligence Principle for Low Intensity Cyber Operations?", Baltic Yearbook of International Law, Vol. 14 (2014).

Clem, A., Galwankar, S., and Buck, G., "Health implications of cyber-terrorism", Prehospital and Disaster Medicine, Vol. 18. No.3 (2013).

Clough, Jonathan, "A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization", Monash University Law Review, Vol. 40, No. 3 (2014).

Coldebella, Gus P. and White, Brian M., "Foundational Questions Regarding the Federal Role in Cybersecurity', Journal of National Security Law and Policy, Vol. 4 (2010).

Cirlig, Carmen Cristina, "Cyber Defence in the EU-Preparing for cyber warfare?", European Parliamentary Research Service (2014).

Cohen, Matthew S., Freilich, Charles D., Siboni, Gabi, "Israel and Cyberspace: Unique Threat and Response", International Studies Perspectives(2016), Vol. 17, No. 3.

Condron, Sean M., "Getting It Right: Protecting American Critical Infrastructure In Cyberspace", Harvard Journal of Law &

Technology, Vol. 20, No. 2 (2007).
Conway, Maura, "Against Cyberterrorism," Communications of ACM, Vol. 54, No. 2 (2011).
Craig, Amanda N., Shackelford, Scott J., Hiller, and Janine S., "Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis", American Business Law Journal, Vol. 52, No. 4 (2015).
Crawford, Michael and Miscik, Jami, "The Rise of the Mezzanine Rulers: The New Frontier for International Law", Foreign Affairs, Vol. 89, No. 6 (2010).
Creekman, Daniel M., "A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China", American University International Law Review, Vol. 17, No. 3 (2002).
Deibert, Ronald J., Rohozinski, Rafal, Crete-Nishihata, Masashi, "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war", Security Dialogue, Vol. 43, No. 1 (2012).
Denning, Dorothy E., "Framework and principles for active cyber defense", Computers & Security, Vol. 40 (2014).
Dever, John and Dever, James, "Cyberwarfare: Attribution, Preemption, and National Self Defense", Journal of Law & Cyber Warfare, Vol. 2 (2013).
Egozi, Arie, "The Secret Cyber War", Military Technology, Vol. 35, No. 3 (2011).
EWI/IISI, "Critical Terminology Foundations 2" (2011).
_____, "The Russia - U.S. Bilateral on Cybersecurity-Critical

Terminology Foundations 2, Issue 2" (2014).
Falliere, Nicolas, Murchu, Liam O, and Chien, Eric, "W32.Stuxnet Dossier Version 1.4", Symantec (2011).
Farwell, James P. & Rohozinski, Rafal, "Stuxnet and the Future of Cyber War", Survival Global Politics and Strategy, Vol. 53, No.1 (2001).
Finnemore, Martha, Hollis, Duncan B., "Constructing Norms for Global Cyber Security", American Journal of International Law (2016).
Foltz, Andrew C., "Stuxnet, Schmitt Analysis, and the Cyber "Use of Force" Debate", JFQ, Vol. 67, No. 4 (2012).
Franzese, PW, "Sovereignty in Cyberspace: Can It Exist?", Air Force Law Review, Vol. 64 (2009).
Geers, Kenneth, Kindlund, Darien, Moran, Ned, Rachwald, Rob, "World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks", FireEye (2013).
Georgiades, Eugenia, William Caelli, Sharon Christensen, W.D. Duncan, "Crisis on Impact: Responding to Cyber Attacks on Critical Information Infrastructures", The John Marshall Journal of Information Technology & Privacy Law, Vol. 30, No. 1 (2013).
Giacomello, Giampiero, "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism", Studies in Conflict & Terrorism, Vol. 27 (2004).
Giordano, Scott M., "Electronic Evidence and the Law", Information Systems Frontiers, No. 6, No. 2 (2004).
Graham, David E., "Cyber Threats and the Law of War", Journal

of National Security Law & Policy, Vol. 4 (2010).

Grosswald, Levi, "Cyberattack Attribution Matters Under Article 51 of the U.N. Charter", Brooklyn Journal of International Law, Vol. 36, No. 3 (2011).

Halberstam, Manny, "Hacking Back: Reevaluating the legality of retaliatory Cyberattacks", The George Washington International Law Review, Vol. 46 (2013).

Heinegg, Wolff Heintschel Von, "Territorial Sovereignty and Neutrality in Cyberspace", International Law Studies, Vol. 89 (2013).

Herring, MJ, Willett, KD, "Active Cyber Defense: A Vision for Real-Time Cyber Defense", Journal of Information Warfare, Vol. 13, No. 2 (2014).

Herzog, Stephen, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", Journal of Strategic Security, Vol. 4 No. 2 (2011).

Hinkle, Katharine C., "Countermeasures in the Cyber Context: One More Thing to worry about", The Yale Journal of International Law, Vol. 37 (2011).

Hoisington, Matthew "Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense", Boston College International & Comparative Law Review, Vol. 32, No. 2 (2009).

Hsu, Kimberly, Murray, Craig, "China and International Law in Cyberspace", US-China Economic and Security Review Commission Staff Report (2014).

Hunchuns, Eric M., Cloppert, Michael J., Amin, Rohan M., "Intelligence-Driven Compupter Network Defense

Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Lockheed Martin Corporation (2011).

Hunker, Jeffrey, Hutchinson, Bob, Margulies, Jonathan, "Role and Challenges for Sufficient Cyber-Attack Attribution", Institute for Informaion Infrastructure Protection (2008).

Irion, Kristina, "Government Cloud Computing and National Data Sovereignty", Policy and Internet, Vol. 4 (2012).

Johnson, David and Post, David, "Law and Borders: The Rise of Law in Cyberspace", Stanford Law Review, Vol. 48 (1996).

Jamnejad, Maziar and Wood, Michael "The Principle of Non-Intervention", Leiden Journal of International Law, Vol. 22 (2009).

Jenkins, Antolin, "Defining the Parameters of Cyberwar Operations: Looking for Law in all the Wrong Places?", Naval Law Review, Vol. 51 (2005).

Jensen, Eric Talbot, "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense", Stanford Journal of International Law , Vol. 38, No. 207 (2002).

_____, "Cyber Deterrence", Emory International Law Review, Vol. 26 (2012).

Jun, Jenny, LaFoy, Scott, Sohn, Ethan, "What Do We Know About Past North Korean Cyber Attacks and Their Capabilities?", CSIS (2014).

Jinks, Derek, "State Responsibility for the Acts of Private Armed

Groups", Chicago Journal of International Law, Vol. 83, No. 4 (2003).

Kallberg, Jan, "A Right to Cyber Counter Strikes-The Risks of Legalizing Hack Back", IT Professional, Vol. 17, No. 1 (2015).

Kanuck, Sean, "Sovereign Discourse on Cyber Conflict under International Law", Texas Law Review, Vol. 88 (2009-2010).

Kaspersen, Henrik W K, "Cybercrime and Internet Jurisdiction", Council of Europe (2009).

Kastenberg, Joshua E., "Changing the Paradigm of Internet Access from Government Information Systems: A Solution to the Need for the DOD to Take Time-Sensitive Action on the Niprnet", Air Force Law Review, Vol. 64 (2009).

_____, "Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law", 64 Air Force Law Review, Vol. 64 (2009).

Katyal, Neal K., "Community SelfHelp", Journal of Law, Economics and Policy, Vol. 1 (2005).

Kennedy, Daniel, "Deciphering Russia: Russia's Perspectives on Internet Policy and Governance", Global Partners Digital (2013).

Kesan, Jay P. and Hayes, Carol M., "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace", Harvard Journal of Law & Technology, Vol. 25, No. 2 (2012).

Kim, Yong-Ho & Park, Won Hyung, "A study on cyber threat

prediction based on intrusion detection event for APT attack detection", Multimedia Tools and Applications, Vol. 71, No. 2 (2014).

Klimburg, Alexander, "Mobilising Cyber Power", Survival, Vol. 53, No. 1 (2011).

Kirchner, Stefan, "Beyond Privacy Rights: Cross-Border Cyber Espionage and International Law", John Marshall Journal of Information Technology & Privacy Law, Vol 31, p. 2 (2014).

Kissel, Richard eds., "Glossary of Key Information Security Terms, NIST US Department of Commerce" (2013).

Koh, Harold Hongju, "International Law in Cyberspace", USCYBERCOM Inter-Agency Legal Conference (2012).

Korns, Stephen W. and KastenbergJoshua E., "Georgia's Cyber Left Hook", Parameters (2008).

Krasavin, Serge, "What is Cyberterrorism?", Computer Crime Research Center (CCRC, 2001-2002).

Krepinevich, Andrew F., "Cyber Warfare: A 'Nuclear Option?'", Center for Strategic and Budgetary Assessments (2012).

Lachow, Irving, "Active Cyber Defense-A Framework for Policymakers", Center for a New American Security (2013).

Leder, Felix, Werner, Tillmann, "Know Your Enemy: Containing Conficker", Honeynet Project (2009).

Lee, Robert M., "The Sliding Scale of Cyber Security", SANS Institute (2015).

Lewis, James Andrew, "Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms", Center for

Strategic & International Studies (2014).
Lewis, James Andrew, “US-Japan Cooperation in Cybersecurity”, Center for Strategic & International Studies (2015).
Liang, Christina Schori, “Cyber Jihad: Understanding and Countering Islamic State Propaganda”, Geneva Centre for Security Policy (2015).
Li, Sheng, “When Does Internet Denial Trigger the Right of Armed Self-Defense?”, The Yale Journal of International Law, Vol. 38, No. 1 (2013).
Liff, Adam P., “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War”, The Journal of Strategic Studies, Vol. 35, No. 3 (2012).
Lin, Herbert S., “Offensive Cyber Operations and the Use of Force”, Journal of National Security Law & Policy, Vol. 4 (2010).
Lipson, Howard F., “Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues” Carnegie Mellon Software Engineering Institute (2002).
Liss, Carolin, “(Re)Establishing Control? Flag State Regulation of Antipiracy PMSCs“, Ocean Development & International Law, Vol. 46, No. 2 (2015).
Litwak, Robert and King, Meg, “Arms Control in Cyberspace?”, Wilson Center (2015).
Macˇak, Kubo, “Decoding Article 8 of the International Law Commission’s Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors”, Journal of Conflict & Security Law, Vol. 21, No. 3

(2016).

Majuca, Ruperto P. and Kesan, Jay P., “Hacking Back: Optimal Use of Self-Defense in Cyberspace”, Illinois Public Law and Legal Theory Papers Series, No. 08-20 (2009).

Maurer, Tim, “Cyber Norm Emergence at the United Nations- An Analysis of the Activities at the UN Regarding Cyber-Security”, Belfer Conter (2011).

McDougal, Myres Smith and Feliciano, Florentino P., “International Coercion and World Public Order: The General Principles of the Law of War”, The Yale Law Journal(1958), Vol. 67, No. 5.

McGhee, James E., “Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy”, Journal of Law & Cyber Warfare, Vol. 2 (2013).

_____, “Hack, Attack or Whack: The Politics of Imprecision in Cyber Law”, Journal of Cyber Warfare, Vol. 4 (2014).

McGee, Shane, Sabett, Randy V., Shah, Anand, “Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense”, Journal of Business & Technology Law, Vol. 8, No. 1 (2013).

Messerschmidt, Jan, “Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm”, Colombia Journal of Transnational Law, Vol. 52 (2013).

Mudrinich, Erik M., “Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the

Attribution Problem“, The Air Force Law Review, Vol. 68 (2012).

Murphy, Sean, “The Doctrine of Preemptive Self-Defense”, Villanova Law Review, Vol. 50, No. 3 (2005).

_____, “Terrorism and the Concept of 'Armed Attack' in Article 51 of the UN Charter“, Harvard International Law Journal, Vol. 43 (2002).

Narayanan, Vineeth, “Harnessing the Cloud: International Law Implications of Cloud-Computing”, Chicago Journal of International Law, Vol. 12 (2012).

Nicholson, A, Webber, S, Dyer, S, Patel, T, Janicke, H, “SCADA security in the light of Cyber-Warfare”, Computers & Security, Vol. 31 (2012).

Noor, Elina, “The Problem with Cyberterrorism”, SEARCCT'S Selection of Articles, Vol. 2 (2011).

Nye, Joseph, “Nuclear lessons for cyber security?”, Strategic Studies Quarterly (Winter, 2011).

O'Connell, Mary Ellen, “Cyber Security without Cyber War”, Journal of Conflict & Security Law, Vol. 17 No. 2 (2012).

Ogun, Mehmet Nesip, “Terrorist Use of Internet: Possible Suggestions to Prevent the Usage for Terrorist Purposes”, Journal of Applied Security Research, Vol. 7, No. 2 (2012).

Pawlak, Patryk and Petkova, Gergana, “State-sponsored hackers: hybrid armies?”, Issue Alert in European Union Institute for Security Studies (2015).

Prakash, Rahul and Baruah, Darshana M., “The UN and

Cyberspace Governance." ORF Issue Brief, No. 68 (2014).

Rid, Thomas & Buchanan, Ben, "Attributing Cyber Attacks", Journal of Strategic Studies, Vol. 38 (2015).

Ringas, Eneken Tikk, "Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012", Cyber Policy Process Brief (2012).

Roscini, Marco, "Digital Evidence as a Means of Proof before the International Court of Justice", Journal of Conflict & Security Law, Vol. 21 No. 3 (2016).

_____, "World Wide Warfare - Jus ad bellum and the Use of Cyber Force", Max Planck Yearbook of United Nations Law, Vol. 14 (2010).

Rosenzweig, Paul, "International Law and Private Actor Active Cyber Defensive Measures", Stanford Journal of International Law, Vol. 50, No. 1 (2014).

Scharf, Michael P. and Day, Margaux, "The International Court of Justice's Treatment of Circumstantial Evidence and Adverse Inferences", Chicago Journal of International Law , Vol. 13, No. 1 (2012).

Schmitt, Michael N., "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", Columbia Journal of Transnational Law , Vol 37 (1999).

_____, "*Bellum Americanum* Revisited: US Security Strategy and the *Jus Ad Bellum*", Military Law Review, Vol. 176 (2003).

_____, "Cyber Operations and the Jus Ad Bellum

Revisited", Villanova Law Review, Vol. 56, No. 3 (2011).

_____, "Classification of Cyber Conflict", Journal of Conflict & Security Law, Vol. 17, No 2 (2012).

Schmitt, Michael N. and Pitts, M. Christopher, "Cyber Countermeasures and Effects on Third Parties: The International Legal Regime", Baltic Yearbook of International Law, Vol. 14 (2014).

Schmitt, Michael N., "In Defense of Due Diligence in Cyberspace," Yale Law Journal Forum, Vol. 125 (2015).

Smith, Bruce P., "Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help", Journal of Law, Econimics and Policy, Vol. 1 (2005).

Sommer, Peter and Brown, Ian, "Reducing Systemic Cybersecurity Risk", OECD/IFP Project on Future Global Shocks (2011).

Soraghan, Joseph R., "Reconnaissance Satellites: Legal Characterization and Possible Utilization for Peacekeeping", McGILL Law Journal (1967).

Stahn, Carsten, "International Law at a Crossroads: The Impact of September 11", Zeitschrift für ausländisches öffentliches Recht und Völkerrecht, Vol. 62 (2002).

Terry, James P. "Responding to Attacks on Critical Computer Infrastructure: What Targets? What Rules of Engagement?", Naval Law Review (1999).

Theohary, Catherine A. and Rollins, John, "Terrorist Use of the Internet: Information Operations in Cyberspace", Congressional Research Service (2011).

_____, "Cyberwarfare and

Cyberterrorism: In Brief", Congressional Research Service (2015).

Todd, Graham, "Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition", Air Force Law Review, Vol. 65 (2009).

Tsagourias, Nicholas, "Cyber Attacks, Self-Defence and the Problem of Attribution", Journal of Conflict & Security Law (2012).

_____, "Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts", Journal of Conflict & Security Law (2016).

US Cyber Consequences Unit, "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008", US-CCU Special Report (2009).

Valeriano, Brandon and Maness, Ryan C, "The dynamics of cyber conflict between rival antagonists, 2001-11", Journal of Paece Research, Vol. 51, No. 3 (2014).

Verhoeven, Sten, "Attacks by Private Actors and the Right of Self-Defence", Journal of Conflict & Security Law, Vol. 10 No. 3 (2005).

Watson, Tim, "Offensive defence: thinking like a blackhat", Computer Fraud & Security (2009).

Watts, Sean, "Low-Intensity Cyber Operations and the Principle of Non-Intervention", Baltic Yearbook of International Law, Vol. 14 (2014).

Warf, Barney & Fekete, Emily, "Relational geographies of cyberterrorism and cyberwar", Space and Polity (2015).

Waxman, Matthew C., "The Use of Force against States that

Might Have Weapons of Mass Destruction", Michigan Journal of International Law, Vol. 31 (2009).

_____, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)", The Yale Journal of International Law, Vol. 36, No, 2 (2011).

_____, "Self-defensive Force against Cyber Attacks:Legal, Strategic and Political Dimensions", International Law Studies, Vol 89 (2013).

Weimann, Gabriel, "Cyberterrorism: The Sum of All Fears?", Studies in Conflict & Terrorism (2005).

Weissbrodt, David, "Cyber-Conflict, Cyber-Crime, and Cyber-Espionage", Minnesota Journal of International Law, Vol. 22, No. 2 (2013).

Williams, Simon O., "The Development and International Regulation of Private Maritime Security", The Corbett Centre for Maritime Policy Studies (2014).

Wilson, Clay, "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress", CRS Report for Congress (2003).

_____, "Botnets, Cybercrime, and Cyberterrorism:Vulnerabilities and Policy Issues for Congress", CRS Report for Congress (2008).

Xiang, Y., Lin, Y., Lei, W.L. and Huang, S.J., "Detecting DDOS attack based on network self-similarity", IEE Proc.-Commun., Vol. 151, No. 3 (2004).

Ziolkowski, Katharina, "Ius ad bellum in Cyberspace - Some Thoughts on the "Schmitt Criteria", International Conference on Cyber Conflict for Use of Force (2012).

3. 기타문서

Action against Terrorism Unit Transnational Threats Department, "Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace", OSCE (2013).

Austria, "Austrian Cyber Security Strategy" (2013).

Belgium, "Cyber Security Strategy" (2012).

Canada, "Canada's Cyber Security Strategy For A Stronger and More Prosperous Canada" (2010).

Colombia, Lineamientos de política para la Ciberseguridad y Ciberdefensa" (2011).

Department of Homeland Security Integrated Task Force, "Executive Order 13636: Improving Critical Infrastructure Cybersecurity-Incentives Study Analytic Report", Homeland Security (2013).

Estonia, "Cybersecurity Strategy" (2008).

European Union, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" (2013).

France, "Information Systems Defence and Security: France''s Strategy" (2011).

French Republic, "French White Paper on Defence and National Security" (2013).

Germany, "Cyber Security Strategy for Germany" (2011).

Italy, "2013 National Strategic Framework for cyberspace security" (2013).

Japan, "The First National Strategy on Information Security"

(2006).
Japan, “Cyber Security Strategy, Government of Japan, Cabinet Decision” (2015).
Montenegro, “National Cyber Security Strategy for Montenegro 2013-2017” (2013).
NEC Global, “Commercial facilities as targets: New Threats to critical infrastructure” (2017).
New Zealand, “New Zealand’s Cyber Security Strategy” (2011).
New Zealand, “New Zealand’s Cyber Security Strategy” (2015).
North Atlantic Treaty Organization Standardization Agency (NSA), “NATO Glossary of Terms and Definitions”, NATO AAP-06 Edition (2014).
Norway, “Cyber Security Strategy for Norway” (2012).
OECD, “OECD Council Recommendation on Principles for Internet Policy Making” (2011).
Organization for Security and Co-operation in Europe, “Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection(NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace” (2013).
Poland, “Cyberspace Protection Policy of the Republic of Poland” (2013).
Romania, “Hotărarea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a Romaniei şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică” (2013).
Russia, “Conceptual Views Regarding the Activities of the Armed

Forces of the Russian Federation in the Information Space" (2011).

Saudi Arabia, "Developing National Information Security Strategy for the Kingdom of Saudi Arabia" (2013).

South Africa, "Notice of Intention to make South African National Cybersecurity Policy" (2010).

South Africa, "A national cybersecurity policy framework for South Africa" (2011).

South Korea, "Defense White Paper" (2012).

South Africa, "South African Defence Review 2012" (2012).

Stewart Baker, Shaun Waterma, George Ivanov, "In the Crossfire-Critical Infrastructure in the Age of Cyber War", McAfee (2010).

Switzerland, "National Strategy for the Protection of Switzerland Against Cyber Risks" (2012).

The White House, "The National Strategy to Secure Cyberspace" (2003).

The White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World" (2011).

Turkey, "National Cyber Security Strategy and 2013-2014 Action Plan" (2013).

UKAS, "UKAS Guidance For Certification Bodies Certifying Private Maritime Security Companies Against ISO 28000/ISO 28007-1:2015" (2015).

United Kingdom, "Parliamentary Office of Science & Technology, POSTnote Number 389: Cyber Security in the UK" (2011).

United Kingdom, “The Cost of Cyber Crime” (2011).

UK Home Office, "Security and Intelligence Agencies’ retention and use of bulk personal datasets" (2016) p. 45.

United States of America, “Framework for Improving Critical Infrastructure Cybersecurity” NIST(2014).

US Senate Permenant Subcommittee on Investigations(Minority Staff Statement), “Security in Cuberspace-The Case Study: Rome Laboratory, Griffiss Air Force Base, NY Intrusion”, Congressional Hearings Intelligence and Security (1996).

Abstract

Introduction of the Concept of Active Defense to Regulate Cyber Attacks in International Law

BAEK Sangme

Graduate School of Law,

Seoul National University

The present study aims to come up with effective measures for regulating cyber attacks in international law. Since nation states perceived that cyber attacks could severely affect national security, they have discussed how to deal with the issue in international law. It is because there are differences between cyberspace and physical space. However, the focus of the discussion has been on whether the current international legal frameworks are sufficient for regulating cyber attacks or whether there is a need to adopt a new regime.

Cyberspace transcends constraints of geography and physical location, and it guarantees anonymity. These are general features of cyberspace. In addition to these features, there is an essential characteristic of cyber attacks that has to be considered in order

to draw up adequate response measures on the international law dimensions. It is the unique relationship between the attacker, a means of attack and the target. When the attacker plans to launch a cyber attack, the hacker normally creates botnets and C&C servers in advance and use them as attack points to carry out the attack. Moreover, since the attacker can build several attack points in multiple places and the attack can take various stages, it is extremely difficult to find the attacker by tracing back to the origin of the attack in real time. Therefore, in order to deter cyber attacks in real time, actions should be taken on the attack point first rather than tackling the attribution matter.

Active cyber defense aims to mitigate or deter the detected threat in cyberspace and the measures include disrupting a malicious botnet, blocking traffic from a malicious IP address, and counterstriking C&C server. This means the strategy focuses on proactive threat detection and taking action on attack points in real time not on the attribution.

What makes these measures significant is that the attack points targeted by the active defense measures are normally located in the place that has nothing to do with the attacker. It is particularly problematic when the attack points-botnets or C&C server-consist of critical infrastructure of a third party which has no relevance to the attacker. Then it is highly likely that the measure would not be justified as circumstances precluding the wrongfulness of conduct if the measure exceeds the level of proportionality and severely damages the targeted system. This means that active defense measures undertaken outside the defender's network across international borders, the legality of

the action can be questioned under international law. Furthermore, active defense measures can take place before the threat reaches the attack stage. In other words, the defender can trace the threat beyond its network and take actions although the threat is detected outside home network and even before the attack is launched to the targeted system. In this case, the measures would raise another legality issue since the actions took place before the breach of an international obligation occurs.

These are the reasons why the legality of active defense measures should be re-examined in international law beyond the need for real-time response for practical reasons. Yet, to date, little or no consideration has been given to the question of whether active defense measures violate any principles of international law or conventions while quite a few nations are adopting active defense as their national cyber security strategies.

Therefore, the study examines whether the measures taken against the intermediate server before the attack occurs can be justified in international law. The study especially analyses whether active defense measures can be legitimatized as circumstances precluding wrongfulness under international law: Self-defence, countermeasure and necessity. The study finds that current international law cannot embrace all the measures of active defense. Thus, the study reaches a conclusion that the concept of active defense needs to be adopted through establishing multilateral treaty regime and regulated by international law.

keywords : Attribution, Sources of Attack, Cyber Attack, Proactive Measures, Active Defense
Student Number : 2014-30462