[UCI]I804:24011-200000265344

2016년 2월

박사학위논문

북한의 사이버 위협이 한국안보에 미치는 영향에 관한 연구

- 국가 및 군의 대응방안을 중심으로 -

조선대학교 대학원

정치외교학과

신 동 만

북한의 사이버 위협이 한국안보에 미치는 영향에 관한 연구

- 국가 및 군의 대응방안을 중심으로 -

A Study on the North Korea's cyber threat and its impact on National Security

- Focusing on the Nation and Miltary Countermeasures -

2016년 2월

조선대학교 대학원

정치외교학과

신 동 만

북한의 사이버 위협이 한국안보에 미치는 영향에 관한 연구

- 국가 및 군의 대응방안을 중심으로 -

지도교수 오 수 열

이 논문을 정치외교학 박사논문 신청으로 제출함

2015년 10월

조선대학교 대학원

정치외교학과

신 동 만

신동만의 정치학 박사학위 논문을 인준함

위원장	원광대학교	교수	김 태 웅 (인)
위 원	조선대학교	교수	김 재 철 (인)
위 원	조선대학교	교수	한 관 수 (인)
위 원	건양대학교	교수	이 종 호 (인)
위 원	조선대학교	교수	오 수 열 (인)

2015년 12월 21일

조선대학교 대학원

목 차

표 목 차

그 림 목 차

국문 초록

북한은 1964년 당 중앙위원회 8차 전원회의에서 전 조선 혁명을 위한 3대 혁명역량 강화노선을 주창하였다. 북한은 이와 같은 노선을 근간으로 현재의 김정은 체제에 이르기까지 변화하는 세계질서와 한반도의 안보환경에 유기체와 같이 전략과 조직의 변화를 통하여 체제유지와 대남 적화전략에 주력하고 있다. 김정은은 전쟁계획 '7일 작전계획'를 만들어 한반도에서 7일안에 전쟁을 끝낼 수 있도록 기습과 속전속결 전략으로 사이버전과 물리전을 동시에 연계시키는 공격계획을 작성한 것으로 알려지고 있다. 작전계획의 핵심은 북한의 전면전과 국지전에서 전면전으로 확전될 경우 미군이 본격적으로 개입하지 못하도록 7일안에 남한전역을 점령하겠다는 내용이다. 사이버 공격과 병행하여 핵·미사일 등 비대칭 전력을 사용하여 초반에 기선을 잡고 재래식 전력을 동원하여 미 증원군이 도착하기 전 늦어도 15일 안에 남한을 점령한다는 계획이다.

북한은 현재 6천여 명의 사이버전 전사를 운용하고 있으며 이들은 남한 내부의 심리적, 물리적 마비를 위해 국가기반시설을 공격하여 남한사회의 혼란과 군사작전의 차질을 유발하는 등 사이버 작전을 적극적으로 전개할 것으로 판단하고 있다. 북한의 사이버전 능력은 세계 최고 수준인 미국과 동등하다는 평가를 받는다. 클린턴 행정부와 부시 행정부에서 백악관 안보담당조정관과 안보특별보좌관 등을 지낸 클라크는 북한의 사이버전쟁 수행능력을 세계 최고 수준으로 평가했다.

반면에 대한민국은 인간과 사물, 사물과 사물 등 모든 것이 네트워크로 연결되고 국가의 중요 인프라가 정보통신기술로 연결되는 초 연결사회로 구성되어 있다. 이와 같이 모든 것이 인터넷으로 연결되는 사물인터넷 시대가 도래함에 따라 국가안보에서 사이버전은 무엇보다도 중요한 요인이 되었다. 그렇기 때문에 북한이 사이버 공격에 물리적인 공격을 병행하여 공격시 우리에게 큰 위협이 될 것으로 예상된다. 이러한 사례는 2007년 에스토니아와 2008년 그루지야에서 발생한 사이버전 과 물리전이 결합한 전쟁에서 그 예를 찾아볼 수 있다. 러시아의 소행으로 추정되는 사이버 공격으로 의회, 국방부, 외교부 등 정부의 주요 인터넷사이트가 마비됐다. 사이버 공격직후 수행된 물리적인 공격으로 양국은 전쟁에 돌입했다. 이미 군 정보 시스템의 다운 등으로 지휘체계가 불안해진 그루지야는 전쟁개시 5일 만에 항복하였다. 이 사건은 사이버 공격이 실제 전쟁에 어떤 영향을

미칠 수 있는지를 보여준 최초의 사례였다.

정부는 그동안 수차례의 북한으로 추정되는 적으로부터 사이버 공격을 당하여 정부차원의 대책을 수립하여 왔다. 2013. 6. 25 사이버 테러를 계기로 7. 4일 정부는 청와대를 컨트롤타워로 지정하고, 국가정보원을 실무총괄로 하는 대응체계를 확립한다는 내용의 '국가사이버안보종합대책'을 밝혔다. 그러나 이러한 '국가사이버안보종합대책'에도 불구하고 2014년 12월에 발생한 한국수력원자력 해킹사고는 충격적이었다. 한수원은 정보보안 관리실태 평가에서 양호한 등급을 받았음에도 사고가 발생했기 때문에 파장은 더욱 컸다.

이와 같이 북한의 사이버 위협과 정부의 종합적인 대책에도 불구하고 우리의 사이버 안보실태는 구조적인 제약과 취약점이 있는 실정이다. 따라서 본 논문에서는 북한을 포함한 주요국가의 사이버 안보실태, 우리의 현실태와 대응방안에 대하여 이를 분석할 수 있는 네 가지 핵심요인을 선정하였다. 첫째, 인식과 사상적인 측면 둘째, 국가전략 등 시스템적인 측면 셋째, 공조체계 등 네트워크적인 측면 넷째, 인력과 기술 등 지원적인 측면에서 이들을 분석하였다. 먼저 우리의 사이버 안보실태에 대하여 분석한 문제점은 다음과 같다. 첫째, 사이버위협이 상존하고 있는데도 안보분야에 종사하고 있는 해당 조직은 필요성을 인식하고 있으나 국민과 정부는 사이버 위협의 실체를 정확히 인식하지 못하고 있는 것으로 판단된다. 이는 북한의 사이버 공격이 지속됨에도 불구하고 정부의 조직과 예산의 지원이 미흡한 것을 통하여 알 수 있다. 둘째, 전략과 정책면에서 정부와 군 등 기관별로 구체적인 전략과 정책이 미흡하고 컨트롤타워의 문제점과 분야별 법령과 제도의 중복과 기준이 상이하게 적용됨으로써 북한의 사이버 공격 시 일사분란하게 조치하고 처리할 수 있는 협조체제가 미흡한 실정이다. 셋째, 기관별로 수행체계와 임무와 역할이 상이하여 공조하는데 어려움이 있으며 정보보호 인프라도 기관간의 격차가 심하고 국가 간의 협력체계도 미흡한 편이다. 넷째, 사이버 전문 인력양성이 체계적이지 못하여 전문성이 부족하고 방어위주의 사이버 훈련을 실시하며 기술개발도 민간업체에 의존하고 있는 실정이다.

다음은 국가의 사이버 안보전략을 심도 있게 분석하여 검토할 필요가 있다. 사이버 전장에서 방어에 집중하고 병행하여 공세적으로 사이버 역량을 강화시키는 전략이다. 남북한의 정보통신 의존도를 고려할 때 공격시 우리가 절대적으로 불리하다. 그럼에도 불구하고 북한의 사이버 공격 능력이 아무리 강하다 할지라도 초기작전의 혼란을 방지하기 위해서는 북한의 사이버 공격에 즉각적인 원상복구

능력을 구비해야 할 것이다. 우리가 공격받는 즉시 조기에 회복하여 초기에 혼란을 최소화하는 복원력을 강화하면 한반도에서 사이버 전쟁억제가 달성될 수 있을 것으로 판단된다. 둘째, 누가 실질적인 컨트롤타워의 역할을 할 것인가 하는 점이다. 현재는 청와대 국가안보실에서 총괄임무를 수행하고 실무차원에서 국정원이 주도권을 가지고 그 역할을 담당하고 있다. 그러나 남북한이 대치하고 있는 한반도 안보상황과 정보통신기술의 특성을 고려할 시 사이버공격 상황이 발생하면 실시간으로 상황을 파악하고 조치해야 하는 임무의 특성상 국가의 최고기관에서 야전군사령부와 같은 임무를 수행해야 한다는 문제점이 있다. 따라서 국무총리실 산하에 '국가사이버안전처(가칭)'을 신설하여 총괄과 실무차원의 컨트롤타워의 역할을 수행하게 하는 방안이다. 그리고 사이버 테러의 성격이 국가위기나 전쟁의 성격에 가깝다면 공공영역에서 국가안보에 핵심이 되는 국가기반시설의 일부를 국정원이 주도하는 역할을 하는 것보다는 군에서 담당하는 것이 바람직하지 않나 판단하였다. 이를 위해서 사이버 안보와 관련한 정부의 조직일부의 개편과 법령의 제·개정에 대한 의견을 제시하였다. 셋째, 법령과 제도의 제·개정이 필요한 실정이다. 현재 국회에서 논의하고 있는 사이버 관련 법령의 제·개정은 국정원이 주도하는 입법안으로 국정원이 주도했을 때 국민의 자유와 인권이 침해받을 수 있다는 우려사항과 사이버전과 관련한 다양한 법률가운데 일부 적용이 상이한 문제점을 해결하기 위하여 단일법령으로 제·개정하는 방안을 제시하였다. 그리고 현재의 통합방위법은 물리적인 힘을 통제하는 법령으로 사이버전에서는 적용이 불가능하기 때문에 북한의 사이버 위협이 국가안보에 심대한 영향을 미치는 경우 위기상황과 전시를 대비한 법령과 제도는 정비가 필요한 실정이다. 넷째, 국내 및 국제적인 공조가 중요하다. 사이버전의 특성상 네트워크를 통해 전달되는 데이터의 양과 그 처리속도는 우리의 상상을 초월하고 있다. 수백만 대의 좀비 pc가 동시에 공격시 순식간에 모든 상황이 종료될 수도 있을 것이다. 전쟁이 일어났다는 사실을 인식하는 순간 전쟁이 끝나 버릴 수도 있다는 것이다.

결론적으로 본 논문은 이론적인 면과 각국의 사이버 역량과 북한의 위협을 근거로 하여 정부와 군의 사이버전 대응태세를 진단해 보고 북한이 사이버전을 감행했을 때 즉각적인 조치와 대응으로 초기의 피해를 최소화 할 수 있도록 하는 전략과 누가 주도를 하며 이를 위한 법령과 제도의 정비, 국내 및 국제공조를 어떻게 하는 것이 효과적인지 살펴보아 정부와 군의 대응발전에 기여하도록 하였

다. 특히 북한은 물론 대한민국을 공격하는 적대세력에 대응하기 위해서는 국가적인 대전략 차원에서 한국은 북한보다 강력한 사이버전 수행능력을 갖출 뿐만 아니라 주변 강대국들의 사이버 공격에도 대비할 수 있도록 역 비대칭전력으로 우위를 삼을 필요가 있다. 국가적인 대형 프로젝트를 계획하여 사이버 전력을 육성할 필요성이 있는 것이다. 이를 위해 국가예산을 과감하게 투자하여 양적이나 질적으로 우월하고 뛰어난 화이트해커인 사이버 전사양성에 최선의 노력을 다해야 한다. 방어형 사이버 무기를 지속적으로 개발하고 공격형 사이버 미사일인 한국형 스턱스넷 등을 하루빨리 개발하여 완성하도록 해야 한다. 전문가들은 사이버전쟁에 대비해 국군사이버사령부의 현재 600여명 수준의 인력을 최소 3,000명은 돼야 적절히 방호할 수 있다고 지적한다. 한미 연합작전을 위해서도 연합 사이버 전력을 강화할 필요성도 있을 것이다. 따라서 정부는 전쟁에 대비하여 국군을 설치하고 민・관・군이 총력전으로 대응하는 것처럼 사이버전에서도 정부와 군은 국민의 적극적인 지지와 협조로 사이버 전력을 대폭적으로 보강하여 억제하고 억제 실패시 북한의 어떠한 공격에도 이를 격퇴할 수 있는 능력을 갖추도록 해야겠다. 이를 위해서는 군・관・민이 총력전의 개념을 가지고 적극적인 정보공유와 협력으로 대응전략을 구축하고 대응책을 마련해야 할 것이다. 3차 세계대전은 사이버전이 될 것이라는 미래학자들의 말을 굳이 인용하지는 않아도 사이버 무기는 한반도에서 핵과 미사일과 함께 가장 위협적인 요소가 될 것이기 때문이다. DMZ 지뢰도발 사건 이후에 정부는 확성기 대북방송으로 북한정권의 아킬레스 근을 끊어놓자, 북한은 즉시 고위급 협상을 제안하여 대한민국에 통쾌한 승리를 맛보게 한 것처럼 사이버 전력도 우리의 역 비대칭전력으로 대한민국의 상징적인 프로젝트로 육성할 필요성이 있을 것으로 판단한다.

Abstract

A Study on the North Korea's cyber threat and its impact on National Security

- Focusing on the Nation and Miltary Countermeasures -

Shin, Dong-Man
Advisor : Prof. Oh, Soo Yol
Dep. of Political Science and Diplomacy
Graduate School of Chosun University

In 1964, North Korea advocated a Three-Part Reinforcement of Revolutionary Force in the 8th plenum of the Central Committee of the Worker's Party of Korea. Leading up to the current Kim Jong-un regime, this policy has been at the core of North Korean politics as it organically adapted to the changing conditions in global order and South Korean security to preserve its political system while attempting to communize its southern counterpart. Kim Jong-un is said to have devised a '7-day operational plan,' which is a blitzkrieg use of both physical and cyber force that incorporates swift surprise attacks to finish the war in Korean peninsula within 7 days.

In essence, this strategy relies on occupying the entire South Korean region in 7 days to prevent U.S. intervention if the Korean war was to develop into a total war. By taking the upper hand in the beginning through asymmetric force of nuclear missiles alongside with cyber-attacks, North Korea planned to follow up with conventional force to occupy South Korea in 15 days at the latest before the arrival of U.S. reinforcements.

North Korea currently commands approximately 6 thousand hackers trained in cyber warfare, and it actively employs cyberwarfare strategies such as engaging in cyber-attacks on national infrastructure and disrupting military operations. The cyberwarfare ability of North Korea is considered to be on par with the United States, a global leader in the field. Clarke, who served as the Special Advisor to the President and the National Coordinator for Security,

Infrastructure Protection and Counter-terrorism in the Clinton and Bush administrations, considered the cyberwarfare capability of North Korea to be the world's best.

Conversely, the Republic of Korea is a hyper-connected society in which individuals and objects are connected through a network, and the vital national infrastructures are connected through information technology. In such a generation of Internet of Things (IoT), where everything is connected via the Internet, cyberwar has become a critical factor in national security. This is why North Korea's combined attack through physical and cyber force will be pose a serious threat.

Similar cases can be observed in the 2007 cyberattacks on Estonia and the 2008 Russo-Georgian War. In cyber-attacks that are presumed to be of Russian origin, main government websites including those of the national assembly, ministry of defense, and the ministry of foreign affairs were paralyzed. The two countries engaged in war from the physical attack that followed the cyber-attacks. Georgia, which already had been disoriented in its line of command due to the paralysis of their military information system, surrendered in 5 days. This was the first case that demonstrated the effect of a cyber-attack in actual war.

The South Korean government has developed countermeasures at a national level as it has been under several cyber-attacks that are believed to be conducted by North Korea. Coming out of the cyber terror of June 25, 2013, the government disclosed a 'National Cyber Security Master Plan' that established a response system with the Blue House as the control tower and National Intelligence Service managing operations. However, despite this 'National Cyber Security Master Plan,' the Korea Hydro & Nuclear Power Co. (KHNP) hacking incident in December 2014, was shocking; it was especially shocking because KHNP had a good rating for its information security management when this incident transpired.

Accordingly, despite the threat of North Korean cyber-attacks and a master plan conceived by the government to counter it, the state of our cyber security

is riddled with the following problems due to structural limitations and weaknesses. Hence, in this paper four key factors are selected to comprehensively analyze cyber security status of major countries including North Korea, our current situation and the countermeasures. They are (1) cognitive and ideological aspects, (2) systematic aspects such as national strategy, (3) networking aspects such as a mutual-assistance system, and (4) human resources and technical supports. First of all, the issues of cyber security are as follows. First, in spite of a pervasive cyber-threat only the personnel working in security-related fields are aware of it; it seems that the government and the people are not fully aware of this threat. This is apparent in the inadequacy in the governmental organization and the funds thereof regarding this issue. Second, a system of cooperation that can readily respond to North Korean cyber-attacks is unavailable due to obscurity in the government and departments' related strategy and policy, as well as the discrepancy in legislation for each field under the control tower. Third, the system of delivery as well as the roles of each institution is different, thus causing difficulty in their cooperation. There are also differences in between the institutions in terms of their infrastructure of information protection, and the system of cooperation between nations is also insufficient. Fourth, there is no systemized training for personnel specializing in cyberwarfare, only defense oriented cyberwarfare training is conducted, and private enterprises are relied for technical development.

Next, there is a need for an in-depth review of the nation's cyber security strategy. Along with the focus on defense in cyberwar, this implies a reinforcement in offensive cyber capabilities. Considering the dependence on information and communication in South and North Koreas, we are at an absolute disadvantage. In spite of this, regardless of North Korea's offensive cyber-attack ability, there needs to be a means for a fast recovery in response to a North Korean cyber-attack in order to prevent disorientation in initial operations. If our means of recovery in case of an attack is reinforced to minimize the initial disorientation, it is possible to achieve cyberwar deterrence

in the Korean peninsula. Second, an issue of who becomes the control tower needs to be clarified. Until now, the Blue House performs general duties and the National Intelligence Service takes control and assumes this position.

Considering the confrontational state between the North and the South and characteristics of information technology, when cyber attack happens, it is not adequate for the highest government organization to take duties to grasp the situation and the measure in real time as a field army headquarter does. It is neither appropriate for the National Intelligence Service in the public sector to lead the entire if cyber terror in resembles that of a national crisis or war. I suggest that 'the National Cyber Security Division (tentative name)' newly established under the Prime Minister's Office acts as a control tower and the military take responsible for part of the national infrastructure that is core to national security as opposed that the National Intelligence Service takes all the charges in national infrastructure in public area. For this, reorganization of the government's cyber security organizations and the amendments of relevant legislation are suggested. Third, enactments and revisions of legislations and systems are required. The current legislation bill under discussion in the national assembly led by the NIS is on the enactment and revision of cyber-related legislations, but it may infringe on the freedoms and rights of the people if directed by the NIS. Furthermore, the current United Defense Act are legislations that govern physical force, and cannot be applied in cyberwar. Thus, the legislations and systems must be renewed in case the North Korean cyber threat jeopardizes national security, or a war breaks out between the two parties. Here, I propose to amend various legislation relating to cyber war into a single Act. Fourth, domestic and international cooperation is imperative. As characteristic of cyberwar, the amount of data transmitted over the network and its processing speed are beyond our imagination. If millions of zombie PC's are incorporated in a combined cyber-attack, we will be able to end this situation immediately. In other words, the war might be over by the time we come to realize that we are under attack.

Therefore, this paper diagnoses the government and military's ability to

respond to a cyberwar from the factors of North Korean threat, the cyber capacity of different nations, and other theoretical aspects. Moreover, this paper contributes to government and military policy-making by examining the strategy for minimizing damages when North Korea commences a cyber war, with respect to who will lead, and what legislations and systems, along with domestic and international cooperation, will be effective therein. In particular, in order to respond to North Korea among other hostile forces, South Korea needs to take the upper hand in reverse asymmetric forces by increasing its cyberwar capabilities above that of North Korea to protect itself from other powerful nations. Expressly, there needs to be a large project on a national scale that fosters cyberwar capabilities. The national budget needs to be heavily invested to produce white-hat hackers trained in cyberwarfare superior both in quality and quantity. Defensive cyber weaponry needs to be continuously developed, and a Korean Stuxnet-an offensive cyber-missile-needs to be developed and completed as soon as possible. Experts claim that the 600 personnel currently employed in the National Cyber Command need to be expanded to at least 3000 in order to make sure that South Korea defends itself from cyber attacks adequately. The united cyber capabilities of the U.S. and South Korea would also need to be strengthened to conduct combined operations. Thus, similar to how the government equips and maintains the military as a precaution to war, the government and civilians must provide the active support and cooperation needed for the military to bolster their cyber forces with the ability to readily deter any North Korean attacks and repel them in failure of inhibition.

To accomplish this, the military, government and civilians need to recognize this situation as a total war, actively sharing information and cooperating with the common goal of establishing countermeasures. We do not need to reference futurologists in their saying that the 3rd World War would be a cyberwar; cyber weaponry, along with nuclear missiles, will be the deadliest instrument in the Korean peninsula.

North Korea proposed top-level negotiations when South Korea had Radio

Broadcastings to North Korea. This was South Korea's victory over North Korea as it severed North Korea's Achilles tendon of communications. Cyberwarfare capabilities need to be developed as a characteristic project of the Republic of Korea's reverse asymmetric force.

제1장 서론

제1절 연구의 목적

북한은 현재 6천여 명의 사이버전 인력을 운영하고 있으며 남한 사회의 심리적, 물리적 마비를 목적으로 사이버 공격을 적극적으로 수행하고 있는 것으로 평가된다.[1] 북한의 사이버전 능력은 세계 최고 수준인 미국에 버금간다는 평가를 받는다. 클린턴 행정부와 부시 행정부에서 백악관 안보담당조정관과 안보특별보좌관 등을 지낸 클라크는 북한의 사이버전 수행능력을 세계 최고 수준으로 평가했다. 클라크는 사이버전 수행능력을 사이버공격력과 사이버방어력, 네트워크 의존도로 나눠 분석했다. 미국과 러시아, 중국, 이란, 북한을 대상으로 한 평가에서 북한이 사이버전 수행능력이 가장 뛰어난 것으로 평가한 것이다.

북한은 1964년 당 중앙위원회 8차 전원회의에서 전 조선 혁명을 위한 3대 혁명역량 강화노선을 주창하였다. 북한 내부의 사회주의 혁명역량 강화와 남한내부의 사회주의 혁명역량 강화, 그리고 국제사회주의 혁명역량 강화노선을 채택하였다.[2] 이중에서 북한은 남한의 혁명역량 강화 노선에 총력을 기울이고 있다. 북한은 이와 같은 노선을 근간으로 현재의 김정은 체제에 이르기까지 변화하는 세계질서와 한반도의 안보환경에 유기체와 같이 전략과 조직의 변화를 통하여 체제유지와 대남 적화전략에 주력하고 있는 상황이다.[3]

이러한 북한의 대남 적화전략은 군사적으로 물리전과 사이버전이 결합할 때 시너지 효과를 볼 수 있을 것이다. 이에 반해 한국은 인간과 사물, 사물과 사물 등 모든 것이 네트워크로 연결되고 국가의 중요 인프라가 정보통신기술로 연결되는 등 초 연결사회로 구성되어 있다.[4] 그렇기 때문에 북한이 사이버 공격에 물리적인 공격을 병행하여 공격시 큰 위협이 될 것으로 예상된다. 군사작전과 연계하여 국가기간망과 군에서 운용하는 국방망과 전장 및 자원관리망 등 지휘통제망이 피해를 입고 제대로 대응을 하지 못한다면 계획하고 준비한 대로 대응조

1) 국방부, 『국방백서』, (2014), p.24.
2) 양무진, "장성택 처형이후 북한의 대남정책," 『북한연구학회보』, 제18권 제1호(북한연구학회, 2014), pp.31-32.
3) 유동열, 『사이버 공간과 국가안보』(서울: 북앤피플, 2012), p.34.
4) 이남용, 『창조경제와 국가전략』(서울: 이든북스, 2013), pp.58-63.

치가 어려울 것이다.

이러한 사례는 2008년 그루지야에서 발생한 사이버전과 물리전이 결합한 전쟁에서 그 예를 찾아볼 수 있다. 러시아의 소행으로 추정되는 사이버 공격으로 의회, 국방부, 외교부 등 정부의 주요 인터넷사이트가 마비됐다. 사이버 공격직후 수행된 물리적인 공격으로 양국은 전쟁에 돌입했다. 이미 군 정보시스템의 다운 등으로 지휘체계가 불안해진 그루지야는 전쟁개시 5일 만에 항복하였다.[5] 이 사건은 사이버 공격이 실제 전쟁에 어떤 영향을 미칠 수 있는지를 보여주었다. 이를 통하여 2013년 NATO 사이버 방어협력센터는 사이버 공격을 무력분쟁의 하나로 규정하고 사이버 공격시 인명과 재산피해가 발생하면 피해국가에서 군사력을 사용할 수 있도록 하는 탈린메뉴얼 작성의 계기가 되었다.[6]

정부는 그동안 수차례의 북한으로 추정되는 적으로부터 사이버 공격을 당하여 정부차원의 대책을 수립하여 왔다. 2013. 6. 25 사이버 테러를 계기로 7. 4일 정부는 청와대를 컨트롤타워로 지정하고, 국가정보원을 실무총괄로 하는 대응체계를 확립한다는 내용의 '국가사이버안보종합대책'을 밝혔다. 그러나 이러한 '국가사이버안보종합대책'에도 불구하고 2014년 12월에 발생한 한국수력원자력 해킹사고는 충격적이었다. 한수원은 정부에서 실시한 정보보안 관리실태 평가에서 양호한 등급을 받았음에도 사고가 발생했기 때문에 파장은 더욱 컸다. 이를 계기로 국가의 주요기반시설을 진단해 본 결과 아직도 다수의 공공기관이 정보보안 전담조직은 물론 전문 인력조차 제대로 확보돼 있지 않다는 사실을 확인하였다. 또한 정보보안 예산과 최고경영자(CEO)의 인식도 매우 부족하다는 사실을 알게 되었다. 이번 사건으로 범국가적인 사이버안보 확립 차원에서 적극적인 사이버 보안활동 강화의 필요성을 느끼게 한 것이다.[7]

이와 같이 북한의 사이버 위협과 이에 대한 정부의 종합적인 대책에도 불구하고 우리의 사이버 안보실태는 구조적인 제약요인과 취약점들로 다음과 같은 문제점이 있는 실정이다. 첫째, 사이버위협이 상존하고 있는데도 사이버 안보분야에 종사하고 있는 기관과 조직은 대비에 대한 필요성을 인식하고 있으나 국민과 정부는 사이버 위협의 실체를 정확히 인식하지 못하고 일반적으로 인식하는 경

5) 손영동, 『iWAR』(서울: 황금부엉이, 2010), pp.227-229.
6) 박노형·정명현, "사이버전의 국제법적 분석을 위한 기본개념의 연구,"
『국제법학회논총』, 제59권 제2호(대한국제법학회, 2014), pp.67-69.
7) 박춘식, "한수원 정보유출사고를 통한 교훈," 『파이낸셜뉴스』, 2015년 1월 15일.

향이 있는 것으로 판단된다. 이는 북한의 사이버 공격이 지속됨에도 불구하고 정부의 조직과 예산의 지원이 미흡한 것을 통하여 알 수 있다. 둘째, 전략과 정책면에서 정부와 군 등 기관별로 구체적인 전략과 정책이 미흡하고, 컨트롤타워의 문제점과 분야별로 시행되고 있는 법령과 제도가 일부 중복과 기준이 상이한 점으로 북한의 사이버 공격시 일사분란하게 조치하고 처리할 수 있는 협조체제가 미흡한 실정이다. 셋째, 기관별로 수행체계와 임무와 역할이 상이하여 공조하는데 어려움이 있으며 정보보호 인프라도 기관간의 격차가 심하고 국가 간의 협조체제도 미흡한 편이다. 넷째, 사이버 전문인력 양성이 체계적이지 못하여 전문성이 부족하고 방어위주의 사이버 훈련을 실시하며 기술개발도 민간업체에 의존하고 있는 실정이다.

따라서 국가의 사이버 안보전략을 심도 있게 검토할 필요가 있다. 첫째, 사이버 전장에서 방어에 집중하고 병행하여 공세적으로 사이버 역량을 강화시키는 것이다. 남북한의 정보통신 의존도를 고려할 때 북한의 공격시 우리가 절대적으로 불리하다. 그러나 북한의 사이버 공격 능력이 아무리 강하다 할지라도 초기작전의 혼란을 방지하기 위해서 북한의 사이버 공격 감행시 즉각적인 원상복구 능력을 구비해야 할 것이다. 우리가 공격받는 즉시 조기에 원상회복하여 초기에 혼란을 최소화할 수 있는 복원력을 강화하면 한반도에서 사이버 전쟁억제는 달성될 수 있을 것이다.[8)]

둘째, 누가 실질적인 컨트롤타워의 역할을 할 것인가 하는 점이다. 현재는 청와대가 총괄을 하고 실무차원에서 국정원이 주도권을 가지고 그 역할을 담당하고 있다. 그러나 청와대는 국정최고기관으로써 위상과 국정원은 정보기관으로써 한계가 있다고 생각한다. 남북한이 대치하고 있는 한반도의 안보환경과 정보통신 기술강국인 대한민국의 현실을 볼 때 북한의 사이버 공격시 청와대나 국정원이 컨트롤타워의 역할을 하는 것보다는 완충역할을 할 수 있도록 국무총리실에 '국가사이버안보처(가칭)'를 두고 국정원이 수행하고 있는 공공영역은 국정원이 그대로 시행하되 그중의 핵심기관 일부를 군에서 담당하는 것이 바람직한 방안이지 않나 판단하였다. 이는 국가의 핵심기반시설들이 위치하고 있는 수도권과 후방지역에서 군·관·민이 함께 통합방위법에 의하여 작전을 수행하듯이 북한

8) 장노순·한인택, "사이버안보의 쟁점과 연구경향," 『국제정치논총』, 제53집 3호(한국국제정치학회, 2013), p.594-599.

의 사이버 공격에도 동일한 기준으로 작전을 수행하는 것이 바람직하고 효율적이라고 판단했기 때문이다.

셋째, 법령과 제도의 제·개정이 필요한 실정이다. 현재 국회에서 논의하고 있는 사이버 관련 법령의 제·개정은 국정원이 주도하는 입법안으로 야당의 반발로 논의조차 못하고 계류 중에 있는 실정이다. 국정원이 주도했을 때 국민의 자유와 인권이 침해받을 수 있다는 우려가 크기 때문이다. 현행의 통합방위법은 물리적인 힘을 통제하는 법령으로 사이버전에서는 적용이 불가능하여 북한의 사이버 위협이 국가안보에 심대한 영향을 미치는 상황이 발생하거나 전쟁 발발시 위기와 전시를 대비한 법령과 제도는 제·개정이 필요할 것으로 판단하였다.

넷째, 국내 및 국제적인 공조체제가 중요하다. 사이버전의 특성상 네트워크를 통해 전달되는 데이터의 양과 그 처리속도는 우리의 상상을 초월하고 있다. 수백만 대의 좀비 pc가 한꺼번에 사이버 공격에 나설 경우 순식간에 모든 상황이 종료될 것이다. 전쟁이 일어났다는 사실을 아는 순간 전쟁이 끝나 버릴 수도 있다는 것이다.

따라서 본 논문은 사이버전의 이론을 살펴보고 각국의 사이버 역량과 북한의 위협을 근거로 정부와 군의 사이버전 대응태세를 진단해 보았다. 아울러 북한이 사이버전을 감행했을 때 즉각적인 조치와 대응으로 초기의 피해를 최소화 할 수 있는 전략과 누가 주도를 하는 것이 효과적인지, 이를 위한 법령과 제도의 정비, 국내 및 국제공조를 어떻게 하는 것이 바람직한지 살펴보아 정부와 군의 대응방안을 기술하고자 하였다. 이를 위한 핵심적인 요인 네 가지를 제시하여 각 요인별 대상들을 분석하여 결론에 도달하도록 하였다. 즉 네 가지 핵심요인인 ① 인식과 사상적인 측면 ② 국가전략 등 시스템적인 측면 ③ 공조체계 등 네트워크적인 측면 ④ 인력과 기술 등 지원적인 측면으로 이를 분석하여 분야별 대응방안을 제시하고자 하였다.

제2절 연구의 범위와 방법

1. 연구의 범위

지금까지 사이버 관련 논문은 많이 나왔으나 국가안보측면에서 국가와 군의 대응방안에 대한 논문은 많은 편이 아니었다. 또한 사이버 관련 용어가 일반적으

로 생소하고 접근하기 어려운 측면이 있고, 눈에 보이지 않기 때문에 쉽게 잡히지 않는 측면도 있으리라 판단한다. 그럼에도 불구하고 한국의 정보통신기술의 비약적인 발전으로 기술개발이나 산업발전 측면에서는 많은 논문들이 나오고 있으나 사이버 국가안보 측면에서는 자료가 그리 많지 않은 것이 사실이다. 또한 연구대상인 정부기관과 군의 자료가 비밀 등으로 통제되는 면이 있어서 연구에 어려움이 있었다. 그렇지만 북한의 사이버 위협이 매우 심각하고 국가안보에 미치는 영향이 심대하기 때문에 본 내용을 연구하고자 하였다. 특히 사이버범죄나 사이버테러의 범위를 벗어나 국가의 위기나 전쟁에 대비하기 위해서는 꼭 필요한 연구라 생각하였다.

연구범위는 북한의 사이버전 위협을 중점적으로 다루었으나 장차 한국이 사이버전에 대비할 필요성을 고려하여 한반도 주변강국인 미국과 중국을 비롯한 일본과 러시아의 능력을 포함하여 연구하였다. 특히 북한의 김정일과 김정은은 2003년 이라크전을 관찰하면서 사이버전의 중요성을 인식한 이후 사이버전력 강화를 위해 국가적인 차원에서 전략적으로 발전시켜왔다. 따라서 이러한 북한의 사이버전 전략과 정책, 전술을 분석하여 국가와 군차원에서 대응방안을 도출하고자 하였다. 특히 북한의 사이버 위협에 효과적으로 대응하기 위하여 연구대상 측면에서 사이버전 관련 국가 및 군사전략과 컨트롤타워의 역할을 수행하는 청와대와 국정원의 시스템을 대상으로 연구하고 이를 뒷받침 할 수 있는 법령과 제도와 조직의 발전, 공조체제와 전문인력 확보 등에 대하여 살펴보고 발전시킬 방안을 도출해 보았다.

연구 내용은 국가와 군의 사이버안보의 확립에 중점을 두었다. 먼저 이 논문의 범위를 한정하고 이론의 체계를 확립하는 분석을 틀을 제시하여 사이버 안보이론 및 사례 등 환경적인 영향을 평가하고 네 가지 핵심요인을 제시하여 국가의 사이버 안보와 군의 사이버 안보실태를 분석하고 대응방안을 도출하였다. 이를 세부적으로 살펴보면 먼저 이론적인 고찰을 통하여 사이버공간의 특성과 진화, 사이버 테러와 사이버전 등 개념을 정리하고 이어서 사이버 안보와 전략에 대한 개념을 알아보고 사이버전의 특징과 양상을 살펴보았다. 그리고 미국, 중국, 일본, 러시아 등 주요국가의 사이버역량과 사례, 북한의 사이버전에 대한 전략, 북한의 사이버 역량과 사례 등을 살펴보고 이를 네 가지 관점에서 분석하여 평가하였다. 또한 한반도에서의 사이버전과 동시에 물리적인 공격이 결합된 북한의

공격양상을 제시해 보았다. 이는 북한이 전쟁을 일으켜 사이버 공격과 동시에 물리전으로 공격시 우리의 전쟁계획을 시행하는데 차질을 주며 전투준비에 지장을 초래할 수 있다고 판단했기 때문이다. 이에 따른 한국의 사이버 안보실태를 국가와 군의 입장에서 분석해 보고 이를 네 가지 요인으로 평가하였다. 이어서 국가차원의 대응방안과 군차원의 대응방안을 제시하였다. 특히 전쟁 발발시 국민이 질서 있게 정부의 전쟁 지도지침을 따라 모두가 총력전을 치러야 하는 입장에서 일반적인 사이버 공격과 무력남침과 연계한 북한의 사이버 공격은 성격이 다르다고 판단하였다. 따라서 이러한 관점에서 우리의 사이버 안보실태를 국가와 군 차원에서 검토해 보고 대응방안을 제시하는데 두었다.

2. 연구의 방법

본 논문의 연구방법은 각종 단행본과 논문과 자료 등 문헌적인 연구방법과 북한을 포함한 미국과 중국 등 주요국의 사이버전 사례와 국가정보원, 한국인터넷진흥원(KISA), 국군사이버사령부 등 사이버 관련 업무를 수행하는 기관을 방문하여 토의한 내용과 군, 산, 학, 연에서 실시한 각종 학술회의, 세미나, 컨퍼런스 등에서 토의된 내용을 근거로 연구하였다. 이를 통하여 북한의 사이버 위협에 대응하기 위하여 현재까지 발전시킨 국가의 사이버 전략과 능력을 검토해 보고 국가와 군의 사이버전을 누가 컨트롤타워하며 관련 법령과 제도를 어떤 내용과 방향으로 정비하는 것이 효율적인지 분석하였다. 그리고 능률적이고 효과적인 사이버전을 수행할 수 있도록 관련 제 기관과 국가 간의 공조체계를 살펴보고 대응방안을 제시하는데 중점을 두고 분석해 보았다. 그리고 이러한 문제점을 해결하기 위하여 “4가지의 쟁점 지향적 접근방법 (issue-oriented approach)을 적용하고자 하였다.” 사이버전을 앞에서 언급한 ① 인식과 사상의 관점, ② 국가전략 등 시스템의 관점, ③ 공조체제인 네트워크의 관점, ④ 인력과 기술 등 지원적인 관점에서 접근해 보고자 하였다.

이를 위해서 문헌연구, 사례분석, 전문가 토론, 현장방문 토론 등을 통하여 연구하였다. 첫째, 문헌연구는 사이버 안보와 사이버전에 대한 단행본과 논문자료, 신문 칼럼 등 각종 자료와 매스컴의 자료들을 이용하였다. 특히 북한의 내남 사이버 공격사례와 세계적으로 사이버전의 중요성이 강조된 시점인 2010년을 전후한 논문들을 대다수 참고하였다.

둘째, 사례분석은 미국, 중국, 러시아, 중동 등 주요국가의 사례와 북한의 사이버 공격사례를 집중적으로 살펴보았다. 특히 2007년 러시아와 에스토니아의 전쟁 시적용된 사이버 공격과 동시에 물리전을 연계한 공격으로 승리한 러시아의 사례를 살펴보았다. 이는 앞으로 한반도에서 전쟁이 발발할 경우 북한이 적용할 가능성이 매우 높은 사례라는 측면에서 우리의 대응방안을 도출하는데 유용한 사례가 될 수 있다고 판단하였다.

셋째, 전문가 토론과 학술세미나 등에 참석하여 발표한 내용에 대한 이슈를 살펴보고 무엇이 문제인지 확인하는 과정을 거쳤다. 이 과정에서 질문과 토의를 통하여 현재 국가와 군의 문제점과 대응방안을 도출하는데 도움이 되었다.

넷째, 현장을 방문하여 관련 자료를 수집하고 현장 토론을 통하여 국가기관의 문제점을 식별하고 대응방안을 찾는데 주력하였다. 국가정보원, 국군사이버사령부, 한국인터넷진흥원(KISA), 국방과학연구소, 정부전산센터, 한국전자통신연구원, 국방부와 합동참모본부, 한미연합군사령부 관련부처, 각 군 본부 관련부서와 협조를 하여 연구를 하였다.

그리고 해외의 사이버전 자료는 주한 미군과 협조를 하고 각 국에 파견되어 나간 한국군 연락장교들과 협조를 하여 군사 및 사이버 자료들을 수집하고 분석하여 연구의 질을 높이고자 하였다.

제2장 이론적 고찰

제1절 사이버전의 이론

1. 사이버 공간의 특성

사이버 공간이란 컴퓨터에 의해 제어되고 통제된다는 뜻을 지닌 ‘cyber’와 공간과 장소 혹은 시간을 의미하는 ‘space’ 라는 단어가 결합된 것이다.
컴퓨터 공학이 가장 먼저 발달한 미국에서는 사이버 공간의 영역을 “사이버 공간은 인터넷, 통신 네트워크, 컴퓨터 시스템, 내장프로세스 및 제어기 등이 포함된 정보 기술기반의 독립된 네트워크로 구성된 정보환경 영역이다.”라고 정의하였다.[9] 이러한 정의를 통하여 군사작전 측면에서 사이버 공간은 육, 해, 공, 우주 영역 중의 하나이다. 미 국방부가 발표한 ‘4개년 국방검토보고서(QDR 2010)’에는 사이버 공간을 처음으로 육지, 바다, 하늘, 우주에 이은 제5의 전장으로 규정했다.[10] 또한 사이버 공간은 육, 해, 공, 우주의 영역과는 다르게 인위적으로 만들어진 공간으로 사이버 공간에서의 활동은 다른 영역에서의 활동에 대한 행동의 자유를 보장하며 각 전장 영역에서의 활동을 하나의 활동으로 연결해 주는 매개체 역할을 한다. 이와 같이 사이버 공간은 인간의 활동 범위를 넓히고 활동의 가능성까지도 확장시켰으며 인간의 생각, 가치관, 창의력, 사회제도 등을 근본적으로 변화시키는 새로운 패러다임을 형성하게 하는 순기능과 해킹, 바이러스 유포, 금융사기, 악성댓글 등 역기능이 동시에 존재하는 공간이다.[11]

사이버 공간은 공간과 시간 개념이 없는 상태에서 자신의 신분을 감추거나 드러내지 않는 익명성과 실시간 정보 유통이 가능한 쌍방향성, 지역의 한계를 벗어나 동시에 넓고 신속하게 모두와 소통할 수 있는 시공간적 무제한성과 동시성, 그리고 정보유통의 다양성 등의 특징이 있다. 첫째, 익명성은 사이버 공간에서 표현의 자유를 촉진시키는 긍정적인 측면과 이용자들이 자제를 하지 못하고 행

9) Joint Publication(JP) 1-02, Departmet of Defense Dictionary of Military and Associated Terms
10) DoD of US, “U.S. Department of Defense Strategy for Operating in Cyberspace,“ Quadrennial Defense Review Report(July, 2011), p.5.
11) 오명호 외, 『사이버전 개론』(서울: 양서각, 2014), pp.44-45.

위에 대한 책임성을 약화시켜 일탈 성향을 조성하고 법 집행의 곤란함을 초래하는 등 부정적인 측면도 있다. 둘째, 쌍방향성은 상호간에 실시간 정보교환이 가능함을 의미하며 사이버 공간의 네트워크적인 특성이 이를 가능하게 한다. 기존의 신문이나 방송매체에 의한 정보의 흐름은 제공자에게 일방적이나, 사이버 공간에서의 정보흐름은 일대 일 또는 일대 다수의 형태로 쌍방향적인 유통이 가능하다. 셋째, 시공간적으로 무제한성이라는 특징도 있다. 이는 누구든지 마음만 먹으면 인터넷을 24시간 이용할 수 있으며 별다른 어려움 없이 세계 어느 곳에 있는 인터넷 사이트와 접속할 수 있다. 또한 정보제공자가 정보를 제공하는 시점과 수신자의 수신시점이 시간적으로 방해받지 않으며 장소적으로도 제약받지 않는다. 넷째, 정보의 형식과 내용면에서 다양한 특성이 있다. 사이버 공간에서의 정보는 문서, 사진, 음향 등의 시각적인 이미지나 동영상 등 멀티미디어 형태로 제공되기 때문에 정보의 양과 질에서 다양성이 있으며, 정보의 내용면에서 통제가 이루어지지 않아 정보의 바다라 불리울 만큼 다양한 정보의 유통이 가능하다. 마지막으로 즉흥성과 동시성이다. 인터넷은 간편한 방법으로 상대방과 정보교류를 가능하게 하므로 이용자는 즉흥적으로 불특정 다수에게 직접 정보를 발송하고 수신할 수 있다. 또한 불특정 다수의 동시접근이 가능함으로써 군중심리가 작용할 염려도 있다. 익명성과 더불어 엄청난 확산속도를 갖고 있는 인터넷은 자칫 미확인 사실의 유포로 명예훼손이나 정책혼선 등 예기치 못한 상황을 불러올 수도 있다.[12)]

초창기는 인터넷 공간을 물리공간의 확장개념으로 사이버 공간을 인식하고자 인터넷에 물질 공간 개체를 형상화하는 일을 시도하였으나 이는 실패하였고, 오히려 컨텐츠와 사람과의 연결 관계를 통한 상호작용으로 만들어 낸 산물이 사이버 공간으로 인식되며 급속하게 팽창하는 사회적 공간의 모습으로 진화하여 왔다. 한편 사이버전을 수행하는 국가적인 입장에서는 사이버 공간에 대한 정의가 매우 중요하며 사이버전의 범위와 능력, 전략과 전술발전에 결정적인 영향을 끼치게 된다. 공간에 대한 인식과 적용이 사람마다 다르듯이 사이버 공간에 대한 개념과 인식도 사람에 따라 다르다. 더구나 사이버 공간이 고정된 크기와 모양을 갖는 물질적 성격이 아니라 지속적으로 변화하고 성장하며 진화하고 있기 때문에 사이버 공간에 대한 우리의 인식을 더욱 어렵게 하고 있다.[13)] 이러한 점이 국

12) 유동열, 앞의 책, pp.12-14.

가안보 분야에서 대단히 중요한 기회와 위험을 동시에 가져오고 있는 것이다. 물질 공간이 가지고 있던 물리법칙이 더 이상 적용되지 않으며 계속 새로운 속성으로 변해가는 사이버 공간은 우리에게 더 이상 기존의 가능한 법칙의 발견을 허락하지 않는다. 따라서 국가는 사이버 공간을 지키기 위한 안보전략과 국가차원의 전담조직을 구축할 필요성을 요구받고 있다.[14]

2. 사이버전의 정의

사이버전의 정의에 앞서 사이버 범죄와 사이버테러, 사이버전쟁의 정의를 살펴볼 필요가 있다. 사이버 범죄는 협의와 광의의 개념이 있으나 범죄방지와 범죄자 처벌을 위한 제10차 UN회의에서는 사이버 범죄에 대해 '네트워크 또는 컴퓨터 시스템의 보안 및 데이터를 대상으로 하는 컴퓨터 사용의 위법행위'로 정의한다. 사이버테러는 다양한 정의가 있으나[15] 사이버공격이 국가안보측면에서 영향력을 고려할 때 '특수한 목적을 가진 개인과 테러집단, 국가 등이 해킹, 바이러스 유포, 웜 바이러스 유포, 논리폭탄[16] 전송, 대량정보 전송 및 서비스 거부공격[17] 등 컴퓨터 시스템의 운영행위 방해 내지 정보통신망 침해행위 또는 전자적 침해 행위에 의하여 사회의 혼란을 야기하거나 국가안보를 침해, 위협하는 행위'라 정의한다. 사이버전쟁의 경우, 우크라이나의 국제법 교수인 알렉산더 메레즈코가 발기한 인터넷 사이버전쟁 방지를 위한 국제회의 프로젝트에서 '한 국가가 인터넷 및 관련기술을 타국의 정치, 경제, 기술 및 정보주권, 그리고 독립성에 대적하여 사용하는 것'이라고 정의하며 즉, 국가와 국가 간에 사이버 공간상에서 벌어지는 일련의 전쟁과정이라고 정의하고 있다.[18]

사이버전은 일반적으로 '사이버 전쟁(cyber war)' 대신에 '사이버전(cyber

13) 이완수, "국가 사이버 안보 구축전략에 관한 연구," 경기대학교 대학원 박사학위 논문 (2014), pp.6-8.
14) 한희, "사이버 공간과 국가안보," 『국가안보전략연구소 학술회의』(2014), pp.11-14.
15) 공진성, 『테러』 (서울: 책세상, 2010), p.22.
16) 논리폭탄 [logic bomb]; 논리폭탄이라는 용어 그대로 프로그램에 어떤 조건이 주어져 숨어 있던 논리에 만족되는 순간 폭탄처럼 자료나 소프트웨어를 파괴하여, 자동으로 잘못된 결과가 나타나게 한다.
17) 분산 서비스 거부 공격 [distributed denial of service]; 인터넷 상에서 연결된 여러 대의 컴퓨터 시스템으로 하나의 표적 시스템에 동시에 다량 접속(공격)함으로써 시스템이 더 이상 서비스를 계속할 수 없도록 만드는 사이버 공격의 일종.
18) http://en.wikipedia.org/wiki/Cyberwarfare(2015. 9. 30)

warfare)' 라는 용어를 사용된다. 이는 화생방전(CBR warfare)의 경우와 같이 특별한 유형의 무기체계가 사용되어 일반적인 전쟁, 즉 무력충돌과 구별하려는 의도로 이해된다. 사이버전의 정의는 보는 시각에 따라 국가별, 학자별로 다소 상이하게 정의하고 있으므로 세계 최첨단 사이버전 능력을 구비한 미국의 정부기관과 한국의 합참에서 규정한 정의를 중심으로 고찰할 필요가 있다.

사이버전에 대해 미국 정부의 보안 전문가인 리처드 클라크(Richard Clarke)는 2010년도 그의 저서 '사이버전(Cyber War)'에서 '특정 국가가 다른 국가의 컴퓨터나 네트워크를 공격하여 피해를 입히거나 파괴할 목적으로 취하는 행동'으로 정의하였고, 이코노미스트지는 사이버전을 '제5의 전쟁영역'으로 묘사하고 있다. 미 국방부 부장관 윌리엄 린(William J. Lynn)은 "펜타곤은 공식적으로 사이버 공간을 전쟁의 새로운 영역으로 인식하고 있으며 육, 해, 공, 우주의 군사작전에 있어 매우 중요한 부분이 되었다"고 언급하였다. 미 국제전략연구소(CSIS)는 사이버전을 '정보시스템과 네트워크에 대한 데이터 공격, 소프트웨어 공격, 물리적 공격이 대규모로 발생하는 상태'로 정의하여 국가차원의 군사적인 행동여부에 관계없이 대규모 사이버 공격에 물리적인 공격을 포함하고 있다고 정의하고 있다. 미국의 랜드연구소는 '정보의 우선순위에 따른 군사작전으로써 상대국의 정보 및 통신시스템을 파괴 또는 무력화하는 행위'로 규정하고 있다.[19] 한편 2010년 펜타곤은 미국의 군사 네트워크를 보호하고 다른 국가들의 시스템들을 공격하기 위해 사이버사령부(USCYBERCOM)를 창설하였다. 이를 통하여 볼 때 사이버 공간이 전쟁의 새로운 영역으로 인식되고 있으며 사이버 공간에 대한 공격 및 방어가 군사작전의 중요한 영역이 된 것이다.

한국의 합참은 사이버전을 "컴퓨터가 합성한 가상현실의 세계와 가상인간의 영역과 같이 인공지능체계가 운용되는 공간(cyber space)에서의 전쟁으로, 이는 정보화 사회의 과학기술 발전을 역이용하여 취약점을 공격함으로써 물리적인 군사시스템 파괴보다 훨씬 결정적인 손실을 가할 수 있는 총체적인 가상공간에서의 정보 마비전을 추구하는 전쟁수행 방식을 의미한다." 라고 정의하고 있다.[20] 군사적 시각에서 사이버 전쟁은 전쟁목적의 달성을 위해 사이버 수단을 사용하여 사이버 전장 공간내의 모든 표적을 대상으로 하는 전쟁이라고 정의할 수 있

19) 박대우, "대한민국 국군의 사이버전 대응," 『군사논단』, 제75호(한국군사학회, 2013), pp.40-41.
20) 합참, 『합동·연합작전 군사용어사전』 (서울: 합동참모본부, 2007), p.219.

다.[21] 이렇게 정의된 사이버 공간작전은 매년 급속하게 확장되고 있는데 이는 물리공간의 주요 표적이 컴퓨터와 네트워크에 연결되어 사이버 공간으로 진입하고 있으며 사회관계적 공간이 정보공간에서 급속하게 확장되는 것은 물론 이를 연결하는 미디어 및 인터페이스 수단에 의해 많은 사람의 인식공간이 사이버 공간으로 진입하고 있기 때문이다.

사이버 영역은 이미 물리영역, 정보영역, 인식영역에 공히 중첩되어 구성되어 있고 육, 해, 공군의 전투영역과 상호의존적으로 중첩되어 있다. 그러므로 한반도에서의 장차전 양상은 사이버 공간을 이용한 전차원적인 전쟁의 형태로 나타나게 되는 것이 불가피하다고 판단된다.

3. 사이버전의 특징과 형태

가. 사이버전의 특징

사이버전의 특징에 대해서는 먼저 전문가들의 생각과 사이버전 사례의 교훈을 통하여 볼 때 눈에 보이지는 않지만 치명적인 특징이 있다. 사이버 공격수단은 하드웨어적 수단이 아니라 소프트웨어적인 수단이다. 적의 전투기가 공격하기 위하여 출격했는데 방공 감시레이더가 갑자기 장애가 발생하거나. 부상자들이 긴급 호송되어 병원에서 응급치료 중에 발전시스템이 해킹을 당하여 전기 공급이 끊긴다면 사회적인 혼란과 무질서 등 그 파장은 매우 클 것이다.

이와 같이 사이버 공간에서 개인이나 집단이 상대국을 대상으로 사이버전을 일으킬 수 있다는 점에서 첫째, 사이버전은 비대칭적인 성격이 있다. 국가 간의 분쟁도 있을 수 있지만 국가는 개인과 집단과도 전쟁을 할 수 있다. 9.11 테러는 알카에다 무장 테러집단이 미국을 공격한 예이다. 공격과 방어 전력에서 상대와의 균형을 이루지 못하더라도 사이버 공간에서 공격자는 언제든지 비대칭 전략을 구사할 수 있다. 둘째, 비용이 저렴하다는 특징이 있다. 비용 면에서 크루즈 미사일이 1기당 약 200만 달러, 스텔스 전투기가 약 1억 2,000만 달러, 스텔스 폭격기가 약 20억 달러인데 비해 사이버 무기는 단 몇 달러에서 많게는 수만 달러 수준이면 충분이 확보할 수 있다. 셋째, 강자와 약자가 바뀔 수 있는 특징이 있다. 사이버 기술을 이용한 공격과 방어는 전통적인 군사 강대국에 반드시 유리한

21) 한희, 앞의 논문, p.4.

것만은 아니다. 선진국들은 국가의 주요기반시설이 정보화되어 있고 유·무선 네트워크 접속 포인트가 많기 때문에 공격 요소나 취약점이 많으나 북한과 같은 최빈국은 인프라가 약하기 때문에 취약점이 상대적으로 적다. 넷째. 방자의 특징은 사후 수습적이다. 방자는 모든 공격에 대응책을 마련하기가 쉽지 않다. 공격자는 세계 어느 곳에 대해서도 상시 공격할 수 있으며 많은 목표물 중에서 하나의 취약점만 찾아도 공격을 시도할 수 있다. 반면에 방자는 공격 징후를 사전에 파악하기가 어렵고 모든 취약점을 제거하거나 보완한다는 것도 현실적으로 쉽지 않다. 다섯째, 공자를 식별하기 어렵다는 특징이 있다. 지금까지 수많은 사이버 공격이 있었지만, 그 배후가 명확하게 밝혀진 것은 없다. 정황상 추측이 가능할 뿐이다. 이는 공격자를 특정하기가 어렵고 공격자와 공격을 지원하는 지원세력의 구별이 모호하고 증거도 남지 않는 특징이 있기 때문이다. 정보통신기술이 발전할수록 방어기술도 발전하지만 공격기술도 함께 발전한다. 공격기술은 은밀하게 개발되고 지능화·첨단화되고 있다. 전 세계 인구의 60%가 보유하게 될 휴대폰은 앞으로 공격수단이자 공격의 중간 경유지로 공격의 매개체가 될 수 있다. 전자장치를 마비시키는 고출력 전자파와 같은 에너지를 이용한 공격 무기에 대응하기 위해서는 여러 분야의 기술들을 융합한 복합적인 방어 전략이 필요할 것이다. 네트워크를 통해 전달되는 데이터의 양과 그 처리속도는 우리의 상상을 초월하고 있다. 이전부터 숨겨놓은 봇넷을 활성화시켜 수백만 대의 좀비 pc를 동시에 사이버 공격에 가담하게 할 경우 그 공격이 성공적이라면 순간적으로 모든 상황이 종료될 수 있다. 전쟁이 일어났다는 것을 식별하는 순간과 동시에 전쟁이 끝나 버릴 수 있는 것이다. 마지막으로 시간·공간의 한계가 없다는 특징이 있다. 재래식 전쟁과 같은 물리적인 전쟁은 전쟁이 발발하면 일정기간 지속되다가 협상이나 항복을 통해서 종결된다. 사이버전에서는 전시와 평시의 구분이 어렵다. 지금도 보이지 않는 공격자들의 공격이 끊임 없이 탐지되고 있다. 2010년 6월 주한미군사령부 제임스 히스 사이버전 자문관은 “현재 사이버 공간에는 초당 200만 통의 이 메일이 발송되고 있으며 4,000여개의 사이트에서 테러집단들이 활동하고 있다. 매일 3만 2,000여 건의 사이버 공격 시도가 탐지되고 있고, 100개 이상의 해외 정보기관이 미국의 네트워크 해킹을 시도하고 있는 것으로 추정하고 있다.”고 밝혔다. 공격의 대상이 군의 정보시스템이라도 네트워크의 특성상 그 피해 범위는 군과 국가, 사회 전반에 걸쳐 영향을 미칠 것이다.[22)]

나. 사이버전의 형태

1990년대 초부터 국가와 민족 간에 이해가 상충하는 사건들이 발생하였고, 사건이 발생할 때마다 그들 속에 잠재되어 있던 갈등이 표면화되면서 군사적 충돌로 이어졌으며, 이는 어떤 형태로든 사이버전이 병행되는 형태로 전개되었다. 비록 사이버전은 20년이라는 비교적 짧은 역사를 갖고 있지만 정보통신기술의 비약적인 발전과 함께 빠르게 변화해 왔다. 사이버전은 물리적 공격과 연계한 통합된 전력 요소로 군사작전의 보조적인 수단에서 군사력의 일부로 편입되어 작전을 수행하게 되었다. 해군과 공군이 전쟁에 등장한 것은 각각 천년과 백년이 되었다. 해군은 보급품의 해상 수송을, 공군은 공중정찰과 폭격이라는 지상군의 보조적 역할로 출발했다. 오늘날의 해군과 공군은 보조적 역할을 벗어나 독자적으로 중요한 역할을 하고 있다. 해군은 항공모함을 비롯해 구축함, 이지스함, 잠수함 등으로 구성된 함대로 움직이며 해상전력을 구축하고 있다. 별도의 해전 및 전투개념이 존재하고 잠수함과 전투기, 헬기와 함께 수중·해상·공중의 입체작전을 펼치는 것이 기본이 되었다. 공군도 비행단을 중심으로 별도의 전투 및 작전 개념을 가진 독자영역을 구축하고 있다. 현대전에 있어 공군력은 전쟁의 승패를 가르는 핵심전력으로 자리 잡았다.

이러한 전례로 비추어 볼 때 사이버전 역시 머지않아 독자적인 영역을 구축하든지 아니면 다른 영역의 상당부분과 연동되거나 포함되게 될 것이다. 이 새로운 분야는 사이버 공간이라는 독자적인 전장을 가지고 있고 전쟁이나 분쟁에 활용되어 그 효과와 가치를 입증하고 있으며, 특히 사이버 공격 무기의 파괴력은 상황에 따라 핵폭탄을 능가할 것이다. 핵 공격과 사이버 공격은 정도의 차이는 있겠지만 사회의 기능을 순간적으로 마비시키고 통제 불능 상태에 빠지게 하는 것과 같은 광범위하고 막대한 피해를 초래할 수 있기 때문이다.[23]

사이버전이 군사적으로 중요한 이유는 군의 무기체계나 전략이 네트워크를 기반으로 한 정보통신기술 중심으로 급속히 진화하고 있기 때문이다. 오래 전부터 세계 각국은 전장 환경 변화에 따른 전쟁수행 전략을 수립하고 추진해 오고 있으며, 그 중심에 네트워크중심전(NCW)이 위치하고 있다. 네트워크중심전은 전차

22) 손영동(a), 앞의 논문, pp.149-157.
23) 김종호, "사이버 공간에의 안보의 현황과 과제," 『한국의 사이버위협 및 대응전략 포럼』, (서울: 새누리당 중앙위원회 사이버단, 2015), pp.35-38.

와 장갑차와 같은 화력체계, 정찰기과 같은 정찰체계 등 모든 전투력 요소를 컴퓨터 네트워크로 묶어 지능화·무인화·고신뢰화를 바탕으로 하는 전투다. 정보통신기술과 무기체계의 융합은 네트워크 중심의 전장 환경에 부합하기 위한 기술 개발에 박차를 가하게 했으며 정보체계의 상호 연동을 기반으로 하는 'C4ISR[24]체계'가 대표적이다. 지휘통제자동화인 C4I체계와 감시·정찰인 ISR체계를 합친 개념의 C4ISR체계는 군사작전에서 지휘관이 가용한 자원을 이용하여 전투력을 최대한 발휘할 수 있도록 지휘·통제하고 감시·정찰을 통해 신뢰성 있는 정보를 획득·처리·활용해 부여된 임무를 분권화하여 시행할 수 있도록 지원하는 총체적인 체계라 할 수 있다.[25]

사이버전은 앞으로 다음과 같은 두 가지 측면에서 공격의 역할을 수행하게 될 것으로 예상된다. 첫째, 물리적인 군사력과 연계는 하지만 사이버의 소프트한 수단만 활용하여 공격하는 방법이다. 마치 해상에서 해군 간에 발생하는 해전이나 공군 간에 발생하는 공중전처럼 될 수 있다. 이를 위해 사이버 공간에서 상대와의 교전을 상정한 사이버전 단독 교리와 전략이 개발되고 이를 구현하기 위한 작전계획도 마련할 필요가 있을 것이다. 둘째, 물리적 군사력과 완전히 통합되어 전쟁을 수행하는 것이다. 전쟁이 육·해·공에 이어 우주와 사이버 공간까지 포함된 5차원적 공격과 방어가 일어나는 하이퍼 입체전이 될 것이기 때문이다.
과거에는 전쟁이 빠르게 적지에 침투해 많은 사상자를 낼 수 있는가의 요인이 전쟁의 승패 요소였다면. 앞으로는 사이버전과 물리전을 어떻게 연계할 수 있는가의 요인이 중요한 요소로 부각될 수 있을 것이다.

따라서 미래 전쟁은 물리적인 공격 이전이나 물리전과 동시에 국가기반시설에 대한 사이버 공격이 병행될 것으로 예상된다. 특히 적이 국가의 통신, 금융, 에너지, 교통과 같은 주요기반시설을 제어하는 시스템을 공격할 경우 상당한 피해가 예상되고 그로 인하여 혼란과 무질서와 공포감은 전쟁수행의지를 마비시킬 것이다. 이러한 공격방법 중의 하나가 기반시설을 제어하는 기능을 가진 스카다 시스템을 파괴하는 것이다. 스카다 시스템[26]은 거대하고 복잡한 설비를 간소화하고

---

24) C4ISR : Command, Control, Communications, Computers, Intelligence, Intelligence, Surveillance and Reconnaossance
25) 오명호 외, 앞의 책, p.200.
26) 스카다 또는 감시 제어 및 데이터 취득(Supervisory Control And Data Acquisition, SCADA)은 일반적으로 산업 제어 시스템(Industrial Control Systems, ICS), 즉 산업 공정/기

자동화하며 원격관리를 가능하게 하는 장점도 있지만 제어시스템이 악성코드에 감염되어 통제 불능상태에 빠진다면 물리적인 전쟁 이상의 피해를 당할 수 있다. 즉 전쟁의 패러다임이 새롭게 변화될 가능성이 높다고 볼 수 있다.

제2절 사이버 안보의 개념과 전략

1. 사이버 안보의 개념

사이버 안보는 냉전 이후 안보개념의 변화 속에서 정보통신기술의 비약적인 발전에 기인하여 새롭게 부각된 개념이다. 사이버 안보는 사이버 위협을 전제로 하여 사이버 위협이 갖는 복합성과 다양성으로 대상을 설정하는 것이 쉽지 않기 때문에 침해 대상에 따라 안보나 범죄 문제가 될 수 있다. 국가별로 인식의 차이와 사이버 안보의 개념, 범위에 대한 정책적 접근의 차이로 아직까지 사이버 안보에 대한 전 세계적인 합의를 이룬 것은 없다.[27] 그러나 사이버안보의 특성상 국제적인 협력이 필수적이기 때문에 국제기구를 통해 관련 개념의 합의는 반드시 필요하다.[28] 세계 각국은 사이버 안보의 개념을 기존의 정보보호, 정보통신망 보호, 정보통신기술안전 등의 특정영역에 대한 보호개념에서 벗어나 폭넓은 사이버 공간의 개념을 도입하여 안보대상을 확장하는 추세에 있다. 즉 사이버 안보를 국가 사이버 공간에 대한 직접적, 간접적 위협으로부터 사이버 공간의 안전을 보호하는 행동 및 조치로 정의하고 있음이 이를 뒷받침한다.

최근의 추세는 보다 더 포괄적인 사이버 안보개념이 나타나고 있다. 유럽연합은 사이버 안보를 '민간 및 군사영역의 사이버 공간을 상호의존적인 네트워크 및 정보기반시설과 관련되거나 이를 손상시킬 수 있는 위협으로부터 보호하기 위하여 이용될 수 있는 보호 장치와 행동'이라 하였다. 미국 역시 사이버 안보를 '사이버공격으로부터 사이버 공간을 보호하거나 방어할 수 있는 능력' 또는 '모든 형태의 정보의 안전과 정보가 저장·접근·처리·전송되는 시스템과 네트워크에 대한 위험으로부터 자유를 보장하기 위하여 필요한 모든 조직적 행동

반 시설/설비를 바탕으로 한 작업공정을 감시하고 제어하는 컴퓨터 시스템을 말한다.

27) 채재병, "안보환경의 변화와 사이버 안보," 『정치·정보연구』, 제16권 2호, (서울: 국가 안보전략연구소, 2013), pp.180-184.

28) 이연수 외, "주요국의 사이버 안전관련 법·조직체계 비교 및 발전방안 연구," 『국가정보연구』, 제1권 2호, (서울: 한국국가정보학회, 2008), p.42.

으로 범죄·공격·사보타지·간첩행위·사고 및 실패로부터 방어하기 위한 예방을 포함하는 것'으로 폭넓게 규정하고 있다. 국제전기통신연합은 사이버안보를 보다 구체적으로 '사이버 환경과 조직체 및 이용자의 자산을 보호하기 위한 다양한 도구· 정책· 기술을 모두 포괄하는 것'으로 정의하고 있으며,[29] 이는 사이버 공간의 안전을 위해서는 유럽연합에서 제시한 포괄적인 정보 및 정보통신망의 보호가 사이버 안보를 발전시킨 개념이라고 볼 수 있다.

더욱이 2012년 경제협력개발기구(OECD)의 국가사이버 안보전략에 관한 분석보고서에 의하면 사이버 안보에 있어서 국제안보 및 국가안보, 국방에 대한 중요성이 증대되고 있다는 것이다. 즉 전략적 측면에서 군사적인 사이버 위협과 사이버 첩보에 대한 인식이 확산되고 있으며 정보기관 등 국가안보 관련 기관이 사이버 안보 문제에 조정자 역할을 하는 경향이 나타나고 있다는 것이다. 이와 같이 국제적으로 포괄적인 사이버 안보 개념이 형성되어 있는 반면에 한국의 경우 사이버 안보를 폭넓게 정의하는 국제적인 흐름에 못 미치는 상황이다. 우리는 '국가사이버안전관리규정'에서 사이버 안전을 '사이버 공격으로부터 정보통신망을 보호함으로써 정보통신망과 정보의 기밀성·무결성·가용성 등 안정성을 유지하는 상태'로 규정하고 있다.[30] 또한 '사이버 위기'는 '사이버 공격으로 정보통신망을 통해 유통·저장되는 정보를 유출·변경·파괴함으로써 국가안보에 영향을 미치거나 또는 사회·경제적 혼란을 발생시키는 국가 정보통신시스템의 핵심기능이 훼손·정지되는 등 무력화되는 상황'으로 정의하고 있다.

안행부, 경찰, 방통위 등 여러 기관 규정의 정의에서도 사이버안전에 대한 용어가 나오고 있으나 사이버 공간을 포괄적으로 규정하지 못하고 제한적이고 협소한 개념으로 규정함으로써 포괄적 사이버안보 개념과는 거리가 멀다.

한국의 사이버 안보전략은 포괄적 개념의 사이버 안보개념을 기초로 사이버 위협 상황에 따라 사이버 공간의 범위와 안보영역을 확정할 필요성이 대두된다. 북한의 사이버 위협과 미국과 일본, 중국 등 한국의 안보현실을 반영해야 하기 때문이다.

---

29) ITU, "Recommendation ITU-T X.1205," Overview of Cybersecurity(2008.4), p.2.
30) 오명호 외, 앞의 책, pp.56-57.

2. 사이버 안보의 전략

범세계적으로 사이버 공간은 더욱 확대될 것으로 예상되며 우리의 일상생활과 정치, 경제, 사회, 문화, 과학, 군사 활동 등 전 영역에 영향을 미칠 것이다. 이는 현실공간과의 융합과 통합 등으로 국가 성장 동력에 긍정적으로 기여할 것이며, 사이버 공간의 익명성과 시공간 상에서 제한이 없다보니 사이버 공간관리에 대한 대책과 국가안보의 부정적 측면에서 사이버 위협에 대한 대책 마련이 필요할 것이다. 사이버 위협은 테러리즘과 비슷하며 테러리즘과 마찬가지로 공격과 방어에 있어 비대칭적인 속성을 갖고 있다는 점이다. 위협의 요인이 되는 공격의 주체가 국가, 집단, 개인 등으로 다양하고 피해가 심대하다는 것도 유사하다.

최근에 이러한 위협의 심각성이 증대됨에 따라 국제사회는 물론 우리나라에서도 사이버 안보 전략을 수립하여 발표하였다.[31] 이것이 바로 '국가사이버안보마스터플랜'이다. 미국 등 서구권 국가들은 사이버 안보 전략을 세분화하여 국제협력 전략과 국방전략 등을 추가적으로 발표하였다. 이에 반해 우리나라는 아직까지 초보적인 단계로 국가차원의 사이버안보 전략을 수립한 것이다. 사이버 공간과 현실공간과의 융합과 통합 등으로 경계가 모호하여 사이버 안보전략의 대상과 범위를 확정하는데 어려움이 있다. 국가안보 전략차원에서 사이버 안보전략의 의미와 필요성을 생각해 볼 필요가 있다. 먼저 목표 설정을 위한 사이버공간의 범위에 대한 것이다. 안보의 범위와 주체에 대해서 다양한 정책과 견해가 존재할 수 있는데 안보의 범위를 어디까지로 할 것인가에 대한 기준설정이 필요하다. 사이버 안보는 사이버 위협을 근거로 성립되는 개념이다. 사이버상의 특징으로 위협의 대상을 결정하기가 쉽지 않다. 위협을 가하는 주체가 개인, 조직, 국가인지에 따라 범죄문제나 안보문제가 될 수 있으며, 침해 대상이 개인이라도 국가에 심각한 위협으로 간주되면 안보문제가 될 수 있다.

따라서 이러한 다양한 관점과 개념에 따라서 전략을 수립하게 되는 것이다. 포괄적 사이버안보 개념을 바탕으로 한국의 사이버 안보 전략의 방향은 사이버 공간에 대한 안정성을 확보하는 것과 사이버 위협에 억지력을 확보하는 것, 사이버 공격역량을 확충하는 것과 국제 사이버정보 공유체계를 구축하는 것이다.[32] 전략

31) 김인중, "국가사이버안보전략수립의 필요성과 추진전략," 『국가안보전략연구소 학술회의』(2014), pp.54-58.
32) 채재병, 앞의 논문, pp.187-188.

을 수립하는데 있어 중요한 것은 국가가 지향하고 추구하는 목표가 무엇인지 명확히 해야 한다. 전략의 목표를 경제적인 측면에 둘 것인지, 아니면 안보적인 측면에 둘 것인지를 고려하게 된다. 우리나라는 경제적 측면보다는 안보적 측면에 두는 것이 국가 안보와 국익에 도움이 될 것으로 판단한다. 경제도 중요하고 안보도 중요하다. 그러나 안보는 죽느냐 사느냐의 생존의 문제이고 경제는 잘 사느냐 못사느냐의 빈부의 문제다. 따라서 이러한 기본적인 목표를 가지고 사이버 안보전략을 수립하여 추진하면 될 것으로 판단한다. 전략의 방향을 제시하기 위한 고려 요소는 한국의 안보에 적합한 목표를 설정하는 것이고, 누가 사이버 안보의 컨트롤 타워를 하는 것이 바람직한가와 사이버 안보와 관련하여 법령과 제도의 정비, 정보의 공유와 협력, 그리고 첨단 사이버 무기의 연구개발 등을 고려하여 전략을 수립하면 바람직 할 것이다.

제3절 사이버전의 수행절차와 양상

1. 수행절차

사이버전의 위협은 시스템의 사용불능, 정보탈취, 위조 및 변조된 정보의 삽입 등 공격자가 의도한 목표를 달성하기 위한 행위를 말한다. 이러한 위협은 여러 단계를 거쳐 다양한 방법으로 사회적 또는 국가적 위험을 야기한다. 과거에는 공격대상 시스템의 컴퓨터나 네트워크에 단순히 바이러스나 악성코드를 유포하거나 네트워크의 자원을 고갈시키는 공격이 주를 이루었다.

최근에는 기술의 지능화 및 고도화에 따라 명확한 목표대상에 대하여 조직적으로 오랜 기간 동안 준비과정을 거치는 APT(Advanced Persistent Threat) 공격으로 정부나 군(軍)의 기밀을 유출하거나 기업의 산업정보 또는 고객정보를 탈취한다. 더불어 국가 기반시설에 침투하여 기간망을 마비시켜 항공기 또는 열차 등의 교통 인프라 뿐만 아니라 원자력 제어체계에 혼란을 준다. 사이버전 수행절차는 먼저 사이버심리전이나 미디어전부터 수행한다. 목표대상인 국민들을 상대로 반국가적 선동이나 유언비어를 언론매체와 인터넷 홈페이지, SNS(Social Network Service), Twitter, YouTube, 카카오톡 등을 통해 퍼뜨리고 선동하여 갈등구조를 만들며 적 국민들의 대항 의지나 거부감, 적 지휘관에 대한 적대감의 변화 등을 유도하고, 적국에 대한 문화적 충돌에 대한 거부감을 희석시키는 것이다.[33] 심리

전을 수행한 이후에 이어서 사이버 상에서 공격을 실시하며 이는 공격대상 국가의 군, 정부, 사회, 기업, 무기체계, 통신, 교통, 가스, 전기, 수도, 원자력, 금융거래, 생활, 인프라 시스템에 공격명령을 실행시켜 인프라의 기능을 조정하거나 파괴하여 상대국의 전투력을 무력화시키거나 마비시키고 파괴한다.[34]

현 추세를 보면 국가 간의 사이버전쟁은 각 단계가 혼합되어 적용되어지는 추세이며 사이버전은 비대칭전력으로 최소의 비용으로 최대의 효과를 발생시켜 상대국의 전력을 무력화하고 자국의 승리를 이끄는 것을 최종목표로 한다.[35]

구체적으로 사이버전의 수행절차를 이해하기 위해서는 정보수집, 공격시스템 접근, 권한변경, 프로그램설치, 불법행위설치, 마지막으로 흔적지우기 및 백 도어 설치 등 6가지의 "사이버전 위협 단계"로 접근하면 훨씬 용이하다. 이를 군의 특수부대가 공격을 수행하는 절차를 사이버전 위협절차와 비교하면 쉽게 이해할 수 있다.

첫째, 정보수집 단계이다. 특수부대가 임무 수행시 가장 먼저 할 일은 테러리스트 근거지의 위치를 확인하는 것이다. 위치를 알기 위해서는 다양한 정보의 수집이 필요하다. 사이버전 위협에 대응하기 위해서도 가장 먼저 필요한 것은 위협대상에 대한 정보수집이다. 적의 공격 시스템, 네트워크 구조, 운영체제의 종류 및 버전, 제공되는 서비스, 취약점 등의 다양한 정보를 수집하는 단계다. 정보 수집은 온라인(on-line)상에서는 자동화된 네트워크 스캔 도구를 이용하여 수집할 수 있고 내부자에 의한 정보나 외부로 유출된 문서 등 오프라인(off-line) 상에서의 정보수집도 있다.

둘째, 공격시스템 접근단계이다. 테러리스트 근거지의 위치를 알아냈다면 모기지에서 테러리스트의 기지까지 다양한 방법으로 병력을 접근시킬 것이다. 마찬가지로 수집된 정보를 가지고 시스템에 접근할 수 있는 권한을 획득하는 단계로 공격 대상시스템에 일반 사용자로서 접속을 할 수 있는 권한을 획득하거나 접속하는 것을 말한다. 일반 사용자 권한을 획득하기 위해서는 해당 사용자의 패스워드를 확보하는 것이 중요한데 이를 통해서 사용자의 ID, 패스워드 정보를 확보하는 방법, 악성코드를 이용한 사용자의 키보드 입출력 기록을 가로채서 확보하는

33) 박대우(b), "대한민국 국군의 사이버전 대응" 『군사논단』, 제75호(한국군사학회, 2013), P.41.
34) 박대우(b), 위의 논문, p.41.
35) 미국 국방부, "Information Operation," DoD Directive S-3600(1996. 12).

방법, 패스워드를 확보하는 방법과 파일을 탈취하는 방법 등이 있다.

셋째, 권한변경 단계이다. 테러리스트를 공격하기 위해서는 그들의 기지에 잠입을 해야 한다. 잠입하는 방법에는 여러 가지가 있을 수 있다. 공격자는 목표달성을 위해 공격 시스템의 관리자 권한을 획득해야 하나 일반 사용자 권한을 먼저 획득한 이후에 관리자 권한을 획득하는 것이 공격하기가 용이하다.

넷째, 보조 프로그램 설치단계이다. 잠입 후에 보다 효과적으로 공격하기 위해서는 보조 수단들을 설치할 수 있다. 위협행위를 보조하기 위한 다양한 프로그램을 설치하게 된다. 관리자의 권한을 정상적으로 획득하였다면 어떠한 프로그램이든 공격자가 원하는 대로 설치가 가능하다. 예를 들면 네트워크에 웜을 감염시켜 시스템 전체를 마비시키거나 DDoS의 경우 관리자의 권한을 획득한 좀비 PC의 명령에 따라 공격대상 서버를 공격하는 프로그램을 설치한 후 외부에서 작동시키는 방법이 있다.

다섯째, 불법행위 실시단계이다. 근거지를 파괴하는 행위를 하거나 적의 주요 기밀을 탈취하는 행위로 실제적으로 위해를 가하는 단계를 말한다. 앞 단계에서 좀비 PC를 이용하여 서버에 DDoS 공격을 하는 행위, 서버내의 모든 자료를 삭제하거나 변경 또는 삽입하는 행위와 정보의 열람 및 탈취하는 방법이다.

여섯째, 흔적지우기 및 백 도어 설치단계이다. 목적달성 후에 잠입한 흔적을 지우거나 공격자가 누구인지 알 수 없도록 하는 단계다. 추후에 재 침투해야 할 필요성이 있을 경우에 대비하여 출입이 편리한 곳을 확보하거나 이동 경로 등을 표시할 필요가 있다. 불법 행위가 종료된 후에 이러한 흔적들을 삭제해야 하며 또한 나중에 재 침입이 용이하도록 백 도어(back door)를 설치할 수도 있다. 백 도어는 서버 관리자나 프로그래머들이 자신이 서버에 편리하게 접근하기 위해 만들어진 시스템 보안이 제거된 비밀 통로를 의미하며, 한번 관리자 권한을 획득한 후 백 도어를 설치할 경우 앞의 단계를 생략하고 바로 관리자 권한을 획득할 수 있다.[36]

2. 양상

가. 사이버전 양상

36) 오명호 외, 앞의 책, pp.214-223.

미래 전쟁의 패러다임을 예측한 펜타곤의 시나리오에 따르면 사이버 전쟁의 1단계 공격은 심리전을 상정하고 있다. 심리전은 군대에 가짜 명령을 하달하여 잘못된 정보를 가진 장교들을 오합지졸로 만들 수 있다. 사이버 부대는 사이버전의 승리를 쟁취하기 위해 상대방 국가의 국영 텔레비전 방송국의 전파를 방해하고 가짜 프로그램을 설치한다. 예를 들면 상대국의 지도자가 술에 취한 모습으로 넋두리를 늘어놓는 화면을 보여줌으로써 국민들이 정부에 반기를 들도록 선동한다는 개념이다. 이어서 취하게 될 2단계 작전으로 컴퓨터 바이러스를 적성국의 전화국에 침투시키는 공격에서부터 시작된다. 컴퓨터 바이러스에 감염된 전화교환기의 불통 또는 고장으로 국가의 기간통신망은 기능을 상실하게 된다.[37] 그리고 컴퓨터 논리폭탄(Logic Bomb)과 전자 펄스 폭탄을 사용하여 주요 정부 기관의 컴퓨터 시스템을 파괴한다. 논리폭탄은 특정한 시간에 활동을 개시하여 컴퓨터 파일에 있는 데이터를 지우도록 프로그램 된 일종의 시한폭탄과 같은 컴퓨터 바이러스이다. 논리폭탄으로 상대 국가의 항공교통관제시스템과 철도노선배정시스템의 컴퓨터를 마비시키면 비행기들은 계획되지 않은 공항에 착륙하고 군수물자를 실은 화물열차들은 방향이 상이한 행선지로 출발하는 사태가 야기될 것이다. 한편 적성국의 수도에 침입한 특공대원들은 손가방 크기의 전자펄스(EMP) 폭탄을 중앙은행 근처에 놓아두게 하면 그 건물에 있는 모든 전자부품을 녹여 버리기 때문에 금융전산 시스템의 기능이 무력화된다. 중앙은행의 업무가 중단되면 국가 전체의 경제활동이 마비되는 것이다.

2003년 미국과 이라크 간의 전쟁에서 미군은 먼저 이라크의 정보시스템을 원격 접속하여 상대의 활동을 볼 수 있도록 백 도어[38]를 설치하고 암호화 시스템의 기반을 파괴하여 보안수준의 낮은 통신채널을 이용할 수밖에 없도록 유도하는 등 광범위한 사이버 공격을 하였다. 미군은 전자전 공격으로 이라크군의 기간시설 네트워크를 무력화하고 이동통신 중계소와 통신 네트워크를 파괴하여 결국은 이라크와 휴대전화 및 위성전화 시스템을 공유하는 주변국에도 일시적인 통

37) 종래의 '위협기반(Threat-Based) 전략'은 특정 국가를 대상으로 특정지역에서 발생할 수 있는 전쟁 시나리오를 상정한 한편, 9·11 이후의 '능력기반(Capability-Based) 전략'은 특정 시나리오를 고려하지 않고 미국을 공격할 수 있는 적의 능력에 기초하고 있다.

38) 백도어(Backdoor) : 사용자 인증 등 정상적인 접근절차를 우회하는 경로를 제공하는 프로 그램이다. 프로그래머의 접근 편의를 위해 시스템 설계자가 고의적으로 만들어 놓은 것이지만, 해커에게는 악의적인 해킹 통로로 활용될 수 있다.

신서비스 장애를 유발하게 하였다. 미군은 사이버 공격 기술들을 군사작전의 보조적인 수단으로 사용했다. 이라크전은 민간 주도의 사이버전에서 물리전력과 연계한 군 중심의 사이버전으로 넘어가는 과도기로 세계 각국은 사이버전의 효용성을 깨닫기 시작한 계기가 되었다. 이와 같이 장차전의 양상은 심리전과 사이버전, 그리고 물리전을 동반하는 개념으로 전쟁의 패러다임이 바뀌게 될 정망이다.

나. 물리적 대응을 허용한 탈린 매뉴얼

사이버전에 물리적인 대응을 하도록 한 국제규범이 탈린매뉴얼이다. 국가간에 무력충돌은 유엔헌장과 제네바 헤이그협약 등 국제법에 따른 교전 규칙에 제약을 받고 있다. 2013년 3월 나토 사이버방위센터(CCDCOE)가 작성한 '탈린 매뉴얼' 이 일종의 가이드라인 역할을 하고 있지만, 나토가 정식 채택한 구속력 있는 문서는 아니다.[39] 탈린 매뉴얼이 규정한 '사이버 전쟁'은 국가와 국가간에 사이버 공간에서 적대적인 군사행위를 하는 '무력충돌'의 한 형태다. 일반적인 사이버 범죄나 사이버 스파이 행위와는 차별화된 개념이다. 반드시 국가만이 전쟁의 당사자는 아니며 테러단체와 같은 비 국가 행위자도 해당된다. 사이버전의 핵심요소인 사이버 공격(cyber attack)은 인명 살상이나 목표물의 손상 등 물리적인 타격으로 이어질 수 있는 사이버 작전을 뜻한다. 상대국의 중요 인프라나 명령·통제시스템을 겨냥한 해킹공격이 대표적이다.[40] 사이버 공격을 당했을 경우 피해국은 비례성의 원칙에 따라 가해국에 대해 대응조치(countermeasures)를 취할 수 있다. 이 경우 공격의 강도와 피해규모에 비례해 적절한 대응을 취해야 한다는 교전수칙을 적용하는 것이다.[41]

국제사회가 주목하는 대목은 사이버 전쟁이 반드시 사이버 공간에만 한정되지 않는다는 점이다. 상황에 따라 물리적인 대응이 가능하고 이는 온·오프라인을

39) 2013년 3월 북대서양조약기구(NATO : North Atlantic Treaty Organization)가 사이버테러에 관한 조항들을 성문화한 최초의 사이버교전 수칙. 구속력은 없으나 사이버교전에서 국제적인 가이드라인 역할을 한다.

40) 박노형·정명형, "사이버전의 국제법적 분석을 위한 기본개념의 연구,"
『국제법학회논총』, 제59권제2호(대한국제법학회, 2014.6), pp.67-69

41) 이 수칙은 에스토니아의 탈린에 위치한 나토 산하 사이버방어협력센터(CCDCOE)의 총괄 아래 20여명의 국제법 전문가들이 3년에 걸쳐 완성하였으며, 무장공격에 상응하는 사이버공격을 받은 국가는 자기방어권 행사가 가능하다. 사이버공격에 직접적으로 가담한 민간인은 국제법상 공격으로부터 보호받지 못한다 등 총 95개의 사이버교전 수칙을 담고 있다.

포괄하는 전면전으로 확전될 수 있다는 전망이 나오고 있다. 탈린 매뉴얼은 국제법상 허용되는 '무력 사용(use of force)'이 사이버 공간에서도 가능하다고 해석하고 있다.[42] 문제는 과연 언제, 어떤 조건 하에서 무력 사용이 가능하느냐 하는 점이다. 합법적으로 무력사용이 인정되는 경우는 유엔헌장 제7장을 원용한 두 가지 경우다. 첫째, 국제평화 유지를 목적으로 안보리 승인에 따라 군사적 강제조치를 취하는 경우와(42조) 둘째, 무력 공격을 당해 자위권을 행사하는 경우(51조)다. 사이버전쟁과 연계된 무력사용은 바로 자위권 행사에 근거할 가능성이 높다는 분석이다. 사이버 공간에서 자위권 발동 요건인 무력 공격이 발생하게 될 경우 이를 어떻게 상정할 것이냐가 관건이다. 탈린 매뉴얼은 사이버 공격으로 인해 인명피해가 발생하거나 국가자산이 손상 또는 파괴되는 경우, 즉 치명적이고 파괴적인 물리적 피해가 발생한 경우에 무력사용이 가능하다고 보고 있다.[43] 이는 앞으로 사이버 전쟁이 재래식 전쟁과 함께 매우 복잡한 양상으로 발전할 것임을 보여주고 있다는 분석이다. 탈린매뉴얼의 편성 및 주요내용은 <표 1>과 같다.

<표 1> 탈린 매뉴얼 편성 및 주요내용

구 분	주 요 내 용
범위	° 전쟁선포의 정당성 및 전쟁행위의 정당성과 관련 국제법 망라 ° 사이버 범죄 등 무력행사 수준 이하의 사이버활동은 제외 ° 사이버작전에 대한 물리전이나 전자전식 대응은 검토에서 제외
Part Ⅰ	° 국제 사이버보안법 · 국가와 사이버공간(규칙1 ~ 10조) · 무력행사(규칙11 ~ 19조)
Part Ⅱ	° 사이버무력충돌법 · 무력 충돌법 일반(규칙20 ~ 24조) · 전투의 수행(규칙25 ~ 69조) · 특정 사람, 시설물, 활동(규칙70 ~ 86조) · 점령(규칙87 ~ 90조) · 중립성(규칙91 ~ 95조)

42) 박노형·정명현, 앞의 논문, pp.73-75.
43) 박노형·정명현, 위의 논문, pp.82-84

리언 패네타 전 미국방장관은 “적의 사이버 공격 징후가 있으면 선제공격도 가능하다”고 밝힌 바 있다. 탈린 매뉴얼 논의에 참여한 학자들도 만장일치로 “사이버 공격으로 전면전이 일어날 가능성이 있다”는 견해를 보였다. 그러나 문제는 사이버 공격의 근원지와 실제 공격자가 누구인지 명확하게 밝혀져야 실효성과 정당성을 확보할 수 있다. 사이버 공격에 대한 물리적 보복은 비례성 측면에서도 고려할 요소가 많이 있다.44)

제4절 분석의 틀

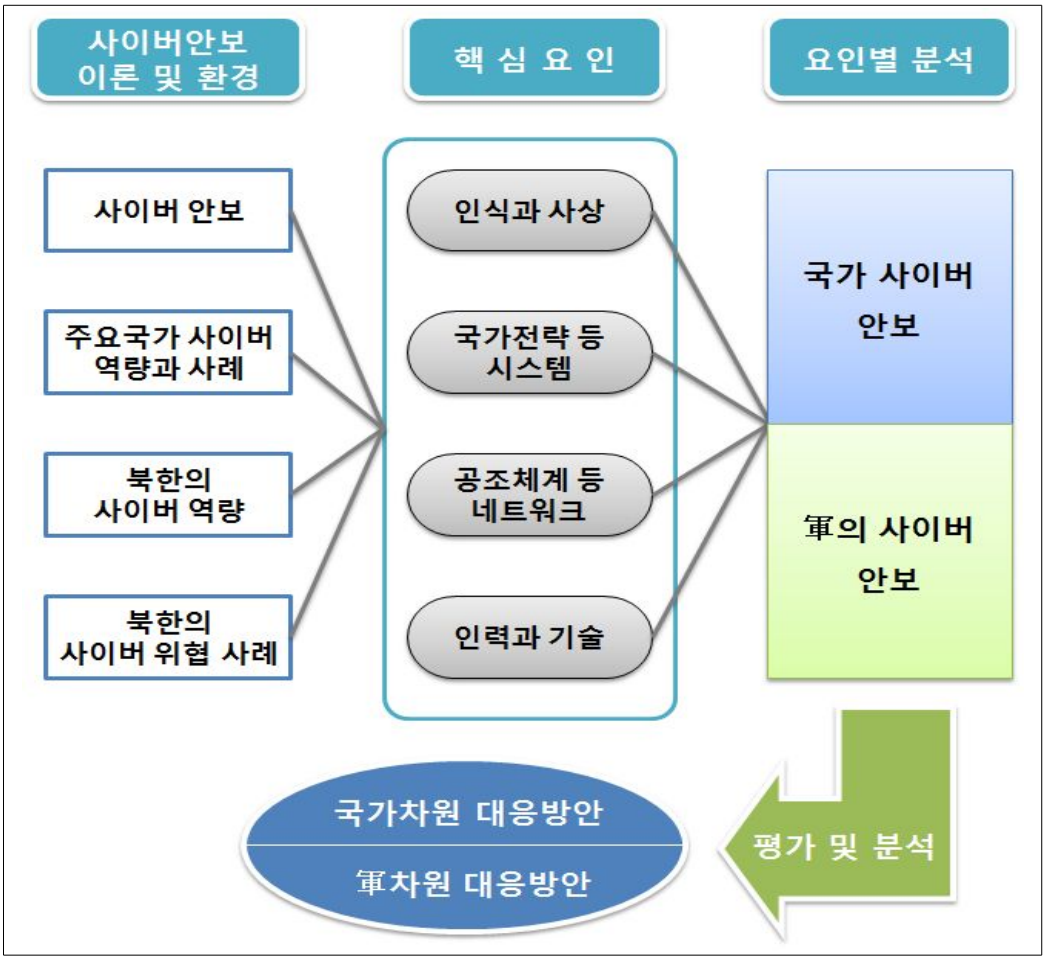
북한의 변함없는 대남적화전략과 국가기반시설 대부분이 네트워크화 된 한국의 안보환경은 북한의 사이버 공격에 상시 노출되어 있는 실정이다. 정부와 군은 북한의 공격에 대비하여 그동안 많은 노력을 하였으나 그 효과는 아직도 많은 분야에서 발전시켜야 할 필요성이 제기되고 있다. 따라서 국가와 군의 사이버 안보태세를 강화하기 위하여 결정적인 요인인 독립변수를 다음과 같이 네 가지로 도출하였다. 첫째, 사이버 국가안보를 위해서 국민과 정부의 사이버전에 대한 인식은 매우 중요하다. 이를 위해서 정부의 예산과 조직의 지원, 대 국민 홍보와 사이버 훈련, 민간의 참여 등이 중요한 요소가 될 것이다. 둘째, 국가전략 등 시스템을 검토하고 보강하는 방안이다. 우선적으로 국가와 군의 전략과 정책의 수립, 컨트롤타워의 주체, 법령과 제도, 중장기 계획 등이 중요한 요인이 될 것이다. 셋째, 공조체제 등 네트워크를 구축하는 방안이다. 이는 사이버 공격이 진행됐을 때 관련기관이 협력하고 공조체제를 구축하여 초기의 혼란을 최소화하며 아울러 미국, 중국, 일본 등 국제적인 공조체제를 구축하여 사전에 사이버전에 대한 정보를 공유하면 상황발생시 신속한 조치가 가능할 수 있기 때문에 중요한 요소로 작용한다. 또한 정보보호 인프라를 잘 구축하여 대비해야 할 것이다. 넷째, 인력과 기술 등 지원적인 면을 보강하는 방안이다. 사이버 전문 인력을 양성하고 기술개발을 전문적으로 할 수 있는 연구소 설립 등을 검토해야 할 것이다.

이를 도출하기 위해서 환경요인을 다음의 네 가지로 분석하였다. 먼저 사이버 안보환경에서 요구되는 사이버 안보의 개념, 사이버전의 특징과 장차 사이버전의 양상을 살펴보고 둘째, 미・중・일・러 등 주요국가의 사이버 역량과 사이버전 사례를 분석하여 우리의 수준과 실태를 비교해 보며 셋째, 북한의 대남 사이버

44) 『경향신문』, 2015년 4월 3일 금요일 A 02면 종합

전략과 역량을 분석하여 북한의 사이버 위협의 실체를 평가해 보고 넷째, 핵심요인별로 국가와 군의 사이버 안보실태를 분석하고, 정부와 군이 어떻게 사이버전에 대응해야 하는지 고찰해 보았다. 이를 위하여 작성한 분석의 틀은 <그림 1>에서 보는 바와 같다.

<그림 1> 분석의 틀



제3장 주요 국가와 북한의 사이버 역량

제1절 주요 국가의 사이버 역량

전통적인 의미의 전력은 국가 경제력을 바탕으로 한 군사전력이다. 물리적인 화력 중심의 무기체계, 군수품의 보급 체계 및 조달 능력, 전장 감시·정찰체계 등이 얼마나 잘 갖춰져 있는가에 따라 군사력의 수준이 결정됐다.

그러나 사이버전력은 기본적으로 소프트웨어를 중심으로 한 정보기술력에 의해 좌우된다. 사이버전력은 컴퓨터와 네트워크에서 작동되는 무기체계의 보호, 사이버공간으로 침투해오는 상대공격의 감시· 탐지· 분석· 차단 등 디지털 정보의 안전성을 확보하는 암호기술력과 피해시스템을 신속히 복구하는 능력 등으로 구성된다고 할 수 있다. 2012년 말 기준 국제연합(UN) 군축연구소에 따르면 세계 193개국 가운데 47개국이 사이버전담부대를 운용하고 있다. 군부대가 아닌 형태로 존재하는 기관을 합하면 사이버전을 수행할 전력을 갖춘 나라는 67개국에 이른다고 한다.[45]

1. 미국

미국은 1980년대부터 사이버공격의 심각성을 깨닫고 대책 마련에 나섰으며 사이버 공격에 가장 많은 투자를 하고 있는 나라다. 특히 미 국방부는 2005년 사이버전의 핵심을 방어에서 공격으로 바꾸고 관련 정책에 적극적으로 투자했다. 미 국방첨단 과학기술연구소(DARPA)의 '플랜X 프로젝터'가 대표적인 사례이다.[46] 미국은 플랜X를 통해 전 세계 컴퓨터 도메인[47], 서버 등의 위치와 연결망

45) 신동주, "총성 없는 전쟁 위협," 『세계일보』, 2013년 6월 24일.

46) 보안은 군사적 목적의 통신 보안(Communication Security)에서 시작되어 컴퓨터 보안(Computer Security), 네트워크 보안(Network Security), 정보보안(Information Security) 등으로 확대되고 발전하고 있다.

47) 인터넷상의 컴퓨터 주소를 알기 쉬운 영문으로 표현한 것으로 도메인은 네트워크를 관리하기 위한 영역이다. 예전에는 숫자로 된 IP주소가 사용되었지만 지금은 시스템, 조직, 조직의 종류, 국가의 이름순으로 구분되어 있다. 도메인 이름은 최 상위 도메인과 서브도메인, 호스트 이름 등으로 계층적으로 구성된다. 최상위 도메인은 '국가'를 의미하여 미국이라면 기관의 성격을 나타낸다. DNS(Domain Name system)란 인터넷의 도메인체계이다. 도메인 이름을 IP주소로 변환하는 역할을 하며, DNS는 인터넷에 연결된 컴퓨터를 구별해 준다.

을 보여주는 사이버 전장지도를 만드는 등 사이버전에 필요한 기본적 토대를 구축 중에 있다. DARPA는 향후 5년간 약 260억 달러의 예산을 투입할 예정이다. 미국은 대규모 국방예산 감축기조 속에서도 사이버전 예산을 매년 10~20%씩 늘려왔다. 2015년 예산은 51억 달러이며 우리 돈으로 약 5조 9000억 원 규모로 오바마 미국 대통령은 사이버 위협을 미국이 직면한 가장 심각한 경제안보와 국가안보문제의 하나라고 지적하고 미국의 디지털 하부구조를 국가의 전략적 자산이라고 평가했다. 따라서 디지털 하부구조를 지키는 것이 국가 안보의 최우선 과제일 수밖에 없다고 천명했다.

가. 안보전략

2009년 5월 미국 오바마 대통령은 사이버공간정책검토(CPR: Cyberspace Policy Review.)를 발표하면서 '사이버보안을 미국이 최우선 정책으로 수호해야 할 핵심적인 국가자산' 이라고 선포했다.[48] 미국은 백악관 및 국방부가 주도하여 전략을 구상하고 대응할 수 있도록 조직과 관련 교리를 발전시키고 사이버무기 개발에 국가적인 노력을 경주하고 있다. 미국의 사이버 안보전략은 2011. 7월 '사이버 공간에서의 국방전략(SOC) 보고서' 를 통해 사이버 안보와 관련된 5가지 전략적 구상(Strategic Initiative)을 <표 2>에서 보는 바와 같이 제시하였다.[49]

<표 2> 사이버 안보의 5가지 전략적 구상의 주요 내용

구분	주요 내용
전략적 구상 1	사이버 공간을 작전영역 (operational domain)으로 포함
전략적 구상 2	국방 네트워크 및 시스템 보호 강조
전략적 구상 3	전(全) 정부 차원(whole-of-government)의 총력 대응
전략적 구상 4	동맹국, 협력국 및 민간 영역과의 협력
전략적 구상 5	우수한 사이버인력 및 신속한 기술혁신

미국은 이러한 전략적 구상을 통해 "사이버 공간의 잠재력을 최대한 이용할 수 있도록 조직하며 훈련하고 장비를 갖추도록 하는 작전영역으로 간주한다" 고 밝히고 있다.[50] 나머지 전략적 구상은 국방부가 운영하는 네트워크 및 시스템에

48) James A. Lewis, "Cybersecurity Two Years Later," 『CSIS』 (2011.1)
49) "Department of Defense Strategy for Operating Cyberspace," (2011)

대한 보안조치를 강화하고, 통제 및 관리능력을 체계화하며 범정부 차원의 유기적 협력을 통한 총체적 대응의 필요성을 제시하고 있다. 2015년 4. 17일 미 국방부 장관은 新 사이버 5대전략을 발표하였다. 핵심내용을 살펴보면 첫째, 사이버 공간작전을 수행하기 위한 전력과 능력을 구축하고 유지한다는 내용과 둘째, 국방부의 네트워크 방어, 데이터 보안, 임무에 대한 위험을 완화하며 셋째, 심각한 결과를 초래할 수 있는 파괴적인 사이버공격으로부터 미국 본토와 미국에 필수적인 국익을 방어할 수 있는 대비태세를 유지하는 내용과 넷째, 실행 가능한 사이버 옵션구축과 유지, 분쟁확산 통제 및 분쟁 환경조율을 위한 옵션사용 계획과 마지막으로 위협억제와 국제안보 증대를 위한 양자 및 다자간 국제협력을 강화하는 내용을 포함하였다.[51]

2011년 7월에 발표한 사이버전략과 2015년의 新 사이버 5대전략의 차이점은 기존의 방어적 조치 내용으로는 현재의 기술발전 속도와 공격양상에 대응하기가 어렵다는 인식하에 방어적, 수동적 대응전략에서 억제(Deterrence) 및 공격적 대응으로 전환을 추진한다는 내용이다. 이를 위한 핵심 이행목표는 급변하는 사이버 공격양상에 대응하기 위해 사이버작전의 기술적 능력의 구축과 연구개발, 전문인력 확보, 국내외적으로 협력체계를 구축하여 적극적으로 추진하는 정책이다. 또한 다수의 우발사태를 상정한 임무목표 달성을 위해 사이버 임무전력의 능력을 검증하기 위한 지침을 구체화하고, 사이버 억제태세를 강화하기 위한 수단으로 실행 가능한 사이버 옵션구축 등 사이버능력의 발전을 추진할 계획임을 밝히고 있다. 新 사이버 5대전략은 사이버수단을 통해 미국의 안보를 위협하는 적대세력에게 억제 또는 선제공격을 통해 미국의 안보를 지키겠다는 강력한 메시지를 전달하는 부수적인 효과도 거둘 것으로 판단하고 있다.

나. 정책 및 조직

미국은 2012년 10월 대통령령 20호로 알려진 행정명령을 통해 대통령이 사이버전에 있어서 선제적인 조치를 취할 수 있게 하였다. 미국은 그동안 사이버공간에서의 적대적인 행위에 대해 필요한 모든 수단을 동원할 것이라고 밝혔다. 사이버전의 속성상 나노세컨드(Nano Second)를 다툴 수 있는 군사적인 작전환경을

50) DoD of US, "Department of Defense Strategy Operating in Cyberspace," (2011), p.5.
51) 국방부 정책실 담당자, "미국의 新 사이버 5대전략 보고서," (서울: 국방부, 2015년 4월)

갖추는 것이 중요하며, 경제안보를 공략하는 사이버공격에 더 신속하게 대응해야 한다는 취지로 대통령령으로 선제적 조치를 취할 수 있도록 바꾼 것이다. 사이버 위협이 점차 증대되고 고도화되고 있는 상황에서 더 이상 소극적인 방어만 할 수 없다는 것이 미국의 판단이다. 2013년 4월 8일 존 하이텐 미 공군 우주사령부 부사령관은 군의 사이버작전 능력을 높이기 위해서 펜타곤의 지원을 받아 사이버무기를 새롭게 지정하여 사이버공격 대책을 결정한다고 밝혔다. 즉 국가 간 전면전쟁이 발생하기 전에 사이버 공격을 통하여 전초전으로써 사이버 무기가 전쟁의 전략적 도구로 사용될 수 있으며, 사이버전의 승패에 따라 전면전의 승패로 가름될 수 있기 때문이다.

2015년 1월 미국은 소니픽처스 해킹과 관련하여 해킹의 주범으로 북한을 지목하고, 북한 인터넷 망을 불통으로 만든 일련의 조치와 사이버안보를 화두로 한 오바마 대통령의 국정연설은 사이버 위협이 얼마나 중요한지 알게 한 사건이었다. 연설에서 오바마 대통령은 악성코드를 이용한 사이버공격이 핵과 미사일보다 더 파괴적인 결과를 초래할 수 있다는 경각심을 강조했다.[52] 미국이 소니 해킹의 주범으로 북한을 지목하고 즉각적으로 이에 상응한 비례적인 대응을 할 수 있었던 이유는 다음과 같다. 미국은 공격자를 즉각적으로 식별(attribution)할 수 있는 기술력을 확보했기 때문이다. 미국은 사이버 맵(Map)과 연계한 '플랜X 프로젝트'와 함께 다양한 정보를 통한 사이버공간에서의 대응 역량을 확보했다. 또 다른 요인은 국제협력을 포함한 사이버전 대응 수행체계 구축능력이다. "미국이 즉시 대응조치를 할 수 있었던 것은 앞서가는 기술력과 국제공조 능력 그리고 사전에 대응작전 계획이 정립돼 있었고, 이에 대한 법적·제도적 뒷받침이 있었기 때문이다."라고 했다.[53] 이와 같이 미국의 디지털 기술력은 압도적이다. 현재 10대 글로벌 정보기술기업 중 9개가 미국 기업이라는 것이 이를 증명한다. 전 세계 정보기술시장 중에서 운영체제는 마이크로소프트, 데이터베이스관리시스템(DBMS)은 오라클, 네트워크 장비는 시스코, 컴퓨터 칩은 인텔의 제품이 지배한다. 인터넷 서비스와 클라우드컴퓨팅은 구글, 모바일은 애플, 비즈니스 컨설팅은 아이비엠과 휴렛패커드가 석권하고 있고, 소셜네트워크는 페이스 북이 장악하고 있다.[54]

52) 손영동, "영화 '인터뷰' 사태가 주는 안보적 함의," 『국방일보』, 2015년 1월 21일.
53) 임종인, "미국의 대북 사이버 응징이 주는 교훈," 『문화일보』, 2015. 1. 7.
54) 채인택•노진호 "빅브라더, 미국에 도전할 나라도 기술도 없다," 『중앙SUNDAY』, 2013.6.16.

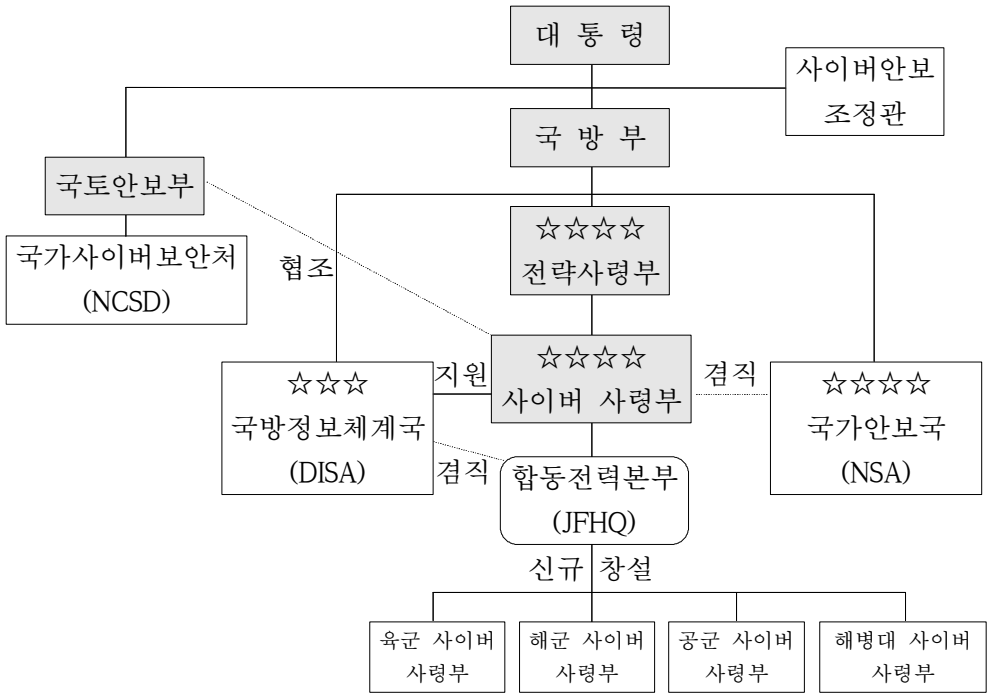
2013년 6월 미 국가안보국(NSA)에 근무했던 스노든의 폭로로 미국과 영국의 디지털 첩보활동이 공개됐다.[55] 그간 공공연한 비밀이었던 '프리즘(PRISM)'[56]을 통한 첩보수집은 물론 첩보수집에 글로벌 정보기술업체들을 동원됐고 중국·이란·파키스탄 등을 해킹한 사실까지 드러났다. 그러나 미국은 '프리즘' 이라는 비밀 프로그램이 존재하고 정보수집 사실도 인정했지만, 이는 해외정보감시법(FISA: Foreign Intelligence Surveillance Act.)에 따라 테러방지를 위해 쓰였고 국가안보에 필수적이라고 맞섰다. 미 정보기관을 총괄하는 국가정보국(DNI)의 제임스 클래퍼(James Clapper) 국장은 "프리즘이 법률에 따라 비밀 해외정보감시법원(FISC: Foreign Intelligence Surveillance Court)의 감시를 받으며 합법적으로 운영되어 왔다." 고 주장했다. 오바마 대통령은 "100% 안전과 100% 프라이버시와 0% 불편함을 모두 충족시킬 수 없다. 약간의 사생활 침해의 우려는 있지만 테러방지를 위해 충분한 가치가 있다" 고 밝혔다.[57] 미국의 경우 주요기반시설을 겨냥한 사이버 공간에 대비한 "사이버안보보호법", 사이버전쟁시 민·관 협력을 규정한 "사이버안보강화법" 등 5개의 관련 법률을 제정·시행하고 있다.[58]
오바마 대통령은 정부의 모든 사이버보안 정책을 통합하고 조율하는 직책을 백악관에 신설했다. 국토안보부와 국가안보국 등 여러 부처에 흩어져 있는 사이버보안업무에 관한 전권을 부여받은 자리는 사이버안보조정관(Cybersecurity Coordinator)이다. 대통령에게 대면 보고하며 안전보장회의(NSC)에도 참석한다. 이와 같은 미국의 사이버 안보 조직체계도는 <그림 2>에서 보는 바와 같다.

2009년 6월 23일 미국 국방부 산하에 사이버사령부(Military Command for Cyberspace)가 창설됐다. 펜타곤에만 1만 5000개의 컴퓨터 네트워크가 있으며 미군은 전 세계 88개국 4,000여 개 군사시설에서 700만 대의 컴퓨터를 사용하고 있는 것으로 알려져 있다. 미국은 9만여 명의 사이버보안 인력을 군과 정부기관에 배치했다. 사이버 사령부는 8만여 명 규모이며, 이 중 전문요원 6,000여 명이 130여개 작전팀에 분산돼 주요국 공격 및 미국의 기반시설보호 임무를 맡고 있다. 미국 사이버사령관은 "20세기가 핵무기의 시대였다면 21세기는 사이버무기의

55) 글렌그린월드 지음/박수민·박산호옮김, 『더 이상 숨을 곳이 없다』(서울: 모던타임스, 2014), pp.7-14.
56) PRISM : Planning tool for Resource Integration, Synchronization and Management.
57) 손영동, 『0과1의 끝없는 전쟁』(서울: 인포더북스, 2013), p.253.
58) 손영동·고성훈, 앞의 논문, p.33.

시대” 라며 사이버전력의 증강을 미군의 최대과제로 꼽고 있다.

<그림 2> 미국의 사이버안보 조직체계도



미 국방부에 대한 사이버 공격은 2009년 상반기에만 54,460건이었고 매년 급증하고 있다. 이에 따라 2010년 1월 미국은 모의 사이버전을 실시했다. 이 모의 전쟁에는 전 세계를 분할해 관할하는 6개 지역별 통합군사령관과 국방부 수뇌부가 참가했는데 시뮬레이션 결과 미국의 전력과 금융네트워크, 통신체계가 마비된 것이다. 이와 같이 사이버 상에서는 공격의 발원지를 찾기도 어렵고 추가 피해를 막기 위한 방법도 어려웠다. 인터넷을 활용하는 사이버 전에서는 거리의 개념이나 공격의 주체도 모르며 예측도 불가능하기 때문이다.

그러나 여기서 우리가 간과해서는 안 될 사항이 있다. 이는 20년 가까이 일관성 있게 추진되고 있는 미국의 사이버안보정책이다. 1998년 5월 클린턴 대통령은 행정명령으로 주요기반시설에 대한 보호체계를 마련하였고 부시 대통령은 2002년 11월 ‘국토안보법’과 12월 ‘연방정보보안관리법’을 제정해 국가의 사이버 보안관리와 통제체계를 일원화시켰다. 2009년 1월에 출발한 오바마 정부는 사

이버안보를 국가정책의 최우선 과제로 선정하고 백악관을 중심으로 실행계획을 마련하여 지속적으로 추진하고 있는 것이다.[59]

다. 사례

미국은 하루에 5만 번의 사이버 공격에 시달리고 있다. 미 중앙정보국을 비롯한 17개 정보기관은 2012년 12월 발표한 국가정보평가보고서에서 미국에 대한 최대의 사이버공격 국가로 중국을 지목했다.[60] 2013년 5월 국방부 보고에서도 미국의 기업과 연방정부기관을 상대로 한 중국의 해킹의 배후에 중국 정부가 있다고 밝혔다.[61] 이에 2013년 3월 중국을 방문한 제이콥 루 재무장관은 시진핑 국가주석 등 중국 지도부를 만나 해킹은 미국의 경제이익을 침해하는 매우 중대한 위협이라며 문제를 제기했다. 오바마 대통령도 시진핑 국가주석에게 취임축하 통화를 하면서 사이버안전에 대한 위협이 양국 사이에 놓인 새로운 도전이라고 언급했을 정도다. 2012년 1월 이후 뉴욕타임스와 애플, 페이스북, 코카콜라 등 주요 기업은 물론 정부기관까지 해킹을 당했다. 코카콜라는 해킹을 통해 중국기업의 인수전략이 노출된 것으로 알려졌다. 미국의 최대 방산업체인 록히드마틴은 지속적으로 피해를 당했다. 미국은 중국의 해킹공격에 의한 경제적 손실을 연간 수백억 달러로 추정하고 있다. 한편 2013년 2월 미국의 정보보안업체 맨디언트는 2006년부터 약 20개국 141개의 다양한 기관이 미국의 정보를 빼갔고 그중 대부분은 미국의 기업과 정부기관이라고 밝혔다. 특히 해킹의 배후로 중국 인민해방군 61398부대를 지목했다. 중국은 보도내용을 부인했지만 미국은 중국이 이미 첨단무기설계도를 절취해가는 등 군사 분야에서도 상당 수준의 해킹 피해를 당한 것으로 확신하고 있다. 미 의회는 2013년 회계연도 예산법안에 연방정부의 중국산 정보기술제품 구매를 금지하는 조항을 넣었다. 상무부와 법무부, 항공우주국, 국립과학재단 등은 중국 정부와 관련된 업체에서의 시스템 구매를 전면 금지한다는 내용의 정부지출 관련 법안이 2013년 3월 발효됐다.

다음 사례는 미국과 이란 간에 국가의 핵심기반시설을 공격한 사이버전의 사례다. 이란의 핵개발을 저지하기 위해 조지 부시 행정부 때부터 사이버공격을 통

59) 유동열, 앞의 책, pp.136-137.
60) 손영동(b), 앞의 책, p.247.
61) 이동범・곽진, “미국정부의 사이버 공격에 대한 보안전략,” 『정보보호학회지』, 제24권 제1호(2014.2), p.16.

해 이란의 핵시설에 물리적인 손상을 가하도록 사이버공격을 시작했으며 이 전쟁은 오바마 행정부가 들어선 이후에도 계속되고 있다. 2011년 1월 뉴욕타임스(NYT)는 이란 핵시설의 원심분리기의 가동중단 사태를 일으킨 스턱스넷을 이스라엘이 미국과 공동으로 시험했다고 보도했다. 이스라엘이 미국의 지원을 받아 지난 2년간 이스라엘 남부 네게브 사막에 있는 디모나(Dimona) 비밀 핵시설에서 스턱스넷의 파괴력 검증시험을 진행해 왔다는 것이다. 이란은 나탄즈 핵개발 단지의 원심분리기들이 오작동하는 원인을 찾아내지 못하다가 나탄즈에만 머물러 있도록 설계된 스턱스넷이 나탄즈를 빠져나와 전 세계로 퍼져 나가면서 사건의 전모를 파악하게 되었다.[62] 2011년 이란은 자국의 핵시설이 사이버공격으로 피해를 당했다는 사실을 인정하면서 상대국에 사이버 공격을 전개하겠다고 선언했다. 2012년 9월 뱅크오브아메리카, 씨티그룹 등 미국의 6개 대형 금융회사들이 디도스 공격을 받았다. 이란 해커그룹은 미국 은행들에 대한 디도스 공격이 자신의 소행이라고 밝혔지만, 미국은 이란 정부의 지원 없이는 이 같은 대규모 공격은 불가능했을 것으로 판단하고 있다. 이란의 공격은 미국과 이스라엘이 자행한 사이버공격에 대한 대응차원이며 경제제재에 대한 보복이었다. 이란은 2012년 8월 사우디의 국영 석유회사인 아람코를 공격했다. 아람코는 이 공격으로 컴퓨터 3만대의 파일이 삭제되고 전체 전산망 가동이 일시 중지되는 등 많은 피해를 입었다.

라. 특징 및 시사점

미국은 사이버 안보를 위해서 군사동맹, 국제협력, 민간영역에 이르기까지 다차원적인 협력을 강화하고 있으며 기존의 국제규범을 사이버 영역으로 확장하여 적용할 수 있도록 노력하고 있다. 아울러 정보보호와 사이버전에 활용하고 있는 다양한 법률을 제정하고 있다. 이러한 법률에는 컴퓨터보안법[63], 국토안보법[64], 애국법(USA Patriot Act)[65], 사이버보안강화법[66], 통신지원법[67], 대통령행정명령[68]

62) 부형욱, “사이버안보의 주요이슈와 정책방향,” 『국방연구』, 제56권 제2호, p.104.
63) 컴퓨터보안법은 1987년에 제정되어 미국표준기술연구소를 중심으로 컴퓨터보안에 관련된 사항을 규정하고 있다.
64) 국토안보법(homeland security Act)은 2002년에 각종 테러로부터 미국의 국가기반을 보호하기위해 제정되었다. 사이버 보안에 관한 규정은 총17개장 중 제2장(정보분석 및 기반시설보호) 및 제10장(정보보호)에 제시되어 있다.
65) 2001년 9.11테러직후에 제정된 법률로써 통신감청을 포함한 각종 테러위협 수사권을 포괄적으

등이 있다. 미국은 사이버 공간이 군 작전영역으로 공식화되어 있으며, 이는 군사적 분쟁에 관한 법률에 적용할 근거가 되고 사이버 위협에 자위권 차원에서 적극적으로 대응할 수 있도록 안보태세를 갖추는 근거가 되었다. 또한 국방예산 감축에도 불구하고 미 의회의 적극적인 협조로 사이버전 예산을 대폭적으로 증액하여 조기에 대응체계를 구축할 수 있도록 하고 있다.

미국의 경우 블레어 국가정보국장은 2010년 위협평가보고서에서 미국의 핵심 인프라가 심각한 사이버 공격에 직면해 있지만 지금과 같이 정부와 국민이 독자적으로 행동한다면 예방하기가 어렵고, 민감한 정보가 정부와 민간분야 네트워크에서 도난당하고 있기 때문에 정부와 민간이 긴밀한 협조체계를 구축해야 사이버 위협에 효과적으로 대응할 수 있다고 강조하였다. 특히 미국은 국가기간망을 흔드는 외부의 사이버공격을 전쟁행위로 간주해 미사일 공격 등 무력으로 대응한다는 방침을 세웠다. 미 국방부가 마련한 사이버전략 보고서는 사이버공격을 전쟁행위로 규정하고, 재래적 방식의 무력으로 대응한다는 것이다. 다시 말해, 송전망 차단과 같은 컴퓨터 네트워크 공격은 미국에 대한 선전포고로 간주하겠다는 경고이다.[69]

2. 중국

중국은 1990년대 중반부터 우주, 전자, 사이버 공간에서의 국가안보 이익수호를 국방목표로 설정하고 사이버전에 대비하기 시작했다. 1995년에 정보전 계획을 수립하기 시작하였으며 1997년부터 컴퓨터 바이러스를 활용하여 국가 및 군사통신망과 방송 등 공공망을 와해시키는 훈련을 시행하고 있다. 1997년 인민 해방군은 중앙군사위원회에 악성코드가 원자폭탄보다 효율적이라는 보고서를 제출한 바 있다.

로 보장해 주고 있다. 사이버테러의 억제와 처벌의 법적근거를 제공하고 있다.

66) 2002년 국토안보법에 포함되어 제정되었다. 사이버공격에 대한 상세한 처벌 근거를 규정하고 있다.

67) 1994년에 제정되어 수사목적을 위한 통신감청에 대해서 통신사업자의 협조의무를 구체화하고 있다.

68) 2008년 1월에 발령된 'HSPD-53: 국가사이버 안보센터 설립' 'NSPD-23: 연방정부기관의 인터넷 모니터링' 등이 있다. 대통령 행정명령은 미국의 국가사이버 안전과 관련된 정책을 수립하고 집행하는데 필요한 근거를 제시하고 있다.

69) DoD of Department of defense, "Strategy for Operating in Cyberspace," (July 2011).

가. 전략과 정책

중국은 사이버 안보 전략을 상세하게 공개하지 않고 다만 2010년 국방백서에 미래 안보환경에 능동적으로 대응하고자 우주, 전자, 사이버 공간에서의 '새로운 형태의 전투력을 개발' 하고 있음을 시인하는 정도로 보안을 유지하고 있다.[70] 2014년 10월 중국공산당 중앙군사위원회는 '군 정보보안 강화방안' 을 발표했다. 주요내용은 전 분야에 걸친 정보보안의 총체적인 설계와 종합적 관리, 정보보안 강화를 위한 사이버군의 임무와 군사투쟁, 정보보안의 등급분류와 평가의 전면적인 시행 등이 포함되었다. 이어서 2015년 7월 전국인민대표회의에서 사이버상의 공격과 유해정보 확산으로부터 사이버 주권과 국가안보를 위한 '사이버 안전법 초안' 을 수립했다. 이 법안은 정부, 기업, 개인에 이르기까지 네트워크상에서 준수해야 할 의무와 역할을 강조하고 사이버 위협 발생시 이를 차단하는 방안이 명시됐다.[71]

중국은 미국의 인터넷 기술종속에서 벗어나기 위해 하드웨어와 소프트웨어의 국산화에 노력하여 왔다. 2007년부터 중국은 '기린' 이라는 운영체계를 개발해 정부기관이 사용하고 있다. 이는 중국이 미국의 '윈도우' 와 같은 운영체제를 사용하지 않음으로써 외부의 침입에 대한 강력한 방어망이 형성됐음을 의미한다. 중국은 '국방과학기술정보센터' 에서 사이버 전쟁을 연구하고 인민해방군 내에 컴퓨터 바이러스 부대를 운영하며 미국의 군사력을 약화시키는 사이버 공격을 준비하여 시행하고 있다. 중국의 사이버전 관련 능력은 사이버 방어측면 보다는 공격측면에 많은 관심을 기울이는 것으로 추측되는데 그 이유는 지속적으로 중국과 관련된 사이버 공격이 관측되고 있기 때문이다. 중국은 전술적인 측면에서도 꾸준한 발전을 이어오고 있다. 전쟁 발발 전에 악성코드를 적 컴퓨터에 잠복시켜 은폐하는 전궤잠복법과 전쟁전날 악성코드를 적 컴퓨터나 무기체계에 장착하는 임기예측법, 악성코드를 컴퓨터 보조시스템에 침투시키는 간접공격법 등 세부기술들을 개발하고 있는 것으로 판단하고 있다.[72]

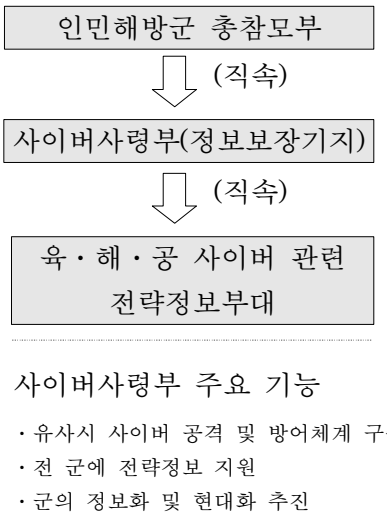
나 조직

중국은 해커부대인 넷 포스와 정보전시험센터, 국방과학기술정보센터 등 해커

70) 유동열, 『사이버 공간과 국가안보』(서울: 북앤피플, 2012), p.149.
71) 국방부 정보본부 담당자, "세계주요국의 사이버전 대응동향," (서울: 국방부, 2015년 7월)
72) 오명호 외, 앞의 책, p.68.

양성기관을 운영하고 있다.[73] 중국은 2000년 컴퓨터 바이러스 부대와 넷 포스 부대를 창설하였고 2003년에는 베이징·광저우·지난·난징 등 4대 군구 예하에 전자전 부대를 창설하였다. 중국의 사이버 사령부의 체계도와 해커부대의 특징은 <그림 3>에서 보는 바와 같다.[74]

<그림 3> 중국 사이버사령부 체계도 / 해커부대



61486부대	부대 이름	61398부대
상하이	부대 위치	상하이
퍼터 판다(Putter Panda)	부대 별명	코멘트 크루(Comment Crew)
미국·유럽·일본의 정치·경제·군사	주요 목표	주요국의 정치·경제·군사
인민해방군 총참모부 제3부 12국	부대 편제	인민해방군 총참모부 제3부 2국
미국 정부, 국방, 연구·개발(R&D), 방산업체, 항공우주산업, 통신 등	해당 타깃	코카콜라, 록히드마틴·웨스팅하우스·US스틸·미국 철강노조 등
CPYY	핵심 인물	UglyGorilla/DOTA
2007년	활동 시작	2006년
수십 차례	해킹 사례	141건
13만명(지원인원포함)	인원	수천명(지원인원제외)

2010년에는 인민해방군 내에 사이버 블루팀이라는 조직을 창설하였는데 이는 사실상 중국 인민해방군의 사이버 사령부로 중국식 표현으로는 '신식정보보장기지'라고 한다. 중국의 사이버 사령부는 유사시 사이버 공격 및 방어체계의 구축, 전군에 전략정보지원, 군의 정보화 및 현대화 추진을 주요 기능으로 하고 있다. 한편 인도 국가안보협의회사무국(NSCS)에 의하면 중국은 사이버전 부대를 비롯해 정부기관 등에 12만 5,000명의 사이버요원을 보유하여 세계 최다인력을 운용하고 있는 것으로 조사됐다고 한다. 해커전문 부대는 인민해방군 61398부대가 있으며 40만여 명에 달하는 민관군 통합 네트워크부대와, 국익을 위해 독립적으로 활동하는 100만여 명의 애국적 해커인 홍커[75]가 있는 것으로 추정되며 이들

73) 안유성, "사이버 안보 대응역량 강화방안 연구," 『정보보호학회지』, 제24권 6호(2014. 12), p.65.
74) 국민일보, "총대신 마우스 중국 '사이버사령부' 창설." (2010 7. 22.).

이 사이버 예비군의 역할을 하고 있는 것으로 알려졌다. 또한 61486부대는 각국 정부와 군 하청업체, 연구기관 등에 대한 대대적인 해킹업무를 수행하고 있는 것으로 알려지고 있다. 인민해방군은 여러 대학 및 연구기관과 협력하여 연구를 수행하며 12개의 사이버전 훈련장을 운영하고 있는 것으로 알려졌다.[76]

이들은 매우 공격적이며 애국심으로 무장하여 미국과 일본 등 전 세계 정부와 기업을 대상으로 사이버 공격을 가하고 있다. 미국은 중국정부가 이들을 직·간접적으로 도우면서 해킹을 부추긴다고 평가하고 있다. 시진핑 주석이 조장으로 있는 '중앙인터넷 안보 및 정보화 영도소조'가 사이버전 관련 모든 업무를 총괄하는 것으로 알려졌다.[77] 상하이 빌딩가에 자리 잡고 있는 총참모부 제3부 산하 61398부대가 대미(對美) 해킹을 주도하고 있다. 이 부대는 2006년 이후 미 IT 업계·우주항공 업체에서 140건 이상의 기술 정보를 해킹한 것으로 알려졌다.

다. 사례

1999년 코소보 사태는 북대서양조약기구(NATO)와 유고 간의 분쟁이다. 당시에 나토군을 지원하는 미군 폭격기가 유고주재 중국대사관을 오폭하자 중국 해커들은 미 백악관·에너지부·내무부 등의 사이트를 해킹하고 오폭에 항의하는 메시지와 폭격으로 희생된 사망자들의 사진을 게시했다. 이들은 또한 미연방수사국(FBI)이 해킹에 관여한 해커들의 수사에 착수하자 이에 대한 보복으로 연방수사국 홈페이지를 바꿔놓았다. 한편 2001년 4월 남 중국해 인근에서 미국 정찰기와 중국 전투기가 충돌한 사건이 있었는데 미국 정찰기는 하이난 섬에 불시착하였고 중국 전투기는 추락하였다. 사건 이후 중국은 미국 정찰기를 추후에 양도하기로 했지만, 이로 인해 양국의 해커들은 상대국 웹 사이트를 해킹하며 대립하였다. 이 사고로 사망한 중국 전투기 조종사를 추모하는 해커들이 미국의 웹 사이트를 공격하여 웹 사이트의 내용을 삭제하고 미국 백악관과 전략군사령부 등 1,038대의 서버를 공격했다. 이후 양국은 사이버 상에서 지속적으로 대립하고 있다. 2012년 중국은 1,802개의 정부 웹사이트와 1,420만 대의 서버가 7만3천개의 해외 인터넷 주소로부터 공격을 받았고 미국에서 시작한 것이 가장 많았다고 주장하는 등 양국은 사이버 상에서 첨예한 대립을 하고 있다. 그러나 2013년 6월

75) 중국의 사이버 공격자. 전 세계를 대상으로 해킹을 시도하는 것으로 알려지고 있다.
76) 유동열, 앞의 책, p.151.
77) 손영동·고성훈, 앞의 논문, pp.27-28.

전 중앙정보국 요원이었던 에드워드 스노든은 미국이 2009년부터 중국과 홍콩의 이동통신업체와 칭화대를 도청했다고 폭로했다.[78] 중국은 이를 통하여 미국이 제기한 해킹 의혹으로부터 반사이익을 보게되는 계기가 됐다.[79]

라. 특징 및 시사점

중국은 사이버전 핵심기술에서 자립이 가능한 국가이다. 미국과의 기술격차도 줄였고 세계 최고성능의 슈퍼컴퓨터를 보유하고 있으며 드론기 분야에서도 첨단 기술 분야를 나타내고 있다. 중국은 소프트웨어 측면에서도 많은 노력을 하여 우리나라를 추월하고 미국과 경쟁할 수 있는 국면으로 발전했다. 중국의 바이두, 알리바바, 텐센트와 같은 회사는 미국의 구글, 아마존, 페이스북과 같은 회사와 동일한 수준이고, 아울러서 화웨이와 샤오미 등 하드웨어와 소프트웨어 분야에서 세계적인 회사를 운영하고 있다. 이는 중국 공산당의 오랬동안 인프라의 확충과 국산화의 정책으로 이룩한 성과로 판단된다.

미 국방과학위원회(DSB)는 2014년 내부 보고서를 통해 첨단 무기시스템설계도 중 최소 24개가 사이버공격으로 유출됐다며 그 배후로 중국 정부를 지목했다. 유출된 설계도 목록에는 최첨단 F-35 전투기, 신형 수직 이착륙기 MV-22 오스프리, P-8A 차세대 대잠수함 초계기, 전략용 무인기 글로벌호크, 이지스 미사일 방어 체계 등이 포함되어 있다.[80] 미 국방부는 중국이 사이버 해킹을 통해 무기개발 기간을 25년 단축했다는 평가를 하였다. 2014 4월 21일 미국의 월스트리트저널(WSJ)은 외국 해커에 의해 록히드마틴사가 제작중인 F-35 통합공격전투기(Joint Strike Fighter)의 자료가 들어 있는 컴퓨터가 공격을 받아 일부 자료가 유출됐다고 보도했다. 미국은 중국이 스텔스 전투기나 대륙간 탄도미사일과 같은 첨단무기를 자국의 연구개발 뿐만 아니라 미국, 일본, 이스라엘, 러시아 등을 대상으로 한 사이버 첩보활동을 통해서 얻은 정보로 이들 체계를 개발하는데 기여한 바가 크다고 평가하였다. 이 사례의 특징은 사이버 공격자가 집단화하고 조직화되기 시작한 것이다. 그 이전의 공격자들은 주로 해커 개인이나 몇몇 해커들이 독자적으로 활동했지만 이번에는 해커들이 사이버 커뮤니티를 통해 자발적으로

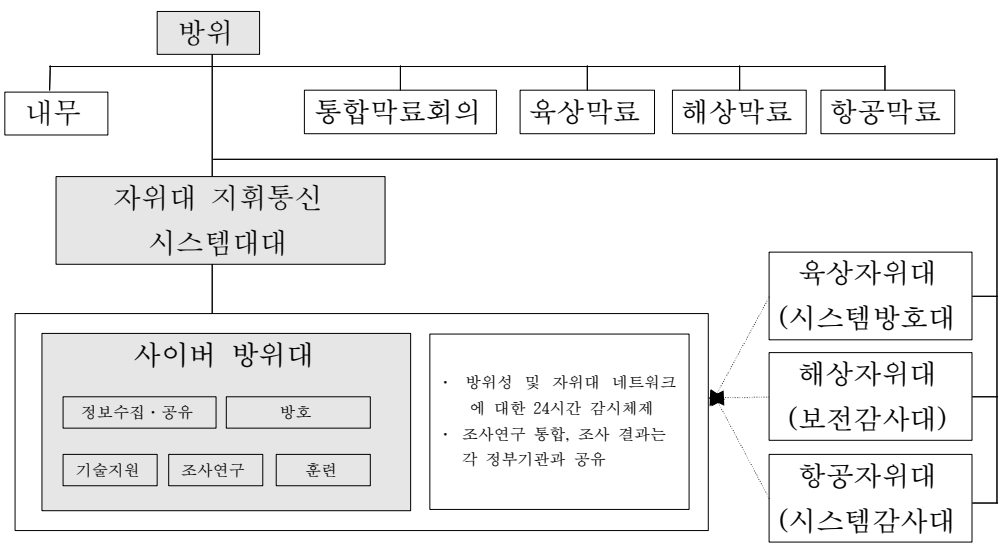
78) 글랜 그린월드 지음/박수민 박산호 옮김, 앞의 책, pp.7-9.
79) 손영동(b), 앞의 책, pp.247-249.
80) 김승주, "세계 각국의 사이버전 수행능력과 국내 피해사례," 『군사논단』, 제75호(한국군사학회, 2013), p.20.

공격목표·시기·방법 등을 모의하고 공격도구를 공유하여 공격한 것이다. 상호 공격이 격해지자 해커들을 지휘하는 리더그룹까지 발생하여 조직적인 해킹이 가능한 계기가 되었다.[81]

3. 일본

2000년 1월 일본사회는 과학기술청과 마이니치 신문 등 16개의 일본 정부 및 언론기관의 웹 사이트가 해킹당하여 충격을 받았다. 이에 영향을 받은 일본은 5년 내에 세계 최고의 정보통신 국가를 이룩한다는 목표를 가지고 'e-Japan 중점계획 2002'를 추진하여 네트워크에 대한 안정성과 신뢰성을 제고하고자 했다. 핵심은 기반시설에 대한 정보보호를 위해 정부와 민간의 협업이 중요하다는 점이 강조되고 있으며 긴급대응팀을 운영하여 효과적으로 대비한다는 개념이다.[82] 일본은 <그림 4>에서 보는 바와 같이 자위대 산하에 사이버 방위대를 편성하여 운용하고 있다.

<그림 4> 일본 자위대 산하 사이버방위대 조직체계



일본의 사이버 관련 조직은 내각관방장관실에 정보보안대책 추진실을 두고 예하에 긴급대응지원팀을 구성하여 즉각적인 임무를 수행하며, 정보보안대책 추진실

81) 손영동(a), 앞의 책, pp.219-221.
82) 안유성, 앞의 논문, p.65.

은 총무성, 경제산업성, 경찰청 등 정부부처와 협력을 도모하고 민·관의 정책추진을 총괄하도록 한 구조다.[83] 아울러 일본은 최근까지 꾸준하게 사이버 안보를 위해 동맹국과 보조를 맞추어 자국의 역량을 발전시켜왔다. 2005년 정보보호대책추진실을 '국가정보보호센터'로 확대하여 조직을 강화하였다. 이의 기능은 정보보호에 관한 기본전략의 수립 및 홍보, 정부기관의 종합적인 대책 추진, 긴급상황시 경보발령 및 피해발생시 관계기관 간의 협조와 원인분석, 그리고 피해복구 등을 수행하는 것이다. 그러나 2006년 2월, 일본 해상자위대의 구축함 암호와 전투훈련 내용 등에 대한 기밀정보의 인터넷 유출사고가 발생하였다. 원인은 방위청 직원이 개인적으로 사용하던 컴퓨터에서 '위니 웜 바이러스'[84]를 매개로 한 중국산 컴퓨터에 의해 자료가 유출된 것으로 조사되어 이들에 대한 사용을 중지시킨 바 있다.

2006년 4월, 미·일 간 방위협력의 일환으로 정보교환 등을 통해 사이버 공격능력을 향상시킬 목적으로 '정보보증과 컴퓨터 네트워크 방어협력에 관한 양해각서(MOU)'를 체결하였다. 2008년 7월, 자위대의 컴퓨터에 대한 사이버 방어임무를 수행하는 '지휘통신시스템대'를 창설하고 사이버전에 대비한 조직개편을 강화하였다. 2013년 3월, 사이버공격에 대응하기 위해 일본 방위성은 사이버방위대를 발족시켰다. 이를 계기로 사이버 공격시 자위대는 지휘명령 계통을 유지하고 작전행동에 지장이 없도록 하는 것을 목표로 하고, 방어 대상은 방위성과 전국 자위대 기지를 잇는 네트워크시스템에 한정되어 있었다. 하지만 일본 정부는 자위대의 활동을 국가 주요기반시설 보호로 확대할 움직임을 보이고 있다.

최근 일본은 원자력 발전소와 교통·통신 등 사회기반시설이 대규모 사이버공격을 받을 경우를 상정해 자위대가 방위나 반격을 할 수 있도록 하는 방침을 검토하고 있다. 사이버공격이 해커에 의한 범죄행위인지 타국에 의한 공격인지 주체를 판별하기조차 어렵기 때문이다.[85] 2013년 일본정부는 네트워크에 대한 감시태세 강화, 사이버연습 환경의 구축 연구, 인재육성 및 확보 등 사이버전 운용기반을 내실화하는데 사이버 관련 예산을 편성하였다. 그리고 미·일 방위협력지

83) KISA, "주요 국가별 사이버방어체제 및 대응동향," 『Internet & Security Bimonthly』, 심층분석, 2014. p.15.
84) 일본의 P2P 프로그램 '위니'는 일본 내 약 200만 명의 네티즌이 이용하고 있으며 하루 평균 40~45만 명이 접속하는 인기서비스다.
85) 오명호 외, 앞의 책, p.74.

침에 의거 사이버분야에 대한 정보를 공유하는 등 '미·일간 사이버 대화', '사이버 방위정책 워킹그룹회의와 공동훈련' 등을 추진하고 있다. 2013년 5월 도쿄에서 '미· 일 제1회 사이버대화'를 개시했고 2014년 4월 제2차 회담은 중국 및 북한의 사이버공격에 대한 협의를 위해서 워싱턴에서 열렸다. 양국은 회담 직후 민·관의 사이버대책 협의를 위한 '사이버보안정책회의'도 개최되었다. 주요내용은 국제적인 사이버정책에 대한 연대와 사이버전력의 비교, 주요기반시설에 대한 위협에 공동으로 대응하기 위한 협력 등이다.[86] 일본은 미국 외에도 유럽연합(EU), 이스라엘 등과 사이버안보 분야에서의 협력 추진에 합의하는 등 해외 공조활동을 활발하게 하고 있다.

일본 자위대는 2014년 3월 26일 사이버공간 공격에 효과적인 대응을 위한 특별방위조직을 확대하여 '사이버방위대'를 창설하였다. 이는 기존의 지휘통신시스템부의 지휘하에 있던 사이버 전문인력 90명으로 구성된 특수부대로, 육상·해상·항공자위대 소속인력을 포함해 일본 정부 내각관방의 사이버보안센터 인력도 파견하여 편성한 것이다. 앞으로 사이버방위대는 육상·해상·항공자위대가 각각 보유하고 있던 사이버방어 체계를 단일화하고 향후 민간 부문까지 포함한 조직으로 개편할 예정이다. 사이버 방위대는 방위성과 자위대의 네트워크를 감시하고 문제 발생 시 즉각적으로 대응할 계획이다. 또한 사이버공격 및 사이버방어와 관련된 정보활동을 총괄하고 관련 기관과 공유하고 있다. 또한 중국의 애국적인 홍커와 유사한 전문 해커를 고용할 수 있다는 것도 강조하고 있다. 일본은 방위산업체나 주요 기반시설 등의 민간 영역은 사이버방위대의 영역 밖이나 사이버전의 특성상 민간과 방위산업체간 협력이 중요한 만큼 사이버방위대의 역할이 앞으로 계속 확장될 것으로 예상되고 있다.

2014년 11월, 일본은 사이버전 발생 시 정부·기업·개인 등 주체별 책무를 규정한 '사이버보안기본법'을 제정했다. 그리고 2015년 1월 내각 산하에 '사이버 보안전략본부' 및 지원조직인 '내각 사이버보안센터'를 설치하였다. 이를 통하여 사이버 안보 전략안을 작성하고 NSC와 협력하여 정부차원의 사이버 보안을 조정 및 통제하는 능력의 강화와 정보시스템에 대한 부정활동을 감시하고 분석하여 대응하는 능력을 갖추게 되었다. 일본은 또한 미국 및 대외기관과 협력을 통해 사이버 위협에 공동대응하고 있다. 인재를 중점적으로 육성하고 한국과

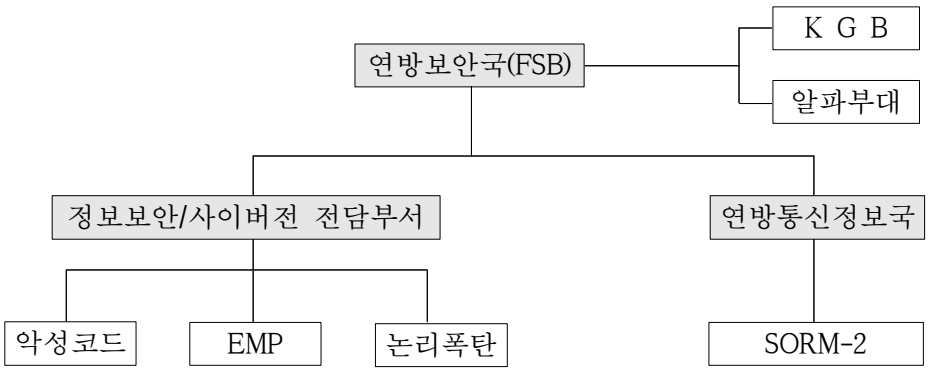
86) 손영동·고성훈, 앞의 논문, pp.35-36.

중국, 영국, 인도, 이스라엘 등과 협력체계 구축에 합의했으며 국내·외 대학 및 연구소에 유학과 연수를 추진하고 있다.

4. 러시아

러시아는 연방보안국에 사이버 전쟁 전담부서를 두고 있으며 사이버 공격을 지상전의 보조전략으로 활용하고 있다. 러시아의 사이버전 수행조직은 <그림 5>에서 보는 바와 같이 국가보안위원회(KGB)와 대테러특수부대인 알파부대를 흡수한 러시아 연방보안국(FSB)'[87]이 관련 기관을 조정·통제하고 있다.[88]

<그림 5> 러시아의 사이버전 수행 조직



연방보안국 예하에 정보보안 및 사이버전 전담부서는 악성코드, EMP탄, 논리폭탄 등 사이버전 무기의 개발 및 배치, 사이버전 교리개발, 훈련 등을 수행하고 있다. 이외에도 사이버 관련 기관으로 내무부의 'K' 국 등이 존재하고 있으나, 연방보안국 예하의 연방통신정보국 SORM-2[89]에서 네트워크 필터링으로 정보를 통제하고 있는 것으로 알려지고 있다. 또한 다수의 정부기관 및 민간기관에서 해킹 등 정보활동을 수행하고 있다. 이러한 조직과 능력을 고려해 볼 때 정보전과

87) 러시아 연방보안국(FSB : Federal Security Bureau) : 구(舊) 소련 체제에서 악명을 떨친 비밀경찰 KGB가 해체된 뒤인 1995년 대통령 직속기관으로 창설됐다.
88) 손영동·고성훈, 앞의 논문, p.36.
89) SORM(System for Operative Investigative Activities) : 러시아어로 '수사활동을 위한 시스템'의 약어로 프로그램을 이용해 자국 인터넷서비스망에 접속해 광범위한 정보를 수집해온 것으로 전해지고 있다.

사이버전 능력을 과소평가 할 수 없는 국가이다. 러시아는 2002년부터 세계에서 처음으로 해커부대를 창설하고 사이버 전문 인력의 양성과 기술개발을 적극 추진하여 사이버 공격에 활용하고 있다. 현재는 7,300여 명으로 추정되는 인원을 운용하고 있는 것으로 알려졌다. 2013년에 러시아 국방장관은 관련 부서에 '사이버사령부' 창설 검토를 지시하였으나 아직 완전하게 결정되지는 않은 것으로 보인다.[90] 2013년 사이버 관련 예산은 약 1억3천만 달러로 세계2위 수준의 사이버전 수행능력을 보유하고 있는 것으로 판단되고 있다.[91] 러시아는 상대국의 C41 및 감시·정찰체계의 무력화 방안과 정보자산 국산화를 위한 사이버무기에 대한 연구를 하고 있을 뿐만 아니라, 이미 상당한 수준의 사이버전 공격기술을 확보한 것으로 추정되고 있다.

사이버전 사례로 2007년 러시아는 에스토니아와의 전쟁에서 승리한 후 전쟁의 패러다임 변화를 선언하면서 전쟁은 국가통제 및 정보시스템, 통신시스템, 정보체계에 대한 공격에 더 많은 노력을 투입할 것을 강조하였다.

2008년 8월 발생한 러시아와 그루지야 간 전쟁에서는 사이버 공격 기술이 공세적으로 사용됐다. 러시아는 지상군을 투입함과 동시에 사이버공격을 개시하였다. 은행과 언론 사이트가 마비되자 그루지야 정부는 시민들로부터 공신력을 잃었고 내부는 혼란에 휩싸였다. 군 정보시스템과 기반 네트워크가 제대로 작동하지 않아 군사작전의 지연을 초래했다. 8월 13일 평화중재안이 수용되면서 러시아와 그루지야 간의 전쟁은 멈추었으나 사이버 기술을 활용한 러시아는 보다 쉽게 승리를 거둘 수 있었다.

이 전쟁의 성격은 사이버전이 물리적 전쟁 수행에 상당한 영향을 끼친 것으로 볼 수 있다. 러시아는 그루지야에 대한 사이버 공격을 진행하기에 앞서 예행연습을 했던 것으로 보인다. 그 근거는 전쟁 발발 약 20일 전인 7월 20일경 미 국토안보부와 보안전문가들이 그루지야의 정부기관, 기반 네트워크, 언론과 은행에 대한 DDos 공격 징후를 포착했기 때문이다. 그루지야 정부는 공격에 사용된 장

90) 국방정보본부, "러시아 국방부 사이버사령부 창설 추진 동향,"(2013).
91) 미국 국방과학위원회(Defence Science Board)가 발간한 기술력 평가항목 15개 가운데 러시아는 7개 분야에서 "막강한 능력", 4개 분야에서 "훌륭한 능력"으로 평가되었고, Jane's Intelligence Review에도 러시아는 "전자공격 및 전자보호분야(the areas of electronic attack and electronic protection),"에서 강점이 있는 것으로 판단하고 있다.

비와 명령어가 러시아 정부가 사용한 것임을 확인했다. 중요한 사항은 사이버전을 공격의 주요수단으로 물리적 공격과 통합하여 전쟁수행 과정에 영향을 주었다는 것이다. 그루지야전쟁에서 보여준 선제적인 심리전과 물리전의 결합한 다양한 사이버 공격은 러시아의 사이버전 능력을 나타내는데 충분하였다.

2008년 러시아 연방정부의 한 고위관료는 "앞으로의 전쟁은 정치·경제·종교 등 여러 가지 문제들이 복합적으로 얽혀서 발생할 것이고 전쟁수행 방식도 적을 섬멸하는 전략보다는 국가통제시스템, 국방정보시스템, 항법과 통신시스템과 군 전력을 통제하는 정보체계에 대한 기능마비에 더 많은 노력을 기울일 것이다" 라며 전쟁의 패러다임의 변화를 예고했다.[92]

이상과 같이 주요 국가의 사이버 역량에 대하여 살펴보았다. 주요 국가들은 지금도 자국의 사이버전 역량을 강화하기 위해 국가적으로 집중하여 사이버전 준비에 최선을 다하고 있으며 이는 국가안보 능력과 직결된다. 마지막으로 각 국의 사이버전 능력을 미국과 한국의 평가기관이 평가한 사이버 역량 평가결과를 알아보도록 하겠다.

먼저 미국의 사이버안보 전문기관인 테크놀리틱스사(Technolytics)는 2009년 사이버무기 및 첩보활동을 하는 160여 국가의 군 사이버역량을 세 가지 분야, 즉 목적 달성을 위한 목표와 심리상태 평가를 한 역량목적(cyber capabilities intent)과, 전시 특수목적을 달성하기 위한 능력인 공격역량(offensive cyber capabilities)과, 사이버 영역에서의 정보수집 적응력을 평가한 정보수집(cyber intelligence rating)능력으로 나눠 평가하고 측정점수 합의 평균으로 역량등급을 산정하였다. 이에 대한 결과는 <표 3>에서 보는 바와 같다.[93] 각 국가의 평가결과 중국과 미국이 공동 1위이고 러시아와 인도가 공동 3위, 이란·북한·일본·이스라엘이 공동 5위이고 한국은 9위를 나타내고 있다.

92) 손영동(a), 앞의 책, pp225-229.
93) The Technolytics Institute, "Cyber Commander's eHandbook version 2.0,"(2011).

〈표 3〉 테크놀리틱스의 군 사이버전 역량 평가

국가	역량목적	공격역량	정보수집	역량등급
중국	4.2	3.8	4.0	4.0
미국	4.2	3.8	4.0	4.0
러시아	4.3	3.5	3.5	3.7
인도	4.0	3.5	3.5	3.7
이란	4.1	3.4	3.4	3.6
북한	4.2	3.4	3.3	3.6
일본	3.9	3.3	3.5	3.6
이스라엘	4.0	3.8	3.0	3.6
한국	3.5	3.0	3.2	3.2
파키스탄	3.9	2.7	2.6	3.1
사우디	3.9	2.9	2.6	3.1
상가포르	3.7	2.8	2.7	3.1
스페인	3.8	2.9	2.5	3.1
영국	3.2	3.0	3.0	3.1
호주	3.0	3.0	3.0	3.0

출처: Kevin Coleman, "The Weaponry and Strategies of Digital Conflict," Proceedings of the 5th International Conference on Information Warfare and Security, The Air Force Institute of Technology, Wright-Patterson Afb, Ohio, USA, 8-9(April 2010), p.498.

둘째, 한국의 국가보안기술연구소(NSRI)는 주요 5개국에 대하여 사이버 역량평가를 실시하였다. 주요 평가요소는 기반체계와 공격 및 방어역량에 대한 평가항목이다. 기반체계시설 평가는 인프라와 예산, 조직을 포함하여 평가하였고, 공격역량 항목은 정보 수집과, 침투, 파괴 및 무력화 능력을 평가하였다. 방어역량은 예방, 탐지, 대응 능력을 고려하였고 이를 종합하여 가장 높게 나타난 국가가 역량평가에서 우수한 능력이 있는 것으로 평가하였다.

국가보안기술연구소의 사이버 역량 평가 결과는 〈표 4〉에서 보는 바와 같다. 평가결과는 미국이 1위이고 중국이 2위, 러시아가 3위, 한국이 4위이고 일본이 5위로 나타났다.[94]

94) 손영동・고성훈, 앞의 논문, pp.36-42.

〈표 4〉 국가보안기술연구소(NSRI)의 사이버역량 평가결과

대분류	중분류	미국	중국	일본	러시아	한국
기반	인프라	6.9	4.3	6.4	3.8	6.5
	자원(예산)	10.0	9.0	4.0	2.0	4.0
	조직	7.5	6.5	1.5	1.5	2.5
	기타	10.0	8.0	5.0	6.0	9.0
	소계	8.6	6.9	4.2	3.3	5.5
공격	정보수집	8.9	8.9	5.3	7.9	6.3
	침투	8.8	9.0	5.1	8.7	5.9
	파괴/무력화	8.9	8.6	6.0	8.6	5.9
	소계	8.9	8.9	5.5	8.4	6.0
방어	예방	9.8	5.9	8.6	5.8	9.2
	탐지	8.8	5.4	3.3	6.9	7.4
	대응	10.0	4.7	6.0	4.0	7.3
	소계	9.5	5.3	6.0	5.6	8.0
총점(10점 만점)		9.0	7.0	5.2	5.8	6.5

제2절 북한의 사이버전에 대한 전략과 역량

1. 사이버전에 대한 전략

가. 인식

무력에 의한 적화통일을 시도했던 북한은 70년대 초 6. 25와 같은 방식으로 적화통일을 할 수 없다는 것을 인식하고 통일전선의 방식으로 대남적화통일 노선을 재정비하였다.[95] 새롭게 정립된 대남적화 노선은 대남 적화통일이 군사적 무력충돌의 직접적인 방식이 아니라 간접적인 방식에 의해서 추진될 것을 밝히고 있다. 이는 오직 군사적인 힘으로 남한을 공격하여 파괴하려는 클라우제비츠식 사고방식으로부터 강점은 피하고 약점을 찾아 공격하는 방식으로 힘의 중심을 간접적으로 공격하는 손자식 사고방식으로 전환하였다는 것을 의미한다.

김일성은 대남적화통일이 장기전이며 휴전선뿐만 아니라 남한 내 중심세력에 제

95) 김동성, “북한의 통일전선 전략전술과 대남 정치심리전”『전략연구』, 통권 제57호(한국전략문제연구소, 2013.3), pp.314-317.

2전선을 구축하고 이를 거점으로 한 지하 역량을 장기간에 걸쳐 완성시켜 남조선혁명역량으로 진화하도록 하였다.[96]

그러나 이러한 전략도 1990년대에 들어서서 소련의 멸망으로 냉전체제가 붕괴되면서 기존의 전략이 약화되자 북한은 걸프전쟁을 통하여 새롭게 등장한 정보전 이론에 눈을 뜨게 되었다.[97] 이때부터 북한의 대남적화전략은 정보전 이론에 따라 물리, 정보, 인식공간으로 전장을 확장하여 전쟁을 준비하고 있는 것으로 판단된다. 물리공간에 대해서 북한은 핵무기와 미사일 등 대량살상무기를 전력화함에 따라 평시에는 대남억제를 달성하되 전시에는 대량살상무기와 대규모 재래식전력과 사이버 공격으로 휴전선의 장벽을 제거하여 적화통일을 하려는 의도로 판단된다. 정보공간에서는 네트워크를 분리하여 취약점을 최소화하면서 네트워크화 된 남한 사회의 취약점을 최대한 역이용하면서 정보의 수집은 물론 국가의 기능마비를 위한 사이버 공격을 계속하는 것이다.

인식공간은 최근까지 구축한 남한 내 혁명역량을 국내정치의 2중대로 세력화하고 인식공간의 장벽을 제거하기 위해 국가보안법을 철폐하고 주한미군을 철수시키는 것을 목표로 하고 있는 것이다.[98]

북한은 2003년 2차 이라크 전을 계기로 사이버전의 위력을 실감한 뒤 사이버 전력을 대폭적으로 증강하고 있으며 매년 사이버 공격을 통하여 남한 내에 사회적인 혼란을 유발시키고 여건이 조성되면 물리전과 연계하여 적화통일을 하려는 망상을 버리지 않고 있다. 더욱이 강경 군부의 대표적인 정찰총국이 군사도발과 전자전 도발 등 다양한 대남 공작을 수행하고 있다는 사실은 북한의 대남 전략이 전통적 방식뿐 아니라 새로운 방식을 통해서도 수행되고 있음을 말해준다. 북한은 한국 정부와 사회에 커다란 혼란을 야기함으로써 후방 침투와 교란을 용이하게 할 수 있는 환경을 조성하고 사회적인 패닉을 유발하여 정부의 대북정책 자체를 뒤흔들어 놓을 목적으로 도발을 감행할 것으로 판단된다.

직접적인 군사도발은 보복당할 위험성이 크기 때문에 한국의 사회적 혼란을 야기할 수 있는 새로운 방법을 강구할 것이다. 그럼에도 불구하고 북한에 대한 정치적 대응이나 도발을 중지하도록 촉구하는 방법 외에 북한의 사이버 공격을 중

96) 오수열 외, 『최신 북한사회의 이해』 (광주: 신성, 2005), pp.60-61.
97) 윤규식, "북한의 사이버전 능력과 위협전망," 『군사논단』, 제68호(한국군사학회, 2011), p.73.
98) 한희, 앞의 논문, pp.8-13.

단시킬 대책이 쉽지 않다는 점은 더욱 큰 문제다. 이 점은 사실상 북한의 또 다른 비대칭 전력의 우월성으로 간주될 수 있다.[99]

북한의 사이버 공격이 위협적인 이유는 물리적인 군사충돌의 위험은 배제하면서 북한이 원하는 시간과 장소에 그들이 원하는 방법으로 우리를 공격할 수 있기 때문이다. 북한은 2000년 이후 매년 반복적으로 사이버 공격을 수행하여 남한의 정보체계를 대상으로 공격하여 왔으며 한국은 최근까지 북한의 공격에 단편적으로 대응하여 왔다. 이는 주로 피해를 회복하는데 집중하고 공세적인 활동으로, 적의 공격으로 노출된 IP체계를 파악하여 대비하는 위주로 대응해 왔다. 북한은 3천여 명이나 되는 해커를 양성하여 한국을 공격하고 있으며 우리의 반응과 효과를 언론을 통해서 보고받는 방식으로 메카니즘을 고착화하는 양상처럼 행동하고 있다. 이는 한국사회에 손실을 유발하기 보다는 그 이상의 어떤 전략적인 의도가 있지 않나 판단된다. 북한 해커의 존재와 역할에 대하여 우리는 어떻게 판단하는 것이 올바른 인식인지 생각할 필요가 있다. 혹시나 우리는 북한이 지금까지 한국의 정부 각 기관, 공공시설과 핵심기반시설에 무언가 심어 놓은 것에 대하여 알지도 못하고 알 수 있는 능력도 없다는 것이 가장 두려운 상황이 될 수 있다. [100]

나. 전략

북한이 남한에 대해 사이버 공격을 감행하는 최종적인 목적은 북한정권의 목표인 민족해방 인민민주주의혁명 과업을 완수하고 온 사회를 주체사상화 하기 위함이다. 즉 북한의 사이버 공격의 최종 목적은 전 한반도의 공산화이다. 이를 위하여 북한은 전자정보전이라는 개념 하에 남한의 네트워크와 인프라 파괴, 지휘통제체계 마비 등을 통하여 정보전 수행능력을 향상시키고 있다. 1980년 중반부터 북한은 경제난 때문에 재래식 전력을 계획대로 보강하지 못하자 남한에 대한 군사력과 경제적인 열세를 만회하기 위해 비대칭무기인 핵무기와 중장거리 탄도미사일의 개발과 함께 사이버전력을 키워왔다. 북한의 비대칭무기인 핵무기와 탄도미사일의 개발이 우선적으로 한국군의 군사력을 능가하고 미국의 핵과

99) 문순보, “북한의 사이버테러와 대화제의의 진정성”『세종논평』, 제217호(세종연구소, 2011.5.4)
100) 한희, 앞의 논문, pp.15-18.

군사력에 대한 억제와 동시에 한국을 공격하려는 성격이 강한 것이라면, 사이버 전력은 직접적으로 대남 및 대미 도발을 위한 것이라고 평가할 수 있다. 북한은 사이버공간을 전략적 중요성이 높은 전장으로 인식하고 사이버전 능력을 전략적인 비대칭 전력으로 적극 활용하고 있다. 김정일은 사이버전에서 한국을 대상으로 반드시 승리해야 한다는 개념하에 우리의 IT능력을 단기간에 뛰어넘을 수 있는 '단번 도약전략'을 구사하여 북한의 사이버전 수행능력의 향상을 서둘러 왔다. 이는 김정일과 김정은이 언급한 것을 통해서 어렵지 않게 이해할 수 있다. 김정일은 '인터넷은 국가보안법이 무력화되는 특별한 공간'으로 "남한 내 인터넷을 적극 활용하라"며 사이버전의 중요성을 피력하였다. '사이버부대는 나의 별동대이자 작전의 예비전력'이라며 사이버 전력 강화의 필요성을 역설하였다.[101] 김정은도 '사이버전은 핵, 미사일과 함께 인민군대의 무자비한 타격능력을 담보하는 만능의 보검'이라며 사이버전의 중요성을 언급하는 한편, "강력한 정보통신기술, 정찰총국과 같은 용맹한 사이버전사들만 있으면 그 어떤 제재도 뚫을 수 있고, 강성국가 건설도 문제없다."며 사이버전력의 필요성을 강조하고 있다. 김정은은 대학에서 컴퓨터공학, 군사학, 물리학을 전공한자로서 사이버전 수행에 최적임자라는 것이다.[102]

실제로 김정은은 2007년 9월부터 이미 해킹 및 전파교란을 전담하는 사이버부대를 자신의 직속으로 통합 관리해 온 것으로 전해지고 있으며, 북한의 소행으로 추정되는 2009년 7.7 DDos공격과 2011년 3.4 DDos공격과 농협 전산망 마비 등의 대남 사이버 공격도 김정은이 지휘 전면에 나선 이후에 발생한 것으로 알려졌다. 북한에서 사이버테러는 핵, 미사일과 함께 인민군대의 3대 수단이고, 사이버무기는 핵과 생화학무기와 함께 3대 비대칭 전력이다. 나아가 사이버전은 최후 결전의 승패를 좌우할 결정적인 요인으로 인식하고 있다.[103]

북한이 사이버전력을 전략적 무기로 활용하는 이유는 사이버공격이 적은 인원, 적은 비용으로 최대의 효과를 누리는 비용대비 효율성을 가지고 있고 활용이 편리하며 확산이 신속하게 이루어져 파급효과가 크기 때문인 것으로 알려지고 있다. 더욱이 직접 물리적으로 침투할 필요가 없고 익명성 보장으로 은밀하게 활동할 수 있어 제재와 보복이 어렵기 때문이다. 북한의 사이버 전략의 목표는 무력

101) 윤규식, 앞의 논문, p.74.
102) 김승주, 앞의 논문, p.20.
103) "북의 최후 결전은 사이버전이다" 『자주민보』, 2013년 5월 20일.

적화 통일은 물론 대한민국을 대상으로 사회혼란 조성, 유사시 군사작전 방해, 국가기능마비, 체제선전, 경제수입 확보를 위한 외화벌이 등을 들 수 있다.[104]

최근에 북한은 직접 공격하는 방식에서 벗어나 중국 등 외국에서 게임 프로그램 제작을 투자받아 악성프로그램을 설치하고 업데이트 기능을 이용하여 좀비 PC를 만들어 DDOS공격에 이용하는 등 실체를 추적할 수 없도록 은밀한 방법으로 진화하고 있는 실정이다. 또한 여기에서 얻은 불법수익은 김정은 통치자금으로 활용되고 있다는 것이다.[105] 이와 같이 북한은 사이버 전략을 군사전략에 적용할 뿐만 아니라 국가안보 전략에도 적용하여 북한의 국가적 목표 달성을 위한 핵심전략으로 활용하고 있다.

그러나 우리가 더욱 유의해야 할 점은 북한의 사이버 전략이 군사전략에 적용되어 사이버 공격과 동시에 물리적 전쟁을 일으키는 시나리오다. 구체적으로 이를 언급하면 평시 한미연합군에 대한 정보적 우위를 선점한 이후에 한국의 국가기간망과 국가주요시설에 대한 사이버 공격을 실시하여 혼란을 조성하는 것이다. 특히 미국의 전문가들은 북한의 사이버공격 목표를 한미 군사동맹을 표적으로 파악하고 있다. 2012년 미 국방부 사이버전 전문가 클라크는 2009년 7월 북한에 의한 디도스 공격의 목적이 한미 간 인터넷 연결을 차단하는 데 얼마의 좀비 PC가 동원되어야 하는지를 알아보는 데 있었다고 결론내린 바 있다.

2. 대남 사이버전 역량

북한이 국가적인 차원에서 사이버전에 집중하는 이유는 비용 대비 막대한 피해를 한국에 줄 수 있기 때문에 비대칭 전력을 강화하고 있는 것이다. 사이버전 속성상 최빈국도 적은 비용으로 강대국을 공격할 수 있을 뿐 아니라 한국과 같은 정보통신기술 강국을 공격하기에 더할 수 없는 환경이기 때문이다. 무기체계를 개발하기 위해서는 수많은 비용과 시행착오를 거쳐야 하는데 비해 사이버 무기는 컴퓨터와 네트워크만 있으면 충분하다. 정보통신기술이 발달한 나라일수록 사이버 공격으로 물리적, 심리적 혼란을 야기시킬 수 있다. 북한은 한국의 사이버 인프라가 세계적인 수준이기 때문에 이러한 점을 최대로 이용하여 사이버전 수행능력을 강화시켜 남한을 공격하는 수단으로 활용할 것이다. 한국은 인터넷

104) 임종인 외, 앞의 논문, p.15.
105) 위의 논문, pp.17-18..

사용인구가 3,900여만 명으로 전체인구의 81%에 달하고 초고속 인터넷 가입자율이 세계 3위에 해당하는 상황을 감안하면 북한은 인터넷(Internet) 즉 사이버공간을 그들이 추구하는 사회주의 혁명을 달성하기 위한 수단의 일환으로 활용하고 있는 것이다. 실제로 북한은 사이버공간을 남조선혁명의 해방구로 활용되고 있다는 것이다.[106]

미 국방부는 자체 모의실험 결과 북한의 사이버 공격능력이 태평양사령부 지휘통제소를 마비시키고 미국 본토의 전력망에 피해를 줄 수 있을 정도의 수준을 갖춘 것으로 분석하는 등 미국은 다양한 통로를 통해 북한의 사이버 공격 능력에 대해 높은 우려감을 표명하고 있다.[107] 백악관 안보 특보를 지낸 사이버전 전문가 리처드 클라크는 북한의 사이버전 수행 능력을 '세계 최고 수준'으로 평가했다. 미국 전문가들은 2013년 3.20 사이버 테러를 기점으로 북한의 사이버 공격 능력에 대한 평가를 상향조정하는 등 최근 들어 북한의 사이버공격 능력이 급상승되었고 현재 북한의 사이버전력이 상당한 수준이라는 데 동의하고 있다.[108] NK지식인연대의 김흥광은 북한의 사이버전력이 미국과 러시아에 이어 세계 3위의 수준이라는 등 매우 높게 평가하고 있다. 해킹 수준이 미국CIA의 능력과 같으며 북한의 사이버 병력은 3만여 명이고 매년 북한 미림대학에서 1천여 명의 정예 사이버요원이 양성된다고 한다. 국방과학연구소의 변재성 박사도 북한 해커들의 수준을 CIA와 맞먹는 것으로 추정하고 있다.[109]

반면 북한의 공격수준이 그리 높지 않다는 분석도 있다. 제프리카는 지금까지

106) 유동열, 앞의 논문, p.4.

107) 미 국방성 마이클 낙트차고나는 북한이 정권 유지를 위한 국가안보 전략의 하나로 사이버공격 능력을 증강 중이라고 우려하고 있다. 주한미국 제임스 서먼 사령관은 북한이 미국, 이스라엘 수준의 사이버전력을 갖추고 있다고 평가할 수도 있다. 미 하원정보위원회 마이크 로저스 위원장은 북한을 미국에 대한 사이버공격을 감행할 가능성이 있는 주요 위협 국가 중 하나로 꼽았고, 미 하원 외교위원회는 북한은 아태지역의 사이버강국으로 북한으로 인해 아시아 지역에서 사이버 분쟁이 발생할 가능성이 커지고 있다고 경고하고 있다.

108) 제임스 A. 루이스. CSIS 연구원, "In cyberams race, North korea emerging as pa power, not a pushover," 『The Christian Science Monitor』, 2013년 10월 19일. 3년 전에는 북한의 사이버공격 능력을 의심했지만 이제는 북한이 한국의 전산망을 뚫고 들어가 심각한 마비를 일으킬만한 능력을 갖췄다고 믿는다. 미국의 군사 시설에 위협이 될 만큼 사이버전 능력을 키웠다"고 밝히고 있으며, 존스 홉킨스대 만수로프 연구원도 "북한의 사이버전 능력은 최근 급성장해 실제로 미국의 정부기관이나 군사기관을 목표로 사이버 분쟁을 일으킬 가능성도 있을 정도로 생각했던 것보다 훨씬 강하다"고 말하고 있다.

109) "북, 작년 언론사 해킹, 해커수준은 CIA 맞먹어," 『머니투제이』, 2013년 1월 16일.

의 한국에 대한 북한의 공격이 심각한 위협이었다는 증거는 없으며 대부분 불편한 정도의 디도스 공격이나 홈페이지 변조 공격 수준으로 북한의 전력을 과장한 측면이 있다고 분석하고 있다.[110] 동아일보의 주성하도 북한의 사이버전력이 과장됐다며 북한의 해킹 능력은 우리의 생각보다 훨씬 취약하다고 평가하고 있다.[111]

한편 북한의 사이버 공격능력에 비해 사이버방어 능력에 대한 분석은 많지 않은 상황이다. 방화벽이나 백신 등 보안소프트웨어 개발이 이루어지고 있다는 사실은 알려져 있지만 실질적인 방어능력에 대해서는 알려진 바 없다. 북한이 진정으로 보호하고 방어하고자 하는 것은 외부 웹 사이트가 아닌 광명성과 같은 인트라넷이고, 지금까지는 폐쇄와 분리전략을 통해 잘 방어되고 있는 것으로 평가된다.[112] 이와 같이 북한은 그들의 사이버 역량을 활용하여 북한의 전략을 안정적으로 수행하는데 있다. 따라서 북한의 사이버전 수행능력을 첫째, 인식과 사상의 관점, 둘째, 국가전략 등 시스템의 관점, 셋째, 공조체제인 네트워크의 관점, 넷째, 인력과 기술 등 지원적인 관점에서 접근하여 분석해 보고 이를 평가해 보고자 한다.

가. 인식과 사상의 관점

사이버전에 대한 북한 지도층의 인식이 변한 것은 걸프전 이후이다. 1991년 미군을 주축으로 한 다국적군과 이라크군의 전쟁을 지켜본 김정일은 정보통신기술과 연계한 첨단무기체계가 전쟁의 승패에 결정적으로 영향을 미친다는 사실을 절감하였다. 이후 북한은 미국과 이스라엘 등의 전쟁수행 방식과 첨단 기술전쟁을 지켜보면서 북한군의 미비점을 보완하였다.[113] 걸프전이 종결되자 첫째, 북한군은 현대전에서 전자전의 중요성을 심각하게 인식하고 국방위원회와 최고사령관 명령으로 고위층과 군사지휘관을 대상으로 첨단정보기술에 대한 교육을 진행하였다. 아울러서 총참모부에 지휘자동화국을 편제하였고 군단급 이상제대에 전자전 연구소를 신설하여 한미연합군 특히 미군의 전자전 공격에 대비하도록 하

110) "Q&A of the Week: The Current State of the Cyber Warfare Threat featuring jeffrey Car," 『ZDNet』, 2012년 5월 11일.
111) 임종인 외, 앞에 논문, pp.18-19.
112) 위의 논문, p.20.
113) 김기수, "북한의 사이버전 위협과 대비방안," 『한국정책학회』(2013년 동계학술대회)

였다. 그리고 북한 전 지역의 영재들을 선발하여 사이버전사로 양성하기 위하여 김일성종합대학, 김책공업종합대학, 평양과 함흥의 컴퓨터기술대학, 미림대학 등에 입학시켜 우수한 졸업생들로 사이버전 부대의 멤버로 활용하기 시작했다. 북한군은 첨단군사기술인 C4ISR[114]이 전장에서 사용된 1999년 코소보 전쟁을 지켜보면서 인터넷과 초고속통신망의 군사적 이용이 전쟁수행에 미치는 영향을 심각히 깨닫고 대비책을 강구하였다. 특히 북한은 유고연방에 군사조사단을 파견하여 미국을 비롯한 나토군의 공습작전의 형태와 결과, 공습을 회피하는 방법 등을 연구하고 분석한 것으로 알려졌다.[115] 이어서 9.11 테러 이후 2003년 사막의 폭풍작전인 '제2의 이라크 전쟁'을 모니터링하면서 미국과 영국 등 다국적군의 전쟁수행방법을 연구하기 시작했다.

사이버전의 중요성은 앞에서 언급한 바와 같이 2003년 이라크전쟁이 종료되면서 김정일이 군수뇌부를 모아놓고 한 연설에 잘 나타나 있다. 김정일은 '사이버공격은 원자탄이고 인터넷을 총'이라며 사이버공격의 중요성에 대해 언급하였고, '사이버부대는 나의 별동대이자 작전의 예비전력'이라며 사이버 전력 강화의 필요성을 역설하였다.[116] 북한은 사이버전 능력을 배양하기 위하여 북한식의 주체적인 정보전과 사이버전에 대한 개념과 전략을 수립하였다.[117] 북한의 사이버 전사들은 한국을 공격하기 위하여 수천 명이 공격목표로 선정한 서버의 보안장벽을 뚫기 위하여 밤낮으로 공격한다면, 방화벽을 치고 인터넷보안관을 서버마다 배치한다고 하여도 결국은 뚫릴 수밖에 없는 결과를 가져올 것이다. 방화벽을 뚫는 것은 시간문제이기 때문에 북한이 사이버전쟁에 올 인할 수밖에 없는 이유이기도 하다. 이와 같이 북한이 사이버 전력증강에 매달리는 이유는 미군이나 한국군에 비해 상대적으로 열세한 재래식 전력의 미비점을 극복하고 비대칭전력의 상대적 우위를 달성하고자 하는 의도이다.

둘째, 사이버 전력증강에 대한 국가차원의 투자와 지도층의 관심이 높다는 것

114) C4ISR [Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance] 군 작전을 효율적으로 수행하기 위하여 C4I에 감시와 정찰을 유기적으로 결합한 용어. C4ISR는 전자 통신기술의 진보와 더불어 감시와 정찰기술이 보다 정밀하고 다양해져 적의 상황을 먼저 보고 먼저 공격할 수 있는 감시와 정찰 기능을 C4I에 결합함.

115) 유영철・문광건, "코소보사태의 전쟁양상 분석 및 한반도안보에 미치는 영향," (서울: 한국국방연구원, 1999), p.134.

116) 김기수, "북한의 사이버전 수행실태와 대비방안," , p.130.

117) 김홍광, "북한의 사이버전 대응과 전략," 『북한민주화네트워크발제문』(2011년. 6월).

이다. 북한은 김정일 국방위원장 당시부터 사이버전략에 높은 관심과 지원이 있어왔고, 현재는 김정은 국방위원장이 사이버전과 전자전 영역을 직접 지휘하고 있다.[118] 2011년 NK지식인연대 김흥광의 말에 의하면 북한은 최고 권력기관인 노동당과 국방위원회에서 사이버전을 직접 통제하는 등 국가전략차원에서 사이버전 조직을 관리해 왔으며 고성능 컴퓨터, 인터넷 훈련망, 첨단장비시설 등에 많은 투자를 하는 등 사이버전 준비에 예산을 집중적으로 투자하고 있다고 한다.[119] 또한 북한은 2000년대 초반부터 북한 내 인트라넷에서 충분한 훈련과 경험을 축적하면서 끊임없이 새로운 해킹 기법과 도구를 개발하고 있다고 하며 아울러 국방과학원 산하의 정보전연구소, 미림대학의 정보전 연구센터, 제2경제위원회 연구개발부서들이 협동하여 정보전 수행에 필요한 각종 무기체계에 대한 연구개발을 담당하고 있으며, 방화벽 등 보안소프트웨어와 암호 관련 연구개발은 주로 김일성대학에서 이루어지고 있다고 한다.[120]

셋째, 사이버 전력의 심각한 비대칭성이다. 북한이 사이버 전력증강에 집중하는 의도는 한국사회가 사람과 사람, 사람과 사물, 사물과 사물 등 모든 것이 연결되는 초 연결사회로 진입했다는 사실이다. 즉 모든 것이 인터넷으로 연결되는 사물인터넷(IoT: Internet of Things)시대가 열림에 따라 사이버위협에 대단히 취약한 구조를 역이용한다는 개념이다. 북한은 사이버 공간의 익명성과 기밀성, 은밀성 등의 특징을 활용하여 자신들의 정체를 감추고 대남침투와 도발을 자행하는 북한으로써는 사이버 공간이 최적의 공격 장소가 되기 때문이다. 모든 것이 북한의 전략적으로 양성한 사이버 전사들에 의해 전투적으로 진행되는 만큼 그 파괴력은 우리의 상상을 초월할 것이다. 사이버전은 남북한 간에 전형적인 비대칭적 위협이다. 한국은 정보통신기술 강대국으로 국가의 주요 기반시설과 기간전산망들이 북한의 해커들에게 노출돼 있는 상황이다. 북한은 지금도 1천여 명에 이르는 국방위 정찰총국의 사이버 전사(戰士)들이 남한 내 공격대상을 물색하고 있다. 미국의 한 방송은 북한이 사이버전쟁을 펼칠 특수병력을 3만 명이나 육성하고 있다고 하였다.[121]

또한 북한은 무력도발의 한계를 느끼고 있는 상황에서 정보통신기술강국인 한

118) "긴급분석 북한의 사이버전 전투력," 『일요신문』, 2011년 5월 9일.
119) 임종인 외, 앞의 논문, p.22.
120) 위의 논문, pp.26-27.
121) 『조선일보』, 2011년 5월 20일.

국 사회를 마비시키고 혼란스럽게 하여 자신들의 목적을 달성할 수 있기 때문이다. 천안함 침몰과 연평도 포격사건, 최근 DMZ지뢰 폭발 사건의 전술적 대응 부재로 국민의 질타를 받고 있는 군은 북한이 또 다시 공격을 한다면 '뼈저리게 후회하도록 강력한 응징'을 할 것으로 판단된다. 이로 인하여 북한의 입장에서 물리적인 추가 도발은 일부 확전을 각오해야 하는 엄청난 부담이다. 실패 시에는 김정은 정권의 붕괴로 이어질 수도 있다. 북한이 물리적 도발을 망설일 수밖에 없는 이유다. 그러나 북한은 사이버 수단으로 공격을 감행할 시 우리는 공격대상과 공격의 진원지를 파악하는 데 상당한 시일이 걸릴 뿐 아니라 북한이 북한 영토가 아닌 중국 등 해외에서 사이버 공격을 시도하기 때문에 진원지를 확인하기가 어렵다.[122] 북한이 아니라고 부인하면 특별한 대책이 없는 것이다. 이러한 익명성과 은밀성, 군사충돌에 대한 부담이 없기 때문에 북한은 사이버 테러를 통해 대남 공격을 강화하는 것이다. 그리고 북한은 사이버 공격을 전통과 비 전통, 대칭과 비대칭 공격이 혼재하는 복합전쟁을 수행하기 위한 효과적인 수단으로 사용하고 있다. 이를 통하여 한국의 국가기간전산망과 기간시설을 공격함으로 사회혼란을 조성하면 군의 작전수행 능력에 치명적인 타격을 줄 수 있기 때문에 사이버 공격에는 민군의 구별이 없다. 한국의 입장에서 북한은 사이버 공격의 대상이 될 만한 정보통신망이 없기 때문에 보복도 어렵다. 이처럼 북한은 지켜야 할 것이 별로 없고 한국은 지켜야 할 것이 너무 많다는 비대칭성에 있어 북한은 방어보다는 공격에 집중할 수밖에 없는 상황이다. 북한은 사이버공간에서 우위를 차지하고 사이버공격의 효과를 강화하기 위한 기본전략으로 자신의 가장 큰 장점인 비대칭성을 유지하고 강화하는 전략을 활용하고 있는 것이다.

넷째, 북한은 사이버전과 물리전을 연계시켜 한국을 공격하려는 의도가 있다. 북한은 사이버 전력을 군사전력의 일부로 편입하여 작전을 수행하고 있으며 공격목표는 국가 기반시설을 목표로 한다는 점이다. 북한은 2010년 11월에 발생한 연평도 포격도발 시 연평도에 대한 포격을 가하기 전에 우리 군의 대(對)포병레이더를 교란시키기 위해 전파교란을 가해왔다. 이 때문에 연평도에 있는 대(對)포병 레이더 두 대가 모두 작동되지 않았다. 북한은 앞으로 사이버공격과 기존의 재래식전력을 결합한 새로운 공격방법을 지속적으로 발전시켜 나갈 것으로 보인다.

다섯째, 사이버 역량은 선전·선동활동에 유용한 도구가 되기 때문이다. 사이

122) 임종인 외, 앞의 논문, p.29.

버전은 평시에 물리적인 공격의 부담을 피하면서도 한국사회를 혼란스럽게 만들고 국가시스템을 마비시킬 수가 있는 장점이 있으며 은밀성을 보장받을 수 있다. 따라서 북한의 지도부는 비용대 효과, 사이버전의 특수성 등을 인식하여 사이버전 역량 강화에 매진하고 있으며 수준도 매우 높은 것으로 평가되고 있다.

나. 국가전략 등 시스템의 관점

북한은 지도층의 인식의 변화로 정보전과 전자전에 대한 필요성을 절감한 이후 여러 논의과정을 통해 1990년대 말 북한식의 독특한 사이버 정보전의 개념과 전략을 완성하여 북한식 사이버 전법, 심리전 전법 등 다양한 정보전 전법들을 발전시켜 왔다. 북한의 사이버전 전략은 중국의 군사교리인 점혈전략을 모방했으며 중국의 사이버 전법들을 벤치마킹했다고 한다.[123] 북한의 사이버 정책에 대하여 공식적인 문서는 공개된 바 없지만, 북한 지도층의 언급과 조직체계, 국가차원에서 조직적으로 수행하였던 사이버 공격들을 볼 때, 국가차원의 사이버전 독트린과 정책이 존재하나 극비로 유지하고 있는 것으로 추정된다.[124]

북한의 사이버 대남전략과 사이버 공격, 대외적인 발표 내용 등을 통해 나타난 북한의 정책은 이중적인 경향이 있다. 자신들의 사이버 독트린은 숨기고 한국에 조직적인 사이버공격을 자행하면서 타 국가들의 사이버공격을 포함한 사이버정책에 대해서 비난을 가하는 태도를 보이고 있다.[125] 예를 들면 외화벌이용 공격도 단순한 경제적 목적이 아니라 악성코드 전파와 좀비 PC를 통해 사이버 공격의 기반을 다지기 위한 경우가 많고, 외화벌이 과정 중 취득한 각종 자료를 이용하여 한국 국민들을 대상으로 한 개인정보 침해공격이나 스피어피싱도 군사적, 전략적 목적으로 활용하는 등 전략목적과 민간대상의 외화벌이와 사이버심리전이 완전히 구분되지 않는다는 점이다.

북한은 국가기관이나 기반시설에 침투해 전산망을 파괴하는 사이버테러를 자본주의 과학기술 발전의 역기능적 결과라며 비판적인 시각으로 보고 있으며, 북한은 사이버공격 의혹들에 대해서는 적극 부인하는 동시에 북한을 대상으로 한 사이버 공격에 대해서는 강력한 항의의 목소리를 내고 있다.[126]

---

123) "북한 사이버전법은 중국의 점혈전쟁술 모방한 것," 『중앙일보』, 2009년 7월 10일.

124) 손영동, "북한 체제의 특성상 제도나 정책의 중요성이 다른 국가들에 비하여 상대적으로 낮고 최고지도자의 의중이 중요하기 때문에 제도와 정책은 큰 의미가 없다는 의견도 존재한다."(2010).

125) 임종인 외, 앞의 논문, pp27-28.

민주조선 신문은 스노든이 사이버공격작전 원칙이 포함된 미국 대통령 PDD-20을 공개하자 미국의 사이버정책은 사이버전쟁 선언으로 인류의 평화를 위해 시대착오적 행위를 당장 멈춰야 한다고 경고한 바 있다.[127]

미국의 사이버 공격무기 개발 기사와 관련하여 노동신문은 '사이버전쟁 준비에 열을 올리는 침략세력들'이라는 제목의 비판기사를 발표하였으며, 미국의 스턱스넷 개발 및 이용에 대해서도 비판한 바 있다. 북한은 독일과 브라질이 유엔에 발의한 미국의 감시활동에 대한 '디지털 시대의 프라이버시 권리' 결의안에 적극적인 찬성 입장을 밝혔다.[128]

둘째, 북한이 구사하는 사이버 전략전술이다. 북한에서는 방어보다는 공격 목적으로 대규모 해커를 양성하고 있으며 사이버공격과 관련된 교육내용은 철통보안사항이라고 한다. 북한은 사이버전략전술을 기습전술, 위장전술, 기만전술, 정보전술, 심리전술, 은폐전술, 파괴전술로 구분하고 있다.[129] 최근 귀순자 증언에 따르면 북한의 교전규칙이 북한 영토 내에서는 사이버공격작전을 수행하지 않는 것으로 변화되었다고 한다. 이를 추측해 볼 때 북한은 다양한 전략과 전술과 사이버 교전규칙을 작성한 것으로 보인다. 북한의 최근 사이버공격 수행전술을 살펴보면, 먼저 사이버공격 작전이 계획되면 북한의 사이버 부대원들은 중국에 위치한 안전가옥으로 이동하여 프록시서버[130]를 가동하여 공격근원지를 숨기면서 수백 명이 하나의 목표물에 대해 공격을 수행한 후 작전이 완료되면 북한으로 돌아간다고 한다.[131] 북한은 공격탐지, 원점추적 방지를 위한 다양한 은폐,

126) 박기갑, 2013년 3월 북 사이트 접속 장애 당시 북은 "적대세력의 비열한 행위가 키리졸브 합동군사 연습과 때를 같이하고 있으며, 수수방관하지 않을 것"이라고 발히고 있다. 2013년 6월에는 어나니머스의 공격 경고에 대해 "오합지졸에 불과한 어나니머스가 감히 우리 체제를 어째보겠다니 크게 웃을 일"이라고 밝히고 있으며, 북한은 북한 김일성방송대학 인터넷강의 사이트에 대한 IP차단에 대해서 "인터넷 중단 조치를 철회하지 않을 경우 남북관계의 전면 파괴로 간주해 책임을 엄격히 계산할 것"이라는 성명서를 발표하기도 했다.

127) "North Korean Newspaper hits out at U.S Cyber Warfare Polocy,"『North Korea Tech』, 2013. 8. 12.

128) "미국 해킹 비판 UC 결의안에 북한도 찬성, 우리나라는?,"『미디어투데이』, 2013년 11월 23일.

129) "6.25 사이버해킹, 북한이 사용하고 있는 사이버 전술은,"『데일리시큐』, 2013년 5월 14일.

130) 프록시 서버 [proxy server]시스템에 방화벽을 가지고 있는 경우 외부와의 통신을 위해 만들어놓은 서버. 방화벽 안쪽에 있는 서버들의 외부 연결은 프록시 서버를 통해 이루어지게 된다.

131) 『전자신문』, 2013년 5월 14일. 3.20 사이버 공격 당시에는 2013년 2월 25일 심양과 훈춘에 위치한 사무실 임대 계약을 한 후, 북한에서 중국으로 사이버부대원들이 최고 6개의 팀 단위

우회기술을 구사하는 한편, 중국에서 사이버 공격을 수행하기 때문에 원점을 식별했다 하더라도 관할권 문제와 외교적 문제로 원점타격이 어려운 상황이다. 또한 공격자 식별에 수개월이 소요되는 사이버공격의 특성상 대응공격이 쉽지 않고 상대적으로 중국 뒤로 숨어 미국이 물리적으로 타격을 가할 수 없는 억지효과와 남남갈등 조장의 효과까지 제공하고 있는 것이다.[132] 북한의 사이버 부대가 중국에서 사이버공격을 수행하는 경우 중국이 국가적인 차원에서 제공하는 방어체계와 인터넷에 대한 네트워크 필터링과 통제의 보호를 받으면서 안전하게 공격을 수행할 수 있다. 중국은 국제사회에서 자국의 영토 내에서 벌어지는 북한의 사이버작전 수행과 관련한 일체의 진술을 일관되게 거부함으로써 정치적으로도 강력한 방어막이 되고 있다.[133] 많은 전문가들은 중국이 자신의 영토에서 북한이 무슨 일을 하고 있는지 알고 있을 것이며 북한의 사이버 공격은 최소한 중국의 묵인 하에 한국과 미국을 비롯한 적대국들을 향해 편하게 공격을 하고 있을 것으로 추측하고 있다.

이와 같이 중국이 북한의 사이버공격 행위를 지원 내지 묵과하는 이유가 중국과 북한 간의 전통적인 신뢰관계라기 보다는 북한의 이러한 사이버공격 행위가 자신들에게는 해가 안 되고 아시아에서의 균형유지 전략을 구사하는 미국과의 파워 게임에 도움이 되기 때문인 것으로 보인다.[134] 북한의 사이버방어 수준은 북한의 방어 수준에 중국의 사이버 능력을 더한 수준으로 평가할 필요가 있다. 이처럼 북한은 다양한 영역과 수준의 사이버전 관련 무기체계와 공격전술을 갖추고 준비를 체계적으로 하고 있는 것으로 파악된다.

셋째, 북한의 사이버전과 관련한 조직체계다. 북한은 폐쇄적인 정보통신망을 운영하고 컴퓨터 보급률이 저조할 뿐 아니라 인터넷감시, 통제가 강해 북한의 전산망에 침투하는 것도 쉽지 않고 효과도 제한적이다. 북한의 대남사이버 조직과 주요임무는 <표 5>에서 보는 바와 같다.[135]

로 급파되어 사건 발생 보름 전인 3월 6일 입주한 후 준비에 들어갔으며, 명령에 다라 17일부터 20일 오후 2시 전까지 사이버공격을 단행한 후 20일 오후 북한으로 돌아갔다고 한다.

132) 임종인 외, 앞의 논문, p.29.

133) "In cyberarms race, North Korea emerging as a power, not a pushopver," 『The Christian Science Monitor』, 2013. 10. 19.

134) 임종인 외, 위의 논문, p.34.

135) 신충근·이상진, "북한의 대남 사이버테러 전략분석 및 대응방안에 대한 고찰," 『경찰학연구』, 제13권제4호(통권제36호, 2013. 12), p.207.

<표 5> 북한 대남 사이버 조직 및 주요임무

기 능	부 서		주 요 임 무
사이버 공작요원 양성 및 연구	김일성 군사대학		1966년 개설, 5년제 전산과정
			1,000여명 사이버전사 양성
	김일성 정치군사대학		1966년 미림대학, 지휘자동화대학
			전자전연구 및 사이버전사 양성(무기제조 전문가양성)
	정찰총국 모란봉대학		정찰총국 작전국 소속
			사이버전 대비 전문가 양성
사이버 공작실행	총참모부	지휘 자동화국	군 통신교란 등 전자전 수행
			31소, 32소, 56소 운영
		적공국 204소	한국군 대상 사이버심리전 전개
			역정보, 허위정보유출(인터넷 심리전 전담부서)
	정찰총국	작전국414, 128연락소	한국 및 해외정보 수집, 해킹
			전담요원 해외파견, 사이버 테러 수행
		기술국 110연구소	기술정찰조 확대
			한국 주요 정보 수집 및 해킹
			사이버 테러(디도스공격 등 감행)
		해외정보국 자료조사실	한국전략정보 수집, 해킹 전담
			사이버 전담요원 해외 주재
	225국		사이버드보크 개발 및 설치
			한국 전략정보수집, 해킹전담(스테가노그라피 등)
	당	통일전선부	대남 사이버심리전 전담
			120여개 친북사이트 운영(우리민족끼리 등)
			트위터, 유튜브 등 SNS 공작
			여론조작 댓글팀 가동
			남남갈등, 사회교란 시도

북한은 김일성 군사대학과 김일성 정치군사대학, 정찰총국 산하의 모란봉 대학에서 사이버 공작요원을 양성하고 사이버 관련 연구 활동을 하고 있다. 북한의 사이버 공작을 실행하는 조직체계는 다음과 같은 네 개의 전담부서로 구성되어 있다. 인민군 총참모부 산하 사이버 전담부서와 국방위원회 직속 정찰총국 산하의 사이버 전담부서, 노동당 225부 소속의 사이버전담부서, 통일전선부 소속의 사이버전담부서로 구분된다. 인민군과 조선노동당 산하에는 사이버테러, 사이버 심리전, 사이버간첩 교신 등 사이버 작전 부대와 이를 수행하는 조직들로 구성된다.[136]

인민군 총참모부의 사이버 전담부서인 지휘자동화국과 적공국 204소는 한국군을

136) 국정원의 2013년 국정감사 보고에 의하면 북한은 정찰총국 소속 사이버 연구소를 중심으로 사이버 사령부를 창설했으며, 북 노동당 산하에 7개 해킹조직 1,700여 명과 4,200여 명의 대규모 사이버전 지원조직이 갖춰져 있다고 한다.

상대로 군사정보 수집과 해킹, 군 지휘통신체계 교란 및 무력화, 허위정보 확산 등 사이버 심리전을 담당하고 있다.[137] 국방위원회 직속 정찰총국의 사이버전담부서인 사이버전 지도국은 대남 사이버전을 총지휘하며, 한국의 각 영역별 전략정보 수집, 국가 공공망 대상 사이버테러 실행, 전담요원 해외파견 및 해외거점을 통한 사이버테러 등을 담당한다.[138] 국방위원회 지시를 받는 노동당 산하 225국의 사이버전담부서에서는 사이버드보크 개발 및 설치, 사이버수단을 이용한 간첩지령, 간첩교신 등의 임무를 담당하는 등 북한은 각 영역에 따라 체계적인 작전수행조직을 운영하고 있음을 알 수 있다. 당 통일전선부 소속의 사이버 전담부서인 작전처에서는 한국 국민을 대상으로 사이버 심리전을 담당한다.[139]

다. 공조체제 등 네트워크의 관점

첫째, 열악한 북한의 인프라체계다. 세계최고의 인터넷 기반이 구축된 한국과 비교해 볼 때 북한은 국가 통제로 인터넷과 인트라넷의 분리정책을 추진하고 있고 정보통신 인프라가 대단히 미흡하고 자원이 부족한 나라다. 이는 독자적인 사이버 전략의 산물이며 미국중심의 인터넷에 참여하지 않은 유일무이한 나라다.[140] 북한은 체제유지와 사이버전의 장점을 활용하기 위해 소수의 특권층에게만 인터넷을 사용할 수 있도록 하였고 폐쇄적인 인트라넷 환경을 유지하고 있다. 극소수 주민과 북한 내부기관에서 활용하는 독자적인 인트라넷의 구축 그리고 국가의 강력한 내부통제 등으로 사이버 활동을 하고 있는 것이다.

북한은 국가적 차원에서 근원적으로 컴퓨터 사용 통제를 강화하고 있다. 북한군이나 정보기관, 경찰들은 외국과 연결되는 인터넷 망과는 별도로 그들 전용의 인트라넷을 설치하는 망 분리를 실시하여 대내 정보의 외부 유출을 방지하고 있다. 북한은 독자적인 컴퓨터 운영체계를 개발하고 주요 기관들이 망 분리를 하는

137) 윤규식, "북한의 사이버전 능력과 위협전망," 『군사논단』, 제68호 (한국군사학회, 2011), pp.77-78.
138) 김기수, 앞의 논문, pp.303-304.
139) 윤규식, 위의 논문, p.77.
140) 고경민(2007)에 따르면 인터넷의 발전을 위해서 북한은 인터넷을 개방하고 이를 적극 활용해야되지만, 이는 정치적으로 북한체제를 위협하는 요인이 될 수 있고, 정치적 통제를 강조하다보면 인터넷의 활용이 제약을 당하게 되는 딜레마 상황에 처하게 된다. 이러한 딜레마 상황에서 북한은 통제와 활용 사이의 선택에서 '선(先) 통제 후(後) 활용'이라는 방어적 전략을 선택하고 있으며, 이것이 인터넷과 인트라넷의 분리 구축에 의한 이중성으로 귀결되었다고 말하고 있다.

등 근원적인 대책을 마련하고 있다. 이와 더불어 북한당국은 일반적인 인터넷 사이트 접속을 제한하고 컴퓨터 작업기록을 확인할 수 있도록 통제하고 있다. 북한이 국제인터넷 도메인 관리기구에 등록한 사이트는 3개로 알려졌다. IP주소가 북한은 1천여 개인 반면, 한국은 1억3천만 개의 IP주소를 보유하고 있다. 북한은 1995년에 인터넷을 구축하여 체제유지를 위해 필요한 요원들에게 공급하고 1996년에 북한에서만 사용하는 인트라넷을 독자적으로 구축하였다.[141]

북한은 일반기관과 주민을 위한 '광명'과 국가보안성에서 활용하는 '붉은 검'과 국가보위부에서 사용하는 '방패'와 군에서 사용하는 '금별'이 있다. 주민들이 사용하는 광명에는 3,700여 기관에 속한 컴퓨터들이 연결되어 있고 이용자 수도 5만 명 정도라 한다. 북한에서 모든 PC는 보안서나 보위부에 등록되며 인터넷에 접근할 수 있는 기능이 차단되고 전기 사정이 좋지 못해 컴퓨터를 쓸 수 있는 시간도 제한된다.[142]

북한은 중국의 차이나 텔레콤으로부터 회선과 중국 IP를 할당받아 중국 단둥과 신의주를 잇는 광통신망을 통해 인터넷을 이용하고 있다. 월드뱅크 통계에 따르면 북한의 인터넷 이용자 수는 인구 대비 거의 제로%로 실제 이용자들은 정부에서 신뢰할 수 있는 간부급 인원 수백 명 정도일 것이라고 한다. 북한의 사이버 인프라는 매우 빈약한 상황으로 판단된다.[143] 북한은 인터넷 의존 시스템이 거의 없기 때문에 북한에 대한 사이버공격은 피해를 주지 못할 것이라고 예상하고 있다. 위기시에 북한은 네트워크 접속을 차단함으로써 외부의 사이버 공격을 미리 예방할 수 있고 사이버 공간에 대한 의존도는 매우 낮아서 사이버공격을 받아도 피해가 거의 없는 장점을 가지고 있다.[144]

반면에 북한의 사이버전력의 약점은 전기 공급이 어렵기 때문에 북한이 자체적으로 운용하고 있는 사이버 인프라가 사이버공격 시 취약하다는 점과 북한 내

141) "북의 최후 결전은 사이버전이다," 『자주민보』, 2013년 5월 20일. 한호석은 세계적 범위의 인터넷과 영구히 단절하고, 일국적 범위의 인트라넷을 지속적으로 발전시키는 북의 정책을 '사이버 자주노선'이러고 부르고 있다.

142) 임종인 외, 앞의 논문, pp.21-22.

143) 위의 논문, p.22..

144) 국정원, "남북 사이버전 땐 우리 피해 훨씬 심각," 『머니투데이』, 2013년. 5월. 2일. 국정원은 남북한 사이버전쟁이 벌어질 경우 북한은 폐쇄적인 정보통신망을 운영하고 컴퓨터 보급률이 저조할 뿐 아니라 인터넷 감시•통제가 강해 우리 측이 북한 전산망에 침투해 공격하는 것은 쉽지도 않을뿐더러 효과도 제한적이기 때문에 남한 측의 피해가 훨씬 더 심각할 것으로 분석하고 있다.

부 IP만 알면 공격자 식별이 쉽다는 점이다. .

둘째, 국제적인 협력 관계다. 사이버전은 특성상 네트워크를 통해 전달되는 데이터의 양과 그 처리속도가 우리의 상상을 초월하고 있기 때문에 사이버 전에 대비하기 위해서는 국제협력이 필수적이다. 북한은 사이버작전에 있어 중국과 특별한 관계를 갖고 있는 것으로 추정된다.[145] 북한은 중국에 대한 의존도가 상당히 큰 것으로 파악되고 있다. 북한의 사이버전력의 인프라와 사이버무기, 전략전술, 국제협력 등에서 의존도가 상당히 높은 편이며 특히 사이버인프라와 공격체계에 있어 중국은 핵심 역할을 하고 있다. 북한은 공격을 위한 인터넷 인프라 부족과 인터넷 보안의 약점을 메우기 위해 중국의 사이버 역량을 효과적으로 활용하고 있는 것이다.[146]

북한에 대한 사이버전력 평가는 북한 단독의 전력 평가로 인력, 교육체계, 조직, 기술 등과 같은 단편적 기준에 의해 평가되어 왔기 때문에 중국의 역할은 잘 드러나지 않았다. 그러나 북한은 중국을 경유하여 공격을 수행하고 있기 때문에 북한의 전력평가 시 중국의 일부 사이버전력 요소들을 포함하여 정의하고 분석할 필요가 있다. 북한은 한국의 약점들을 최대한 활용하는 한편 자신의 한계와 약점들을 중국의 인프라와 자원들을 통해 보충함으로써 사이버전에서의 우위를 달성하고 있는 것으로 보인다. 중국은 평양에 중국제 고급서버와 라우터, 네트워크, 하드웨어들을 제공하고 있으며 중국과는 광케이블로 연결되어 있다.

북한은 사이버 공격 장소로 중국을 이용하며 중국 내에 최소한 한개 이상의 부대가 있다고 한다. 북한은 최고 지도자의 관심과 지원으로 중국이나 러시아의 해킹기술도 연구하고 있으며 나름대로 강력한 공격력이 있는 것으로 평가하고 있다. 북한은 해커 팀을 운용하여 한국 팀, 미국-일본 팀, 중국-러시아 팀, 동남아 팀 등으로 구성하여 각 국가 동향, 군사정보, 전파방해, 전파교란, 감청, 암호해독 등을 수행하고 있다. 이처럼 북한은 인터넷 인프라와 산업이 가장 미발전한 국가임에도 불구하고 국가적인 목적을 달성하기 위해 다양한 영역에서 사이버공간을 체계적이고 효과적으로 활용하고 있는 국가들 중의 하나로 평가할 수 있다.

미국은 사이버작전과 관련해서 북한과 중국을 동맹관계로 파악하고 있으며 이들이 미국을 위협하고 있는 것으로 평가하고 있다. 최근 북한의 미국에 대한 사

145) 임종인 외, 앞의 논문, p.29.
146) 김기수, 앞의 논문, pp.304-305.

이버공격들을 평가한 결과 중국과 북한이 북중 군사동맹을 통해 한미 군사동맹에 타격을 주기 위한 것으로 북한의 배후에 중국 사이버부대인 넷 포스가 있다고 분석하고 있다.[147] 그러나 북한과 중국의 사이버전을 둘러싼 관계가 전략적 동맹관계인지 아니면 단순한 지원관계인지는 명확히 확인된 바 없지만 북한은 중국의 많은 지원을 받고 있는 것으로 추정된다.[148] 북한은 지금까지 국제회의 참석 등 사이버전과 관련하여 국제협력 활동은 전무한 실정이다.

라. 인력과 기술 등 지원적인 관점

북한은 전략적으로 군사적 목표를 달성하기 위하여 최근까지 많은 사이버 전문 인력을 양성하여 왔다.[149] 북한의 김정일은 걸프전과 이라크 전을 통해 체제의 위협에 사이버 역량을 강화함으로써 적극적으로 대응하였다. 북한은 김일 군사대학을 선두로 연간 수백여 명 씩 IT전문가를 배출하는 등 전문 인력이 3만 명 정도나 된다는 탈북자 증언도 있다.

국내 기업들이 북한에서 훈련받은 정보통신 기술자들의 능력을 평가할 수 있는 기회가 있었는데 북한의 IT인력을 중국에서 고용할 때 그 인력들이 생각보다 매우 우수한 수준을 보유하고 있었다는 것이다. 북한은 이렇다 할 산업이 없기 때문에 인재들을 군수산업에 집중하여 이 분야만큼은 뒤떨어지지 않는다는 얘기다. 북한의 IT인력은 최고의 우수한 엘리트 계층에서 나오며 온갖 특혜가 사이버전사들에게 주어지기 때문에 우수한 인재가 몰릴 수밖에 없다는 것이다. 수년 동안 해외 유학까지 시키며 특혜를 줘서 키운 북한의 우수한 사이버전사들이 사이버전선에서 수 년 동안 경험을 축적하고 실전에 나타나기 시작한 것으로 분석된다.[150] 이들의 능력을 과소평가해서는 안 된다. 더욱이 북한은 국가적 차원에서 국방위원회와 노동당이 직접 나서서 사이버전 능력을 향상시키고 있다. 북한처럼 전체주의 국가에서 특정한 목적을 위해서 국가적 역량을 집중하는 것은 상상 이상의 능력을 발휘할 수도 있다. 북한이 대남 공작이나 남조선혁명 차원에서 국가적으로 지원하는 사이버전쟁을 경시해서는 안 되는 이유다.[151]

---

147) "북한의 사이버 공격 뒤에 중국이 있다," 『미래한국 데일리』, 2011년 6월 26일.
148) 임종인 외, 앞의 논문, pp.29-30.
149) 김기수, 앞의 논문, pp.300-302.
150) 위의 논문, p.24.
151) 한희, 앞의 논문, pp.16-17.

북한의 사이버 전사의 수는 3천명에서 3만명까지 의견이 다양하며 여기서 말하는 인력의 수가 해커의 수인지 지원인력까지 포함된 수인지 명확하지 않다. 사이버 부대원, 사이버전 지원인력, 사이버 전사, 해커 등 다양한 주체들이 언급되지만 상호 어떤 관련이 있는지도 명확하지 않다. 가장 혼란스러운 부분이기도 해서 종종 북한의 사이버전력에 대한 과장 논란으로 이어지기도 한다.[152]

따라서 북한의 교육기관에서 배출되는 졸업생 수로 규모를 역 추적하기도 하는데, 이 또한 교육과정의 목적이나 배출인력의 성격이 명확하지 않아 정확히 추정하기는 어려우나 매년 수백 명씩 배출하는 것으로 판단하고 있다.[153]

북한은 전체주의 사회로 자원과 인력배치의 집중성과 계획성으로 사이버 전사를 양성하는데 매우 유리한 환경이다. 지금까지 사이버공격 사례를 볼 때 북한은 한국을 위협할 수준의 사이버 전사들은 충분히 확보하고 있는 것으로 보인다. 사이버공격은 실력 있는 해커들이라면 불과 수십 명의 소수 정예만 있어도 큰 위력을 발휘할 수 있기 때문에 사이버 전사의 숫자는 크게 중요하지 않을 수 있다.

북한은 사이버전력의 전략적 중요성에 걸맞게 사이버전사들에게 높은 보상체계로 사회적 대우를 통해 안정적으로 우수한 인력을 확보하고 있다.[154] 사이버 전사들은 북한 사회에서 상당히 높은 봉급과 포상, 유학과 같은 특혜를 받고 있다는 점이다. 금성중학교를 최우수 성적으로 졸업하는 학생에게는 명문대학 진학, 외국유학, 부모의 평양생활보장 등 특혜를 주고 있다고 한다. 또한 영관급 이상 정보전사 가족들은 매달 미화 400달러 정도를 받는 등 안정된 생활을 하고 있다고 한다.[155] 실례로 2009년 7월 디도스 공격에 참여했던 해커 전원에게는 유학 등 다양한 특혜를 주었다고 하며 KBS를 포함한 대남 사이버공격에 참여했던 사이버전사들은 김정은의 직접 지시로 평양의 고급 아파트를 배정받고, 훈장 등 포상을 받았다고 한다. 따라서 북한 사이버 전사들은 높은 봉급과 호화로운 생활

152) 주성하, "해킹을 이슈로 북한 사이버전사와 직접 나눈 대화," 『서울에서 쓰는 평양이야기』(2013년 3월 31일). 북한의 현직사이버부대원과 대화를 나눴다는 그의 주장에 다르면 북한의 해킹능력은 우리 생각보다 훨씬 취약하며, 미림대학은 사이버전사 양성소가 아니고 미림대 졸업생 전부가 해커들은 아니라는 것이다.

153) 북한의 교육기관에서 배출되는 사이버전사의 숫자와 전공, 수준에 대해서도 논란이 존재한다. 실제 배출되는 인력 중의 사이버전사 비율과 그 중의 해커 비율에 대해서도 명확하지 않다. 미림대학만 하더라도 한 해 졸업생으로 100여 명부터 200명으로 제시되는 수치가 다양하다.

154) 임종인 외, 앞의 논문, pp23-24.

155) "북한군 정찰총국, 사이버 요원 해외 급파," 『자유아시아방송』, 2013년 3월 21일.

로 북한의 엘리트들 사이에선 선호되는 직업이라고 한다.[156]

둘째, 교육훈련체계다. 국가차원에서 체계적으로 사이버전사들을 배출하고 있다. 해킹능력은 세계적인 수준으로 알려져 있으며 졸업 후에는 군에서 해킹요원으로 활용하고 있다. 2013년 하태경 국회의원에 따르면 북한은 가장 우수한 인재들을 조기에 뽑아 최고의 교육기관에서 중등교육, 고등교육, 부서교육 등의 세 단계로 나누어 집중적인 해커전문 교육훈련을 시킨다고 한다.[157]

북한은 2001년 금성 제1·2중학교 내에 컴퓨터 수재 반을 만들어 운영하고 있으며 컴퓨터 수재 반에 편성된 학생들은 매년 500시간에 달하는 전문교육을 받는다. 우리나라 대학의 컴퓨터학과 교육시간 보다도 길다. 중학교 교육과정에서 특출한 재능을 보인 학생들은 평양과 함흥에 있는 김일성 종합대학이나 김책공과대학 등에 진학하며 프로그래밍, 명령어 자동화, 전산화된 연산, 기술 정찰, 사이버전 등의 전문적인 과목이 교육내용에 포함돼 있다. 졸업생들은 정찰총국이나 총참모부 소속 부대에 투입되거나 훈련을 위해 해외로 나가는 경우가 있다. 중학교 6년과 대학교 5년 동안 교육받은 영재들을 실전에 투입하면서 북한의 사이버전 수행능력은 한 단계 도약했다.

북한의 해킹 교육은 자신들의 능력을 검증하기 위해 수시로 실전 훈련 형태로 진행된다. 글로벌 포스트 지는 인터넷 인프라가 취약한 북한이 사이버공간에서 가장 위협적인 국가가 될 수 있었던 주요한 이유로 효과적이고 강력한 교육훈련 시스템을 꼽고 있다.[158] 북한은 정보전 능력을 개발하는 데 많은 돈을 투자하고 기술훈련을 위해 정보전 전사들을 인도와 중국의 일류대학에 보내는 등의 노력으로 사이버전사들이 잘 훈련되어 있다고 한다.[159] 이처럼 북한은 높은 대우와 체계적인 교육시스템을 통해 수준 높은 사이버전사를 배출하는데 안정적인 생태계를 만든 것으로 보인다.

셋째, 사이버 무기체계와 기술개발 능력이다. 북한은 2000년대 초반 전 세계의 해킹사례를 분석하여 바이러스나 웜, 스파이웨어, 트로이 목마 등 해킹 툴을 직접 만들어보고 고급해킹 툴을 다뤄보면서 새로운 해킹수법들과 도구들을 준비했

156) "앞으로 북한이 노릴 사이버공격 대상은?," 『TV조선』, 2013년 10월 17일.
157) 임종인 외, 앞의 논문, p.25.
158) "North Korea: How the least-wired country became a hacking superpower," 『Global Post』, 2013. 5. 22.
159) Q&A of the week: the current State of the Cyber Warfare Threat featuring Jeffey Carr," 『ZDNet』, 2012. 5. 11.

다. 사이버 공격기술은 디도스 공격, 지능형 지속위협(APT), 봇 넷 운용, 악성코드 개발 등 다양한 공격수행 기술을 연구하여 보유하고 있고, 역 추적 방지 및 공격 우회기술, 통신암호화, 흔적삭제 등 진화된 공격기술을 갖추고 있다.[160]

특히 개미보다 작은 로봇인 나노 머신을 이용하여 적 정보체계에 잠입하여 컴퓨터 하드웨어를 파괴하거나 전도성과 흡착성이 우수한 탄소섬유 분말탄을 이용하여 전력이나 전기에 문제를 일으켜 기능을 마비시키거나 파괴하는 물리적인 파괴방법도 연구하고 있다.[161] 이처럼 북한은 공격무기체계나 내부통제기술에 대해서도 꾸준히 연구개발을 해오고 있다. 기술적인 측면에서도 단기간의 디도스 공격과 같은 단순한 공격에서 장기간에 걸친 높은 수준의 APT공격으로 진화하고 있으며 악성코드의 기능도 사용자 정보 수집이 아닌 데이터나 하드디스크 파괴로 강력하다. 사이버 방어무기 체계로는 사이버 공격을 막는 금성철벽이라 부르는 인트라넷 광명과 독자 운영체제인 붉은별, 암호화기술, 방화벽, 백신 등 보안도구 등이 있고 심리적 무기체계로는 사회공학기술, 스피어피싱, 종북어플 등을 활용하고 있다.[162]

북한은 우리의 국방망과 같은 폐쇄적인 인트라넷을 공격할 수 있는 기술을 또한 보유하고 있다. 북한은 몇 년 전부터 광자기 도파기라는 인트라넷 해킹 기술을 연구하고 있다. 광자기 도파기는 광(光)케이블의 배선 근처에 갖다 놓으면 케이블 안에 흐르는 데이터를 미세한 전파 신로로 바꿔서 인트라넷에 접속하는 기술이다. 통신선이 연결되지 않아도 소리, 열, 빛 등으로 데이터를 주고받는 최신 기술이 등장하여 기술적으로 인트라넷에 대한 사이버 테러가 가능해졌다.

북한은 전 세계적으로 인트라넷 공격용 바이러스로 악명 높은 스턱스넷(Stuxnet)을 확보했다고 한다. 이는 한미 핵심기반시설인 원자력과 같은 시설의 인트라넷에 대한 공격기술을 갖추고 있다는 의미이다. 그리고 스마트폰 등 모바

160) Technolytics(2007)의 사이버위협 매트릭스 평가 자료를 보면 북한은 바이러스, 트로이 목마, 디도스 공격, 브루트포스 공격, 해킹, 사이버 첩보와 같은 기본적인 데이터 무기들을 개발할수 있는 능력을 가지고 있는 반면 식별, 탐지를 어렵게 하는 기능을 갖춘 고급 데이터 무기들은 갖추지 못한 것으로 평가하고 있다. 하지만, 최근 3.20 사이버공격 사례들을 보면 우회, 탐지회피 등의 기능을 갖춘 고급 무기 개발능력을 갖춘 것으로 추정된다.

161) 김기수, "북한의 사이버전 수행실태와 대비방안," 『전투발전지』, 2010, pp.127-128.

162) 대표적인 방어용 소프트웨어로는 능라방화벽과 백신 프로그램인 클락새, 주작, KJAV 이외에도 보안조작체계(K-Selix), 보안인식체계(CBVoicein), 유, 무선 전화통신 암호화 장치(청송, 번개), 보안자료 은폐용 소프트웨어(SGVistion), 인증소프트웨어(BS Crypt), 워터마킹프로그램(BS 워터마킹), 접근통제솔루션(보검), 방화벽(어은) 등이 있다.

일 기기를 이용한 무선 사이버 공격에 대해서도 집중적인 대응준비를 하고 있다.[163] 북한은 전자적, 논리적, 심리적 무기체계를 갖추고 다양한 공격을 수행할 수 있는 능력을 확보하고 있다. 전자적 무기체계로는 전자장치들을 무력화시키는 EMP, GPS 신호를 교란시키는 GPS 재머를 개발하고 있다.[164]

이상과 같이 북한의 사이버 능력을 네 가지 관점에서 분석해 보았다. 공식적인 자료가 제한되어 탈북자 증언 내용을 참고하였으며 외국의 전문가들의 연구결과를 토대로 분석해 볼 때 북한의 사이버전 능력은 상당한 수준으로 평가할 수 있겠다. 또한 사이버 전사들에게 국가에서 다양한 인센티브를 부여하여 동기유발을 자극하고 있으며 집중적인 훈련과 중국과의 협조를 통해서 한국을 비롯한 미국과 자유주의 국가들을 공격하고 있는 특징이 있다.

마. 사례

한국을 목표로 동시 다발적이고 정교한 사이버 공격을 수행할 집단은 북한뿐이다. 7·7 디도스 공격, 3·4 디도스 공격과 농협 전신망 마비, 3·20 사이버 테러와 6·25 사이버 테러에 이르기까지 북한의 사이버 공격으로 정보통신기술강국 한국은 많은 피해를 입었으며 제대로 응징보복을 하지 못했다. 북한이 자행한 디도스 공격은 수십 대에서 많게는 수백만 대의 PC를 원격조종해 특정 웹 사이트를 동시에 접속시킴으로써 단시간에 과부하를 일으키는 공격이다. 이들은 서버나 네트워크 대역이 감당할 수 없는 많은 양의 트래픽을 순간적으로 일으켜 서버를 마비시킴으로써 사용자들의 웹 사이트 접근 및 사용을 차단한다. <표 6>는 최근에 북한이 한국을 향해 공격한 주요 사이버 공격 사례다.[165] 북한은 국가기관과 공공망, 일반망에 대하여 무차별적으로 사이버 공격을 자행하였다. 몇가지 중요한 사례를 살펴보고자 한다.

가. 7·7 디도스 공격

2009년 7월 7일 18시 44분경 정부통합전산센터와 한국인터넷진흥원의 인터넷

163) "구멍난 사이버안보컨트롤 타워 시급, 미국•북한 사례로 본 우리의 방향," 『디지털타임스』, 2013년 7월 3일.
164) 임종인 외, 앞의 논문, p.23.
165) 신충근·이상진, 앞의 논문, p.209.

침해대응센터는 청와대와 국회 등의 홈페이지가 DDOs 공격을 받고 있음을 인지하고 이를 관련 정부부처인 국가정보원과 방송통신위원회, 안전행정부 등에 통보했다. 정부는 관련 인원의 비상대기를 유지하고 악성코드를 유포하는 것으로 의심되는 숙주사이트를 차단했다. 이어서 범정부 차원의 회의를 소집하고 관계기관, 인터넷 서비스 사업자, 보안업체 간의 긴밀한 공조체계를 유지했다.

<표 6> 북한의 최근 대남 사이버 공격 사례

일 자	주 요 임 무
국가기관	청와대(2006), NCS(2008)
	제18대 국회 261건 해킹사고
	외교통상부 대외비 문건 해킹의혹(2011)
	통일부 해킹시도
	한국원자력연구원, 무역보험공사, 산업기술원, 가스공사 등 지경부 산하기관에 40여 차례 해킹시도(2011)
공 공 망	7·7 DDoS, 3·4 DDoS, 농협전산망 해킹(2009-2011)
	고려대 정보보호대학원 이메일계정 해킹(2011. 11.)
	육사 동창회 사이트 해킹(2011)
	페이스북 이메일 위장 악성코드 유포(2011. 10.)
	군관계자 해킹메일 유포(2012. 1.)
	320 사이버 테러(2013. 3. 20.)
	625 사이버 테러(2013. .6 .25.)
일 반 망	북한 해커의 국내 게임사 해킹 및 오토프로그램 제작(2011)
	네이트, 사이월드 300만명 고객 개인정보 해킹(2011. 7.)
	(주)넥슨 게임사 회원 1320만명 개인정보 해킹(2011)
	TV조선, 중앙일보 서버 해킹(2012. 6.)
	북 정찰총국 연계 악성코드 유포(2012)

결과적으로 국내 34개 사이트와 미국 15개 사이트가 접속장애가 발생하고 하드디스크 및 파일의 파괴, 부팅 에러 등과 같이 PC가 손상되었다. 이를 계기로 보안업계 뿐만 아니라 공공기관과 일반기업에서도 사이버 공격은 상시 발생할 수 있다는 사실을 알게 되었다. 따라서 지금으로서는 예측하기는 어렵지만 그 동안의 사이버 테러 사례와 패턴을 통해 다음번의 공격 대상을 유추하여 예방할 수는 있을 것이다.[166]

166) 손영동(a), 앞의 책, pp.90-98.

나. 3·4 디도스 공격

2011년 3월 4일 청와대와 국가정보원, 국회 등 24개 주요 정부기관과 네이버와 다음, 옥션 등 16개 민간 웹 사이트에 대한 디도스 공격이 발생했다. 3·4 공격은 국가안보와 경제안보 두 축을 표적으로 공격했다. 대상은 우리나라를 대표하는 상징적인 40개 기관이다.[167] 이중 금융기관이 10개로 가장 많았고 국방 분야도 9개였다. 7·7 공격 때는 북한이 61개국에 있는 435대의 공격명령 서버를 이용해 동일한 악성코드로 여러 차례 공격했으나, 3·4 공격 때는 70개국 746대를 이용 서버가 늘었고 6개 이상의 변종코드를 사용했다. 공격 때마다 악성코드의 구성이 달라지고 새로운 기능이 추가됐다. 한국의 문제식별 능력과 얼마나 빠르게 복구하는지를 알아보기 위한 탐색의 성격이 강했다. 2차에 걸친 대규모 디도스 공격은 언제든지 다시 발생할 수 있음을 나타냈다. 공격자는 이전과 다른 방법으로 예상치 못했던 취약 부분을 집중적으로 공격하였다.

다. 농협 전산망 공격

2011년 4월 12일 농협의 금융사업부문은 총자산 250조 원에 거래고객이 2,000만 명에 이르는 방대한 회사로 거대 금융기관의 전산시스템이 좀비 노트북 한 대로 정지된 것이다.[168] 소프트웨어 명령어 하나가 대형 전산시스템을 파괴하여 수많은 고객에게 피해를 끼쳤다. 농협 서버 공격은 금융기관 전산망에 직접 침투해 데이터 삭제는 물론 범행흔적까지 지우려 했다. 농협 전산망 마비는 조직 리더의 보안 불감증을 보여준 대표적인 사례가 됐다. 농협의 당시 보안예산은 금융감독원의 권고 수준인 정보통신 투자예산의 5%에 모자란 1.6% 수준이었다.

라. 3·20 사이버 테러

2013년 3월 20일 KBS, MBC, YTN, 농협, 신한은행, 제주은행 등 방송과 금융 인프라가 북한의 사이버공격을 받아 장애가 발생했다.[169] 컴퓨터 백신 소프트웨어를 배포, 관리하는 회사의 서버에 악성코드가 침투, 사내 네트워크에 연결된 각 PC에 백신 프로그램을 업데이트해 주는 과정에서 악성코드로 모든 PC가 감염됐다. 지능형 지속위협기법을 이용해 오랫동안 피해 기관의 백신업데이트 서버

167) 신충근·이상진, 앞의 논문, p.210.
168) 위의 논문, p.210.
169) 김기수, "북한의 사이버전 위협과 대비방안," 『한국정책학회』, (동계학술대회, 2013), p,301.

에 악성코드가 잠복해 있으면서 정보를 빼내고 주기적으로 업데이트할 때마다 PC를 감염시켰다. 북한은 일반시민들의 금융거래 혼란과 방송 사고를 동시에 타격했다. 금융은 경제안보의 핵심이며, KBS와 같은 기간방송에 대한 사이버공격은 비상사태 때 우리 정부가 시민들에게 정확한 상황과 행동요령을 전달하지 못하게 할 수도 있다는 것을 의미한다.

마. 6·25 사이버 테러

북한은 6월 25일부터 7월 1일까지 64개 기관과 업체를 타깃으로 최소한 5개월 전부터 사전작업을 했고 정부기관 홈페이지를 일시에 마비시키려 계획했다. 청와대 홈페이지가 점령당해 전 세계 언론 홍보의 장이 됐다. 국무조정실, 새누리당, 조선일보, 매일신문, 대구일보 등도 공격을 받았다. 북한의 사이버 테러는 계속될 수밖에 없다.[170] 이상과 같이 우리의 사이버 공간은 북한 해커들에게 완전히 노출돼 있다. 북한은 대남사이버공격 뿐만 아니라 사이버범죄에 직접 개입하고 있고 그 유형도 다양하다.[171]

이를 평가해 보면 북한의 사이버 공격이 대상과 범위가 확대되고 피해수준도 점차 커지고 있다는 사실이다. 범죄에 영역에서부터 국방시스템, 공공기관, 언론사, 방송사, 금융시스템, 기반시설, 통신사, 대기업 등으로 공격이 확대되고 있다. 앞으로 북한은 교통과 전력 등 주요기반시설 제어망과 금융망의 취약점을 파악해 동시다발적인 정밀타격을 시도할 가능성이 있으며 교통, 통신, 금융, 전력망 등을 한순간에 마비시킬 수 있도록 공격할 것으로 추정된다.[172]

제3절 소결론

결론적으로 미국·중국·일본·러시아 등 주요 국가들의 사이버전 수행역량은 급속도로 발전하고 향상되고 있다. 국가안보의 핵심적인 요소로 등장하게 됨으로써 국가적인 관심과 투자로 전략과 정책이 수립되고 조직이 강화되고 있으며 인력과 기술면에서 많은 발전이 이루어지고 있다. 주요 국가들의 사이버 역량과 사례를 분석해 보면 <표 7>에서 보는 바와 같다.[173]

---

170) 손영동(b), 앞의 책, pp.137-147.
171) 신충근·이상진, 앞의 논문, p.210.
172) 양정아, "북 사이버전 능력, IT강국 위협하는 세계3위권," 『NK비전』, 2013년 5월 9일.

<표 7> 주요 국가별 사이버역량 비교

핵심요인		미 국	중 국	일 본	러 시 아
인식과 사상		사이버안보를국가우선 현안으로정부가대응,향후5년간260억$투자	방어성격의사이버존재 주장,적극적인예산투자	정부차원의 사이버보안 조정통제 능력강화	중요성 인식 적극적인 예산투자
국가전략 등 시스템	전략/정책	新사이버전략 ('15.4.23)	사이버안보정책 수립	사이버안보전략안 작성 /NSC와 협력	물리전과 사이버전의 통합
	콘트롤타워	백악관,국가안보국내사 이버위협정보센터창설 추진	정부 : 국무원 중심 군 : 사이버사령부	사이버보안전략본부/내 각사이버보안센터설치 ('15.1.9)	내무부산하K국과연방 보안국정보보안센터
	법령/제도	사이버정보공유법안 발의('15.1.8)	사이버안전법제정('15.8)	사이버보안기본법수립 ('14.11)	사이버사령부설립법 추진('14.3)
	수행체계	국토안보부,국가안보국, 사이버사령부	중앙사이버안전및정보 화소조,사이버판공실 설립	사이버보안전략본부, 내각 사이버보안센터	연방 보안국 중심으로 수행
공조체계 등 네트워크	정보보호 인프라	네트워크 수준(5위) 시스템 수준(1위)	네트워크 수준(36위) 시스템 수준(56위)	네트워크 수준(19위) 시스템 수준(16위)	네트워크 수준(77위) 시스템 수준(59위)
	국제공조	아태・유럽・중동동맹 국과협력체제 구축	UN GGE, OECD, 런던 회의 등 참석	한,중,영,인도,이스라엘 과 협력추진,	UN GGE, OECD, 런던 회의 등 참석
인력과 기술	사이버 전문인력	14만명,국가차원훈련,육 군사이버학교 창설 추진('15년내)	105만명 61398부대,61486부대	미국 사이버스톰 훈련 참가(2010년 부터)	전문인력 8천여명 훈련
	기술개발	정보보호예산 (7조3천억)	정보보호예산 (2조1천억)	국내외연구소,정보보호 예산(3조6천억)	정보보호예산 (2천4백억)

이를 네 가지 핵심요인별로 주요국가의 사이버 역량을 살펴보면 첫째, 사이버 안보관련 입법화와 전담조직의 설립 등 군을 넘어서 국가차원에서 주도적으로 대응하는 추세이며 둘째, 금융기관과 국가기반시설에 대한 공격에 대응하기 위해 정보공유와 협력을 위해 민・관・군의 공동대응방안을 모색하는 추세이고 셋째, 사이버 안보의 전략적인 개념이 방어위주에서 피해를 받는 즉시 보복공격이나 선제공격을 통하여 목표를 달성할 수 있도록 공격역량을 강화하는 추세로 전략이 전환되고 있으며 넷째, 국가별로 대응의 한계를 인식하여 국가 간에 협력 체제를 구축하고 국제 규범을 마련하기 위한 모색을 하는 것으로 평가된다. 그러나 한편으로는 사이버 보안에 대한 국가 간의 협력과 갈등으로 블럭화되는 경향을 보이고 있는 것으로 평가된다. 특히 중국과 러시아는 사이버 협약을 체결하여 상호간에 신뢰를 구축하고 사이버 위협에 공동으로 대응하는 것을 추진하고 있으

173) 강정민 외, "국가 사이버 역량평가 방법론 연구," 『정보보호학회논문지』, 제22권 제5호 (2012.10), pp.1048-1051.

며, 미국도 사이버 안보분야에서 동맹국을 중심으로 협력을 강화하고 있는 것으로 판단된다. 또한 미국과 서방, 중국과 러시아가 상호간에 공격주체로 지목하는 등 실질적인 갈등의 요인이 되고 있는 것으로 판단된다. 그러나 이와 같이 사이버 위협은 국가 간의 갈등의 원인이 될 가능성과 동시에 초국가적인 협력을 필요로 하기 때문에 국가 간에 협력의 촉매 요인이 될 가능성이 있을 것이다. 사이버전은 앞으로 계속 진화할 것이며 장차전은 사이버 공격과 물리전이 병행하는 공격추세로 전쟁양상의 패러다임 변화가 예측된다.

아울러서 북한의 사이버전에 대한 전략과 역량을 통하여 본 소결론은 인식과 사상의 관점, 국가전략 등 시스템의 관점, 공조체제 등 네트워크의 관점, 인력과 기술 등 지원적인 관점에서 보면 다음과 같다. 먼저 인식과 사상의 관점에서 볼 때 사이버전의 중요성에 대한 북한지도부의 인식은 대단히 높다는 것이다. 특히 사이버전을 비대칭전력으로 육성하고 국가차원의 투자와 지원이 전폭적으로 이루어지고 있다는 사실이다.

둘째, 국가전략 등 시스템의 관점에서 살펴보면 공식문서나 공개된 자료는 제한되어 정확히 파악하는 것이 쉽지 않지만 사이버 역량과 관련하여 극비로 취급하고 있는 것으로 추정된다. 아울러서 사이버 전략전술은 공격위주로 전력을 강화하고 있으며 내용은 철통보안사항이라 한다. 귀순자 증언에 따르면 북한영토 내에서 공격작전을 수행하지 않는다는 것이다. 이를 추측해 보면 북한은 다양한 전략전술과 사이버 교전규칙을 작성한 것으로 보인다.

셋째, 공조체제 등 네트워크의 관점에서 살펴보면, 우선 북한의 사이버 수행체제는 국방위원회 직속 정찰총국으로 단일화하여 임무수행이 용이한 것으로 판단된다. 열악한 인프라체계는 방어에 유리할 수 있으나 공격에는 불리하기 때문에 북한은 중국에 크게 의존하고 있는 것으로 보인다. 인터넷 기반시설이 열악한 북한은 중국 각 지역에 사이버 전사들을 보내 실제 훈련과 공격임무를 수행하고 있기 때문에 책임을 회피할 수는 있는 장점이 있으나 미국과 한국과의 관계개선에 악영향을 초래한다면 중국도 자신의 영토에서 이루어지는 북한의 사이버 공격을 지속적으로 묵인하기가 곤란할 것이다.[174]

또한 북한의 낙후한 사이버 인프라는 방어에 유리하여 북한의 능력을 높이 평

174) 김인수, "북한 사이버전 수행능력의 평가와 전망," 『통일정책연구』, 제24권 1호(2015), pp.139-141.

가하는 요인이 되고 있으나 이는 동시에 사이버 공격능력을 현저하게 제한할 수 있는 요인이 될 수 있다. 사이버 전사들에게 많은 인센티브를 부여한다 하더라도 인프라의 부족과 북한 주민의 사이버 공간에 대한 이해의 부족은 천재적인 해커나 뛰어난 사이버전사를 육성하는데 제한이 될 수 있다.

넷째, 인력과 기술 등 지원적인 관점에서 북한은 사이버 전사를 안정적으로 양성하고 활용하고 있는 것으로 판단된다. 또한 사이버 무기체계와 기술개발 능력도 우수하다고 평가할 수 있다. 북한은 중국, 러시아, 이란과 긴밀하게 협력하고 있다. 중국은 사이버 기술교육 외에도 서버, 라우터 등 하드웨어를 제공하고 있다. 중국과 러시아는 사이버 전자정찰국인 121국이 중국심양에서 활동하도록 협력하고 있고 러시아는 프룬제 군사학교 출신 교수 25명을 파견하여 사이버 전문가 양성교육을 지원하였고 전자파 공격기술과 인터넷 통제정보를 북한에 제공한 것으로 알려져 있다.[175]

북한은 각 학교마다 사이버 영재학교를 설립하여 집중교육으로 사이버 영재를 양성하고 있다. 단기적으로는 외국기술의 모방과 당 주도의 기술발전 전략은 효율적일 수 있으나 자유민주주의 체제에서 이루어지는 민간차원에서 신속하게 변화하는 다양한 기술개발 추세를 따라잡기는 어려울 것이다. 이는 혁신적인 기술을 개발하기보다는 기존의 기술을 습득하는데 치중할 것이기 때문에 장기적으로는 기술경쟁에서 수세적인 위치에 처하게 될 것으로 판단된다.

175) 윤규식, “북한의 사이버전 능력과 위협전망,” 『군사논단』, 제68호 (한국군사학회, 2011), pp.76-78.

제4장 한국의 사이버 안보 실태

제1절 물리전과 연계한 북한의 사이버전 위협

1. 장차전 양상

북한은 사이버 공격으로 남한 내 핵심기반시설을 마비시키고 혼란한 상황을 틈타 군사공격을 하는 방식의 하이브리드 전쟁방식을 선택하여 공격할 것이다. 이와 같이 혼란한 상황이 전개된다면 한국은 전쟁을 계획한대로 수행하기가 어려울 것이다.[176] 최근 언론에 공개된 북한군의 새로운 작전계획은 김정은의 주도로 만들어 졌으며 이는 '7일 작전계획' 이라고 한다.[177] 이 계획은 한국과 미국이 유사시를 대비해 작성한 '작전계획 5027' 과 유사한 일종의 전쟁수행계획이라고 한다. 특히 김정은은 새 작전계획에 따른 전쟁 준비를 2013년까지 완료하라고 지시했으며 2013년 싸움준비 완성의 해에 준비가 늦어지자 2015년을 통일대전 완성의 해로 선포했다고 한다.

북한군의 신 작전계획은 2012년 8월 25일 원산에서 열린 당 중앙군사위원회 확대회의에서 승인됐으며, 신작전계획의 골자는 북한이 기습 남침을 하거나 국지전이 전면전으로 확전될 경우 미군이 본격적으로 개입하지 못하도록 7일 안에 남한 전역을 점령하겠다는 것이다. 그러나 한미연합군의 반격으로 전황이 녹록치 않을 경우 최대 15일 안에 전쟁을 마무리한다는 내용이 포함됐다고 한다. 북한은 이를 위해 사이버 공격과 동시에 핵과미사일, 방사포, 특수전 요원 등 비대칭 전력을 이용해 초반에 기선을 잡은 뒤 재래식 전력으로 전쟁을 마무리한다는 수순을 정했다고 한다. 김정은은 핵과 미사일 사용을 작전계획에 포함하라고 직접 지시했으며 핵무기 소형화를 추진하고 미 본토까지 공격할 수 있는 장거리 미사일을 개발하는 것 등도 모두 새로운 작전계획에 따른 것이라고 한다. 특히 초전에 핵무기를 사용하면 방사능에 오염된 한반도에 미군의 증원전력이 들어오기 어려운 데다 남측 지도자들이 더 이상의 피해를 막기 위해 항복할 수도 있다는 계산에서다. 이는 일본이 히로시마에 원자폭탄이 떨어지자 항복한 것처럼 북한도 이

176) 김승주, "세계 각국의 사이버전 수행능력과 국내 피해사례," 『군사논단』, 제75호(한국군사학회, 2013), pp.19-20.
177) 『중앙일보』, 2015년 01월 08일 목요일 001면 종합.

같은 상황을 노린 것으로 추측된다.[178]

북한은 김정일 시대에 군부대를 경제 재건에 투입했던 것과 달리 김정은 집권 후에는 대규모 군사훈련을 자주 실시하고 군사력을 증강해 왔으며 2013년 이후 김정은은 군단급 부대를 2~3차례 반복해 방문하며 새 작전계획에 따른 훈련 상황을 점검하고 있다고 한다. 김정은은 훈련현장 지도 때 군부대를 불시에 비상 소집시켜 훈련실적이 저조한 부대의 지휘관을 보직 해임하고 부대를 해체하는 등 훈련 열풍을 조성하고 있다고 한다. 특이한 몇 가지 사례를 소개하면 북한군은 AN-2기를 이용한 특수부대 공수강하 훈련을 예년에 비해 20배를 실시했다고 한다. 김정일 시대엔 거의 없었던 고공침투 낙하훈련인 날다람쥐 전술은 레이더에 잡히지 않는 패러글라이딩이나, 여기에 모터를 단 패러모터 등 초경량 항공기를 이용한 기습 침투로 기존의 레이더로 탐지하기가 힘들어 AN-2기보다 더욱 효과적이라는 것이다.[179] 이는 수도권 곳곳의 산악에서 동일한 도구로 레저를 즐기는 일반인과 구별하기가 쉽지 않고 북한군이 새벽에 기지에서 출발하면 3시간 정도면 수도권에 도착할 수 있다고 한다. 해 뜨기 전에 관측되지 않고 침투할 수 있다는 판단에서다. 실제로 2008년 레바논 군은 이를 도입하여 시행했다고 한다. 북한은 2014년에 중부내륙고속도로 축선을 중심으로 한국의 발달한 고속도로망을 이용하여 기습 공격하는 훈련으로 연료는 고속도로 주유소를 이용하고 식량은 고속도로 식당과 휴게소를 각각 이용한다는 전술훈련을 실시했다고 한다. 이는 전통적으로 사용하였던 빨치산식 기습공격이다. 또한 노후화로 창고에 넣어둔 미그-15, 미그-17 전투기를 꺼내 훈련하다가 추락하는 일도 발생했다. 구형 비행기를 활용한 것으로 미뤄보면 유사시 '가미가제식 자살특공대 전략도 있는 것 같다' 고 한다. 특히 전쟁의 개념을 육·해·공을 넘어 사이버공간과 지하까지 확대하고 있다는 증언과 첩보도 있다. 김정일은 50개 이상의 대남 남침용 땅굴을 파라는 명령을 내렸다는 증언이 대표적이다. 모두가 상식을 넘어서는 북한식 두더지 전술이다.[180] 뿐만 아니라 최근 3년 동안 전방에 모두 5천여문의 방사포를 배치했다. 방사포는 신형으로 교체하고, 교체된 구형방사포는 예비군인 노농적위대에 배치하고 있다. 김정은은 포병부대를 불시에 방문해 초시계를 들고 실제 사

178) 김진, 『2015년 김정은 급변 터질 것인가』 (서울: 늘품플러스, 2014), pp.190-194.
179) 채인택, 『중앙일보』, 2015년 06월 25일 목요일 028면 사설/칼럼.
180) 『세계일보』, 2014년 12월 11일 목요일 006면 종합.

격까지 걸린 시간을 점검한다고 한다. 2015. 10월. 10일 북한 노동당 창건일에 300미리 방사포와 이동식 대륙간 탄도미사일(ICBM)이 등장하여 이를 과시한바 있다.

북한군은 최근에 인사 교체가 빈번히 계속되고 있다. 2011년 12월 김정일 사망 이후 3년 동안 군의 지휘부인 총정치국장, 총참모장, 인민무력부장은 6개월에 한 번 씩 교체됐다. 개인비리로 계급이 강등되는 경우도 있지만 대부분 작전계획 수립과 훈련을 제대로 이행하지 못한 지휘관들이 대상이며 새 작전계획의 준비상황이 미흡할 경우 교체하거나 계급을 강등시키는 징계가 이어지고 있다고 한다. 김정은은 배가 나온 사람들은 전쟁을 할 수 없다며 지휘관들의 솔선수범을 강조하고 군단장급의 80%이상을 상대적으로 젊은 50대로 교체했으며 연평도 포격전을 일으킨 4군단 이성국 상장의 경우 40대 후반이라는 것이다. 신 작전계획에 따른 전쟁준비를 하면서 북한군의 고위간부가 물갈이 된 것이다. 이와 같이 북한은 물리전을 준비하면서 사이버 전을 동시에 연계하여 공격함으로써 남한사회를 단번에 적화통일하려고 시도할 것으로 예측된다.

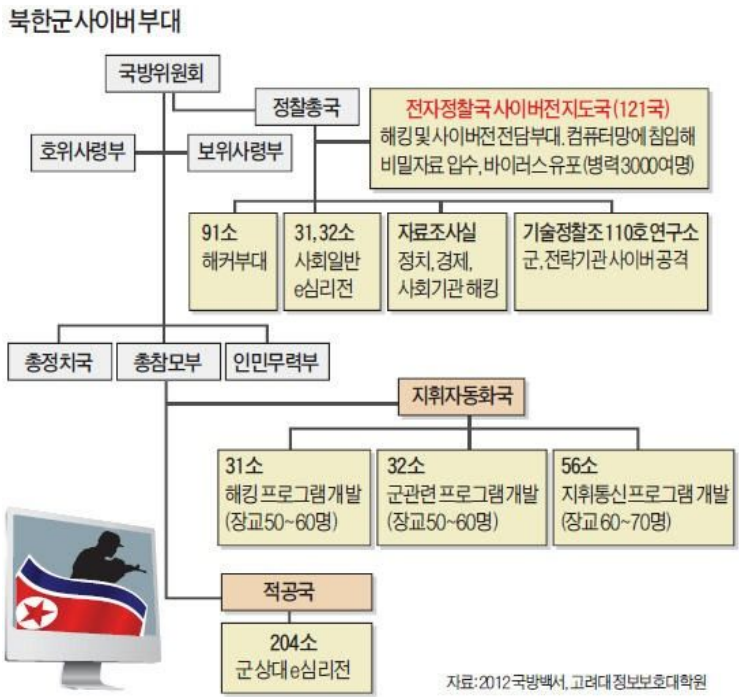
2. 사이버전 위협

북한은 강력한 사이버공격 능력 보유와 북한의 극히 제한적인 IT 환경을 고려할 때 사이버전이 발발할 경우 북한보다 우리의 피해가 훨씬 더 심각할 것으로 예상된다. 사이버전의 경우 한국군이나 미군이 북한에 비해 상대적으로 취약성을 갖고 있을 뿐만 아니라 익명성 때문에 북한은 쉽게 도발을 감행할 수가 있다.

북한의 사이버병력 규모는 6천여 명 정도로 추산된다. 북한 전체 인구가 약 2,490만 명인데 반해 미국의 사이버사령부 8만여 명 중 전문인원이 대략 6천여 명 수준이라는 점을 감안하면 상당한 규모다. 정찰총국 산하 해커 전문부대인 전자정찰국(121국)이 중심이 돼서 1천여 명의 해커가 남한 주요기관에 바이러스 악성코드 등을 퍼뜨린다. 사이버심리전을 주 임무로 하는 적공국 204호는 전시에는 적군와해 공작을 하며 평시에는 대남선전, 선동을 한다. 110호 연구소는 중국 곳곳에 테러 거점을 구축하고 남한의 군 관련기관에 사이버 공격을 담당한다. 북한의 사이버 조직도는 <그림 6>에서 보는 바와 같다.[181]

181) 김기수, “북한 사이버전 수행능력의 평가와 전망,”『통일정책연구』, 제24권 1호(2015), pp.135-136.

〈그림 6〉 북한의 사이버 조직도



북한의 사이버 공격은 지속적으로 행해져 왔으며, 사이버 관련 조직은 중국 등 제3국에 해외거점을 구축한 가운데 조별로 분산되어 활동하고 있는 것으로 추정된다. 북한은 국내 언론사와 금융기관을 대상으로 사이버 기습공격을 실시하는 등 과시 및 협박용으로 위장하고 있는 것으로 추정된다. 북한의 사이버 기술능력은 공개된 공격기술을 변형하여 우리의 취약점을 공격할 수 있으며, 사회 공학적 기법[182]으로 군사 기밀을 수집할 수 있다. 북한은 외부체계와 연계된 첩보활동을 강화하면서, 신종 사이버무기 개발에도 집중하고 있다. 북한은 사이버전에 대한 명백한 의도와 능력을 갖추고 구체적인 사이버 작전계획과 치밀한 준비를 통해 4세대전쟁 방식[183]과 연계한 사이버전 수행을 계획하고 있는 것으로 추정된다. 반면 평시에 수행하고 있는 간헐적인 인터넷 침해는 이러한 의도를 감추기 위한

182) 사회공학적 기법(Social Engineering): 시스템이 아닌 사람의 취약점을 공략하여 원하는 정보를 얻는 공격기법, 기술적인 방법이 아닌 사람들의 신뢰를 기반으로 사람을 속여(이메일, 페이스북, 트위트 등 사람을 속여) 비밀정보를 획득하는 기법.

183) 4세대 전쟁: 강자가 약자를 이기는 지금까지의 고정관념을 뒤집는 새로운 형태의 전쟁 양상. 적의 군을 패배시킴으로써 승리를 달성하는 기존의 전쟁 개념과는 달리, 적의 정치적 의지에 타격을 주어 승리하는 데 목표를 두는 전쟁 양상.

기만 방책이고 우리가 사이버전을 사이버 테러 및 범죄 수준에서 대응하도록 하기 위한 것임을 간과해서는 안 될 것이다.

한반도에서 사이버전쟁이 벌어질 경우 북한은 비대칭전력으로써 사이버전력을 집중 육성했다는 특수적인 성격과 물리전을 병행하여 공격할 경우 시너지 효과까지 고려하면 북한의 사이버공격역량은 매우 위협적일 것이다.[184] 북한은 전·평시 구분이 모호한 사이버 영역에서 사이버전을 수행하다가 여건이 조성되면 전면전을 수행하고자 할 것이다. 먼저 금융 및 방송망, 전력망, 교통망, 지휘통신망 등 주요 체계에 은밀히 침투하여 컴퓨터 네트워크의 마비와 해킹을 시도하여 정보를 탈취하며 사이버 심리전을 통해 남한사회를 혼란케 할 것이다. 그리고 한국의 핵심기반시설인 스카다체계(SCADA) 전 영역에 동시다발로 공격하여 국가기능을 마비시키려 할 것이다.[185] 위기에서 전시로 넘어가면 보다 공격적인 사이버전으로 군사적 위협을 가할 것이며 군의 정보체계 및 국가기반체계에 대한 공격을 통해 전쟁지휘체계를 마비시키거나 전쟁수행 의지를 약화시키려 할 것이다. 예상되는 북한의 사이버 작전활동은 <표 8>에서 보는 바와 같다.[186]

<표 8> 예상되는 북한의 사이버 작전 활동

평 시 / 위 기 시	① 네트워크를 통해 민간 컴퓨터에 악성코드 오염 ② 네트워크를 통해 정보수집, 금융, 전력, 교통 등 주요체계 장악 ③ 사이버 공간을 통한 정치개입 남한 혁명세력 조정 · 통제 ④ 결정적 시기를 위한 심리전 병행
전 시	① 남한 내 핵심기반시설에 대한 동시 공격 ② 봇넷 등으로 국가와 군 지휘통제체계 공격 ③ 국가 기능의 50% 이상을 일시적으로 마비시킴으로써 혼란 조성, 전쟁지속능력과 의지 약화 ④ 국가와 군의 리더십 마비

이상과 같이 장차전 양상과 사이버 위협을 결합한 북한의 공격 시나리오는 다

184) 부형욱, "사이버안보의 주요이슈와 정책방향," 『국방연구』, 제56권 제2호, pp.118-119.
185) 스카다(SCADA, Supervisory Control And Data Acquisition): 전력, 발전소, 철도, 댐, 유전 등 주요 국가 기반산업에 대한 원격 통합감시제어 체계로 피해 발생 시 큰 사회적 혼란을 야기할 수 있음.
186) 군사적 위협: 국가기반체계에 대한 침투 · 공격(전력망 · 통신망 · 수송망 공격으로 혼란 조성), 군 인터넷, 국방망 · 전장망 침해 · 공격(내부 포섭자활용, 정보수집 및 자료 변조 시도), 전장관리 · 자원관리 체계에 대한 침해 및 해킹, 무기체계 운용 시스템 무력화 시도.

음과 같이 예측해 볼 수 있다. 북한군은 전면전에 앞서 심리전과 사이버 공격을 수행할 것이다. 사이버 공격은 일차적으로 한미연합군의 정보망을 공격하여 미군의 전쟁증원을 지연시키고, 이어서 우리 군의 C4ISR 체계를 타격해 전투기 등 무기체계와 군수지원체계 등을 무력화시켜 한미연합전력을 마비시키고 속전속결로 한미연합군을 신속히 패배시키는 것을 목표로 하는 전략을 수행할 것이다.[187] 미국 백악관의 안보보좌관을 지낸 사이버 보안 및 대테러 전문가인 리처드 클라크는 2010년 6월 미국에서 발간한 그의 저서 '사이버 전쟁: 국가안보의 다음 위협과 대응(Cyber War: The Next Threat To National Security AND What To Do About It)' 에서 사이버 전쟁이 발발하면 15분 내에 재앙적인 결과를 초래할 것이라고 지적한 바 있다.[188]

군사적으로 가장 우려되는 것이 사이버전과 핵과 특수전 등 비대칭전력을 결합한 새로운 방식의 전면전이다. 특히 물리전에 앞서 우리 정부기관이나 국가 기반시설과 서비스 망에 사이버 공격을 가한다면 우리사회는 혼란과 무질서가 극한 상황에 이르게 될 것이다. 인터넷은 물론이고 군사, 통신, 교통, 정유, 금융, 철도, 항공관제, 궤도위성 등 사회 인프라가 가동을 멈추고 통제 불능상태가 될 수 있다는 것이다.[189] 북한은 금융기관을 공격하여 은행이 마비되고 주식시장은 초토화되며, 병원은 환자를 치료할 수 없는 상태에 이르고, 각종 교통수단은 제 기능의 마비로 운행이 제한될 것이다. 항공기는 운항관제가 불통되어 어느 비행기가 어느 공항에 이착륙이 가능한지 혼란스러울 것이며 고속열차제어 통제기가 작동불능이 되어 탈선하거나 지연하는 사례가 속출할 것이며 심지어는 서로 충돌하는 상황도 발생할 것이다. 또한 교통신호 처리체계의 오작동으로 도로는 버스와 승용차, 기타 차량들끼리 추돌하고 뒤엉켜 엉망이 될 수 있을 것이다. 한국수력원자력 발전소가 해킹되어 기능이 정지되거나 파괴되어 전력을 사용하지 못하게 되면 가정이나 직장은 물론 사회 전체가 불편과 어려움에 봉착될 수 있을 것이다. 폭동과 약탈, 파괴, 방화 등 무질서가 곳곳에서 벌어질 것이다. 통신망의 두절과 통신소의 파괴로 민관군이 서로 통합하여 군사작전을 지원하고 수행해야 함에도 소통이 되지 않는 상황이어서 어떻게 후방지원을 할 것이며, 후방에 침투한 적을 어떻게 격멸할 것인가 작전수행과 준비태세에도 많은 문제점과 혼란이

187) "북의 최후 결전은 사이버전이다," 『자주민보』, 2013년 5월 20일.
188) "안보강국의 길을 묻다 한반도 주변국 사이버전력," 『세계일보』, 2013년 10월 22일.
189) 김승주, 앞의 논문, pp.23-24.

야기될 수 있을 것이다. 정부기관과 교통망, 전력과 언론사 등 공공기관이 마비되어 남한사회가 암흑천지로 변하게 되면 병력동원과 동원된 자산의 전방추진을 어떻게 계획대로 완수할 것이며, 방송국과 인터넷의 두절시 국민들은 현 상황을 파악하고 대처할 수 있는 수단은 있는지, 유언비어에 대한 대비는 어떻게 하는 것이 좋은지 어려움이 많을 것이다. 군의 작전시설인 지휘통제시설이 마비되고 군에서 사용하는 필수망인 국방망이 불통되고 전투부대의 전장관리망과 군수지원망이 마비되어 부대 지휘와 작전을 협조하고 시행하기도 어려울 것이다. 또한 미군의 한반도 지원을 위해 공항과 항만에 도착한 병력과 장비가 제대로 전방지역으로 전개가 되어 전투에 투입될지도 의문이다.

이와 같은 혼란한 상황하에서 적의 비대칭 무기인 핵무기와 미사일, 각종 장사정포와 특수전 부대를 침투시켜 공격한다고 가정해 보자. 과연 우리는 계획대로 전쟁을 수행할 수 있을 것인가? 미군의 한반도 전력 전개는 계획대로 이루어져 강력한 한미동맹군으로 북한군을 격멸할 수 있을지 생각해 볼 필요가 있다. 군과 국가의 핵심 요원의 통신수단이 도청되어 자료가 유출되거나 적의 디도스 공격으로 병무행정이 마비되고 방산업체가 해킹을 당해 기술이 유출되는 상황이 발생할 수도 있을 것이다. 북한은 전쟁개시 전에 우리 군의 대응능력을 마비시킨 후 북한군은 재래식 전력으로 전 전선에서 공격을 시작하여 전차와 기계화 부대에 의한 속도전으로 단기결전을 기도할 것으로 예상된다. 미군의 증원을 방해하기 위하여 노동, 대포동, 무수단 미사일로 일본열도, 오끼나와, 괌 등을 공격하여 미증원군이 한국작전전구에 전개하는 것을 방해 또는 차단하려 할 것이다.[190] 북한은 미 증원군의 한반도에 도착 전에 속전속결로 전쟁을 조기에 승리하려고 할 것이기 때문이다.

제2절 한국의 사이버 안보 실태와 문제점

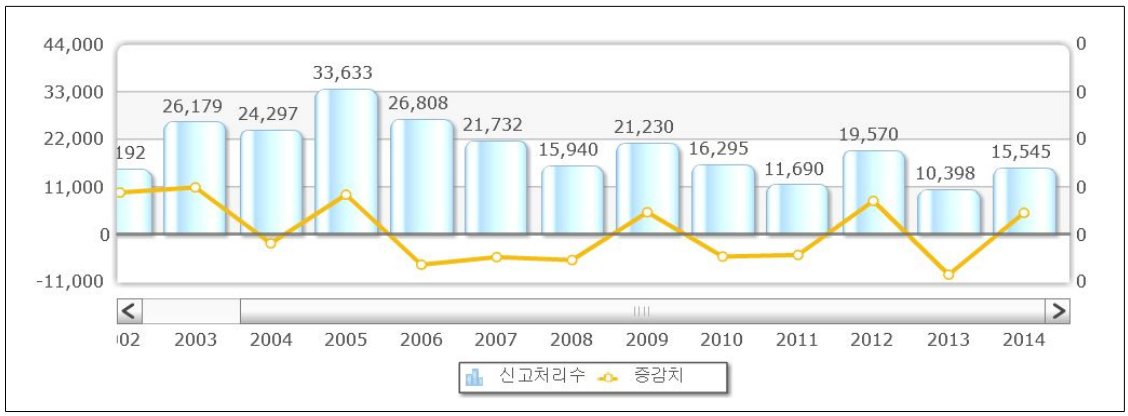
북한은 사이버 공격과 병행하여 앞에서 언급한 바와 같이 '7일 작전계획'이나 '15일 작전계획'을 수립하여 기습적인 속전속결 전략을 구사하려는 의도를 가지고 공격하리라 예상할 수 있다.[191] 그러나 정부는 북한이 2012년 8월 작성한 유사시 핵과 미사일을 사용해 7일 안에 남한을 점령키로 한 '7일 작전계획'과

190) 김진, 앞의 책, pp.191-192.
191) 김종래, 『CEO칭기스칸』 (서울: 삼성경제연구소, 2002), pp.67-71.

관련해 한국과 미국이 해당 정보를 공유하고 공동으로 대비책을 세우고 있다고 한다. 한미 연례안보협의회(SCM)에서 한미 국방장관이 동맹의 포괄적 미사일 대응작전개념 및 원칙을 만들기로 한 것은 북한의 핵과 미사일 개발이 마무리 단계라는 판단 때문이라며 현재 한미 군 당국은 북한의 신작전계획에 대응하는 공동작전계획을 만들고 있다고 한다.[192] 북한 핵과 미사일 위협 상황을 단계별로 평가하면서 이를 탐지하고 무력화하기 위해 어떤 무기를 사용할지 구체적인 시나리오를 포함시킬 예정이며, 주한미군은 물론이고 주일미군이 보유한 전투기와 미사일, 항공모함 등을 동원하는 방안도 검토하고 있다고 한다.[193]

따라서 물리전과 연계한 북한의 사이버 공격을 효과적으로 저지하고 격멸하여 한미연합군의 의도대로 사이버 작전이 수행될 수 있도록 유관기관과의 협조는 매우 중요하리라 판단된다. 우리나라는 북한의 사이버 공격을 비대칭전력의 핵심적인 위협요인으로 분석하고 국가안보와 군사적인 측면으로 접근하여 대응하고 있다. 정부는 2010년에 국군사이버사령부를 창설하고 2011년에는 유관부처 합동으로 '사이버안보마스터플랜'을 작성하여 사이버 위협에 대비하고 있으나, 북한의 사이버 공격기술이 진화하고 있는 반면 정책의 추진효과는 미미하여 북한의 사이버 공격에 매번 당하고 있는 상황이다. 북한을 포함한 연도별 사이버 공격현황(해킹신고 접수현황)은 <그림 7>에서 보는 바와 같다.[194]

<그림 7> 연도별 해킹신고 접수현황



192) 『중앙일보』, 2015년 01월 08일 목요일 001면 종합.
193) 『중앙일보』, 위의 글, 01월 09일 금요일 001면 종합.
194) KISA, 『2015 국가정보보호백서』

이는 정부의 '사이버안보마스터플랜'의 작성에도 불구하고 정부기관별 실질적인 컨트롤타워의 역할과 공조체제상에 상호협조와 정보공유가 잘 이루어지고 있는지 검토할 필요성이 있다. 북한의 사이버 능력은 대남적화통일을 실현하기 위한 새로운 수단이며 위협의 본질은 단편적인 공격과 대응이 아니라 한국사회를 일시에 무력화시키려는 전략적 의도가 숨어있을 수 있기 때문이다. 한국은 아직까지 북한의 사이버 공격에 국가기반시설의 파괴나 인명의 손실 등의 국가적인 위기를 겪어보지 못했기 때문에 대응태세가 미흡하지 않나 판단된다. 우리 사회는 상시 사이버전에 노출되어 있는 상태라고 평가할 수 있다. 정부와 군, 민간 등 관련부서는 전략과 컨트롤타워, 법령과 제도, 공조체제, 인력 등 분야별로 발전시킬 많은 문제점을 안고 있는 실정이다. 따라서 우리의 사이버전 실태를 네가지 핵심요인인 ① 인식과 사상의 관점, ② 국가전략 등 시스템의 관점, ③ 공조체제인 네트워크의 관점, ④ 인력과 기술 등 지원적인 관점에서 접근하여 분석하고자 한다.

1. 인식과 사상의 관점

전 세계적으로 사이버전은 가장 심각한 안보위협 요인으로 인식되고 있으며 선전포고 없이 전력망, 통신망, 교통망, 송유관 및 가스관, 상하수도 체계 등 주요 국가기반시설을 순식간에 기능을 마비시키거나 파괴할 수 있다. 한국은 정보통신기술 강국임에도 불구하고 국민들의 사이버 안보에 대한 인식은 미흡한 편이다. 2004년에 중국 발 대규모 공공기관 해킹사건이 발생하기 이전에 국가차원의 사이버전 대응체계는 제대로 갖춰지지 않았고 인식도 매우 낮은 수준이었다.[195] 그러나 금융, 방송, 원자력발전, 의료, 가스, 교통, 항공 등 기간산업에 대한 사이버공격이 늘면서 사이버보안 능력이 국가안보 및 사회 안전의 핵심으로 떠올랐다. 북한은 <표 9>에서 보는 바와 같이 한국의 국가·공공·민간의 주요기반시설에 대한 공격대상 분석을 면밀히 하여 사이버 공격을 감행할 것으로 판단된다. 항공·철도·항만·도로 등 교통과 수송 시설, 원자력 발전소·전기·석유·가스 등 에너지 시설, 댐 등 수자원시설, 통신국과 관문국·망관리 센터 등 정보통신시설, 보건·의료시설, 금융시설, 방송·언론시설, 산업시설, 연구시설, 정부기관, 민간시설 등이 포함될 것이다.

195) 부형욱, 앞의 논문, p.98.

<표 9> 사이버 공격 시 주요 대상 분석(국가・공공・민간)

구분	대상	구분	대상
교통 수송	항공	보건 의료	응급의료정보센터
	철도		병원
	지하철		혈액관리시설
	항만	금융 시설	금융전산망
	물류		은행
	도로		증권거래소
	교량	방송 언론	방송시설
	터널		언론사
원자력	원자력발전소	산업 시설	대규모산업시설
	원자력본부		군수산업체: 중화기 시설
	핵폐기물 보관시설		군수산업체: 총・포・화약류 시설
에너지 시설	전기		군수산업체: 기타 전투장비 시설
	석유	연구 시설	원자력, 국방과학 연구소 등
	가스	기타	교정시설
수자원 시설	정수시설		대도시 지하 공동구
	댐	정부	행정정보망
화력	화학물질 보관시설		외교정보전용망
정보 통신 시설	통신국		정부통합전산센터
	망관리센터		G4C 시스템
	인터넷 관문국		정부시설(청와대, 국회 등)
	해저케이블		정부기관 홈페이지
	주요 DNS 서버	민간	민간PC
	국가보안통신망: 국가통신망		개인 스마트폰
	국가보안통신망: 경호통신망		SNS
	재난통신망		인터넷 포털 / 홈페이지
	민방위경보통신망		데이터센터(분당 IDC 등)
	인공위성, 국제위성지구국		민간보안업체(백신업체)

한국은 북한을 비롯한 국제적인 해킹그룹의 사이버 공격으로 많은 피해를 입었다. 원자력발전소를 비롯한 금융기관, 방송국, 정부기관 등이 매년 계속되는 사이버 공격으로 피해를 당하고 있음에도 불구하고 사이버 안보를 위해 국가의 시스템을 어떻게 구축할 것인지 명확한 계획수립과 세부 시행계획이 아직도 미흡한 것으로 판단된다. 특히 전력망은 매우 중요하며 문제가 생겼을 때 인터넷과 네트워크로 연결되어 관리되는 모든 기간 산업분야에 큰 영향을 미치게 될 것이다. 한국인터넷 진흥원의 조사에 의하면 3세 이상 우리국민 중에 인터넷 이용자

비율은 전체 인구의 82%로 네트워크 의존 사회의 전형을 보여주고 있다. 그럼에도 불구하고 유사한 사이버 위협 상황이 자주 발생하고 있는 것은 우리의 대응 능력 수준이 미흡하다는 증거다. 이와 같이 자주 발생하는 사이버 공격으로 해당 기관과 정부에 대한 신뢰도는 물론이고 피해액도 급증하고 있는 실정이다.[196] 최근 수년간 북한으로 추정되는 공격으로 알려진 피해는 정부 추계로 약 8,600억 원에 이른다고 한다.[197] 우리나라의 정부와 기업들은 정보보호 예산을 편성하고 집행하는데 대단히 미흡한 실정이다. 미래창조과학부의 국내 정보보호 실태조사 결과 2014년 기준 정보보호 예산이 IT예산의 5% 이상인 기업은 조사대상 기업 중 2.7%에 불과했다. 같은 기준으로 미국과 영국은 각각 40%와 50%가량이 정보보호예산 비중을 전체 IT예산의 5%이상으로 책정하는 것과는 대비를 이룬다. 일례로 국내 18개 은행의 정보보안 투자예산은 2,500억원 규모로 미국의 뱅크오브아메리카(BoA) 은행의 정보보안 투자예산 4,000억원 규모에도 미치지 못했다. 2010년부터 3년간 국내 금융권의 정보보호예산 대비 집행비율이 62%에도 미치지 못했다는 점에서 정보보호 투자가 제대로 이뤄지지 않고 있는 것으로 분석됐다.[198] 이러한 실정에도 불구하고 사이버 안보를 위한 정부와 민간의 예산편성을 위한 종합적인 대책은 미흡한 실정이다. 그러나 다행스럽게 2013년 3・20과 6・25 사이버 테러, 2014년 말 소니픽처스 공격, 한수원 공격 등 북한의 거듭되는 사이버 공격으로 우리 사회에서 어느 정도 사이버 공격의 위험성과 폐해에 경계감이 형성되고 있는 실정이다. 그러나 우리는 북한의 공격에 제대로 대응한 적이 없었고 보복할 의지도 없었던 것이 사실이다. 따라서 북한의 사이버 공격에 피해를 최소화하고 즉각적인 대응을 할 수 있는 국가와 군을 육성하는 것은 우리에게 주어진 사명이며 과제라고 할 수 있다.

2. 국가전략 등 시스템의 관점

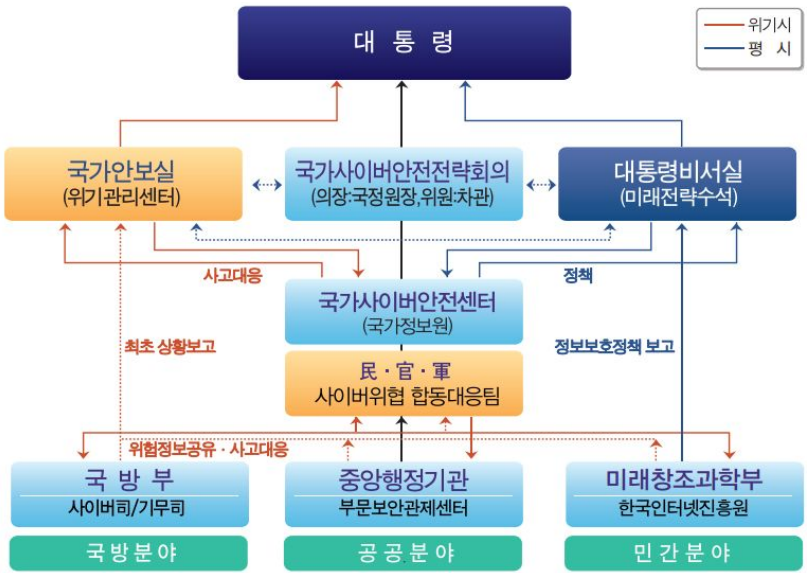
정부는 사이버 위협에 대비하여 위기와 평시의 수행체계를 구축하여 북한의 사이버 공격에 대비하고 있다. 이를 살펴보면 국정원장이 의장으로 있는 국가사이버전략회의에서 총괄을 담당하며 사이버 상황이 발생하면 민・관・군 합동대응팀을 운영하여 상황의 본질을 파악하고 필요한 조치를 수행하게 된다. 국방 분

196) 임채호・전상훈, 『사이버전쟁의 위협과 대응전략』 (서울: 인포더북스, 2013), pp.23-26.
197) 박인휘, 『세계일보』, 2015년 1월 7일 (수) 오피니언 30면.
198) 김명철, 『중앙일보』, 2015년 1월 16일 금요일 29면 사설/칼럼.

야는 국군사이버사령부에서 공공부문은 중앙행정기관의 보안관제센터에서 담당하고 민간분야는 한국인터넷진흥원에서 담당하게 된다. 국가 사이버안보 수행체계도는 <그림 8>에서 보는 바와 같다.[199]

이를 구체적으로 살펴보면 정부는 사이버 위협의 심각성을 인식하여 2005년 1월 '국가사이버안전전략회의'와 '국가사이버안전대책회의'를 설치하고 국가정보원, 국방부, 정보통신부를 중심으로 공공부문, 국방, 민간부문의 사이버안전 관련 핵심 업무를 관장하게 하였다.[200]

<그림 8> 국가 사이버안보 수행체계도



'국가사이버안전전략회의'는 국가정보원장을 의장으로, 외교통상부 차관, 법무부 차관, 국방부 차관, 안전행정부 차관, 미래창조과학부 차관, 국가안전보장회의 사무처의 사무차장 및 전략회의 의장이 지명하는 중앙행정기관의 차관급 공무원 등으로 구성되어 있다. 이들은 국가사이버안전관리체계에 대해 각 기관의 역할조정, 사이버안전체계의 수립 및 개선사항에 대한 거시적인 전략을 마련한다. '국가사이버안전대책회의'는 국가사이버안전전략회의 예하에 있는 조직으로 국가

199) KISA, 『2015 국가정보보호백서』, p.11.
200) 오명호 외, 앞의 책, pp.56-58.

정보원의 사이버안전업무를 담당하는 차장이 의장이 되고 각 기관의 사이버 안전관련 실·국장급 공무원으로 구성된 실무대책반이라고 할 수 있다.

국가정보원은 관련 법령에 따라 국가정보보안 업무의 기획, 조정, 수립, 시행 등 국가와 공공기관에 대한 정보보안업무를 총괄하고 있으며 민간부문에 대해서는 직접적인 관리를 하지 않지만 간접적인 지원 활동을 하고 있다. '국가사이버안전센터'는 국가정보원내에 설치한 총괄기관으로 국가 사이버안전과 관련된 체계적이고 종합적인 대응을 위해 정책을 수립하고 지원하며 정보보안위협 관련 정보의 수집, 분석, 전파, 국가정보통신망의 안정성 확인, 국가 사이버매뉴얼 작성 및 배포, 사이버 공격으로 인한 피해 조사와 복구 지원, 외국 관련 기관과의 업무협조를 중점사항으로 추진하고 있다.

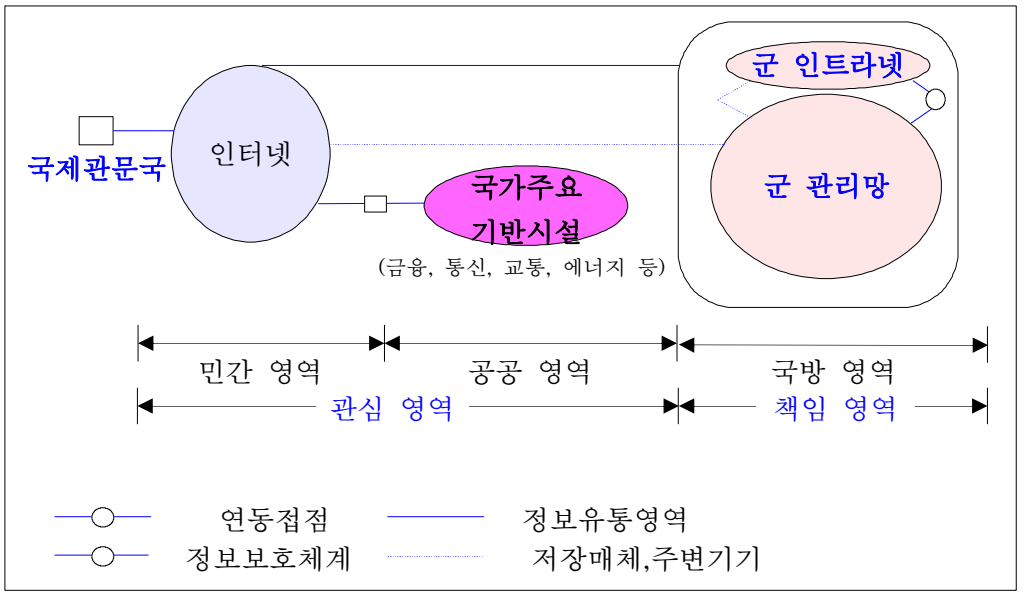
이 중에서도 '국가사이버안전센터'의 '사이버위협 경보발령시스템'은 이 센터가 국가의 사이버 안전을 담당하는 총괄기관임을 의미하는 중요한 기능이다. 국가정보원장은 사이버 공격에 대한 체계적인 대응을 위하여 사이버 공격의 위험, 피해규모 수준을 고려한 경보체제를 마련하고 색깔구분을 통한 경보단계를 수립하였다. 즉 '초록색(정상)', '청색(관심)', '황색(주의)', '주황색(경계)', '빨간색(심각)으로 색채별 경보를 발령하고 있다. 정상에 해당하는 초록색은 국가 전 분야에서 정상적인 활동이 이루어지고 있으며 위험도가 낮은 웜이나 바이러스가 발생한 상황이므로 국가 차원의 대응이나 전략회의가 필요하지 않은 단계를 의미한다. 그러나 청색 이상의 단계부터는 실질적인 경계 단계로 진입하며, 피해 수준에 따라 네 단계로 구분된다. 가장 낮은 수준의 경계 단계인 '관심(청색)'은 웜, 바이러스, 해킹에 의해 피해 발생 가능성이 증가하고 해외로부터 사이버 공격 피해가 확산되어 국내 유입이 우려되는 상황에서 발령하며 사이버 위협에 대한 탐지활동이 강화되는 단계를 의미한다. 주의 단계는 황색으로 표시하며 일부 네트워크 및 정보 시스템에 장애가 발생하여 침해사고가 다수 기관으로 확산될 가능성이 있을 때 발령한다. 이 상황에서는 국가 정보시스템 전반에 보안태세를 강화한다. 경계 단계는 주황색으로 표시하며 특수 정보통신서비스 제공자 또는 기간망의 장애와 마비로 인해 대규모 피해로 발전될 가능성이 증가될 때를 의미한다. 이 경우 다수의 기관이 서로 공조하여 대응하도록 조치한다. 마지막으로 심각 단계는 빨간색으로 나타내며 국가적 차원의 네트워크 및 정보시스템이 사용불능의 상태를 뜻한다. 침해사고 및 기능장애사고가 전국적으로 발생하여 대

규모 피해를 입는 경우로 국가적 차원의 공동대처를 필요로 하는 가장 심각한 단계를 의미한다.

사이버공간은 기회와 위험이 상존하는 국가안보의 핵심영역이다. 즉 개인과 사회구성원이 일하고 생활하는 공간이자 사회기반서비스와 국가기반시설, 군의 전술 및 전략체계 등 모두가 연결되어 상호 의존할 수밖에 없는 공간이다. 특히 사이버공간은 위기시나 전시에 군사작전 측면에서 어떠한 경우에도 전쟁수행 및 전쟁지속능력과 아군의 행동의 자유가 보장되어야 하는 공간이다. 이를 영역별로 살펴보면 국방부는 국방분야를 담당하고 국가 주요기반시설이 위치하고 있는 공공영역은 국가정보원이 담당하며 인터넷과 개인의 스마트폰, 민간 데이터센터 등 민간영역은 미래부 산하의 한국인터넷진흥원이 담당하고 있다.

<그림 9>에서 보는 바와 같이 북한의 사이버 공격시 군은 자체 인트라넷을 포함한 군 관리망에 대한 책임영역과 국가기반시설과 인터넷이 위치한 공공 및 민간 영역은 관심영역으로 구분하여 전 영역을 식별하고 대응할 수 있어야 한다.

<그림 9> 사이버전 수행을 위한 임무영역 식별



공공의 영역에 있는 정부의 각 기관은 자체적으로 사이버 관제센터를 운영하고 있다. 그렇기 때문에 사이버 관련 업무가 부처별로 산재되어 있어 효과적인 조정

통제가 어려운 실정이다. 아래 <그림 10>에서 보는 바와 같이 정부의 각 기관은 33개의 보안관제 센터를 운영하고 있다.[201]

<표 10> 정부기관별 보안관제센터 운영현황(33개)

부문	담당기관	관제센터
행정	행정자치부	정부통합전산센터(대전)
		정부통합전산센터(광주)
		사이버침해대응센터(G-CERT)
국방	국방부	사이버사령부
외교	외교부	외교 사이버안전센터
국토교통	국토교통부	국토교통 사이버안전센터
보건・의료	보건복지부	보건・의료 사이버안전센터
교육	교육부	교육 사이버안전센터
에너지	산업통상자원부	산업통산 사이버안전센터
통신과학	미래창조과학부	미래창조과학 사이버안전센터
		KISA 인터넷침해대응센터
		과학기술 정보보호센터
금융	금융위원회	금융 ISAO(금융결재원)
		증권 ISAO(KOSCOM)
치안	경찰청	경찰 전산보호센터
특허	특허청	특허 관제센터
관세	관세청	관세 관제센터
국세	국세청	국세 관제센터
방위산업	방위사업청	방위사업 관제센터
재정	기획재정부	재정 관제센터
문화	문화체육관광부	문화체육관광 관제센터
기상	기상청	기상 관제센터
노동	고용노동부	노동 관제센터
공공	국가보안기술연구소	보안관제 기술지원센터
환경	환경부	환경 관제센터
법무	법무부	법무 관제센터
통일	통일부	통일 관제센터
농식품	농림축산식품부	농식품부 사이버안전센터
검찰	대검찰청	대검 사이버안전센터
병무	병무청	병무청 사이버안전센터
해양	해양수산부	해양수산 사이버안전센터
중소기업	중소기업청	중기청 사이버안전센터
공정위	공정거래위원회	공정위 사이버안전센터

201) KISA, 앞의 책, p.68.

다음은 사이버 컨트롤타워의 운영실태를 살펴보고자 한다. 정부는 2015년 3월 사이버전에 대응할 수 있는 컨트롤타워 역할을 목적으로 청와대 국가안보실에 사이버 안보비서관을 신설하고 국가안보실에서 사이버전 관련 컨트롤타워의 역할을 수행하고 있다. 2015년 5월 국가안보실 주관으로 국정원, 군, 경찰, 미래부, 행자부 등 정부 부처 고위 관계자들이 모여 청와대 국가안보실을 중심으로 관련 부처의 역할을 분담하여 사이버전 대응을 강화하는 방안을 논의했다. 하지만 관련 부처와의 업무조정과 법령의 미비, 국정원측이 제시한 법적 근거의 부족이유, 관련기관의 제 역할 등으로 회의가 성과 없이 끝났고 국가안보실의 개선 방안 추진도 미약한 상태라 하였다.[202] 정부는 국가안보실에 대통령을 보좌하는 사이버 안보비서관을 편성하고 운용하지만 실질적인 실무총괄은 국가정보원이 수행하고 있다. 국가정보원이 수행하는 이유를 미국의 사례에서 살펴보면 미국은 다양한 기관에서 사이버 정보를 수집하고 있으나 가장 큰 규모의 정보 수집은 국방부 소속기관인 국가안보국(NSA)에서 수행하고 있다고 한다.[203] 이러한 체제는 평시에 정보기관이 사이버 국가안보를 국가정보 차원에서 관여하는 것이 적절하다는 판단에 근거한 것으로 평가된다. 물론 우리도 마찬가지이며 사이버 국가 안보에 관한 출발은 국정원이 시작하여 지금까지 많은 변화와 발전을 이룩했으며 능력도 우수하다고 판단한다.

그러나 사이버 공격의 성격이 사이버 범죄나 테러의 성격에서 벗어나 사이버전의 성격으로 진화되고 있으며 한국의 안보 현실을 고려할 때 북한의 도발이 사이버전과 물리전을 결합한 기습적인 공격양상으로 전환될 것을 고려하면 국가정보원에서 한국의 사이버 안보를 총괄하는 것이 효율적인가를 검토할 시점이 된 것으로 판단된다. 국가정보원의 대국민 이미지는 국가의 서비스 기관이라기보다는 권력기관으로 인식된다는 점이 우려스러운 부분이다.

한편 미국은 9.11테러 이후 사이버 업무와 테러업무를 주관하는 부서로 국토안보부(DHS: Department of Homeland Security)가 창설되어 미국의 전체국가기반을

202) “사이버 컨트롤타워 무엇이 문제인가?,” 『보안뉴스』, 2015년. 5월. 6일.

203) 위키백과, NSA 인터넷자료(검색일. 2015.10.29.), 국가안보국은 미 정보기관 중에서 가장 큰 규모와 정보수집력을 가지고 있으며 석사급 학력을 가진 3만8천여명의 요원이 근무하며 정보수집 대상국의 암호를 해독하기 위해 세계 최대의 수학자 채용기관이고 슈퍼컴퓨터를 보유하고 있으며 한해 예산은 대략 80억 달러를 사용하고 있다고 한다. 국가안보국장은 대장이 지휘관이며 매일 17조개의 이메일, 전화통화 수집, 신호정보수집의 임무를 수행하며 2013년 프리즘과 관련하여 국가안보국의 무영장 감시 논란이 문제가 되고 있는 기관이다.

보호하기 위해 제정된 법으로 총 17장으로 구성된 국토안보법(Homeland Security Act of 2002)이 있으며, 테러위협에 대응하기 위한 수사력 강화와 국가안보의 확립을 목적으로 한 법률인 애국법(USA Patriot Act), 국가안보 관련기관과 법 집행기관의 정보보호 노력을 조정함과 동시에 사이버 위협에 대해 효과적으로 대응할 수 있도록 한 법률인 연방정부보안관리법(Federal Information Security Management Act of 2002) 등이 있다.[204] 특히 국토안보부에 프라이버시 담당관과 민권 및 자유 담당관을 둠으로써 국민이 국가기관에 대해 갖는 근본적인 의구심을 해소시켜 주며 세련된 정책실행을 위한 고도의 조직체계를 구성하고 있는 것과 비교할 필요성이 있다.

다음은 사이버 법령체계의 실태를 알아보도록 하겠다. 국가 사이버안보에 관한 사이버위기대응체계와 관련하여 '국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버 공격으로부터 국가정보통신망을 보호함을 목적'으로 대통령훈령인 '국가사이버안전관리규정'이 있다.[205] '국가사이버안전관리규정'은 대통령 훈령 제291호(2012년 1월2일 일부개정)로 국가정보원장은 사이버안전정책을 효율적이고 체계적으로 수행하기 위하여 사이버 안전 기본계획을 수립하고 시행하도록 하며 사이버 위협에 대한 국가 차원의 종합판단, 위협요인 분석 및 합동조사 등을 위하여 사이버 안전센터에 민·관·군 합동대응반을 설치 및 운영하며 사이버 공격에 종합적이며 체계적으로 대응하기 위하여 중앙행정기관, 지방자치단체 및 공공기관의 사이버 위기 대응훈련을 강화하는 등 현행 제도의 미비점을 개선하고 보완하는데 중점을 두고 있다는 내용을 포함하고 있다.[206]

훈령은 상급관청이 하급관청을 대상으로 권한행사를 위한 일반적인 명령으로 민간에는 어떠한 구속력도 행사할 수 없으며 법령이 아니므로 국민의 기본권을 제한 할 수 없다. 이는 국가 및 공공기관에만 영향을 미치는 '대통령훈령'에 불과해 민간까지 포괄하는 효율적이고 신속한 업무수행에 제약을 받는다. 헌법은 사생활의 비밀과 자유를 침해받지 아니할 권리를 보장하고 있기 때문이다. 그러

204) 이완수, "국가사이버 안보 구축전략에 관한 연구," 경기대학교 대학원 박사학위 논문 (2013), p.40.
205) 오명호 외, 앞의 책, pp.56-57.
206) 이완수, 위의 논문, p.80.

나 이를 제한하기 위해서는 법률로 규정할 수밖에 없다.[207] 이런 이유로 첫째. 국내에 진출한 외국계 정보통신 사업자들과 국내 사업자들이 정당한 이유 없이 합법적인 안보수사 협조요청에 응하지 않아도 규제할 수단이 없다. 형사법적 대응은 한계가 있다. 둘째, 수사와 재판에 많은 시간이 소요됨에 따라 즉시 강력한 제재로 효과를 보기도 어렵고 외국에서 발생할 할 경우 시간이 많이 걸리고 해당국과 관련 협약이 없을 경우에는 처벌이 불가능하다. 셋째, 정보통신망법에 따르면 안보수사 당국의 정당한 사이버상에서 정보수집행위도 해킹으로 불법화하고 있기 때문에 국가안보상 핵심위협 요인으로 부각된 사이버상에서 안보위협과 활동을 효율적으로 제어하기 위한 안보수사 측면의 법적근거 마련이 시급하다.[208] 따라서 사이버전을 효과적으로 대비하기 위해서는 민간의 협력이 필수적이며, 국민의 기본권이 때로는 침해될 수도 있는 만큼 대통령 훈령이 아닌 법률로 제정하는 것이 바람직할 것으로 보인다.

국회는 사이버안보에 관한 법률을 제정하기 위한 논의를 계속해 왔다. 17대 국회에서 '국가사이버위기관리법'이 발의되었으나 국정원이 이를 관리한다는 야권의 비난을 받으면서 자동 폐기된 적이 있다. 그러나 사이버안보를 확보하여 국가의 안전보장과 국민의 이익에 이바지할 수 있는 법적근거가 필요하여 18대 국회에 들어와서 다시 상정하였으나 야당의 반발로 폐기되었다. 19대 국회에 들어와 2013년 3월 하태경의원이 발의한 "국가 사이버 안전관리에 대한 법률안"과 2013년 4월 서상기 의원이 발의한 "국가 사이버테러 방지에 관한 법률안"이 있다. 그러나 두 의원이 발의한 법안도 2015. 7월 국정원 해킹사건으로 사이버테러 법안이 여야 정치권의 정쟁에 휘말려 논의조차 하지 못한 채 계류 중에 있다. 여야가 합의를 하지 못하는 이유는 해당 법률안들이 국정원의 권한 강화를 주는 내용들로 구성되어 있기 때문이다. 양 법률안 모두 사이버공격과 사이버테러에 국가차원의 종합적인 대응체계를 구축하여 사이버 위기발생 가능성을 조기에 차단하는 등 사이버 안전을 확보하려는 측면에서 발의한 법률안이다. 하태경 의원은 이러한 책임과 의무를 중앙행정기관, 지방자치단체와 공공기관에 부여한 반면, 서상기 의원은 공공부분과 주요 민간부문을 포함한 사이버 테러방지 및 위기

207) 헌법 제37조 제2항; 국민의 모든 자유와 권리는 국가안전보장. 질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법률로써 제한할 수 있으며 제한하는 경우에도 자유와 권리의 본질적인 내용을 침해할 수 없다.

208) 유동열, 『문화일보』, 2015년 05월 06일(수) 오피니언 37면.

관리 책임기관인 국정원에게 각종 책임과 의무를 부과한 차이점이 있다.[209] 하태경・서상기 의원이 제기한 발의법안의 차이점은 <표 11>에서 보는 바와 같다.[210]

<표 11> 하태경・서상기의원이 제기한 발의법안의 차이점

구분	하태경 의원안	서상기 의원안
적용범위	중앙행정기관 외에 주요 정보통신기반시설, 민간정보통신망 등 포함	
국가사이버안전센터	국가정보원장 소속 (민・관・군 합동대응기구 유지)	
사이버위기대책본부	국가정보원 주도로 운영	
기본계획	국가정보원장이 수립	
국가사이버안전 전략회의	국가정보원장 소속	국무총리 소속
국가사이버안전 대책회의	국가정보원장 소속 (전력회의 산하)	관련규정 없음
민・관 협의체	구성・운영 명시	관련규정 없음
보안관제센터	설치범위 확대 (주요정보통신기반시설, 민간정보통신망 포함)	현형유지 (공공부문만 운영)
연구개발	연구기관을 통한 추진 명시	시책강구를 선언적으로 정함
국방부문 특례	폐지 (국방부문에도 법안 적용)	현행유지 (국방부분 국방부장관이 주관)

두 의원이 제기한 법률안의 공통적인 내용을 구체적으로 살펴보면 사이버 테러나 사이버 위기시 기본적으로 안전행정부, 미래창조과학부, 국방부 등 국가행정사무의 체계적이고 능률적인 수행을 위하여 국가행정기관의 설치. 조직과 직무범위는 정부조직법에 규정하고 있다. 따라서 사이버안전에 대한 총괄대응을 국정원에서 담당하게 한 법률안은 국가정보원법을 넘어선 것으로 새로운 직무와 권한을 만들어 낸 것으로 문제점이 되고 있다. 여러 중앙행정기관의 정책조정이 필요한 경우에는 국무조정실에서 하도록 규정하고 있어 국정원에서 사이버테러에

209) 오태곤・성관실, "국가 사이버안전 관리 법제의 개정방향에 관한 소고," 『Journal of The Korea Society of Computer and Information』, March 2014, p.169.
210) 이완수, 앞의 논문, p.86.

총괄대응을 맡게 한 동 법률은 정부조직법과 상충되는 면이 있다. 또한 정보기관은 자체 특성상 입법, 사법, 행정기관 등을 통해 국민의 감시와 통제가 어려우며 부처 간 정보공유에도 부적절한 측면이 있다. 또한 국정원장에게 사고조사 권한의 전권을 부여함으로써 헌법에 명시되어 있는 국민의 기본권 침해문제를 고민해 볼 필요가 있다. 그 밖의 사이버테러와 사이버위기에 대한 개념과 정의의 문제, 정보의 협력부분에서 위협정보에 대한 국정원의 보고요구 등 의미와 규정에도 문제점이 식별되고 있는 실정이다.

아울러서 사이버 안보와 관련한 입법추진 실태를 살펴보면, 현행법상 사이버공격 대응에 관한 정보보호 관련 주요 법률로는 <표 12>에서 보는 바와 같이 국가기밀보호, 중요정보의 국외유출방지, 전자서명 및 인증, 정보통신망과 정보시스템의 보호추진, 침해행위의 처벌, 개인정보보호와 형법 등이 있다.[211]

<표 12> 정보보호 관련 주요 법령

구분	법령명
국가기밀보호	군사기밀보호법, 보안업무규정, 군형법 등
중요 정보의 국외유출 방지	산업기술의 유출방지 및 보호에 관한 법률, 기술의 이전 및 사업화 촉진에 관한 법률, 민·군겸용기술 사업 촉진법, 부정경쟁방지 및 영업비밀보호에 관한 법률 등
전자서명 및 인증	전자서명법, 전자정부법 등
정보통신망과 정보시스템의 보호추진	국가정보화 기본법, 정보통신기반 보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 전자정부법, 전사문서 및 전자거래 기본법, 국가사이버안전관리규정 등
침해행위의 처벌	정보통신기반 보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 전자무역촉진에 관한 법률, 형법 등
개인정보보호	개인정보 보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 신용정보의 이용 및 보호에 관한 법률 등

이러한 법들의 문제점은 관련규정이 하나의 법률로 체계적으로 정비되어 있지 않고 수많은 법률에 산재되어 있어 적용이 어렵고 혼란스럽다는 것이다.[212] 특히

211) KISA, 앞의 책, p.48.
212) 위의 책, p.48.

적용대상별로 개별적이고 산발적인 규정으로 조직적인 대응체계가 미흡하며 사이버 보안과 관련된 다양한 주체들의 임무와 기능이 명확하지 않아서 균형있는 규제가 이루어지고 있지 않은 실정이다. 또한 기관별로 소관부처 중심의 업무를 수행함으로써 국가차원에서 전, 평시 사이버전에 효율적으로 대처하기 위해서는 정보화촉진기본법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 국가사이버안전관리 규정 등 10여개로 분산되어 있는 사이버전 관련 법령을 가능한 한 '단일법령'으로 통합해야 할 것으로 보인다.[213] 즉 단일 법령에 의한 부처별 협조체제, 정보의 공유, 국제협력 및 공조체제 등을 총괄할 수 있는 사이버전에 관한 컨트롤타워 법안이 필요한 실태다.[214]

한편 민간, 공공이 합동으로 대응할 수 있는 대규모의 침해사고 정보공유시스템이 필요하다는 논의도 진행되고 있다. 기존 정보공유분석센터는 정보통신기반보호법 16조에 따라 정부 산하기관의 단체를 중심으로 33개가 설치돼 운영 중이다. 또한 안전행정부 산하 한국지역정보개발원이 지방자치단체들을 위한 정보공유분석센터를 신설했고 이밖에도 금융, 증권 등에서 악성코드 분석이나 침해사고 대응에 필요한 정보를 공유하고 분석해 전달하는 센터를 각각 운영 중이다.

최근 논의는 이렇게 각 기반시설에 구축된 정보공유분석센터를 모아 국가 단위의 사이버 공격에 대응할 수 있는 상위 정보공유분석센터를 마련할 필요가 있다는 것이다. 이와 관련하여 전문가들은 기존에 방화벽, 침입탐지시스템(IPS)과 같은 하드웨어기반의 보안체계가 갖춰져 있었다면 최근에는 지능형지속가능위협(APT) 공격이나 사이버테러 위협은 데이터를 전체로 취합해서 봐야만 공격 징후들을 종합적으로 판단할 수 있다. 이와 같이 사이버공격의 패러다임이 바뀌고 있는 만큼 이에 대비하려면 정보공유를 통한 소프트웨어적인 접근법에 대한 내용이 포함되어야 한다는 의견이 있다.[215]

한편 국제질서를 이끄는 G2인 미국과 중국 간에는 사이버전쟁이 한창이다. 문제는 새로운 전쟁터가 국제법의 역할이 전혀 미치지 않는다는 점이다.[216] 2013년

213) 김기수, 앞에 논문, p306.
214) 윤영준·이정희, "국가사이버 위기관리법 제정시 고려사항에 관한 연구," 『디지털포렌시스저널』(2014년 6월), pp.75-76
215) 안철수연구소, 『보안뉴스』, 2013년 6월 27일. 관련기사 참조 미국의 경우 민·관·군을 하나로 묶어 분석센터를 마련하였는바, 2009년 설립된 국토안보부 산하 국가사이버보안 및 통신통합센터(NCCIC)와 사이버사령부가 하나의 조직으로 운영되고 있다.
216) 김홍석, "사이버테러와 국가안보," 『전투발전지』, 제137호(2011), p.102.

린 매뉴얼 발간을 계기로 사이버전쟁 교전수칙을 어떤 방향으로 만들 것이냐를 놓고 미·영과 중·러 간에 이견이 노출되고 있다.[217] 미국과 영국은 제네바·헤이그 협약 등의 국제법을 사이버 공간에도 그대로 원용하자는 입장이다. 중국과 러시아는 사이버 공간은 완전히 별개의 공간이어서 새로운 차원의 조약을 만들자고 주장한다. 그 이유는 미·영 중심의 현 국제법 질서를 바꿔 보려는 의도다. 탈린 매뉴얼은 기본적으로 미·영의 입장을 반영하고 있다. 사이버전쟁 교전규칙을 준비 중인 미국은 탈린 매뉴얼을 가장 중요한 근거 자료로 삼을 예정이다. 영국도 탈린 매뉴얼을 기초로 한 교전수칙 논의에 찬성하고 있다.[218] 그러나 미·영의 이니셔티브에 중, 러가 동의할 가능성은 없다고 판단한다. 국제사회는 뒤늦게 국제법적 룰을 적용해보려는 시도를 시작했다. 양대 그룹으로서는 논의를 서둘러야 한다는 공감대가 커지고 있기 때문에 해결방안이 도출될 것으로 예상된다.

3. 공조체제 등 네트워크의 관점

먼저 정보보호 인프라 실태다. 한국은 사이버 네트워크 기반이 고도로 발달되어 있고 국민들의 사이버 활용 성향도 매우 높다. 정보통신기술 인프라가 잘 발달된 국가일수록 사이버 공격의 취약성도 증가하여 위협의 강도가 높아지는 경향이 있다. 국내에서 개인정보 유출과 해킹 등 사이버 보안사고가 잇따른 가운데 한국의 정보기술 (IT)의 정보보호 여건은 해외에 비해 여전히 취약한 것으로 나타났다. 한국개발연구원(KDI)과 정보기술업계에 따르면 한국은 정보보호특허 중 암호화기술특허 건수가 6,947건이지만 미국은 56,740건, 일본은 26,255건, 유럽은 16,157건이었다. 중국도 12,771건 암호화기술 특허를 보유하고 있다. 국내 암호화기술 특허건수가 미국의 10분의 1, 중국의 절반가량에 그쳤고 보안서버 수 또한 유럽의 5분의 1, 일본의 4분의 1의 수준으로 전반적인 여건 자체가 크게 개선되지 않은 것으로 분석됐다. 물리적 보안인프라도 여전히 부실한 것으로 집계됐다. 경제협력개발기구(OECD)에 따르면 지난 2012년 기준 인구 10만 명당 보안서버

---

217) 북대서양조약기구(NATO) 합동사이버방위 센터(CCDCOE)는 2013.3 15일 총 95개 조항의 교전수칙을 담은 '탈린 매뉴얼'(tallinn manual)을 발표했다. 탈린 매뉴얼은 에스토니아 수도 탈린에서 발생한 사이버 테러를 계기로 국제사회가 교전수칙 논의를 시작해 붙여진 이름이다.

218) 박노형·정명현, '사이버전의 국제법적 분석을 위한 기본개념의 연구, "『국제법학회논총』, 제59권제2호(대한국제법학회, 2014.6), pp.69-71.

수도 한국은 21개에 그쳤다. 미국은 166개, 독일 113개, 일본은 83개의 보안서버를 구축한 것으로 나타나 편차가 크다. 이에 따른 국내 인터넷 이용자의 피해 규모도 해외 이용자에 비해 다소 큰 것으로 나타났다.

자칫 해커들의 타깃으로 고착화될 수 있는 만큼 대책 마련이 시급하다는 지적이 나왔다.[219] 해커들의 해킹 능력에 대한 연구에 의하면 한국 출신 해커들의 해킹 능력은 수준급인 것으로 밝혀졌다.

둘째, 사이버 국제공조 실태를 알아보도록 하겠다. 국제사회는 국가 간 사이버 안보문제 해소를 위한 투명성과 신뢰성 제고, 사이버안보 규범의 확립 등을 위해 많은 노력을 기울이고 있다.[220] 유엔을 중심으로 UN 정보안보 정부전문가그룹(GGE)에서는 사이버안보를 위한 국가 간 규범문제를 논의하고 있다. UN총회 제1위원회에서는 사이버공간에서 신뢰구축 및 국가안보 문제를 논의하였으며 사이버범죄에 관한 국제조약으로 '부다페스트 사이버범죄 협약'이 제정되어 2004년 7월에 발효되었다.[221] 이 협약은 유럽 국가들을 중심으로 발효 중이며, 유럽 국가 외에는 미국만이 유일하게 발효시켰다. 아시아 국가 중에서 일본은 가입했으나 발효시키지 않았고, 한국은 아직 가입하지 않았다. 저작권 침해, 컴퓨터 사기, 아동 포르노금지 등에 관한 국내법의 의무화 규정과 사이버범죄 수사에 대한 상호협력 의무 등을 규정하고 있다.

또한 '사이버공간에 관한 총회'가 2011년부터 매년 열리고 있다. 경제, 사회, 범죄, 안전, 안보 등 다양한 영역에서의 사이버규범 문제를 논의하기 위해 정부, 학계, 산업계 등 다양한 행위자들이 모두 참여하여 안보(security)뿐만 아니라 경제, 사회, 안전(safety) 등 상호 연관되어 있는 다양한 이슈들을 종합적으로 논의한다. 첫 회의는 영국, 두 번째 회의는 2012년 헝가리, 세 번째 회의는 2013년에 서울에서 개최되었다. 그러나 모든 회의에서 원론적인 수준에서 정보보호와 사이

219) 『파이낸셜 뉴스』, 2015년 03월 17일 (화) 종합 08면.

220) 외교부, "사이버안보," UN 정보안보 정부전문가그룹(GGE: Group of Governmental Experts on Information Security)을 통해 사이버안보 확보를 위한 국가간 규범 문제를 논의 중이며, 우리나라는 2014년 7월 발족한 제4차 UN 정보안보 GGE에 참여.

221) 부다페스트 협약은 인터넷상에서 발생되는 범죄행위에 대해 상세한 규정을 두고 이를 처벌하도록 한 최초의 국제조약이다. 그런데 부다페스트 협약이라는 이름은 일종의 별칭으로 정식 이름은 말 그대로 '사이버범죄 조약(Convention on Cybercrime)'이다. 부다페스트라는 지명이 붙은 별칭의 배경은 2001년 헝가리의 부다페스트에서 개최된 사이버범죄 국제회의에서 출발된 협약이기 때문이다. 여기에 가입이 되면 가입된 국가들끼리 각국에서 겪고 있는 사이버범죄에 대해 핫라인이 설치되어 공동으로 대처할 수 있게 된다.

버전에 대한 언급만 했을 뿐 구체적인 행동방침을 합의한 적은 없다.

4. 인력과 기술 등 지원적인 관점

먼저 사이버 전문인력 관리 실태를 살펴보면 우리나라의 사이버 전문 인력은 수백 명 수준에 불과하다. 인력 양성은 시간이 오래 걸리는 면이 있으나 사이버 안보에 있어서는 핵심요소다. 한국정보보호진흥원이 조사한 사이버보안 전문인력 현황을 가지고 실력에 따른 분류를 해보면 특급 사이버보안 전문가 그룹이 전체 사이버보안 인력의 9%에 불과한 것으로 나타났다. 그동안 우리나라는 정보통신 분야에 정부의 많은 지원과 산업구조의 특성상 많은 인력이 양성되었으나 소프트웨어 분야인 정보보호 분야는 미흡하였다. 최근에 그 중요성이 부각되어 대학교와 대학원의 정보보호 관련학과가 설립되어 전문 인재들을 배출하고 있는 실정이다. 대학교의 경우 <표 13>에서 보는 바와 같이 고려대 사이버 국방학과 등 정보보호 관련 학과들이 개설되어 있으나 졸업생을 배출한 실적은 미미한 편이나 시간이 지나면 많은 수의 학생들이 관련분야에서 두각을 나타낼 것으로 판단하고 있다.[222]

<표 13> 대학교의 정보보호 관련 학과 현황

학교명	학부/학과/전공명	재적학생수	2014년 배출실적
건양대학교	정보보호학과	237	25
경기대학교	융합보안학과	100	-
경동대학교	정보보안학과	74	-
경일대학교	사이버보안학과	130	-
경주대학교	사이버수사경찰학과	209	19
고려대학교	사이버국방학과	90	-
고려사이버대학교	정보관리보안학과	360	52
광운대학교	사이버정보보안학과	13	-
광주대학교	사이버보안경찰학과	174	-
극동대학교	사이버안보학과	52	-
대구가톨릭대학교	정보보호학전공	84	-
대전대학교	해킹보안학과	239	14
동명대학교	정보보호학과	353	13
동신대학교	정보보안학과	107	-

222) 대학알리미, http://www.academyinfo.go.kr(2015.12.10.)

동양대학교	컴퓨터・정보통신군사학과	40	-
	사이버정보전학과	42	-
목포대학교	정보보호학과	212	23
배재대학교	사이버보안학과	42	-
상명대학교	정보보안전공	42	-
	국방정보공학과	40	-
서울여자대학교	정보보호학과	252	30
서원대학교	정보보안학과	32	-
성신여자대학교	융합보안학과	43	-
세종대학교	정보보호학과	96	-
세종사이버대학교	정보보호학과	323	55
수원대학교	정보보호학과	266	11
순천향대학교	정보보호학과	284	43
숭실사이버대학교	융합정보보안학과	155	21
영동대학교	정보통신보안학과	207	13
영산대학교	사이버경찰학과	195	22
우석대학교	정보보안학과	187	10
위덕대학교	사이버경찰보안학과	73	-
중부대학교	정보보호학과	257	20
한양사이버대학교	해킹보안학과	61	-
호서대학교	정보보호학전공	280	26
호원대학교	사이버수사경찰학부	350	38
합 계		5,701	435

대학원은 정보보호 연구를 목표로 조직된 교육기관으로 정보보안을 위한 기술 개발과 분석에 치중하고 있으며 최근에 정보보호가 강조됨에 따라 회사나 관련 기관에 근무하는 많은 실무자들이 <표 14>에서 보는 바와 같이 대학원 교육을 수강하고 있다.[223] 또한 해킹산업이 발달함에 따라서 대학 및 대학원 해킹 동아리의 활동을 한국정보보호진흥원에서 적극적으로 지원하고 있다.[224]

223) 대학알리미, http://www.academyinfo.go.kr(2015.12.10.)
224) 이 사업은 2년간 중단되었다가 2006년부터 다시 재개되어 현재 40개 대학의 해킹 동아리에 교육과 세미나 관련 비용을 지원하고 있다.

<표 14> 대학원의 정보보호관련 학과 현황

학교명	학부/학과/전공명	학위과정	재적 학생수	2014년 배출 실적
건국대학교 정보통신대학원	정보보안학과	석사	59	-
경기대학교 일반대학원	정보보호학과	석사/박사	-	-
	산업보안학과	석사/박사	9	4
경북대학교 일반대학원	정보보호학과야간 협동과정	석사/박사	4	-
고려대학교 정보보호대학원	KB금융보안학과	석사	20	-
	금융보안학과	석사	34	12
	공공보안정책학과	석사	22	-
	디지털포렌식학과	석사	20	16
	사이버보안학과	석사	15	19
	정보보호학과	석사/박사	199	35
과학기술연합대학원대학교	정보보호공학과	석사/박사	7	-
남서울대학교 일반대학원	지식정보보안학과	석사	6	-
단국대학교 정보지식대학원	컴퓨터학과(보안소프트웨어개발)	석사/박사	58	3
대전대학교 일반대학원	전산정보보호학과	석사/박사	3	-
동국대학교 국제정보대학원	정보보호학과	석사	180	48
목포대학교 일반대학원	정보보호 기술학협동과정	석사/박사	8	-
부경대학교 대학원	정보보호학 협동과정	석사/박사	8	2
상명대학교 일반대학원	지식보안경영학과	석사	24	-
성균관대학교 정보통신대학원	정보보호학과	석사	136	47
세종사이버대학교대학원	정보보호학과	석사	82	2
수원대학교 공학대학원	정보보호학과	석사	9	5
순천향대학교 일반대학원	정보보호학과	석사/박사	18	8

숭실대학교 정보과학대학원	정보보안학과	석사	112	24
아주대학교 정보통신대학원	지식정보공학과(모바일보안 전공)	석사	19	11
연세대학교 정보대학원	지식서비스보안	석사	18	14
	금융정보보호학과	석사	15	-
전남대학교 대학원	정보보안협동과정	석사/박사	62	4
전북대학교 대학원	정보보호공학과	석사/박사	5	-
충북대학교 대학원	정보보호경영학과	석사/박사	21	7
한국과학기술원 일반대학원	정보보호대학원	석사/박사	56	14
한국산업기술대학교 산업기술경영대학원	기술정보보호학과	석사	7	5
호서대학교 일반대학원	정보보호학과	석사/박사	5	1
합 계			1,241	281

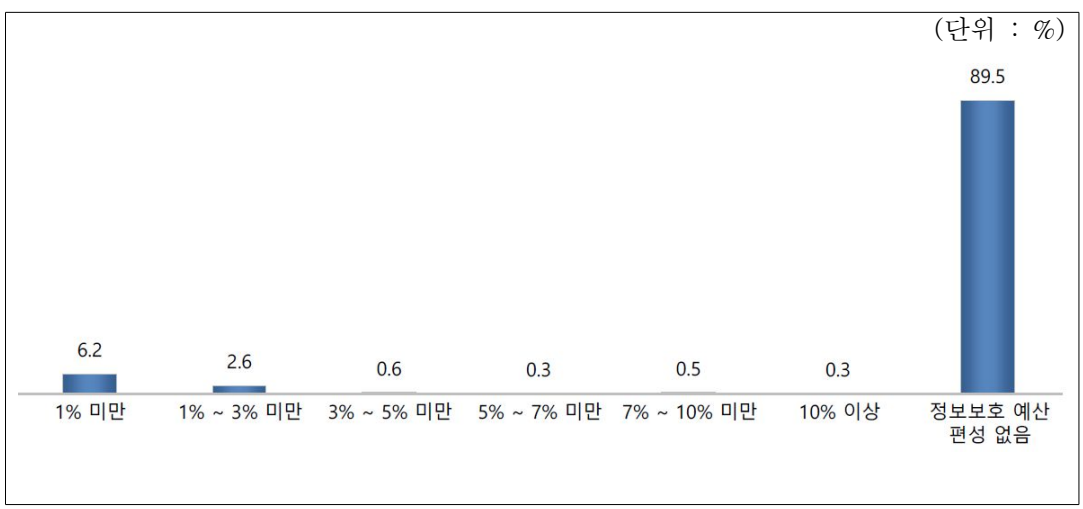
이들 동아리에 가입한 회원의 경우, 자발적인 해킹 동호인의 성향을 띠기 때문에 국가에서 집중 관리함으로써 음성적으로 활동할 수밖에 없는 해킹행위를 공개적으로 활성화시키는 좋은 계기가 되고 있다. 최근에는 정보보호분야 학술대회(ACM CCS 2014)에서 채택된 우리나라 논문 숫자가 미국, 독일, 스위스, 중국 다음으로 많을 정도로 국내 인재들의 사이버보안 능력이 매우 우수하다고 평가받고 있다.

또한 국가기관과 민간기관에서 정보보호에 대한 교육을 단기과정으로 실시되고 있다. 국가나 공공기관의 보안 담당자와 주요 정보통신기반시설 관리기관의 정보보호 책임자가 교육 대상자들이다. 국가정보보안정책 및 관련법령, 해킹사고 조사 및 복구 방법, 취약성 분석 및 평가방법, 정보보호시스템 운영관리 방법 등이 해당교육 내용에 속한다. 교육은 주로 국가정보원, 안전행정부 정보화능력개발센터, 한국정보보호진흥원에서 실시하고 있다. 민간교육 과정도 상당히 활발한 편이다. 주로 자격증 취득과 관련되기 때문에 교육수요도 일정한 편이다. 정보보

안관련 국제자격증으로는 공인정보시스템감리사(CISA), 공인정보시스템관리자(CISM), 공인정보시스템보안전문가(CISSP)가 있고, 국내 자격증으로는 정보보호전문가(SIS), 정보보안관리사(ISM), 정보시스템감리사, 인터넷보안전문가 과정이 있다. 그러나 정부의 적극적인 지원과 정보보안 업종에 대한 미래직업 선호도의 상승과 전망 있는 직업군에 사이버 보안전문가가 속해 있음에도 불구하고, 국내에서의 대우부족과 정보보호에 대한 기업과 사회의 인식부족으로 많은 유능한 인재들이 미국이나 유럽, 중국 등으로 떠나고 있는 실정이다.

둘째, 기술개발 측면에서 알아보면 지속적으로 진화하는 사이버 공격을 기술적으로 완벽히 막아내기란 불가능하다. 국내 정보기술보안 관련기술에 대한 투자 또한 활발하지 않다. 정부는 사이버공격의 진화에 따라 사이버안보를 위한 대응기술, 시스템 향상과 신규 보안위협 분석, 공격기법 예측 등 고도화를 위한 지속적인 연구개발 투자를 요청하고 있다. 현재 국내 정보통신의 보안을 담당하고 있는 보안제품이나 서비스기술 수준은 낮은 편이다. 한국인터넷진흥원은 한국의 보안제품 기술이 미국, 일본, 유럽 대비 80% 수준으로 격차를 보이는 것으로 파악하고 있다.[225] 2014년 정보보호 예산편성 현황은 <그림 10>에서 보는 바와 같다.[226]

<그림 10> 정보보호 예산 편성현황(2014년)



225) 박대우, 앞의 논문, p.57.
226) KISA, 『정보보호실태조사 최종보고서』(2014년), p.35.

제3절 한국군의 사이버 안보실태와 문제점

1. 인식과 사상의 관점

2013년 국방부는 국군사이버사령부의 인원을 앞으로 1천여 명으로 확대하고 사이버전에 대비해 정보 수집과 공격, 방어무기개발 능력을 확보하는 한편 사이버작전을 수행할 수 있는 프로그램과 백신개발 등 종합적인 능력을 갖추게 될 것이라고 했다. 사이버사령부는 2010년에 창설되어 현재는 인력이 600여명 수준인 것으로 알려졌다. 한국군은 북한군과 비교해 볼 때 아직까지 사이버전력과 대응전략 측면이 미흡하여 이에 대한 많은 노력을 기울이고 있는 것으로 파악하고 있다. 한국에서는 사이버공간이 육, 해, 공 영역만큼의 지위를 갖지 못하고 있고 사이버사령부는 사이버공격에 대응하기 위해 독립적인 작전을 수행할 수 있는 수준이 아직까지 미흡한 실정이다.[227] 군 수뇌부의 관심과 인식의 부족, 대통령 선거 때 발생한 댓글사건으로 국민적 의구심, 사이버전에서 국내 및 국제공조의 중요성에 대한 인식이 미흡한 편이다. 또한 사이버국제규범 마련, 국제법적용 원칙 마련을 위한 국제협력과 사법공조를 위한 외교적 노력과 같은 국제적인 차원의 대응 노력이 부족한 것으로 판단된다. 또한 북한의 사이버공격 시 중국의 역할을 간과하고 합당한 대응전략을 수립하지 못하고 있는 것으로 알려졌다.

기술적인 인식에 있어서 사이버공격에 능동적으로 대응할 수 있는 자동화된 사이버방어 기술이 부족하고 수동적인 개념 하 방어위주의 사이버전 인식과 기술 중심의 사이버방어 개념도 문제점으로 작용하고 있는 것으로 보인다. 공격자의 위치와 신원을 신속하게 찾아낼 수 있는 원점추적기술과 사이버포렌식 기술에 대한 투자가 부족하고, 식별된 원점에 대한 적절한 대응과 자위권행사를 할 수 있는 사이버공격 무기체계가 부재한 면도 있다. 사이버무기 연구개발 예산은 방어적 개념의 연구개발로 매우 제한되어 있는 실정이다.[228]

물리적인 타격체계와 작전의 연계성 측면에서 인식도 부족한 편이다. 기존의 물리적인 타격체계와 효과적인 대응체계 구축이 필요한 것이다. 미군의 사이버 공

227) “美사이버보안 책임자가 본 한국 사이버전력,” 『ZDNet Korea』, 2013년 5월 3일.
228) “사이버전 인력, 북한의 7분의 1,” 『뉴스원』, 2013년 10월 14일.

세작전시 네트워크와 전자전과 물리적인 공격을 포함하여 교리화한 것을 참고할 필요가 있다.

사이버전사를 양성하기 위한 국가적인 차원의 체계적인 계획수립과 이들에 대한 활용계획, 적절한 대우와 포상정책이 미흡하며 사이버전사들을 효과적으로 활용하기 위한 사이버 병과도 없는 상황이다.

사이버 작전개념과 사이버전 교리, 전략전술, 사이버전 교전규칙 등이 아직까지 미흡한 상황이다. 이러한 인식과 문제들 때문에 남북한 간 사이버전 준비에 있어서의 비대칭적인 간격이 더욱 심화되었으며 지금까지 북한의 사이버공격에 효과적으로 군이 대응하기에는 아직 많은 문제점이 있는 것으로 판단된다.

2. 군사전략 등 시스템의 관점

먼저 정부의 '국가사이버마스터플랜'에 국방 분야에 대한 정책적인 강조가 미흡한 실정이다. 현재 우리 군의 사이버전에 대한 상위 정책지침 및 전략의 주요 개념들은 현존하는 북한의 위협과 미래의 잠재적 위협 그리고 다양한 형태의 비군사적 위협을 동시에 대비한다는 포괄적인 개념하에 국방부에서 발간하는 '국방기본정책서'에 일부 지침이 제시되어 있다. 국방기본정책서에 포함되어 있는 주요 내용은 "사이버전의 대응태세를 강화하고 민·관·군 통합방위태세 확립 및 정보공유체계를 구축하여 초국가적, 군사적 위협에 대한 대비태세를 발전시키고 한미 정보화분야 협력 중진을 통해 정보통신기술 정책 및 정보보호분야 협력을 강화한다." 라고 기술하고 있다[229] 우리 군은 모든 작전의 기획, 소요, 수행은 상위 정책, 전략지침 및 지시를 근거로 수행하고 있으나, 사이버 정책은 구체적인 수행지침이 부재하고 각 군마다 시행정책이 달라 합동성 발휘가 어려운 실정이다. 북한의 사이버 공격은 현실적인 위협으로 네트워크 보호를 위해 컴퓨터침해사고대응팀(CERT)을 편성하여 대응하고 있으나 각 군이 독립적인 임무를 수행하고 있어서 사이버 정책은 물론 사이버전에 대한 개념도 상이한 것이 현실이다.[230]

둘째, 국방부와 합참에서 운용중인 사이버 관련 조직의 구성에 대하여 알아보

229) 박환수, "북한사이버 위협대비 사이버전 발전방향," 『합참』, 제60호, 2014.7, pp56-59.
230) 김희수, "북한사이버위협의심각성과사이버전수행발전방향," 『합참』, 제59호, 2014.4, pp74-75.

겠다. 최근에 전개되는 사이버전의 특징을 살펴보면 정치, 군사, 사회 등 전 분야로 확대되는 추세이며 피해지역도 범세계적이라는 것이다. 사이버 공격자는 시간, 장소에 구애받지 않고 전 세계 어디든지 공격할 수 있는 반면, 방어자는 공격징후를 사전에 파악하기도 어렵고 모든 공격에 대한 방어가 불가능할 뿐만 아니라 자체적으로 취약점을 제거하고 보완하기도 어려운 실정이다. 사이버전이 현존하는 위협임에도 불구하고 사이버전을 주도하고 있는 책임부서의 업무의 연계성 측면에서 살펴볼 필요가 있다. 국방부와 합참의 조직을 살펴보면, 국방부는 정보화기획관실에 'TF가 편성' 되어 있는 반면 합참은 군사지원본부의 민군작전부에 '사이버작전과' 가 편성되어 작전의 연계성과 업무의 연계성이 상이한 실정이다. 2013년 국방정책실에 '국방사이버 정책 TF'가 설치되어 있다가 정보화기획관실로 이전하여 사이버전과 관련한 업무를 수행하고 있다. 합참에서도 2014년 말에 사이버작전과를 신설하여 군사작전과 연계하여 사이버전 관련 업무을 추진하고 있다.[231] 또한 국군사이버사령부에 대한 합참의장의 지휘관계가 설정되어 있는 법적 근거가 반영되어 있지 않아서 2015년 2월에 국무회의를 통해서 사이버사령부에 대한 합참의장의 지휘를 포함하는 법령 개정안이 의결되었다. 그러나 합참의장의 사이버전 수행을 보좌할 수 있는 사이버전 수행부서가 아직까지 조직적으로 갖추어져 있지 않으며 전문성도 부족하며 사이버전 교리와 작전계획 또한 미흡한 실정이다.

반면에 미군은 2009년 사이버사령부를 창설하여 각 군별 사이버 조직을 구성하고 군 차원에서 사이버작전수행을 위한 능력을 발전시켰다. 2012년에는 'Capstone Concept for Joint Operations: Joint Force 2020' 을 발간하여 2020년 미 합동군이 수행할 합동작전에 대한 기본개념에 미국의 글로벌 리더십 유지를 위해 10개의 주요한 임무를 제시하였다. 이중에서 사이버공간 및 우주공간에서의 효과적인 작전수행을 강조하며 합동 및 각 군의 사이버작전 교범을 발간하였다. 이처럼 미군은 미래전을 준비하며 합동작전 영역에 사이버공간을 포함한 작전개념과 교리를 발전시켜 나가고 있는 실정이다.

3. 공조체제 등 네트워크의 관점

231) 김희수, 앞의 논문, pp.75-76.

첫째, 정보보호 인프라 구축 실태다. 군은 사이버 위협에 즉각적으로 대응할 수 있는 사이버 방어체계구축과 보강을 위해 해킹 역 추적체계 구축과 비인가 PC차단이 가능한 네트워크접근통제체계 확대구축, 침입방지체계구축 등 다단계 정보보호체계 보강을 추진하고 있다. 아울러서 기반체계에 대한 취약점 분석 및 평가와 네트워크보호대책을 검토하여 업무에 반영하고 있다. 또한 다수의 암호장비도 성능을 보강하여 운용하고 있는 것으로 알려졌다.

그러나 아직까지 사이버 공격에 대한 역 추적 기술과 악성코드의 분석 기술 연구, 지휘통제기술, 무기체계에 대한 보호기술 등 공세적인 사이버전 준비는 미흡한 실정이라고 한다.[232]

다음은 공조체제 관련 실상이다. 국군사이버사령부는 사이버전 관련 업무를 청와대 국가안보실 예하에 공공부문을 담당하는 국정원과 민간부문을 담당하는 한국인터넷진흥원(KISA)과 협력하여 임무를 수행하고 있다. 주한미군은 합동사이버센터(JCC: Joint Cyber Center)를 통해서 한국과 전 세계의 사이버 상황을 모니터하고 필요한 내용은 한국측에 전파하고 있는 것으로 알려지고 있다.

합참은 국군사이버사령부와 한미연합사를 통해서 주한미군이 제공하는 정보에 기초하여 사이버 상황을 일부 관제하고 있는 실정이나 한국과 미국은 사이버 전쟁에서 서로 협력하기로 정식적인 동맹관계는 아직까지 맺고 있지 않다고 한다.[233]

4. 인력과 기술 등 지원적인 관점

첫째, 사이버작전을 전담하고 임무를 수행할 전문인력 관리 실태를 살펴보도록 하겠다. 군은 국군사이버사령부를 중심으로 전문 인력을 운용하고 있으나, 이를 양성 및 관리하기 위한 대책들은 미흡한 실정이다. 각 군은 매일 전개되는 국방관련체계에 대한 해킹시도에 관제위주의 컴퓨터침해대응팀을 운용하고 있다.

그러나 사이버특기를 가진 전문성 있는 간부가 부족하고, 일부 병력은 정보통신병과와 전투병과에서 일부 전문성과 관심이 있는 인원을 차출하여 운용하고 있는 실정이다. 그리고 사이버 영역에 대한 이해의 부족으로 사이버 상황을 작전계획에 반영하는 능력이 미흡하며 사이버 상에서 운용되고 있는 각종 무기체계, 즉

232) 김희수, 앞의 논문, pp.73-74.
233) 『조선일보』, 2015년 7월 24일 금요일 A03면 종합.

공격과 방어체계의 특성과 구조 등에 이해가 부족한 실정이다.
현재 국방부와 협약으로 고려대학교를 통해서 소수의 전문 인력을 양성하고 있지만 국방 분야의 소요를 충족시키기에 매우 부족한 실정이다.

그러나 미군의 경우를 살펴보면 사이버 인력 확보를 위해 현역 군인은 물론, 민간 전문가와 사이버전 발발시 운용할 사이버예비군 등 다양한 인력을 증강시키고 있는 것으로 알려졌다. 특히 민간 IT 전문가들을 고용하여 사이버 임무부대(Cyber Mission Force)를 2016년까지 6천여 명 수준으로 창설하여 미국의 핵심 기반체계에 대한 방호와 필요시 사이버 공격에도 운용할 예정인 것으로 알려졌다. 사이버임무부대는 지휘부를 중심으로 사이버방호부대팀, 취약점분석팀, 적전술연구팀, 적침입탐지팀 등 임무를 세분화하여 담당할 것으로 알려졌으며, 이중에서 사이버방호부대팀의 세부 임무 및 편성을 살펴보면 <표 15>에서 보는 바와 같다.[234]

<표 15> 미국 사이버방호부대팀[235]

구분	임무	규모
국가임무부대(CNMF)	· 교통시스템, 발전소 등 국가 안보에 핵심적인 주요 인프라 방호	64명×13개 팀
전투임무부대(CCMF)	· 적의 지휘통제시스템 사전 무력화 등 전투사령부를 지원	64명×27개 팀
사이버방호부대(CPF)	· 국방 네트워크 방호	39명×68개 팀
직접지원부대(DST)	· NSA 인원으로 구성되어 CNE, CNA 임무 수행	25개팀(미상)

둘째, 사이버 기술 실태다. 각 군은 한국인터넷진흥원(KISA)와 협약을 맺고 KISA에서 추천하는 대학의 정보보호 동아리 우수인원을 간부와 기술병으로 선발하고 은닉악성코드 탐지체계구축, 악성코드분석, 전문기술전수를 위한 교육파견, 인터넷침해사고 징후분석체계를 KISA와 공유하는 등 대응기술능력 향상에 노력

234) 김경호, "사이버위협 양상변화에 따른 우리군의 대응방안," 『합참』, 제58호, 2014.1, pp.79-84.
235) CNMF: Cyber National Mission Force, CCMF: Cyber Combat Mission Force, CPF: Cyber Protection Force DST: Direct Support Team.

하고 있다. 그러나 사이버 상황관리와 통제를 위한 체계통합 표준화관리 기술이 미흡하고 자산에 대한 운영관리체계가 구축되지 못한 실정이다. 컴퓨터 네트워크 작전을 중심으로 방어위주의 기술에 주안하고 있으나 사이버위협 제거를 위한 공세적인 사이버 무기체계의 개발과 기술혁신이 필요한 실정이다. 그리고 사이버전에 대한 개념요구능력서의 부재로 전력소요와 기술소요 등이 구체화되어 있지 않은 문제점도 있다.

제4절 소결론

북한은 사이버 공격과 물리전을 병행하여 기습적으로 공격할 것이다. 이에 대해 정부는 심각한 안보문제로 인식하고 사이버 안보전략을 수립하여 대비하고 있으나 예산과 조직의 제한으로 현장에서의 실제 상황은 그렇지 않는 것으로 평가된다. 정부는 사이버 안보전략을 수립하고 대응방안을 제시하여 필요한 조치를 취함에도 불구하고 북한의 사이버 공격에 매번 당하고 있는 실정이다. 이는 사이버컨트롤타워 분야에서 누가 주도권을 가지는 것이 합당한지 법령문제로 실질적인 합의가 이루어지고 있지 않기 때문에 대응체계를 구축하는데 문제점이 있으며 북한의 사이버 공격시 이러한 악순환 때문에 매번 피해를 보고 있는 것으로 판단된다. 또한 국회는 사이버 법령에 대한 제· 개정의 발의로 여당과 야당이 대립하고 있는 실정이다. 그리고 북한의 사이버 공격이 발생할 때마다 이에 대응하기 위해 사안에 따라 필요한 법령이 제정되어 운용하다 보니 법령마다 기준이 상이하고 명확치 않은 면이 있어 적용하는데 어려움이 있는 실정이다. 따라서 사이버 법령에 대한 단일의 기본법을 제정할 필요성이 있다.

아울러서 북한의 사이버 공격시 공격목적이나 의도를 분석하여 범죄와 테러, 전쟁차원에서 검토할 필요성이 있을 것으로 판단된다. 그리고 한국은 사이버 안보 측면에서 북한의 위협과 정보통신기술의 발달로 북한의 사이버 공격에 취약성이 많기 때문에 공공영역에 위치하고 있는 국가핵심기반시설의 일부는 통합방위차원에서 군이 주도하여 임무를 수행하도록 하는 방안을 검토할 필요가 있을 것이다. 그리고 사이버 공조와 관련하여 국내적으로 관련기관의 협조는 물론, 한·미간에 공조를 넘어서 국제간의 사이버 공조와 협력도 매우 중요하다. 특히 국가간의 협력을 주도하고 이를 계기로 국제사회에서 역량을 넓힐 수 있는 기회와 대비책도 아울러 강구할 필요가 있다. 우선적으로 한미 사이버 공조체제를 포

함한 중국 등 주변국과 협력을 적극적으로 검토할 필요가 있을 것이다.

군차원에서 살펴보면 우리 군은 국군사이버사령부를 창설하여 임무를 수행 중에 있으나 대통령 선거시 댓글사건으로 일부 조직이 분산되어 임무를 수행하는데 어려움이 있을 것으로 판단된다. 또한 국방부는 사이버관련 부서를 정보화기획관실에 편성하고 있으나 물리전과 연계한 적의 군사공격에 대응하기에는 조직의 구성면에서 검토할 필요성이 있을 것으로 판단된다. 합참도 군사지원본부에 관련조직을 편제하고 있으나 정상적으로 임무를 수행하는데 많은 시간이 걸릴 것으로 판단된다. 북한의 사이버 위협에 대비한 각 군의 사이버 조직도 미흡한 실정이다. 아울러서 업무의 연계성 측면에서 국방부와 합참, 각 군 본부의 조직을 검토할 필요가 있다. 또한 군의 사이버전략을 검토할 때에도 우선적으로 한반도의 안보환경에 부합하도록 전략을 검토하는 것이 무엇보다도 중요하다고 판단된다. 물리전에서만 효력이 있는 현행 통합방위법의 개정도 검토할 필요가 있을 것이다. 적의 사이버 공격으로 대한민국에 사상자가 발생하고 물리적으로 큰 피해를 입었을 경우 자위권차원에서 응징보복이 이루어질 수 있도록 교전규칙을 검토할 필요성이 있을 것이다. 뿐만 아니라 전시에 대비하여 국제사회와 공조하여 사이버 전쟁법도 아울러 검토할 필요가 있을 것으로 판단된다.

특히 국가적인 프로젝트 차원에서 사이버 전력을 획기적으로 증강하여 역 비대칭전력의 운용을 검토할 필요성이 있을 것이다. 또한 과감한 예산의 증액과 사이버 중장기 종합발전계획의 수립을 검토할 필요가 있으며 사이버영토 방위를 위해 합참과 후방지역을 담당하는 작전사령부에 군사작전과 사이버작전을 통합할 수 있는 합동지휘통제관제실(가칭)을 구성하여 임무를 수행하는 방안도 검토할 수 있으리라 판단된다. 이와 같은 실태를 정리하면 <표 16>에서 보는 바와 같다.

이를 구체적으로 살펴보면 먼저 인식과 사상의 관점에서 국가나 군 공히 관련 조직의 실무자는 필요성을 절감하는 반면 관련기관장이나 지휘관은 당장의 현행 임무에 바쁘다 보니 필요성을 덜 인식하는 것으로 판단된다. 또한 전략 등 시스템적인 측면에서도 국가나 군 공히 구체화된 정책의 시행이 미흡하며 컨트롤타워의 문제와 이에 따른 법령과 제도의 문제점이 있으며 수행체계상에서도 기관별 상이한 문제점 등이 있다. 공조체계 등 네트워크에서도 정보보호 인프라 구축이 미흡한 실정이며 국내 및 국가 간의 협조와 협력이 미흡하며 아울러 인력과 기술적인 측면에서도 제한적이며 기술도 민간업체에 의존하고 있는 실태이다.

<표 16> 핵심요인별 사이버안보 실태

핵심요인		국 가	군
인식과 사상		· 해당조직: 필요성 인식 · 기관장/국민:일반적 인식	· 해당조직 : 필요성 인식 · 지휘관/간부 필요성 인식, 조직/예산 지원 미흡
국가전략 등 시스템	전략/정책	· 조직별 임무구체화 미흡 · 민간참여 제한	· 정책 수립 중
	콘트롤타워	· 청와대 · 국정원 주도	· 사이버사령부
	법령/제도	· 분야별로제정(중복,기준상이)	· 민 · 관 · 군 협력 미흡
	수행체계	· 기관별 상이한 수행체계 운용	· 기관별 임무/역할 정립 필요
공조체계 등 네트워크	정보보호 인프라	· 기관별 구축수준 상이 * 대부분 미흡한 실정	· 유형별 정보보호 인프라 보강 필요
	국제공조	· 국가간 협력체계 미흡	· 제한적 한 · 미 공조
인력과 기술	사이버 전문인력	· 미흡	· 민간 전문기관과 제한적 협력, 전문직능 부재 · 방어 위주 사이버훈련
	기술개발	· 민간업체 의존	· 민간업체 의존

제5장 대응방안

제1절 국가차원의 대응방안

1. 기본개념

북한은 국가기관과 우리 군을 대상으로 사이버 공격을 은밀하게 시행하고 있다. 따라서 우리는 국가안보적인 차원에서 북한의 사이버 공격의 실체를 확인하고 이들의 능력과 의도를 파악하는 것이 중요하다. 단순히 기술적인 차원이 아니라 국가 전략적인 차원으로 접근하여 우리의 대응능력을 어떻게 갖추는 것이 효과적인 방안인지 검토가 필요하다.

국가차원의 사이버 전략의 기본개념은 장기적인 안목을 가지고 예산을 집중적으로 투입하여 국가의 공공시설과 기간산업시설에 정보보호를 위한 인력과 장비를 대폭 보강하여 방어적인 수단을 확보하는데 집중하는 것이다. 이를 위해서 사이버전의 기본개념은 원점을 추적하여 공격하는 것도 중요하지만 복원력 증진을 통해 사이버 공격의 억제를 달성하는 것이 궁극적인 목적이 될 수 있도록 방어전략에 집중하는 것이다.

또한 북한의 사이버 공격시 누가 현장에서 컨트롤타워의 역할을 할 것인가도 매우 중요한 사항이다. 이를 통하여 법을 어떻게 제·개정하고 조직의 편성과 수행체계를 어떻게 하는 것이 효율적인 방안인지 소요가 나올 수 있기 때문이다. 정부와 국회는 북한의 사이버 위협의 심각성을 인식하고, 현재 여러 가지 법률에 분산되어 적용되고 있는 법령들을 종합하여 시행할 수 있도록 단일의 기본법 제정의 필요성을 검토할 필요가 있다. 북한의 사이버 위협이 상존하는 한 현재 운용하고 있는 사이버 안보와 관련한 법령과 제도의 정비는 반드시 필요한 실정이다. 아울러서 국가 안보차원에서 적의 사이버 공격과 위협에 대응하기 위하여 총력전 차원에서 국가방위요소를 통합하여 운용하는 통합방위법을 개정할 필요가 있을 것이다. 아울러 북한의 사이버 공격으로 국가안보에 치명적인 영향을 끼칠 경우에 '사후적 자위권' 차원에서 적의 전쟁지도부 또는 사이버 공격의 근거지를 물리적으로 타격하는 등 다양한 방안을 검토하여 북한의 사이버 공격에 대한 억지력을 높여야 할 필요성이 있을 것이다. 또한 우리도 사이버 공격에 대하

여 전쟁법적 대응에 관한 본격적인 논의를 시작할 필요가 있을 것이다. 북한의 대남적화야욕에 상시 노출되어 있는 환경과 물리전과 연계한 사이버전의 위협에 대응하기 위해서는 전쟁법적인 관점에서 논의가 필요하다는 것이다.

그리고 국가는 중장기계획을 마련하고 큰 틀에서 전략과 정책을 수립하여 사이버전 대비태세에 실질적인 진전이 있도록 할 필요성이 있을 것이다. 뿐만 아니라 국내 및 국제간의 공조체제 유지도 매우 중요하다. 사이버전의 특성상 전쟁이 일어났다는 것을 인지하는 순간 전쟁이 끝나 버릴 수도 있는 것이다. 그렇기 때문에 국내의 제 기관은 물론 국제간의 공조와 협력강화가 매우 중요할 것이다. 특히 한반도는 동북아의 국제질서에 많은 영향을 받고 있는 특수한 안보환경이다. 최근에 일본의 자위대법 개정으로 일본의 역할이 매우 중요하게 되었다. 한반도에서 전쟁이 발발하면 한·미·일과 북·중의 구도로 전개될 양상이 매우 클 것이다. 따라서 사이버 전에서도 미국과 일본과 공조체제가 중요하며 중국과의 사이버 외교관계를 강화할 필요가 있다. 핵무기 등 비대칭전력의 강화를 추구하는 북한의 군사전략과 사이버전의 잠재력을 고려해 볼 때 향후 북한에 의한 대남 사이버 공격의 가능성은 더욱 증대될 것으로 예상된다.

사이버 공간에서도 한미연합 전력이 매우 중요하다는 점을 명확히 인식할 필요가 있으며 사이버 전력의 우세 달성을 위한 노력을 집중해야 할 것이다.

2. 분야별 대응방안

가. 인식과 사상의 관점

먼저, 국민의 사이버전에 대한 인식의 제고가 필요하다. 북한의 사이버테러 위협에 직면하고 있는 우리나라는 기본적으로 전 국민의 사이버 보안의식이 지속적으로 제고돼야 한다. 언제 어디서든 사이버 공격을 당할 수 있으므로 경각심을 갖고 정부기관과 국가기반시설, 기업과 개인의 컴퓨터(PC)나 스마트폰 등 전 분야에서 보안대책을 숙지하고 필요한 예방조치를 해야 한다. 날로 교묘해지고 있는 사이버테러에 대비해 사이버공격의 심각성을 국민들에게 알리고 공감대를 형성할 수 있도록 할 필요성이 있다.[236]

북한의 사이버 공격에 즉각적으로 대응하기 위해서는 관련기관 간 구체적인 업

236) 유동열, 앞의 책, pp.15-18.

무분장이 이루어져야 하며 정부와 민간 기관과의 원활한 공조체제의 구축과 적절한 연습이 필요하다. 특히 국가사이버연습장을 건립하여 사이버전에 대한 연습과 훈련, 시스템의 취약성 점검, 네트워크시스템 도입 시 점검 등의 역할을 담당하게 할 필요가 있다. 특히 온·오프라인에서의 공격을 동시에 받고 있는 한국은 시스템과 네트워크 보안뿐만 아니라 국민의 인식 제고나 직원의 내부통제, 민감한 조직에 공급되는 소프트웨어를 감시하는 보안이 이루어져야 한다.

또한 정부는 민간이 자발적으로 사이버 안보에 적극 참여할 수 있도록 환경을 조성하는 것이 무엇보다 중요하다. 정부가 모든 것을 주도하여 책임을 떠안고 민간은 부수적으로 참여하게 하는 시스템은 민간이 가지고 있는 능력을 발휘하지 못함으로써 국가의 대응능력을 저하시킬 수 있다. 사이버테러 위협은 핵, 미사일에 버금가는 현실적인 위협이 되고 있다. 국민들은 가상공간에서 수많은 ID를 가진 수많은 내가 존재하듯이 국가안보를 지켜야 하는 능력과 수단의 차원도 매우 복잡해지고 있다는 사실을 인지하고 사이버 안보에 대한 인식을 새롭게 해야 할 것이다.

나. 국가전략 등 시스템의 관점

사이버 안보분야에 미국은 세계 최고의 능력과 국가적인 전략을 가지고 있는 것으로 알려졌다. 북한의 군사적 위협에 한국과 미국은 한미동맹을 바탕으로 강력한 억지력을 가지고 대비하고 있다. 한국은 정치, 경제, 사회, 문화 등 다방면에서 미국의 도움과 특히 안보분야에서는 절대적으로 중요한 혈맹의 관계다. 사이버 전략에서도 우리는 미국을 벤치마킹할 부분이 많이 있을 것이다.

미국은 사이버 안보를 국가 안보의 핵심 부분으로 간주하여 국가 차원에서의 대응방안을 강구하고 있다. 백악관과 국토안보부, 국방부가 주도하여 전략을 구상하고 대응할 수 있도록 조직과 관련 교리를 발전시키고 사이버무기 개발에도 집중하고 있다. 2011년에 발표한 미국의 전략적 구상은 사이버 공간의 잠재력을 최대한 이용할 수 있도록 관련기관을 조직하며, 훈련하고, 장비를 갖추도록 하는 작전 영역으로 간주한다는 것이다.[237] 또한 국방부가 운영하는 네트워크 및 시스템에 대한 보안조치를 강화하고, 통제 및 관리능력을 체계화하며, 범정부 차원의 유기적 협력을 통한 총체적 대응의 필요성을 제시한 것이다. 이 전략은 사이버안

237) DoD of US, 『Department of Defense Strategy Operating in Cyberspace(SOC)』, 2011, p.5.

보를 국가안보의 중요한 위치에 둔 역사적인 사건이다. 미국은 이 전략에 의거하여 국가의 핵심기반시설을 요새화하고 있다. 앞에서 언급했지만 2015년에 발표한 미국의 新 사이버 5대전략은 사이버수단을 통해 미국의 안보를 위협하는 적대세력에게 억제 또는 선제공격을 통해 미국의 안보를 지키겠다는 강력한 메시지를 전달하는 부수적인 효과도 거둘 수 있을 것이다.[238] 이밖에도 OECD와 EU 등 주요국들은 이미 사이버전 관련 국가전략을 채택하고 있다.[239]

2014년 7월 청와대는 '국가안보전략'을 발표하고 사이버 공격을 심각한 안보 문제로 확인했다. 이 전략은 '국가사이버안보전략'을 수립해 국가 차원의 통합 대응체계를 발전시켜 사이버안보 강국으로 도약할 기반을 구축할 것임을 밝혔다. 여기에 포함된 내용은 전문인력 육성, 기술과 장비의 보강, 우방국들과 협력강화 등이다. 이를 통해서 본 미국과 한국의 사이버 국가안보전략의 차이점은 첫째, 미국의 전략에서 사이버 공격은 테러의 위협과 함께 국가 안보에 대한 전반적인 위협으로 확실하게 인식하고 있는데 반해 한국의 전략은 사이버 공격을 심각한 안보 문제로 인식하지만 사이버안보 비중은 그렇게 크지 않다는 것이다. 둘째, 미 국가안보전략은 사이버 안보를 위한 법과 제도의 정비를 의회와 협력해 도입할 것임을 명시하고 있지만 한국에서 관련 법 개정은 정쟁대상이 되고 있는 것이다. 셋째, 미국은 2011년 첫 국가안보전략 발표 후 2015년 新 사이버 5대전략을 발표해 전략적이고 체계적인 사이버 안보를 실현하고자 노력하는데 반해, 한국은 2013년 사이버스페이스 총회를 주최하고서도 2014년 국가 안보전략에 명시된 '국가 사이버안보전략'의 향방이 모호한 실태다. 넷째 미국은 사이버안보 강화를 위해 동맹과 우방국들과 협력을 강화하는데 비해 한국은 미국과 군사동맹 관계이지만 사이버 상에서는 아직까지 동맹관계가 아니다. 이와 같은 것을 고려하여 다음과 같이 한국의 대응방안을 제시하도록 하겠다.

1) 먼저 국가 사이버안보 전략의 방향이다. 사이버안보가 국가안보에 있어서 최우선적으로 중요한 전략임을 인식하고 한국의 안보현실에 적합한 목표를 설정하는 것이 중요하다. 우리의 안보환경과 현실을 바라볼 때 우리사회는 정보통신기술의 의존도가 매우 높으며, 북한은 비대칭전력으로 사이버전력을 집중적으로 강화하여 공격하고 있기 때문에 국가차원의 사이버전쟁 전략을 연구할 수 있는

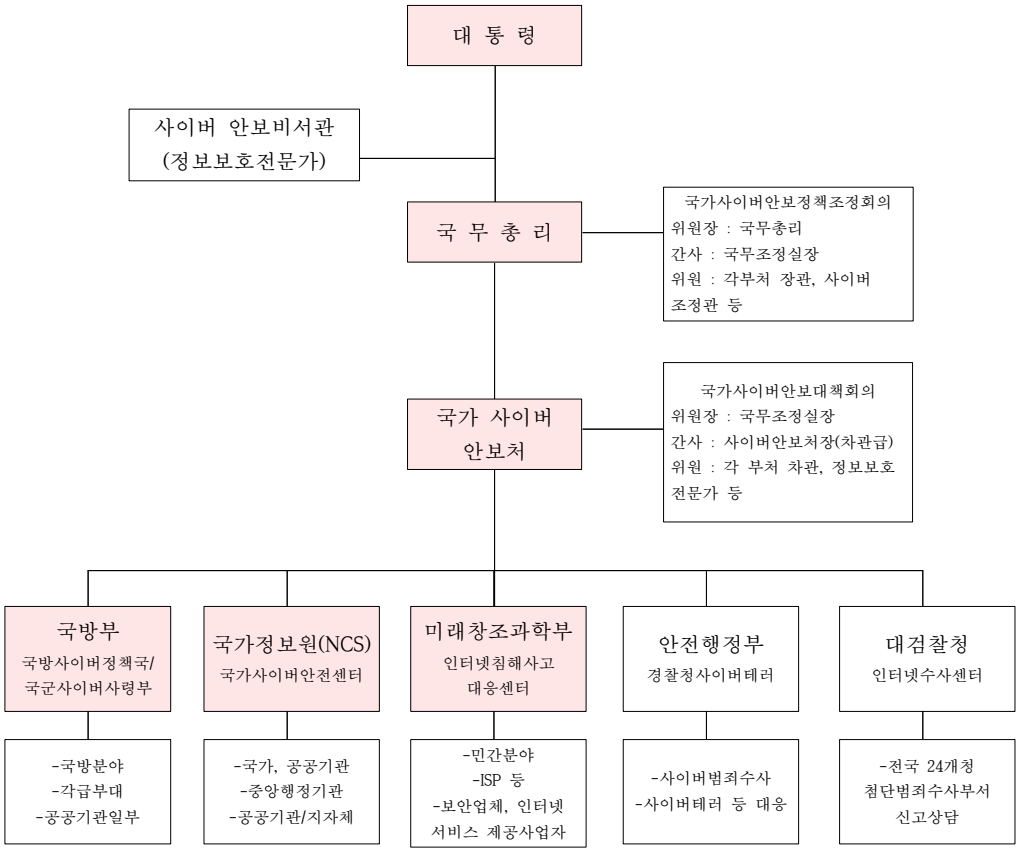
238) 최성주, "외교부 국제안보대사" 『세계일보』, 2015년 1월 5일 월요일 030면 오피니언.
239) 박노형, 『조선일보』, 2015년 2월 17일 (화) 오피니언 25면.

연구소와 연구조직, 최고의 창의적인 인재를 발굴하여 전략과 이노베이션 전문가 풀을 조성하는 것이다. 적극적인 방어 전략을 수립하여 복원력에 집중하는 한편, 공격무기체계도 개발하는 전략을 병행할 필요가 있다. 한국이 우선시하여 투자할 분야는 공격수단보다 방어적인 수단을 확보하는데 집중할 필요가 있다. 북한의 사이버 공격에 원점을 추적하여 공격하는 것도 중요하지만 복원력 증진을 통하여 사이버 억제를 달성하는 것이 궁극적인 목적이 되기 때문이다. 따라서 국가 핵심시설에 대해서 망 분리를 의무화하고, 백신 프로그램의 취약점을 관리하고 검증하며, 핵심기반시설에 보안인력을 대폭 확충해야 한다. 또한 북한이 이용하고 있는 해외거점을 색출하여 해당국 정부에 폐쇄를 요청해야 한다. 북한이나 제3국의 사이버 공격으로 국가의 주요기반망이 크게 파괴되고 인명이나 물적인 피해가 발생할 경우에는 사이버 공격의 주체를 색출한 뒤 이에 대한 적절한 대응공격을 가할 필요가 있다.

둘째, 국무총리 산하 국무조정실에 '국가사이버안보처(가칭)'과 같은 조직을 신설하여 임무를 수행하는 방안이다. 부처별로 분산되어 있는 각 기관을 통제하여 체계적인 대응과 신속한 정보공유, 실시간 관리로 능동적인 대응을 할 필요가 있다. <그림 11>은 개선된 사이버 안보 조직체계도이다.[240] 국무총리가 '국가사이버안보정책조정회의(가칭)'의 위원장의 역할을 수행하고 간사는 국무조정실장, 위원은 각 부처 장관과 국가안보실의 사이버안보 비서관 등을 위원으로 편성하는 방안이다. 실무 총괄을 담당하는 '국가사이버안보대책회의(가칭)'는 국무조정실장이 위원장이 되고 '국가사이버안보처장(가칭)'이 간사의 역할을 수행하며 각 부처 차관으로 위원을 편성하는 방안이다.

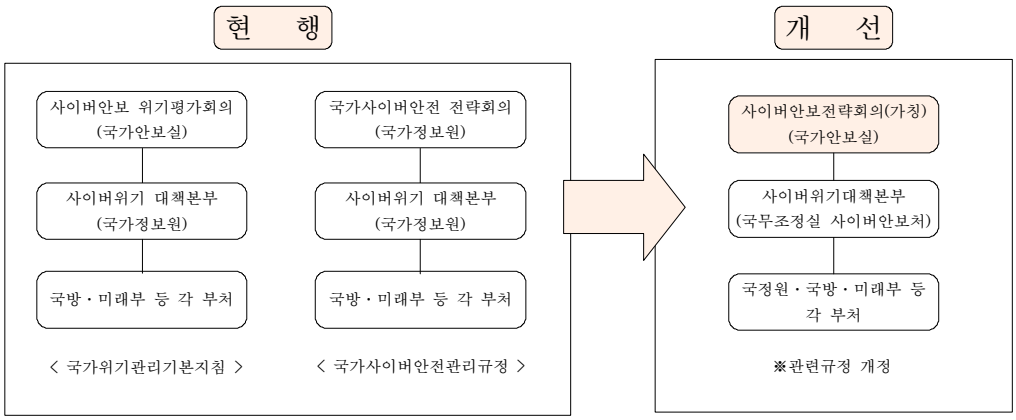
240) 이완수, 앞의 논문, p.101.

<그림 11> 사이버안보 조직체계도(개선)



이는 사이버위협으로부터 신속한 대응태세를 확립하여 정부의 일원화된 정책과 조정통제, 신속한 정보공유로 대응시간을 단축하고 보안의 구조를 확립하고 표준화 관리를 통하여 정책추진의 일관성을 유지하여 대응태세를 확립하도록 하는 것이다. 아울러서 <그림 12>에서 보는 바와 같이 청와대의 국가안보실에 '사이버안보전략회의(가칭)' 을 신설할 필요가 있다. 사이버 안보와 관련하여 범 국가안보차원에서 전반적인 전략과 정책의 방향을 제시하고 사이버 안보를 국가안보 차원에서 통합하여 대통령을 보좌하고 사이버 안보와 관련한 협의체로서 기능을 수행하도록 하는 것이다.

〈그림 12〉 국가안보실 '사이버안보전략회의(가칭)' 신설



셋째, 사이버 안보관련 법령과 제도를 정비할 필요가 있다. 핵심은 두 가지로 기존의 정보보호 관련법들을 통합하여 하나의 기본법으로 만드는 방법과 또 하나는 우리의 안보현실을 고려하여 사이버안보관련 법을 새롭게 제정하는 방안이다. 사이버전은 물론 사이버 테러의 성격에 따라 전쟁의 영역에 비중을 두게 될 경우 국회의 정보위와 국방위에서 국가안보차원의 위기시와 전시를 대비한 법령을 발의하는 것도 고려할 만한 것이다.

아울러서 사이버전쟁에 대비한 전쟁법도 제정하는 것을 검토할 필요성이 있다. 미국과 독일 등에서 사이버 공간에 대한 군사력 활용 가능성을 언급한 사례에 비추어 사이버 공격에 대한 즉각적인 대응, 사이버 공격징후시 예방차원의 선제적 대응과 사이버 공격과 물리전의 연계시 어떻게 대응할지 등 다각적인 검토가 필요할 것이다. 전시에 사이버 공격을 즉각적으로 차단하는 방안은 공격원점을 물리적으로 공격하는 방안이다. 적의 사이버 공격을 사이버 공간상에서 대응하기보다는 물리적인 차단이 효과적일 수 있기 때문이다.

다음은 정보공유와 협력에 대한 방안이다. 전 국민과 각 기관은 국가안보가 생명이라는 인식을 가지고 북한의 사이버 공격에 총력전 체제로 대응해야 한다. 특히 정보보호 예산과 투자를 활성화하며 부처 간의 벽을 허물고 정보보호 종사자의 근무환경을 개선할 필요가 있다. 대외적으로 국가안보차원에서 군사 동맹국과 경제 분야의 협력국과 공조 및 협력을 강화해야 한다. 아울러서 첨단 사이버무기체계의 연구 및 개발전략이 중요하다. 사이버 공간에서는 최고의 기술만이 존재

한다. 우리의 안보현실을 고려해 볼 때 복원력에 중점을 둔 방어기술과 스턱스넷과 같은 공격무기를 병행하여 개발해야 한다. 사이버 공격무기는 적의 핵무기 시설과 미사일 제조시설, 군수산업시설, 적의 방공망체계 등 전쟁을 준비하고 수행할 수 있는 시설과 전장망을 공격하는 수단으로 개발할 필요성이 있다.

사이버전 관련 전략적인 개발사업을 범정부적차원에서 사업화하는 획기적인 대책과 그에 합당한 기술개발 예산을 대폭적으로 반영하도록 조치할 필요성이 있다. 특히 창조적이고 자유로운 환경에서 지속적으로 일할 수 있도록 능력있는 인재를 양성하여 엘리트 사이버전사를 확보하는 것이 중요하다. 또한 실전에 대비할 수 있도록 사이버전투 훈련장을 구축할 필요가 있다.

이와 같이 북한의 사이버 위협에 국가안보 차원의 대응에 새로운 전략이 필요한 이유는 오늘날의 시대적인 환경이 기술의 부가가치를 주도하는 시대에서 창조적인 아이디어가 기술과 결합하는 창조혁신의 새로운 시대로 접어들었기 때문이다. 사이버 안보에는 여야를 불문하고 국민 모두의 국가 철학이 반영된 국가전략이 필요한 이유다.

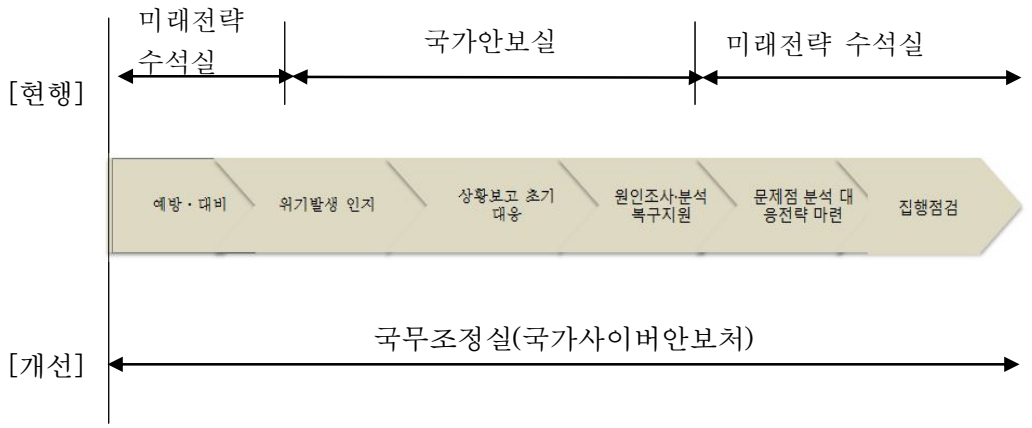
2) 다음은 실질적인 임무수행이 가능한 사이버안보 컨트롤 타워를 구축하는 방안이다.[241] 첫째, 국가 차원에서 사이버 안보는 국가 최고의 조직인 청와대가 컨트롤타워의 역할을 하는 것이 이론적으로는 바람직하다. 그러나 국가안보실에서 실질적인 컨트롤타워의 역할을 하는 것이 바람직한지는 검토해 볼 필요성이 있다. 국가안보실은 국가안보 전반에 대한 국가전략상에서 방향을 제시하고 사안에 따라서 필요한 지침과 모니터로 충분하다고 판단한다. 국가안보실이 직접 컨트롤타워의 역할을 하게 되면 완충할 수 있는 중간지대가 없기 때문에 문제가 있다고 판단된다.

따라서 앞에서 언급한 대로 이를 대신할 국무조정실에 '국가사이버안보처(가칭)'와 같은 조직을 편제하여 대응할 필요는 없는지 검토할 필요가 있을 것이다. <그림 13>에서 보는 바와 같이 국무조정실에 '국가사이버안보처(가칭)'를 신설하여 실질적인 총괄업무를 수행하게 하는 방안이다. 국무조정실의 '국가사이버안보처(가칭)'는 국무총리가 주관하는 '국가사이버안보정책조정회의'에서 하달된 지침을 '사이버위기대책본부'를 통해서 임무를 수행하며 사이버 안보

241) 『중앙일보』, 2015년 3 18일 (수) 사설/칼럼 30면.

와 관련하여 예방·대비에서부터 집행·점검까지 모든 업무를 총괄하게 하는 방안이다.

<그림 13> 국무조정실(국가사이버안보처) 컨트롤타워 역할 수행



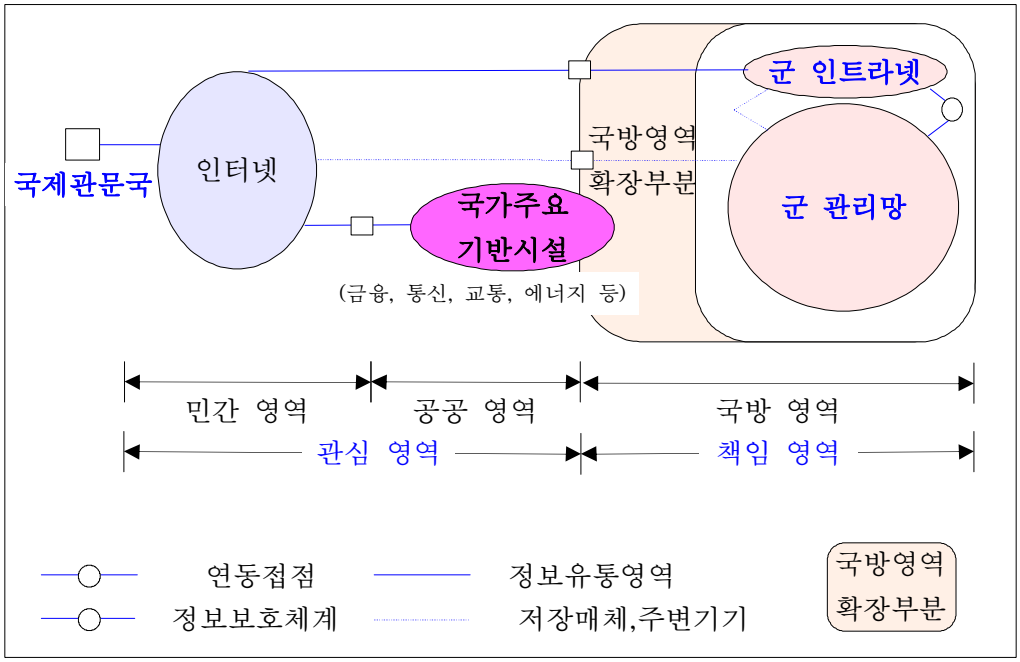
이를 위해서 정부, 군, 공공기관 및 산업체를 포함해 국가 전체의 사이버안보 정책과 운영을 직접 통제하고 유사시 사이버전 상황을 실시간으로 지휘하고 통제할 수 있는 전문 인력과 시스템이 필요할 것이다. 국가사이버안보처(가칭)의 역할이 사이버 방어와 공격에 대한 야전군 사령부이기 때문이다.

둘째, 미래는 초연결사회로 사이버 안보에 대한 중요성이 사회 곳곳에 미치게 될 것이다. 국가와 국민 모두가 사이버 상에서 활동하고 모든 기능들이 사이버 상에서 움직일 것이다. 국정원은 정보기관으로써 지금까지 사이버전의 실무총괄을 주도하였으나 국정원의 정체성과 임무와 기능을 고려할 때 제한사항이 있을 것이다. 따라서 앞에서 언급한 바와 같이 국무조정실의 '국가사이버안전처(가칭)' 에서 실무총괄의 임무를 수행하는 것이 바람직하리라 판단한다. 그리고 사이버전은 그 특성상 전평시를 구분하기 어렵기 때문에 평시에도 국가안보를 위해 군의 존재하여 전쟁준비를 통하여 전쟁을 억제하고 억제 실패시 전쟁에서 싸워 승리하듯이 사이버 전에서도 동일한 개념으로 군의 역할을 확대하여 대비해야 한다는 측면에서 군의 책임영역에 대하여 검토할 필요성이 있다고 판단된다.

따라서 국정원은 국가안보에 관한 정보기관 고유의 임무와 역할에 충실하고

국정원이 담당하던 공공영역의 일부를 전·평시 군사작전과 국민의 생명과 안전에 직결되는 핵심적인 국가기반시설에 관해서는 <그림 14>에서처럼 국방부에서 담당하는 것을 검토할 필요가 있다. 이를 위해서 군이 전시를 대비하여 평시부터 전투력을 강화하여 대한민국을 방어할 수 있는 역량을 갖추듯이 사이버전에서도 평시부터 군이 대한민국을 방어할 수 있도록 대폭적인 역량을 갖추는 것이다. 아울러서 한국인터넷진흥원(KISA) 등 관련 기관의 조직을 보강하여 각자의 역할에 맞는 임무를 수행할 뿐만 아니라 명에 의거 군을 지원하게 하는 방안이다.

<그림 14> 사이버전 수행을 위한 임무영역 식별



이를 구체적으로 언급하면 군은 지금까지 운용하던 군 인트라넷과 군 관리 망뿐만 아니라 국가안보에 영향을 미치는 정부기관과 핵심국가기반시설 등 공공영역에 대한 방어역량까지 능력을 확충하는 것이며, 전·평시 국가기관과 핵심기반시설이 안전한 가운데 정상적인 운영이 가능하도록 보장하는 것이다. 민간부문에 대해서는 한국인터넷진흥원의 조직을 더욱 보강하여 평시부터 공공시설과 민간시설들의 사이버 공격을 차단할 수 있는 기능을 갖추도록 그 임무와 역할을 강화하도록 하는 것이다.

셋째, 시행측면에서 북한의 사이버 공격상황이 발생하면 먼저 '국가사이버안보처(가칭)'의 민·관·군으로 구성된 '민·관·군 합동초기대응반(가칭)'이 상황을 분석하여 평가한 후 '국가사이버안보처(가칭)'에서 총괄적으로 주관할 상황인지, 아니면 산하 국정원이나 국방부가 주도할 사안인지 성격에 따라 주관부서를 지정하여 운영하는 방안이다. 또한 사이버 공격의 주체를 식별하여 사이버 범죄와 테러의 성격인지, 사이버전쟁의 성격인지를 구별하여 누가 주도할 것인지를 결정하는 것이다. 따라서 각 기관은 문제 해결을 위해서 평시부터 적극적으로 통합적인 공조체제를 이루어 실시간 정보를 공유하고 협력하는 것이 중요할 것이다.

임무전환 방안은 당분간 국정원이 수행해 오던 임무는 그대로 국정원이 시행하되 '국가사이버안전처(가칭)'를 창설하여 '임무전환마스터플랜'을 작성하여 임무를 전환할 수 있는 여건과, 기반이 조성되면 단계별로 시행을 검토할 필요가 있을 것이다. 아울러서 국방부나 한국인터넷진흥원의 능력이 향상됨에 따라 국정원이 담당하고 있는 공공영역의 업무를 일부 전환하고 국정원은 기본 임무와 정보기관 고유의 임무에 전념하도록 여건을 보장하는 방안이다.

각국은 사이버 안보의 중요성을 감안하여 국가수반이 직접 업무를 관장하고 있다. 특히 안보선진국인 미국과 이스라엘은 사이버 안보조직을 국가 최고지도자의 직속조직으로 두고 있다. 또한 국가의 전 기관에 분야별로 '사이버안보담당관'을 둬서 관리할 필요성이 있다. 사이버 안보가 국가안보에 필수적이기 때문이다.

3) 다음은 국내 사이버 법령체계 정비의 필요성이다. 최근에 사이버 공간의 중요성이 강조되어 사이버 공간을 효율적으로 활용하고 역기능을 최소화하기 위한 법률과 대통령훈령 등이 목적에 따라 다양하게 존재하게 되었다. 그러나 우리나라는 사이버전에 대한 포괄적인 기본 법률이 존재하고 있지 않기 때문에 북한의 사이버 공격으로부터 정부의 각 부처, 군, 민간 등 분야별로 대응조치를 독립적으로 수행함에 따라 정보공유와 협력대응에 문제점이 있었다. 따라서 기본법 제정이 필요한 것이다. 기본법 제정은 국민 모두가 공감하는데 반하여 이 법을 집행할 주관부서를 누구한테 주느냐에 합의가 필요한 상황이다. 현재 국회에서 발의하고자 하는 사이버테러 관련 법률안은 국가정보원이 주도하는 안으로 여야간 합의가 이루어지고 있지 않는 실정이다. 따라서 정부와 국회는 북한의 사이버 위협의 심각성을 인식하고 특히 사이버 공격과 물리전이 연계되는 상황을 상정

하여 ‘국가사이버안보처(가칭)’가 주도적으로 임무를 수행하게 하는 방안을 검토할 필요가 있다. 북한의 사이버 위협이 상존하는 한 사이버안보와 관련한 법령과 제도의 정비는 반드시 필요한 실정이다. 따라서 ‘국가사이버안전처(가칭)’가 주도하는 ‘국가사이버안보기본법(가칭)’을 제정하는 방안이다.[242] 이는 민간, 공공, 군사 분야를 담당하는 여러 부서들 간의 협력을 어떻게 얻어낼 것인가가 법안의 핵심이라고 할 수 있다. 기존의 법제도와 상충되는 부분이 어떤 것인지, 각 기관들의 직무의 성격과 내용이 무엇인지, 위기시에 각 기관과 어떻게 협조하고 정보를 공유해야 할 것인가와 민간의 자발적인 참여를 어떻게 이끌어 낼 것인가가 관건이다. 이를 위해서 각 기관간의 책임을 명확하게 인식할 필요가 있을 것이다. 즉 정책수립과 이를 집행하는 정부기관과의 임무와 역할을 분명히 할 필요가 있다. 정보기관은 정보에 대한 수집과 분석 및 처리를 하는데 집중하고, 정책을 수립하고 시행하는 것은 그 업무를 추진하는 집행력이 있는 부서에서 담당하는 것이다. 아울러서 기존의 법률과 어떻게 조화를 이루느냐가 중요하다. ‘국가정보화기본법’, ‘정보통신기반보호법’, ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’, ‘전자정부법’ 등 다양한 법률에 비해 ‘국가사이버안보기본법(가칭)’은 기본법의 지위를 차지하는 방안이다.

따라서 기존의 다른 법률과 조화가 이루어져야 하며 상호 모순되지 않도록 해야 한다. 특히 위기 발생 시 사고조사 요건과 방법에서도 국민의 기본권이 침해되지 않도록 세심한 주의가 요망된다. 국민적 합의가 없으면 사이버 공격에 국가적인 역량의 집중과 국가와 국민의 안전을 보호하는 목적달성도 어려워지고 오히려 혼란만 가중될 가능성이 있다. 용어상에서도 기존의 법률과 상충하는 부분이 없는지 자세히 살펴볼 필요가 있다. 그리고 몇 가지를 추가적으로 포함할 사항은 선진국들이 자국의 안보를 위해 허용하고 있는 정당한 정보수집인 화이트해킹과 온라인 원격지 압수수색제도를 위한 법제화를 검토할 필요가 있다. 국내에 진출한 외국계 정보통신사업자들과 국내 사업자들이 정당한 이유 없이 합법적인 안보수사 협조에 불응할 경우 국내 사업을 제한하는 규정을 신설해야 한다. ‘통신비밀보호법’ 상 통신사실 확인 자료와 인터넷 접속 로그기록 등의 보관의무를 위반했을 때 처벌조항을 신설할 필요성이 있다. 안보에 중대한 지장을 초

242) 박대우(c), “국가 사이버안보 관련 법률안 제안” 『국가사이버안보정책포럼』, 2013년 5월. p.68.

래하고 있는 통신자료 제공을 의무화하는 법적 근거를 마련해야 한다.

또한 국가보안법상 확정판결을 받은 반국가단체 및 이적단체 사이트의 자동폐쇄 및 자동삭제 의무를 정보통신사업자에게 부여하는 조항도 검토할 필요가 있다. '정보통신망법'에 인터넷상 허위사실을 유포했을 때 처벌할 수 있는 법 조항의 신설을 검토하여 '전기통신기본법' 제47조 제1항에 대한 2010년 헌법재판소의 위헌결정을 참고해야 할 것이다. 이는 천안함 폭침, 연평도 포격도발 사건 등 국가적으로 중대한 위기 상황에서 정보통신망을 통해 유포되는 허위불법정보에 대한 법적 처벌이 불가능하게 됨에 따라 이를 보완할 법적 근거의 필요성이 마련돼야 할 것이다. 국내외 안보 위해사이트의 폐쇄 절차를 간소화하는 방향으로 정비를 검토하여 현재의 복잡한 사이버 안보관련 법제의 정비를 검토하고 제반 규정을 포괄하는 사이버안보 관련 법률안을 제안할 필요가 있는 것이다.[243] 하지만 간과하지 말아야 할 중요한 사항은 이러한 법률과 제도의 제. 개정 시에 핵심조정기관의 역할을 수행해야 할 기관은 민주적인 감시와 견제장치도 제도화해야 한다는 것이다. 이와 같은 내용이 '국가사이버안보기본법(가칭)'에 포함되어야 한다.[244]

다음은 '국가사이버안보기본법(가칭)'이 제정되면 이를 근간으로 '통합방위법'을 개정하여 북한의 사이버 위협에 대비해야 한다. 현재의 '통합방위법'은 물리적인 힘을 통제하는 법으로 사이버전에서는 적용이 불가능하다. 종전의 패러다임으로는 접근이 어렵기 때문에 새로운 전략으로 발전시킬 필요가 있는 것이다. 북한의 사이버 위협이 상존하고 있는 가운데 국가적인 사이버위기에 대응하기 위하여 총력전 체제로 위협정보를 공유하고 초기의 혼란과 피해를 최소화하여 조기에 공격자를 응징하는데 어떠한 내용이 법률로 규정해야 할 것인가에 대해서는 전문가들의 폭넓은 의견청취와 공청회 등을 통한 국민의 의견을 수렴하는 노력이 폭넓게 실시되어야 할 것이다. 이 분야는 군차원의 대비방안에서 구체적으로 언급하도록 하겠다.

'국가사이버안보기본법(가칭)' 제정과 관련하여 우리정부는 미국의 오바마 대통령이 사이버안전 입법제안과 관련하여 대통령이 직접 의회를 설득하는 등의

243) 박대우(c), 앞의 논문, pp.69-71.
244) 박노형, "국내외 사이버 안보 법제정 동향과 시사점: 미국을 중심으로"『사이버공간과 국가안보』, (서울: 국가안보전략연구소, 2014)

노력의 과정을 참고할 필요가 있다. 오바마 대통령은 미국정부가 국가핵심기반시설내의 사이버안전의 취약성을 보완하도록 법을 제안하였다. 오바마 대통령은 사이버 안보를 미국의 최우선 과제로 정하고 입법과 정책수립에 많은 노력을 기울였으나 미국의회와의 대결국면에서 법안채택이 무산되었다. 미국 의회는 사이버 안보관련 입법제안을 위하여 민주당은 개인의 프라이버시와 시민적 자유를 옹호하고, 공화당은 전통적으로 국가안전을 옹호하고 있다. 무산된 이유의 핵심은 개인의 프라이버시가 중요하기 때문이었다. 그러나 오바마 대통령은 2013년 2월 사이버 공격으로부터 미국을 보호하기 위한 행정명령 13636을 발표하였으며 핵심기반시설의 안전을 위한 정부와 산업의 조정을 개선하기 위해 대통령 정책지침에 서명하였다. 남북한이 대치하고 있는 우리의 현실과 정보화 환경의 발달추세에서 사이버 공격에 취약한 대한민국은 어떠한 스탠스로 '국가사이버안보기본법(가칭)'을 제안할 것인가 참고할 필요성이 있는 것이다.

이어서 사이버공격에 대해 적용 가능한 국제법에 대하여 살펴보도록 하겠다. 국제법은 '국제전쟁법', '유엔헌장', '국가책임법' 등이 있으나 2013년 에스토니아의 수도 탈린에서 미국과 영국을 중심으로 한 서방국가의 학자들이 모여 이러한 국제법들을 사이버공격 환경에 맞춰 해석하고 적용하는 '탈린매뉴얼'을 발간하였다.[245] 탈린매뉴얼은 사이버 공격으로부터 물리적인 파괴와 인명피해가 발생할 경우 무장공격에 해당한다고 규정하고 있다. 탈린매뉴얼 13조에 "무장공격 수준에 상응하는 사이버작전의 목표가 된 국가는 고유의 자위권을 행사할 수 있다"고 규정하고 있다.[246] 만일 북한이 한국의 기반시설에 대해 사이버공격으로 물리적 파괴나 혹은 인명피해를 야기한다면 무장공격에 해당하므로 자위권 행사 차원의 대응공격이 가능해진다는 얘기다. 동 매뉴얼 9조에서 사이버공격은 비례성 원칙에 따라 동일한 유형과 동일한 수준의 대응조치를 취할 수 있도록 하고 있다.[247] 이에 국내외 전문가들도 디도스 공격과 3.20테러 등에 대해 비례성 원칙에 따라 동일한 수준의 사이버공격을 가할 수 있다고 평가하고 있다.[248] 과거에 불특정 다수를 대상으로 벌어지던 사이버테러 형태도 최근에는

245) 탈린 매뉴얼: 사이버 교전규칙:NATO CCDCOE (Cooperative Cyber Defense Centre of Excellence, IT 및 대테러 전문가들로 구성된 사이버전 관련 국제군사조직)의 지시로 국제전문가 그룹이 제작한 사이버전에 적용되는 국제법에 대한 매뉴얼.

246) 박노형·정명현, 앞의 논문, PP.69-71.

247) "Are there international rules for cyberwarfare?," 『CBC News』, 2013. 3. 21.

248) 문규석(2012)은 7.7 디도스 공격의 경우 대규모 경제적 손실이 발생하였으므로 무력사용에 해

원자력발전소 같은 기간산업으로까지 확산되고 있는 추세를 고려하면 더욱 심각한 상황이다.[249] 사이버전의 위협과 영향이 국가의 기간망과 공공기반시설 체계를 마비시킬 수 있음을 고려하여 전쟁준비 차원의 대응체계로 발전시켜나갈 필요가 있는 것이다. 구체적인 내용은 군차원의 대비방안에서 언급하도록 하겠다.

4) 사이버전에 대한 국가차원의 중장기계획 수립이 필요한 실정이다. 국가안보차원에서 사이버 안보정책의 거시적인 대응방안과 국민 개개인의 보안의식 제고가 병행되어야 할 필요가 있다. 이를 위해서 사이버전에 대한 중장기 계획을 마련하는 것이 필요하다. 국가차원의 대응전략과 발전계획을 수립하고 주기적이고 지속적인 점검을 통해 국가의 사이버전 능력을 보강해야 한다. 현재 국가 사이버 안보 컨트롤타워의 역할을 맡고 있는 청와대 국가안보실과 관련기관은 사이버전의 위협과 중요성에 정책의 우선순위를 높이고 예산을 대폭 확충하여 획기적으로 사이버 안보 분야를 발전시킬 필요가 있다. 정부의 각 기관은 예산확보시 현재의 보안실태를 정확히 진단하고 지향하고자 하는 목표달성을 위해 인력, 수단, 자원 등의 예산을 요구할 필요가 있다. 또한 예산의 집행결과를 보고하여 체계화함으로써 예산확보 방안을 표준화시켜 효율성을 제고시키는 노력이 필요하다. 아울러서 국가차원의 보안체계 개선뿐만 아니라 정보통신기반시설의 지정을 확대하고 양질의 보안전문가들을 배치해야 한다. 사이버테러와 같은 사건의 재발방지를 위해서는 한국수력원자력발전소 등 국가기반시설과 금융 및 방송사 등과 같은 주요기관에 보안전문 인력을 대폭 확충해야 한다. 무엇보다도 북한에 많은 사이버 공격목표를 제공하는 남한은 충분한 방어능력을 확보하는 것이 선행되어야 하며 북한의 전자적, 논리적, 심리적 사이버전력에 대응하기 위한 종합적인 방어체계를 마련할 필요가 있다.

사이버 위협에 대한 정보공유와 교육도 병행하여 추진할 필요성이 있다. 정부는 사이버위협의 정보를 실시간으로 민간 전문기업들과 공유하는 시스템을 구축하고 악성코드의 확산 방지를 위한 교육을 강화할 필요가 있다. 그리고 국가 중요시설에 대한 망 분리를 의무화해야 한다. 방송사와 금융기관 같은 민간 중요시설에도 망 분리 의무화를 확대 적용하여 외부에서 악성코드가 유입돼도 내부 망에는 영향을 끼치지 못하도록 하는 등 사이버위협을 선제적으로 차단할 필요성

당한다고 결론을 내리고, 북한이 공격한 것이 맞다면 한국은 비례성의 원칙에 근거하여 북한에 대해 동일한 사이버공격으로 대응조치를 취할 수 있다는 입장을 보이고 있다.

249) 임종인 외, 앞의 논문, p.39.

이 있다. 또한 백신 프로그램의 취약점 관리와 철저한 검증이 필요하다. 3·20 사이버 테러는 국내 백신 제품의 중앙관리 서버를 통해 악성코드가 전파되어 공격의 통로로 악용한 것으로 보인다. 다양한 백신의 도입을 확대하고 백신 프로그램의 철저한 취약점 관리와 검증을 통해 악성코드가 백신 업데이트 과정에서 각 기업이나 기관 전체 PC로 확대되는 것을 막아야 한다.[250] 북한은 공공, 민간, 군 등 영역구분 없이 전략적 차원의 공격을 해오고 있으며 공격은 향후 사이버테러나 사이버전에 사용될 수 있음으로 영역별로 대응하되 상황에 따라 민· 관· 군이 사이버위협에 정보를 공유하고 공동대응체계를 확립할 필요가 있다.

다. 공조체제 등 네트워크의 관점

첫째, 우선적으로 사이버 위협에 대비한 방어망의 사전구축과 실질적인 조치가 필요하다. 이를 위해서 북한이 우리를 공격하지 못하도록 억제하는 것이 중요하다. 공격을 해도 원하는 결과를 얻지 못하게 대비태세를 강화하는 것이다. 외부로부터 침입하는 적을 효과적으로 막으려면 적이 올 수 있는 길목을 차단하는 것이다. 인터넷 국제 관문을 차단하는 방안이다. 공격하는 IP를 식별하여 차단하거나 그와 같은 유형의 IP를 먼저 발견하여 조치를 취하는 것이다.

차단 실패 시 적이 목표를 공격하지 못하도록 각 기관에서 운용하는 서버를 효과적으로 방어할 수 있도록 조치하는 것이다. 전장에서 병력과 장비가 위치해 있는 주둔지를 방어할 때 겹겹이 3선 개념으로 방어하듯이 서버를 중심으로 방어망을 구축하는 전략이 필요한 것이다. 각 기관에서 운용하는 서버의 핵심기능을 중심으로 방어망을 내곽방어망과 외곽방어망, 적이 오는 것을 미리 경고하고 차단하는 전초성격의 방어망을 3선으로 구축하여 공격하는 적을 사전에 차단하거나 격멸하는 것이다. 이는 원거리부터 근거리에 이르기까지 적합한 무기체계를 개발하여 체계적으로 적을 격멸하도록 하는 것이다. 그러나 방어망을 뚫고 적이 공격을 계속하여 인터넷과 서버와 네트워크가 많은 피해를 받게 되면 빠른 시간 내에 적의 공격원점과 경유지를 식별하여 외교적인 수단과 물리적인 방법 등으로 응징할 필요가 있다. 그러나 문제는 누가 어디서 어떻게 공격을 했는지 증거가 불명확하기 때문에 제재가 쉽지 않다는 것이다. 스모킹 건인 결정적 증거가 부족하니 공격을 하는 쪽이 이를 악용할 수 있는 것이다. 핵개발이나 장거리 미

250) 신충근·이상진, 앞의 논문, pp.217-219

사일 발사에 대한 유엔안전보장이사회 제재는 있어도 사이버 공격에 대해 공식적으로 승인된 국제적인 제재는 아직까지 없는 실정이다. 치명적인 공격에 있어 피해자는 있어도 가해자를 특정하기가 어렵고 가해자를 알더라도 처벌이 불가능한 공공연한 비밀 전쟁이 바로 사이버전이기 때문이다. 사이버 공격의 당사자가 정부기관인지 정부가 지지하는 해커 집단인지 아니면 불량배 해커인지 식별하는 것도 매우 어려운 실정이기 때문에 실질적인 대비태세가 매우 중요하다.

둘째, 다음은 국제 공조체제의 구축이다.[251] 먼저 한국은 북한의 사이버 관문인 중국과의 사이버 협력체계 구축에 외교력을 집중하는 것이 중요하다. 북한의 사이버공격은 국제적인 성격을 가지며 중국의 개입으로 복잡한 양상을 보이고 있기 때문에 국제적인 대응 없이는 한계가 있을 수밖에 없다.[252] 북한의 사이버 공격에 대응능력을 갖추고 공격을 하려고 해도 가장 큰 걸림돌이 되는 것은 바로 중국의 존재이므로 국제적인 차원의 대북 사이버전략의 핵심은 중국으로부터 북한의 분리·고립시켜 북한이 자신의 영토에서 공격을 수행할 수밖에 없도록 만드는 것이다. 한국은 북한의 불법적인 사이버공격 행위를 규제하고 중국의 지원과 방관행위를 막을 수 있는 국제적 차원의 사이버 안보규범 형성을 위한 노력을 주도하고, 북한의 사이버공격에 대한 국제법 적용 방안에 대해 국제적인 합의를 이끌어낼 필요가 있다. 북한의 사이버전력은 중국의 사이버전력을 잃는다면 감소될 것이다. 중국과 한국은 양자 간 사이버 수사공조와 사이버 안보협력을 성사시켜 북한을 압박하고 중국으로부터 분리시키는 외교적 노력도 병행하여야 한다. 동시에 북한의 사이버테러에 대한 이중적인 태도를 비판하면서 북한을 사이버 국제규범 테이블로 들어오도록 강제하는 전략도 고려할 필요가 있다.[253] 이와 같이 한국은 사이버공간에의 국제법 적용과 사이버규범 개발에 적극 참여하여 북한의 불법적인 사이버공격에 대해 국제사회에서 규제할 수 있는 원칙을 마련하고 북한에 강제할 수 있도록 노력해야 한다.

사이버 공격이 진행되면 국가기관은 물론이고 한국인터넷진흥원, 민간보안업체 등과 공조가 매우 중요하다. 그러므로 효율적이며 상호 신뢰할 수 있는 정보공유 시스템마련이 중요하다. 현행법 상 정보공유는 통신비밀보호법에 금지하고 있기

251) 김종하, 『문화일보』, 2015년 1월 27일 화요일 오피니언 31면.
252) 임종인 외, 앞의 논문, p.38.
253) 위의 논문, pp.38-39.

때문에 이를 해결하여 정보공유시스템 구성과 기관별 정보접근 권한에 대해 시행령 제정도 필요할 것이다. 특히 한국은 미국 및 일본과의 사이버 국제 안보협력 강화가 필요하다. 한국과 북한이 공통 언어인 한국어를 사용한다는 사실은 북한이 한국의 네트워크를 활용해 미국과 일본의 네트워크까지 공격할 수 있음을 보여준다. 중국 인민해방군 사이버부대 해커들이 자국의 사이버 공격 전략을 시험하기 위해 대만의 민간 네트워크를 해킹해 활용한 사례도 있다. 이를 위하여 정부는 한미 국방장관 회의시 제43차 한미안보협의회(SCM)에서 양국 간 사이버 안보 협력을 강화하기로 하였으며 제44차 한미안보협의회(SCM)에서 협의체를 구성하기로 합의하였다. 한편 각 국가는 지향하는 가치와 추구하는 국가 이익이 다르기 때문에 국제적인 공조체제를 구축하는 것이 쉽지 않다. 국제협력을 통해 사이버위협에 대한 국제적인 감시와 정보공유, 조기경보체계 등 대외적인 협력 강화가 절실하며 협력을 통한 비용분담도 고려할 필요가 있다. 다자간 협력체계를 구축하는 것은 사이버전의 특성상 매우 시급하고 중요하기 때문이다.

라. 인력과 기술 등 지원적인 관점

사이버 안보에 있어서 가장 중요한 것은 전문 인력을 확보하는 것이다. 이를 위해 국가적인 전략과 정책의 우선순위를 높여야 할 것이다. 특히 국가적인 관심과 예산의 확보가 중요하다. 사이버 전문 인력을 양성하려면 무엇보다도 직업이 안정되고 장차 비전이 있어야 젊은 청년들이 이 분야에 종사하게 된다. 사이버 공격에 대응할 수 있는 보안인력은 수요에 비해 공급이 부족한 것이 현실이다. 대응인력을 양성하기 위해서는 사이버전을 위한 특성화 대학을 육성하는 등 국가차원의 지원이 필요하다. 아울러 공공기관의 정보보호인력의 채용을 확대하고 인재에 대한 지속적인 관리가 필요하다.[254] 사이버 보안체계에 대한 예산투자도 사고발생 후 되풀이되는 단편적인 예산투자 보다는 지속적인 투자로 인력을 양성하고 체계를 보완하며 연구개발에 집중해야 한다. 국가에 도움이 되는 전문 인력은 다양한 해킹기술을 이해하고 공격하는 해커의 특징과 심리적인 성향을 알 수 있는 능력을 소유해야 유능한 인재다.

이와 같은 인재를 육성하기 위해서 첫째, 정규교육을 통하여 현장에 필요한 전문 인력을 양성하는 것이 중요하다. 정부는 2015년 7월 소프트웨어 중심대학 선

254) 김기수, 앞의 논문, P.306.

발 추진계획을 발표하는 등 소프트웨어와 정보보호에 많은 관심을 가지고 있다. 논문의 앞부분에서 언급한 바와 같이 특히 대학과 대학원의 경우 정부에서 혁신계획을 가지고 많은 지원을 하고 있다. 정부는 정보보호 정책을 강화하여 양성된 우수한 인재들이 국내에서 제대로 대우받고 근무할 수 있는 환경을 만들어 줄 필요가 있다. 정부는 정보보호 없이는 개인도 기업도 정부도 존재할 수 없다는 사실을 명확히 인식하고 인재양성에 집중할 필요가 있다.

한편 해킹 매니아들은 초·중학생 때부터 호기심으로 출발하여 사이버해킹에 대한 시간과 노력을 집중하여 고등학교 과정에서 일반대학에 진학하기 보다는 해킹관련 학원이나 전문대학에 진학하는 경우가 있다.[255] 이들을 국가에서 활용할 경우에 해커의 관심과 적성이 어디에 있는지를 파악하는 것이 매우 중요하다. 이들의 적성과 진로를 가이드하고 흥미를 유발하여 해커로서 사회생활이 정상적으로 가능하도록 관심을 가지며 국가의 이익에 부합되는 국민으로서 활용가능성에 염두를 두고 맞춤형 전략을 취할 필요가 있다. 이들이 대학을 진학하면 국가사이버 안보전략의 일환으로 이들에게 국가가 필요로 한다고 하는 사명감을 주고 군에 입대해서도 전문직 보직을 통하여 사이버안보 실전 경험과 전술을 익히도록 배려하는 방안도 있을 것이다. 군 전역 후에는 국가사이버 안보에 대한 전략과 전술을 배울 수 있는 대학원 진학을 통하여 국가 사이버안보 전략에 대한 교육과정을 이수하게 할 필요가 있다. 포인트는 중학교 졸업 전 취미활동의 활성화와 고등학생 해킹동아리의 네트워크를 구축하고 대학교의 해킹동아리를 조직화하여 군에서 해킹전문가로서 복무하도록 하는 시스템의 구축이 중요하다. 대학원에서도 해킹인력의 조직화와 인적 네트워크를 조직하여 동아리활동과 국가의 적극적인 지원을 통해 전문해킹그룹과 쉽게 동화할 수 있도록 관계기관의 협조와 지원을 하는 방안도 강구할 필요가 있다.[256]

둘째, 해킹 매니아 출신의 해킹 전문인력을 활용하는 방안이다. 국가간에 사이버 전쟁은 해킹 기술을 이용한 양자 혹은 다자간의 대결구도이다. 해킹을 예방하고 사이버 범죄를 소탕하는 기술을 익힌다고 해서 모두가 사이버 전쟁을 치를 준비를 갖추는 것은 아니다. 국가 간에 사이버 전쟁에 대비하기 위해서는 정규 및 비정규 교육 외에도 실제 해킹경험이 많고 사이버 전쟁에 대한 확실한 의식

255) 박대우(b), 앞의 논문, P.52.
256) 위의 논문, p.52.

을 갖춘 전문가를 양성할 필요가 있다. 이런 의미에서 자격증 취득이나 취업을 위해 정보보호 교육을 이수한 사람들과 달리 자발적인 성격이 강한 해킹 동아리 등에 대해 국가의 적극적인 관리가 필요하다. 국가를 부정적으로 인식하는 해킹 동아리는 국가의 전략적 이득에 큰 손실을 가져올 수 있다.

그러나 국가가 공개적으로 해커를 양성한다는 것 자체가 국제적 이슈가 될 수 있고 타국과 심각한 외교 및 군사적 대립 상황을 만들 수 있다. 동시에 우리나라와 갈등관계나 경쟁관계에 있는 국가로부터 의심을 받기가 쉽다. 따라서 매우 신중하고 합법적으로 사이버 보안전문가를 양성해야 하고 평시와 유사시에 이들을 어떻게 이용할 것인가에 대해서도 각각의 전략이 필요하다. 이를 통해 국가에 이익이 될 수 있는 사이버 전문가를 선발하고 이들을 전문직 공무원이나 이에 준하는 연구위원 수준으로 대우하고 신분을 보장함으로써 자연스럽게 국가의 이익을 위해 복무하게 만드는 방안도 검토할 필요가 있을 것이다.

셋째, 해커의 교육과 선발, 심사체계를 제도화하고 과학적 지수를 개발할 필요가 있다. 전문적인 해커를 육성하기 위해서는 커뮤니케이션학, 심리학, 윤리학, 정보보안학의 전문가들로 구성된 TF 팀을 만들고 이에 대한 장기적인 연구가 필요하다. 표준화된 해커 유형을 선정하고 수준별 사이버 보안전문가를 양성하여 각 기관에 적합한 인물을 배치해야 한다. 해킹대회를 개최하면 원너비[257] 해커에서부터 특급 해커에 이르기까지 해커들의 관심이 매우 높은 편이다. 해킹대회는 해커를 발굴하기 위한 매우 합법적인 장치이다. 최고 수준의 해킹레벨을 통과한 참가자의 경우 일단 기술적 측면의 자격은 확보한 것이다. 이들을 활용하려면 적극적인 필터링 작업을 시행해야 한다. 해커의 심리구조, 윤리의식, 해킹 경험, 국가관, 안보관 등 다양한 측면을 측정하기 위한 과학적 조사방법이 동원되어야 할 것이다.

해커의 심리구조를 분석하여 해커의 공격성과 사이버 테러 가능성에 대한 예측변수를 도출한 결과는 다음과 같다.[258] 첫째, 해커의 심리적 변인인 플로우 지수와 해킹 빈도 간의 상관성에서 플로우 지수가 높은 해커일수록 자주 타인의 컴퓨터 시스템에 침입하는 것으로 나타났다. 이 결과는 해커의 이데올로기 유무

257) 워너비는 “유명인을 동경하는 사람, 유명인을 동경하여 행동 · 복장 등을 그들처럼 하는 사람“을 뜻한다. “무언가가 되고 싶다“ 뜻의 영어 want to be를 연음으로 발음한 말로, 1981년부터 사용되었다.

258) 니테쉬 외, 『해커의 공격기술』, (서울: 에어콘출판사, 2015), p.138.

에 상관없이 해킹하는 동안 심리적인 행복감을 높게 느낀 해커일수록 자주 불법 해킹 행위에 관여한 것으로 해석된다. 둘째, 타국으로부터 위협을 받는 가상 상황에서 자국이 타국에 의해 비난 · 위협 · 침공을 받았을 경우, 애국심이 높은 해커 집단의 경우 애국심이 낮은 집단에 비해 더욱 적극적으로 상대방의 컴퓨터 시스템을 해킹하겠다는 의지를 보이는 경향이 있다. 셋째, 목적형, 비목적형, 가치지향형 해킹과 타국에 대한 해킹 의지간의 상관관계에서 가치지향형 해킹을 수행하는 해커들이 타국에 대한 해킹 의지가 높은 것으로 나타났다. 즉, 특정 이데올로기를 가지고 있는 해커들이 사이버 테러를 감행할 가능성이 높은 것으로 해석된다. 넷째, 타 국가에 대한 사이버 테러 가능성을 예측하기 위한 변인 도출 결과 애국심, 자의식 상실, 공격적 성격 및 행위가 유의미한 변인인 것으로 밝혀졌다. 이것은 민족주의적 성향이 높고, 해킹을 하는 동안 쉽게 플로우 상태에 빠지며 성격적으로 공격성이 높은 해커일수록 타 국가에 대한 사이버 테러를 벌일 가능성이 높은 것으로 이해된다.

결국 우리나라의 사이버 안전을 책임져야 할 해킹 기술을 보유한 해커들은 앞의 연구결과에서 나타난 심리적 구조와 성향을 지닌 사람들일 것으로 예상된다. 따라서 국가관과 안보관이 높은 플로우 지수와 공격성과 심리적 안정감, 강한 자기통제력, 높은 윤리의식을 겸비한 해킹 전문가들이 우리나라의 사이버 안전을 책임질 수 있는 적임자가 될 수 있다는 사실이다. 이 모든 조건과 절차는 사이버 전 관련 전문 인력을 관리할 장기적인 계획과 국가안보 차원의 전략을 수립한다는 전제에서만 가능할 것이다. 정부는 사이버 안보 요원을 학생시절부터 특기생으로 양성하는 방안을 검토해야 한다. 군도 사이버 전문부대 확대와 함께 사이버 인력자원의 효율적인 활용방안을 마련할 필요가 있다. 민간기업도 사이버 보안인력 확보와 교육, 시스템 확보에 충분한 투자가 필요하다. 해킹 사고가 발생하고 사회적 관심이 고조될 때 한시적으로 인력양성을 논할 것이 아니라 평시에 양성한 전문 인력이 안정적으로 취업하여 고급 인력으로 성장할 수 있는 사회적인 기반을 마련할 필요가 있다. 또한 강력한 사이버 레드팀을 운용하여 우리 사회전체의 사이버 공격에 대한 위협의 실체를 확인할 수 있도록 국가적인 연습과 훈련이 필요하다. 아울러서 정부행정기관과 국회 등 국가 주요 정책입안기관에 사이버 안보전문가를 진출시켜 정책입안 초기부터 사이버 안보정책을 반영할 수 있도록 해야 한다.

다음은 기술적인 대응방안이다. 대한민국은 아직도 정보보호를 투자가 아닌 비용으로 인식하고 있다. 사이버 안보에 투자를 하고 산업자산을 지키기 위해선 정보보호 분야에 집중적으로 투자해야 할 필요가 있으며 공격기술보다는 방어기술에 투자를 집중해야 한다. 2015년 6월 22일 정보보호 산업진흥법이 공포됨에 따라 대한민국의 기업과 보안기술기업이 선진화된 기술경쟁력을 연구개발(R&D)할 수 있게 되었다.[259] 또한 첨단기술은 자체 연구 개발하는 것 외에는 대안이 없기 때문에 무엇보다 기술력 확보가 선행되어야 한다. 사이버전이 발생하면 우선 근원지를 역 추적하고 공격자의 신원을 식별하며 사이버공격 증거들을 확보하고 공격 원점을 타격하거나 동일한 수준의 목표물에 대해 부수적인 피해 없이 동일한 수준의 대응공격을 할 수 있는 능력을 갖춰야 한다[260]. 근원지 역 추적기술, 포렌식기술[261], 사이버 게놈기술[262], 사이버 반격기술에 대한 연구개발이 요구된다.[263] 이는 신속 정확한 원점 추적능력과 공격자 식별능력이 핵심적인 기술이자 억지력 확보의 기술이기 때문이다. 공공기관과 국가기반시설과 같이 민감한 기관의 인터넷과 인트라넷은 망 분리 및 보안 자동화 기술을 마련해야 한다. 기술탐색에서 연구개발에 이르는 프로세스가 빠르게 진행돼야 한다. 미래에는 모든 사물이 인터넷과 연결될 전망이다. 아무리 좋은 제품, 서비스도 사이버보안이 확보되지 못하면 다른 분야에 막대한 악영향을 미칠 수 있다. 인터넷 성장 규모에 비례하여 알려지지 않은 해킹기술을 연구하기 위한 지속적인 투자가 병행돼야 할 것이다.[264]

---

259) 『전자신문』, 2015년 07월 24일 (금) 오피니언 27면.
260) 임종인 외, 앞의 논문, p.40.
261) 디지털 포렌식 [digital forensics] : 디지털 기기를 매개체로 하여 발생한 특정 행위의 사실 관계를 법적으로 규명하고 증명하기 위한 절차와 방법을 말한다. 사건의 정확한 진상 규명을 위해 현대적 기술 및 장비와 과학적 기술 및 지식을 활용하는 과학 수사의 한 분야로, 과학수사는 원래 주로 법의학(forensic)을 기반으로 하였으나 1980년대 이후 디지털 포렌식 영역까지 확장되었다.
262) 사이버 게놈 [cyber genome] : 2010년 미국 국방부 산하 고등방위연구계획국(DARPA)이 처음 사용한 용어로, 인간의 유전체를 분석하듯 인터넷 악성코드를 분석하여 사이버 공격의 배후나 공격 경로 등을 밝혀내고 보안사고 등을 예방하기 위한 지능형 보안기술이다.
263) 위의 논문, p.40.
264) 주대준,『국민일보』, 2015년 02월 03일 화요일 026면 오피니언.

제2절 군차원의 대비방안

1. 기본개념

한국의 사이버 안보전략은 북한의 사이버 능력과 환경을 고려하여 방어위주로 작성하되 방어와 공격의 비율을 얼마로 하는 것이 최선인지 검토할 필요가 있다. 2012년 말 북한을 방문한 구글 회장은 북한의 인터넷 사용인구가 수천 명임을 고려해 볼 때 사이버 공격수단을 발전시킨다 하더라도 이를 인터넷에 적용하는데 많은 어려움이 예상된다고 하였다. [265]

사이버 공격수단 강구와 방어능력 확충이라는 선택에서 방어력 향상에 역량을 집중하는 것이 억지력 확보의 기본임을 확인할 수 있는 기회가 된 것이다.

북한의 사이버 공격으로 손상된 네트워크를 신속히 복원하여 사용할 수 있다면 그 자체로 억지력이 확보되는 것이다. 만약 북한은 계속해서 사이버 공격으로 효과를 보지 못하고 그 피해가 미미하다면 더 이상 사이버 공격의 매력을 느끼지 못하게 될 것이다. 한국은 국제사회에서 우호적인 협력관계와 한미 군사공조관계라는 장점을 가지고 있다. 그러나 사이버 공격과 방어 차원에서 북한과 달리 개방적인 사회의 운영과 표현의 자유, 프라이버시 등 민주적인 가치와 높은 인터넷 의존도와 같은 한국의 특징들은 사이버방어 차원에서 단점으로 작용할 수 있기 때문에 우리의 장점을 확대하고 단점을 보완하는 기본개념을 정립할 필요가 있다.

따라서 군차원에서는 국방사이버 전략을 구축하고 민·관·군 거버넌스(governance) 체계를 구축하여 임무를 수행할 필요가 있다. 군은 자체적인 정책과 수행개념을 발전시키고 인재를 양성하고 지휘체계를 보장해야 한다. 특히 한미 간에 긴밀한 사이버 공조체제를 구축하고 한미연합훈련을 통하여 사이버전 수행능력을 향상시킬 필요가 있다. 통합방위차원에서 군의 역할과 임무를 고려하여 군의 고유한 임무를 수행할 수 있도록 군의 역량을 대폭 강화해야 한다. 아울러서 북한의 사이버 공격에 한미가 상호 협력할 수 있도록 안보협의회 등에 그러한 내용을 포함시킬 필요성은 없는지 검토할 필요가 있다.

이와 같은 안보 환경에서 국가적인 프로젝트로 사이버 전력을 집중적으로 육성하여 국가안보에 치명적인 위협을 주는 북한의 사이버 공격이 국가기반시설에

265) 부형욱, “사이버안보의 주요이슈와 정책방향,” 『국방연구』, 제56권 제2호, p.113.

집중될 것에 대비하여 사이버전에서의 압도적인 능력을 보유할 필요가 있다.
우리는 북한을 포함한 한국을 공격하는 적대세력에게 국가적인 대전략 차원에서 강력한 사이버전 수행능력을 갖출 뿐 아니라 주변국들의 사이버 공격에도 대비할 수 있도록 역 비대칭전력으로 우위를 삼을 필요가 있다. 이를 위해 국가예산을 과감하게 투자하여 양적이나 질적으로 우월하고 뛰어난 화이트해커인 사이버 전사를 양성해야 한다. 방어형 사이버 무기를 지속적으로 개발하고 공격형 사이버 미사일인 한국형 스턱스넷 등을 하루빨리 개발하여 완성할 필요가 있다. 이를 위하여 사이버전에 대비한 중장기 종합발전계획을 수립하여 발전시켜야 한다.

특히 사이버 영토에서 군의 역할을 증대시킴으로써 사이버공간과 물리적인 공간의 위협을 효과적으로 통제하고 통합하여 적의 공격을 격퇴할 수 있도록 통합방위법을 포함한 전쟁법과 자위권 차원의 교전규칙 등 법률의 제·개정을 검토할 필요가 있을 것이다. 아울러서 사이버 전쟁에 대비한 국군사이버사령부의 임무와 역할을 재정립하고 내부조직을 강화할 필요가 있으며 각 군 본부와 국직부대, 작전사급의 사이버전 수행 조직에 대한 임무수행 능력을 진단하고 보강 계획을 구체화하여 지속적인 발전이 되도록 검토할 필요가 있다. 또한 기존의 육·해·공 전장에 사이버 전장과 우주를 포함시키는 5차원 전장 영역을 통합적으로 운용해 작전 속도와 효율성도 높일 필요성도 검토되어야 할 것이다.

장차 한반도에서 사이버전과 물리전의 동시전쟁 상황을 고려할 때 사이버전에서 승리하기 위하여 군은 정부와 국민의 적극적인 지지와 협조로 사이버 전력을 대폭적으로 보강하여 북한의 어떠한 사이버 공격에도 주도적으로 이를 해결할 수 있는 능력을 갖출 필요성이 있을 것이다.

2. 분야별 대응방향

가. 인식과 사상의 관점

전쟁에서 억지력(deterrent)은 공격자가 공격하려고 해도 상대방의 반격이 두려워 공격하지 못하게 하는 힘이다. 억지력을 위해 기본적으로 확보되어야 하는 것이 응징력이다. 이는 물리적인 전쟁은 물론 사이버전에서도 당연히 성립하는 전제조건이다. 그러나 사이버전은 공격자의 익명성이 상당 수준 보장된다는 점에서 응징력의 확보만으로 억지력을 가졌다고 할 수 없다. 공격자의 식별이 우선되어

야 하는데 즉각적인 신원파악이 어려운 만큼 보복하기가 어렵고, 공격자에게 공격 이상의 피해를 입힐 수 있다는 확신을 줄 수 없기 때문이다.
즉 물리적 억지력은 공격자의 식별이 가능한 반면 피해를 감내하는 것은 거의 불가능하나, 이에 반하여 사이버전은 공격자의 식별이 매우 어려운 반면 피해를 감내할 수 있는 정도의 피해라면 공격자로 하여금 공격에 대한 실행의지를 감소시킬 수 있다.

이를 구체적으로 살펴보면, 첫째, 사이버전의 억지력은 공격자를 식별하기 위한 기술개발 노력과 함께 방어를 강화함으로써 공격의 효과를 무력화시켜 달성할 수 있다. 만일 공자가 공격으로 인해 자신이 원하는 목표를 달성하지 못한다고 판단될 경우 공격자는 자신에 대한 역 추적 및 역공격의 위협을 무릅쓰고 무리하게 공격을 감행하기가 어려울 것이다. 이와 같이 사이버전에서 억지력 확보는 기본적인 보복역량을 갖추고 방어능력을 강화하여 공격의 효과를 크게 반감시키는 것이다. 이를 위해 공격주체를 식별하고 근원지를 무력화할 수 있는 능력을 확보하여야 하며 신속하고 효과적인 대응을 위한 법령과 제도의 정비가 요구된다. 둘째, 회복력이 대단히 중시된다는 점이다. 미 국방부는 우선적으로 네트워크의 구조적 결함을 근원적으로 해결할 방법을 찾아 네트워크 자체를 신뢰할 수 있는 상태로 만드는데 많은 노력을 하였다. 이렇게 보완된 네트워크에 보안장비 및 솔루션 등을 탑재하여 단말기부터 서버까지 보호하는 것이다. 이 방법을 사용하면 기술적으로는 어떠한 사이버 공격도 네트워크에 직접 침투하기가 어려운 장점이 있다. 설사 인간의 심리를 파고드는 사회공학기법[266]으로 일부 네트워크가 침투당하더라도 다른 네트워크들은 확실히 보호받을 수 있어 빠른 시간 내에 정상 수준으로 회복할 수 있는 것이다. 기술력이 아무리 뛰어나도 인간이 가진 취약점 때문에 회복력은 더욱 중시된다. 미국처럼 네트워크를 신뢰할 수 있게 만드는 방법에서 사이버 보안의 해법을 찾는 사고의 대전환이 필요한 이유다.

266) 컴퓨터 등 정보 전달 기술의 발전이 급속도로 진행되면서, 이것을 응용한 범죄 방지, 교통운수의 통제, 공해 방지 등을 능률적으로 수행하기 위해 여러 가지로 연구. 오늘 날 PC의 발전은 인간에게 막대한 영향을 끼치면서 이 분야에 대한 하나의 학문으로 자리잡아가고 있다.

나. 군사전략 등 시스템의 관점

1) 먼저 군가전략 등 시스템의 관점에서 본 군의 사이버전략 추진방향이다. 군의 사이버전략은 우선적으로 사이버 방어능력을 확충하는 것과 공격능력을 갖추는 것이다. 군은 북한의 사이버 공격에 대비하여 방어능력을 갖추는 것에 집중하되 공격무기 개발도 병행하여 추진하는 전략을 도입할 필요가 있다. 방어 대 공격능력의 비율을 얼마로 하는 것이 가장 효과적인 비율인지 안보환경과 정보통신기술의 능력에 따라 다르기 때문에 전문가들마다 의견이 다양하다. 미국의 국가안보전략연구소(CSIS)의 사이버 안보전문가 Jame Lewis 박사는 미국의 경우 5:5의 비율로 노력을 투입하는 것이 바람직하다는 평가를 하였다.[267] 한국의 경우 전문가들의 의견은 북한의 인터넷 인프라를 고려할 때 방어보다 공격수단의 적용가능성이 상대적으로 떨어지기 때문에 방어와 공격비율을 7:3 정도로 보고 추진하는 것이 바람직하다고 한다.[268] 즉 국방부의 사이버 전략의 방향은 방어에 중점을 두는 것으로 방어능력의 강화는 복원력의 증대를 가져오며 이는 곧 사이버 억지력으로 이어질 수 있기 때문이다.

따라서 북한의 사이버공격에 망 분리, 백신프로그램 설치, 보안전문인력 확충 등 수동적인 방법에서 적극적으로 북한이 이용하고 있는 해외의 사이버공격 거점을 색출하고 해당국 정부에게 폐쇄를 요청하는 등 북한의 사이버공격에 대한 억제효과를 갖도록 하는 것이 필요하다. 이는 북한의 사이버공격이 해외거점에서 수행되거나 해외 망을 통해서 이루어지기 때문이다. 대남 사이버공격에 사용된 IP를 집중적으로 추적하고 별도의 인적 정보를 활용한다면 북한의 해외 사이버 공격 거점을 확인할 수 있을 것이다.[269] 군은 국가안보를 위해 현재 운용중인 국방망과 자원망, 전장망 뿐만 아니라 군사작전에 영향을 미치는 정부의 핵심기간망과 핵심인프라에 대한 방어에도 영역을 확장하여 선제적으로 방어할 필요가 있다. 한편 미국과 러시아는 사이버 공격에 군사력으로 대응을 실시하겠다고 천명하였다. 그러나 우리나라가 이 방법을 채택하기에는 고려할 요소가 많다고 판단한다. 가능한 방법은 '비례성의 원칙'에 입각해 우리가 피해를 받은 만큼 사

267) 미국 '국제전략문제연구소(Center for Strategi c &International Studies)'를 말한다. 워싱턴DC에 본부를 두고 있으며 국제 전략적인 이슈를 연구하는 싱크 탱크로. 62년 공화당 하원의원을 지낸 데이비드 앱시러가 영국의 국제전략문제연구소(IISS)를 본떠 만들었다.
268) 부형욱, 앞의 논문, p.115.
269) 임종인 외, 앞의 논문, pp.39-41.

이버상에서 대응공격을 가하거나 물리적으로 상응한 보복을 하는 방안을 찾아야 할 것이다. 이를 통해서 군은 억지력을 강화하고 필요시 공세적인 전략을 구사하기 위해 구체적인 목표와 추진방향을 담은 '국방사이버안보전략'을 수립하여 적의 공격을 사전에 억지할 수 있도록 전략을 발전시킬 필요가 있다.

2) 다음은 군이 사이버전을 주도하되 민, 관, 군 거버넌스(governance) 체계를 구축하는 방안이다.[270] 세계 각국은 사이버공간의 주도권 확보를 위해 각축을 벌이고 있다. 특히 국가적 차원에서 적극적인 사이버안보전략수립 및 홍보를 통하여 주도권 경쟁을 벌이고 있다. 사이버테러와 전쟁에 대한 대응은 군의 주도로 이루어지고 있다. 미국은 사이버사령부가 모든 사이버전에 대한 실질적인 컨트롤타워 역할을 수행하여 민·관·군 모든 기관의 지원을 받고 있다. 중국은 인민해방군 총참모부가 사이버전을 기획, 실행하며, 민간 기구를 통제하여 국가 관리차원의 광통신망과 IP를 제공받고 있다. 한국도 물리전과 연계한 북한의 사이버 공격에 효과적으로 대응하기 위해서 군이 주도적인 역할을 하도록 수행 인원과 조직을 대폭 증원하여 임무를 수행하도록 하는 것이다.

따라서 <표 17>과 <표 18>에서 보는 바와 같이 북한의 사이버 공격이 예상되는 국가핵심기반시설의 대상을 사전에 선정하고 대상별로 적의 공격을 사전에 예측하여 공격시 피해의 심각성과 군사 작전의 영향을 미치는 강도를 1~5로 구분하여 군이 어디서부터 관여하는 것이 효과적인지 판단할 수 있는 도표를 작성하였다. 특히 군사작전에 영향을 심각하게 미치는 기준을 3으로 선정하여 3이상에 해당하는 대상 국가핵심시반시설은 평시부터 군이 주도하여 민·관·군 통합방위를 하는 방안을 제시하였다.

270) 국가경영' 또는 '공공경영'이라고도 번역되며, 최근에는 행정을 '거버넌스'의 개념으로 보는 견해가 확산되어 가고 있다. 거버넌스의 개념은 신공공관리론(新公共管理論)에서 중요시되는 개념으로서 국가·정부의 통치기구 등의 조직체를 가리키는 'government'와 구별된다.

<표 17> 사이버 공격 시 주요 대상 분석(국가·공공·민간)

구분			가능성					심각성					군 작전에 미치는 영향				
			1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
교통수단	항공		■	■				■	■	■	■	■	■	■	■	■	■
	철도		■	■	■			■	■	■	■		■	■	■	■	
	지하철		■	■	■			■	■	■			■	■			
	항만		■	■	■			■	■	■			■	■	■		
	물류		■	■				■	■				■	■	■		
	도로		■	■	■			■	■				■	■			
	교량		■					■					■	■	■		
	터널		■					■	■				■	■			
원자력	원자력발전소		■	■	■			■	■	■	■	■	■	■	■	■	■
	원자력본부		■	■				■	■	■	■		■	■	■	■	
	핵폐기물 보관시설		■					■	■	■			■	■	■		
에너지 시설	전력		■	■	■	■		■	■	■	■	■	■	■	■		
	석유		■	■				■	■	■			■	■	■		
	가스		■	■				■	■	■	■		■	■			
수자원 시설	정수시설		■	■				■	■	■			■	■			
	댐		■	■				■	■	■	■		■	■	■		
화학	화학물질 보관시설		■	■				■	■	■	■	■	■	■	■	■	■
정보통신 시설	통신국		■	■	■			■	■	■			■	■	■	■	
	망관리센터		■	■	■			■	■	■	■		■	■	■		
	인터넷 관문국		■	■	■			■	■	■	■		■	■			
	해저케이블		■	■	■	■		■	■	■	■	■	■	■	■		
	주요 DNS 서버		■	■	■			■	■	■	■		■				
	국가안보 통신망	국가지도통신망	■	■	■			■	■	■			■	■	■		
		경호통신망	■	■	■			■	■	■			■	■	■		
	재난통신망		■	■				■	■				■				
	민방위경보통신망		■	■				■	■				■				
	인공위성, 국제위성지구국		■	■				■	■				■				

군은 국가의 모든 역량을 총 동원하여 총력전 형태로 대응해야 한다. 따라서 정부와 민간기관의 적극적인 협조와 참여를 유도할 필요가 있다.[271] 그렇게 하기 위해서는 방어할 목표를 정확히 식별해야 한다. 즉 국가지정 핵심시설과 같은 시설에 우선순위를 부여하여 목표를 선정하는 것이다. 교통수단, 원자력, 에너지시설, 수자원시설, 화학시설, 정보통신시설, 보건의료시설, 금융시설, 방송언론시설, 산업시설, 연구시설, 정부기관, 민간기관 등에 우선순위를 부여하고 방어차원에서 군이 민과 관을 선도하는 시스템을 구축하는 것이다.

271) 부형욱, 앞의 논문, pp.114-115.

<표 18> 사이버 공격 시 주요 대상 분석(국가・공공・민간)

구분			가능성					심각성					군 작전에 미치는 영향				
			1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
보건의료	응급의료정보센터		■	■				■	■				■				
	병원		■	■				■	■				■				
	혈액관리시설		■	■	■			■	■	■			■	■	■		
금융시설	금융전산망		■	■	■			■	■	■	■		■				
	은행		■	■	■			■	■	■	■		■				
	증권거래소		■	■	■			■	■	■	■		■				
방송언론	방송시설		■	■	■	■		■	■	■	■		■				
	언론사		■	■	■	■		■	■	■			■				
산업시설	대규모산업시설		■	■	■			■	■				■				
	군수 산업체	중화기 생산시설	■	■				■	■				■	■			
		총・포・화학류 생산 시설	■	■				■	■				■	■			
		기타 전투장비 생산 시설	■	■				■	■				■	■			
연구시설	원자력, 국방과학 연구소		■					■	■	■			■				
기타	교정시설		■					■	■				■				
	대도시 지하 공동구		■					■	■				■	■			
정부	행정정보망		■	■	■			■	■	■			■	■	■		
	외교정보전용망		■	■				■	■				■				
	정부통합전산센터		■	■	■			■	■	■			■	■	■		
	G4C 시스템		■	■	■			■	■	■			■	■	■		
	정부시설(청와대, 국회 등)		■	■				■	■	■			■	■			
	정부기관 홈페이지		■	■	■			■	■				■				
민간	민간PC		■	■	■	■	■	■	■	■			■				
	개인 스마트폰		■	■	■	■	■	■	■				■				
	SNS		■	■	■			■	■				■				
	인터넷 포털 / 홈페이지		■	■	■			■	■	■			■	■			
	IDC 센터(분당IDC 등)		■	■	■			■	■	■			■				
	민간보안업체(백신업체)		■	■				■	■	■	■		■	■	■		

사이버 방어능력을 확충할 수 있도록 확실한 유인책이 필요하고 범정부 차원의 TF를 구성하여 임무를 수행하는 방안도 있다. 민에 대해서는 합의 형식의 규제 체계를 구축하고, 관에 대해서는 협조체계를 명령, 규정 등에 포함하여 운영하는 것이다. 이렇게 하여 사이버 공격에 대한 후속조치를 책임지고 수행하며 차후에 이와 같은 일이 반복되지 않도록 사후조치를 철저히 검증하고 관리하는 것이다.

또한 각 군은 독자적으로 사이버전을 수행할 수 있도록 조직을 정비하고 인원을 증원하여 실질적으로 사이버 도발 현장에서 관련 기관을 주도할 수 있어야

한다. 따라서 '통합방위법'의 개정을 할 수 있는 기반을 만들어 군· 관· 민이 통합적으로 대응하는 총력전체계를 구축하는 방안이다. 주기적으로 관련기관과 협조회의를 통하여 전략 전술을 발전시키고 사이버 공격 상황이 발생하면 자체 조직과 유관기관이 협력하여 대응하여야 한다. 이를 위해 군은 북한의 사이버 공격에 따른 군사적 대응 시나리오를 개발해야 한다. 또한 한미 간에 연합작전을 고려하여 한미 안보협의회의(SCM)나 한미 군사협의회의(MCM)에서 사이버 위협에 공동으로 대응할 수 있는 방안을 찾아서 한미연합 사이버전 수행체계를 구축하는 방안도 검토할 필요가 있다.

3) 다음은 군의 사이버전 법령과 제도의 발전이다. 세계 각국이 사이버 공간에서 전쟁을 치르고 있지만 우리는 사이버 안보에 관한 기본 법률조차 없는 상태다. 따라서 현재 국회에서 발의하고 있는 사이버테러에 관련한 법령의 개정방향을 검토할 필요가 있다. 사이버 공격이 사이버범죄와 테러 쪽에 가까우면 형법 등 형사법적으로 처리하는 방안과 국가안보를 위해하는 성격이면 전쟁법적 대응방식을 검토하는 방안이다. 전쟁법적 규율에 있어서는 Jus ad Bellum의 법과 Jus in Bello의 법이 있다. Jus ad Bellum이란 무력충돌을 다루는 법으로 국가가 어떤 방식으로 무력을 사용해야 하며 어떠한 경우에 군사력의 사용이 법적·도덕적으로 정당한지 기준을 제공해 준다.[272] Jus in Bello는 무력충돌이 일어난 후 국가들의 행동을 통제하는 법으로 전쟁수행 단계에서 어떠한 법적·도덕적 제지가 있는지 규정하고 있는 법이다.[273] Jus ad Bellum의 관점에서는 국가가 사이버테러에 대한 방어의 목적으로 군사력을 사용할 수 있는가 하는 점이고 Jus in Bello 관점에서는 국가가 무력충돌시 적법하게 대상세력에 사이버공격을 감행할 수 있는가 하는 점이다.[274]

한편 미국은 탈린매뉴얼 수칙에 참여한 Schmitt 교수가 주장한 효과위주 접근방법에서 사이버 공격으로 인해 물리적 피해나 인적피해가 발생할 경우에 자위적차원의 무력대응을 정당화한다는 개념이다. 다시 말하면 사이버 공격의 효과가 기존의 전쟁수행방식에 의한 효과와 유사할 경우 즉 사망, 부상, 피해 및 파괴를

272) Operational Law Handbook, The Judge Advocate General's Legal Center & School. 2007. p.121.
273) Michael N. Schmitt. Wired Warfare : Computer Network Attack and Jus in Bello. 846 International Review of the Red Cross. 2002. p.368.
274) 김홍석, 앞의 논문, pp.97-101.

야기하는 경우에 무력공격에 해당한다고 본 것이다. 따라서 우리도 북한의 사이버 공격에 대하여 전쟁법적 대응에 관한 논의를 시작할 필요가 있다. 즉 북한의 물리전과 연계한 사이버전에 대응하기 위해서는 전쟁법적인 관점에서 논의가 필요하다는 것이다. 탈린매뉴얼을 근간으로 사이버 전쟁에 관한 법령과 제도의 대책을 위한 '국가사이버전쟁에 관한 법률(안)'을 검토할 필요가 있을 것이다.[275]

아울러서 전·평시에 적용할 현행 통합방위법의 개정도 검토할 필요성이 있다. 이 법령에는 군이 영토, 영공, 영해를 수호한다고 돼있지만 사이버 공간은 포함돼 있지 않기 때문이다. 군사작전과 연계한 군의 역할과 작전임무 수행을 보장할 수 있는 법적 기반이 부재하기 때문에 능동적으로 사이버 대응작전을 체계적으로 수행할 수 있는 법과 제도의 개선이 필요한 것이다. 따라서 적의 사이버 공격 시 총력전 개념의 통합방위작전을 수행하도록 통합방위법의 개정이 필요한 실정이다. 이러한 통합방위법의 개정방향은 첫째, 통합방위 관할구역에 지상, 해상, 공중의 관할구역에 사이버 영역과 책임자를 추가적으로 포함하는 것이며 둘째, 통합방위사태에 '사이버공격'으로 인하여 발생한 비상사태를 포함하며 셋째, 방호작전에 '사이버 방호' 활동을 포함하는 것이다. 이를 위해서 국방부와 국정원, 국무총리실과 국가안보실간에 긴밀한 협의가 필요하리라 판단된다.

또한 평시에 자위권 차원에서 북한의 사이버 공격을 억제하기 위한 방안을 검토할 필요가 있다. UN헌장 제2조 제4절은 국가가 다른 국가에 군사력을 사용하거나 위협하는 것을 금지한다. 예외적인 경우는 UN안전보장이사회의 허가가 있는 경우와 자기방어의 경우가 있으나 UN헌장의 정신은 가급적 전쟁을 억제하는 데 있다. 미국의 '사이버 공간에 대한 국제 전략보고서(ISC)'에 따르면 "사이버 공간에서 법의 지배를 지원하는 환경을 구축하고 이러한 규범과 관련하여 근본적인 자유보장, 재산권 존중, 프라이버시 중시, 범죄로부터 보호를 위해 자위권을 행사할 수 있다."고 제시하고 있다.[276] 그러나 이에 따른 자위권 적용과 관련하여 먼저 사이버 공격의 주체를 확인하는데 장기간 시간이 소요됨을 고려하여 '사후적 자위권' 조치의 개념에 대한 공감대가 필요하다. 이는 미국의 9.11 테러에 대한 대응과정을 통해 테러를 자행한 알카에다 조직 과 아프가니스탄의 탈레반 정부에 대한 '사후적 자위권'을 행사한 경우에서 그 예를 찾을 수 있

275) 박대우(c), "국가 사이버안보에 관한 법률(안)," 『국가사이버안보정책포럼』, (2013년 5월 14일), p.56.
276) International Strategy for Cyberspace(ISC)(White house, 2011), p.10.

다. 따라서 북한이 사이버 공격을 감행하여 국가안보에 치명적인 영향을 끼칠 경우에는 '사후적 자위권' 차원에서 적의 전쟁지도부 또는 사이버 공격의 근거지를 물리적으로 타격하는 방안에 대해서도 가능성을 열어놓아 북한의 사이버 공격에 대한 억지력을 높여야 할 것이다.[277] 이는 합동작전의 영역이 우주, 사이버 영역까지 확장되고 북한의 사이버전 능력과 위협이 심각하게 증가되는 안보환경과 이를 통하여 물리적 파괴 가능성이 있는 현실을 고려한다면 사이버 상에서도 적의 공격에 대한 자위권을 행사할 수 있도록 적극적으로 교전규칙을 검토할 필요성이 있을 것이다.

4) 다음은 사이버전과 관련한 기본정책과 수행체계의 발전방안이다. 사이버 안보를 총괄하는 국무조정실의 '국가사이버안보처(가칭)'와 연계하여 국방부, 합참, 사이버사령부, 각 군은 사이버전에 대비한 기본정책개념과 이를 수행할 수 있는 계획을 발전시켜야 한다. 첫째, 군은 사이버전의 특성을 고려하여 전·평시와 위기시 대응개념을 발전시킬 필요가 있다. 사이버전의 개념은 방어에 집중하되 공세적으로 북한의 사이버 공격에 능동적으로 대응할 필요가 있다. 먼저 방어능력 확충을 위해 평시부터 북한의 공격이 예상되는 국가·공공·민간 대상의 기간망과 국방망의 공격수단을 탐색하고 제거하는 방호활동을 추진하며 해외에서 활동 중인 북한의 공격수들을 감시하고 추적하여 제거하는 역할을 해야 한다. 위기시는 초기대응능력 강화에 중점을 두어야 한다. 특히 국제공조를 통해 빠른 시간 내에 정보를 공유할 수 있어야 한다. 신속한 정보공유가 문제를 해결하는 결정적으로 중요한 요소가 되기 때문이다. 국내 유관기관 간 협조를 통해 2차, 3차 공격의 파급력을 제어하면서 신속하게 복구에 주력하는 것도 중요하다.[278] 아울러 사이버 공격원점을 파악하여 국제적인 공조와 비례성의 원칙하에 대응공격을 실시함으로써 피해를 최소화하는 것이다. 이러한 노력은 평시에 유관기관과의 협조체제가 위기시에 그 능력을 발휘할 수 있기 때문에 사전에 준비가 대단히 중요하다. 전시에 사이버 공격에 대한 대응은 물리적인 타격이 가장 효과적이다. 따라서 평시에 적이 어디서 어떻게 공격하는지 공격원점을 확인하여 표적화할 필요가 있다.

둘째, 사이버전 수행체계를 발전시키는 방안이다. 북한의 사이버 공격이 물리

277) 임종인 외, 앞의 논문, pp.38-39.
278) 부형욱, 앞의 논문, p.117.

전과 연계하여 대한민국을 위협한다면 엄청난 시너지 효과로 인하여 한미 연합전력의 운용에 큰 차질을 빚게 될 것이다. 한국은 북한의 사이버 공격과 물리적인 공격에 효과적으로 방어할 수 있는 전쟁수행체계를 마련해야 할 필요성이 있다. 특히 사이버 영토에서도 군의 역할을 증대시킴으로써 사이버공간과 물리적인 공간의 위협을 효과적으로 통제하고 통합하여 적의 공격을 격퇴하여야 한다.
다행스럽게 정부는 2015년 2월 국무회의를 통해서 합참의장의 권한에 '사이버작전의 조정 및 통제'를 추가한 것이다. 따라서 합참은 사이버 역량을 활용하여 군에서 운용하는 C4ISR과 무기체계인 PGM을 포함한 국가기관과 국가기반시설을 방어하는데 임무와 역할을 확대하여 재조정할 필요가 있다. 공공영역의 일부를 평시부터 군이 주도하여 관리하는 것이다.

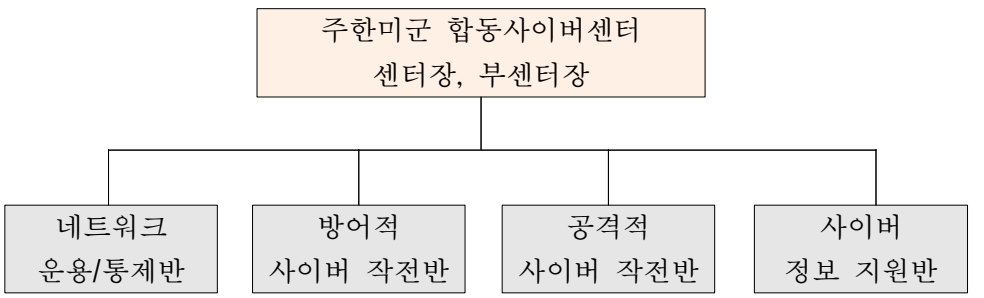
이를 위해서 합참은 사이버작전과 군사작전을 지휘통제실에서 통합하여 운용할 수 있는 수행체계를 검토할 필요가 있다. 즉, 사이버 상황과 군사상황을 동시에 보고받고 처리할 수 있는 지휘통제실과 연계한 상황관제시설이 위치할 공간이 필요한 것이다. 이와 같이 '사이버상황관제실(가칭)'은 합참의 지휘통제실과 함께 위치하면서 물리적인 상황과 동시에 사이버 상황을 동시에 보고받고 처리하는 개념이다. 이는 북한군의 장사정포 위협에 효과적으로 대응하기 위하여 지구사의 '대화력전수행본부'와 같은 기관을 운용하여 초기에 적을 격멸하는 개념으로 '사이버상황관제실(가칭)'을 발전시키면 가능하다고 판단한다. 이는 '사이버상황관제실(가칭)'이 어느 제대에 위치하든지 명령이나 지침을 하달하는 임무뿐만 아니라 현장에서 실시간으로 직접 사이버 전투임무를 수행하는 기관이 될 것이기 때문이다. 또한 합참에서 효과적으로 사이버 작전임무수행이 가능하려면 정보본부장과 작전본부장, 사이버사령관이 대등한 위치에서 사이버작전과 군사작전을 통합하고 조정하는 임무를 수행하는 방안이다. 사이버사령관 부재시는 사이버사령부에서 '사이버작전협조관(가칭)'을 합참에 파견하여 임무를 수행하게 할 수 있다.

따라서 사이버사령관의 임무수행 방안을 국방부에서 합참과 협조하여 세부적으로 검토할 필요성이 있을 것으로 판단된다. 사이버 사령부의 임무가 확장되면 아울러 공공영역의 업무를 일부 군으로 이양할 필요성도 동시에 검토되어야 할 것이다. 또한 사이버사령관의 계급도 소장에서 중장으로 상향조정하여 업무의 효율성과 작전수행능력의 향상을 위해 검토할 필요성이 있다. 사이버 작전임무수행

과 관련하여 합참은 작전지원본부에서 작전본부로 사이버 작전의 임무를 전환하여 수행하는 것이 바람직할 것으로 판단되며 조직도 강화하여 작전본부 예하에 '사이버작전부(가칭)'를 설치할 필요가 있다.

또한 국방부도 국방정책실에 '사이버정책국(가칭)'을 설치하여 국방사이버전과 관련한 업무를 전담하는 것을 검토할 필요가 있다. 그리고 국방의 총괄과 조정역할을 할 수 있는 '사이버국방조정위원회(가칭)'의 설치도 고려해 볼 필요가 있다. 각 군 본부도 '사이버사령부(가칭)'를 설치하는 것을 검토할 필요가 있다. 특히 육군은 국가의 기반시설이 대부분 수도권과 2작사 후방지역에 위치함을 고려하여 '육군사이버사령부(가칭)'의 창설이 더욱 필요할 것으로 판단된다. 또한 수방사와 2작사에도 '사이버신속대응팀(가칭)'을 설치할 필요가 있다. 북한의 사이버 공격이 시행되면 즉시 통합방위법에 의거하여 지역의 실질적인 작전수행을 총괄할 수 있도록 역량을 갖춰야 할 것이다. 그리고 작전사급 부대에서 사이버작전을 전담할 조직은 작전부서에서 임무를 수행하는 것이 바람직할 것으로 판단된다. 전반적으로 각 군 본부와 국직부대, 작전사급 사이버전 수행조직에 대한 임무수행 능력을 진단하고 보강계획을 구체화할 필요성이 있다.

<그림 15> 주한 미군 합동사이버센터



* JCC : Joint Cyber Center(합동사이버센터)의 임무
 - 사이버 관련 주한미군 사령관 보좌,
 - 한국전구 내 사이버 위협 정보수집 및 대응,
 - 주한미군 정보작전방호태세(INFOCON) 업무 수행(태세 변경 건의 등)
* 편성 : 00명

아울러서 한미연합 사이버 작전을 효율적으로 수행할 수 있도록 공조체제를 강

화해야 한다. <그림 15>에서 보는 바와 같이 연합사에 주한미군의 합동사이버센터(JCC: Joint Cyber Center)와 같은 개념의 '연합사이버센터(가칭)'를 편성하는 방안도 검토할 필요가 있다. 그리고 주변국과 사이버 협력체계를 지속적으로 발전시켜 나갈 필요성도 있을 것이다.

5) 다음은 사이버 작전계획과 전투발전계획을 보강하는 방안이다. 북한의 사이버 공격능력과 방어 능력을 종합적으로 분석하고 우리의 사이버전 수행 능력을 고려하여 실효성 있는 사이버 방어와 공격, 지원계획을 발전시켜야 한다. 이는 적의 사이버 공격으로부터 아군의 정보체계를 보호하면서 사이버 공격을 통하여 적의 정보체계를 파괴 또는 마비시키는 것이다. 즉 사이버 수단을 공세적으로 활용하여 적의 전쟁지휘체계 등을 마비시키는 계획발전이 필요한 것이다. 합참에서 주도적으로 작전계획을 발전시키되, 사이버사령부도 관련기관과 협조하여 계획을 발전시켜야 한다. 특히 평소부터 국정원, 한국인터넷진흥원, 경찰 등과 협조하고 국회와 민간기관과 협조하여 공조체계를 긴밀히 하고 각종 학술대회나 세미나를 통해서 지식과 기술을 연구하고 발전시켜야 한다.

또한 전투발전 차원에서 교리, 조직, 교육훈련, 무기 · 장비 · 물자, 인적자원, 시설 등 사이버전을 뒷받침할 수 있도록 종합적인 발전계획을 수립하여 추진할 필요가 있다. 첫째, 사이버전 교리는 미국과 이스라엘의 사이버 작전교리를 참고하면서 한국적 현실에 부합된 교리로 정립하는 것을 검토할 필요가 있다. 국정원, 한국인터넷진흥원, KIDA, 국방대, 합동대 등 관련기관을 포함하는 교리발전 TF구성도 검토할 필요가 있다. 둘째, 교육훈련은 사이버 요원 양성 및 보수교육 체계 등 개인훈련과 팀 훈련체계를 정립하고, 연합 및 합동 훈련 시 사이버 상황과 연계된 훈련과 부대별 사이버전 대응 수준을 평가하여야 한다. 셋째, 사이버 무기는 선진 사이버무기 발전추세 연구 등 소요기획과 연계하여 체계적인 사이버전 기술과 무기를 발전시켜야 한다. 넷째, 인적 요소는 기술적인 전문 인력과 사이버전 기획 및 운용 분야의 전문 인력으로 구분하여 획득하고 관리하며 사이버 특기 등 저변을 확대해야 할 것이다. 다섯째, 시설은 현재의 사이버전 대응 시설들의 취약성을 재진단하고 물리적인 취약점과 네트워크적인 취약점 등을 고려 종합적인 사이버전 시설을 확충하여야 할 것이다. 그러나 이와 같은 노력에도 불구하고 사이버 위협의 실체를 정확히 진단하는 것은 쉽지 않은 일이지만 예산의 대폭적인 투자로 기존의 능력을 체계화하고 관련기관과 공조하며 유능한 인

재를 적극적으로 영입하여 획기적으로 능력을 향상시켜야 할 것이다.

다. 공조체제 등 네트워크의 관점

사이버 도발을 억제하기 위해서는 국제적인 협력과 공조체제가 중요하다. 사이버 공격이 외국의 경유지를 통해서 이루어지는 경우 다자간 또는 양자간 국제협력 강화는 필수적이다. 특히 한국은 북한의 사이버 공격을 방어하기 위해서 미국을 비롯한 중국, 일본 등 동북아 지역의 국가들과 정보공유와 협력을 강화해야 할 것이다. 국내에서 협력만큼 국제적인 협력도 중요하다. 사이버 공격이 자국에서 일어나지 않고 외국에서 시작되거나 경유지를 통해 이루어진다면 최종 목적지인 자국에서 차단하는 것은 용이하지 않다. 많은 예산을 투자하여 방어하는 것도 중요하지만 원천지에서 차단하거나 중간 경유지에서 해결할 수 있는 방안이 있다면 방어에 매우 효과적이다. 국방 분야에서 대외 협력을 위해 '한미 사이버 정보교류회의(가칭)'의 실시, '서울안보대화(SDD)' 내에 '사이버워킹그룹 운영(가칭)' 등을 통한 협력방안을 마련하는 것을 생각해 볼 수 있다.

군이 관심을 가지고 참가할 수 있는 사이버전과 관련된 대표적인 훈련은 2006년부터 미국의 국토안보부에서 주관하고, 민·관·군이 참여하는 '사이버 스톰(Cyber Storm)'으로 사이버 공격에 대한 대응훈련이다. 국제공동 모의훈련에 국제기구 수준인 '아시아태평양 침해사고 대응협의회(APCERT, Asia-Pacific Computer Emergency Response Team)'에서 주관하는 국제모의훈련이 있다. 2013년의 경우 한국, 중국 등 22개국의 컴퓨터침해대응팀(CERT)팀이 참여하였다.[279] 모의훈련은 사전에 시나리오가 공개되지 않는 '블라인드 드릴(Blind Drill)' 형태로 진행되고, 여러 국가에 걸친 서비스거부공격(DoS, Denial of Service)을 주제로 하여, 공격 IP 차단, 악성코드 분석 등의 훈련이 이루어진다. 이와 같은 훈련은 사이버 공격은 국경이 없는 만큼 발생 초기에 각국이 공조하여 피해확산을 방지할 수 있는 공조체계를 발전시키는데 그 의미가 있다고 평가된다. NATO에서도 2013년에 실시된 '락키드 쉴드(Locked Shields)' 훈련에는 군인과 민간전문가, 민간기업의 보안전문가가 참여하여 사이버 방어훈련을 하였다.

279) KISA, "아태지역 사이버 공격 국제공도 모의실험 참여," 『KISA 보도자료』(2013.1). 2003년 설립된 APCERT는 아·태지역 국가의 대표적 침해사고대응팀(CERT)이 참여하는 협의체로 KISA는 부의장 및 운영위원으로 활동 중이다.

국제적 협력을 위해 우리가 먼저 해결책을 제시하거나 이에 필요한 각종 기반 시스템을 상대국에 제공할 필요도 있다. 이를 통하여 우리의 사이버 안보 능력이 국제적으로 인정받는 것은 물론, 우리나라의 관련 정보보호 산업 활성화에 크게 기여하게 될 것이다. 정부 대 정부 협력 외에 국외 민간기업, 국제 NGO와의 정보교류가 증대될 것을 고려하여 이에 대한 채널을 구축할 준비도 필요할 것이다.

라. 인력과 기술 등 지원적인 관점

먼저 전문인력 확보방안이다. 국방 분야에 있어서 우리 군이 배울 수 있는 모델은 이스라엘이다. 이스라엘도 한국처럼 국민개병제로 의무 복무하는 시스템이다. 모든 나라에 명문 대학이 있다면 이스라엘은 8200부대와 같은 명문 엘리트 부대가 있다. 8200부대는 구성원들 간에 평등하며 중요한 사태가 벌어졌을 때 현장 부대 책임자에게 독립성이 부여되며 실제로 현장 지휘관에게 중대한 작전결정권을 부여한다. “지원은 없다. 스스로 해결하라”는 것이 이스라엘군의 기본 방침이다.[280] 지휘방침이나 상황조치방식 등을 놓고 상하급자들이 동등한 입장에서 부단한 토론과 회의를 하며 토론석상에서 하급자가 상급자에게 도전하는 것은 기본이며 장려된다. 이를 통해 부대원들은 군복무를 통해 실전을 겪으면서 혁신적 사고를 발달시키며 창의성, 민첩성, 리스크테이킹 등 국가안보와 기업 활동에 필요한 능력을 키운다.[281] 이스라엘은 군복무를 통해서 형성된 인적네트워크가 중요하며 8200부대 출신이면 한평생을 같이 할 평생 전우가 된다. 이처럼 우수한 청년들이 8200부대에 들어가고, 국가안보를 위해 가장 최신의 학문과 기술, 최고의 IT기술을 배운다. 이 과정에서 장병들은 실전경험을 쌓고, 양자역학, 분석 알고리즘 등 최신 학문을 배우게 된다.[282] 8200부대는 뛰어난 젊은이들에게 기술을 연마할 기회를 제공하며 창의성을 일깨우고 장려하는 곳이다. 기업은 사람을 뽑을 때 당연히 8200부대 출신을 우선시하며 8200부대 출신자들은 이스라엘의 성공적인 하이테크산업에 인적 및 기술자원을 공급함으로써 국가에 엄청난 공헌을 한다. ‘나이스’, ‘컴버스’, ‘체크포인트’ 등 이스라엘 3대 하이테크 업

280) 박대우(b), 앞의 논문, PP.48-50.
281) 리스크 테이킹 [risk taking] : 위험을 감지해서 위험의 크기를 평가하는 것은 위험지각(risk perception) 또는 위험인지(risk cognition)라 하며, 위험을 지각한 뒤, 굳이 행동하는 것이 위험감행(risk taking)이다.
282) 박대우(b), 위의 논문, p.49.

체는 8200부대 출신이 세운 것들이다.[283] 미국 나스닥에 상장된 '체크포인트'의 CEO인 길 슈웨드는 이스라엘의 최고 부자로 18세부터 4년간 8200부대 근무한 경험이 있으며 8200부대 출신자들 가운데 이스라엘의 IT산업을 세계 최고 수준으로 올려놓은 기업가나 엔지니어들이 다수 배출되었다.[284]

이와 같이 우리 군도 이스라엘의 '탈피오트 프로그램'과 같은 방식으로 우수한 인재를 선발하여 사이버 분야의 전문 인력으로 양성할 수 있는 다양한 방안을 강구할 필요가 있다. 각 군에서는 이스라엘의 8200부대와 같은 '사이버 연구소(R&D)'와 '정보체계단'과 같은 조직을 활용하여 사이버 전사를 배출하고 이들이 창업할 수 있는 여건을 부여하는 방안이다.[285] 예를 들면 고려대학교 사이버국방학과에서 양성되는 인력이 2016년부터 매년 30명 규모로 배출되며 7년의 의무복무를 고려시 활용 가능한 인원은 210여 명 규모로 판단할 수 있다. 기존에 있는 자원들과 이들을 중심으로 팀을 편성하여 한국군 사이버 임무부대로 활용할 경우 210개 팀장×10명= 2,100여 명 규모의 정예 사이버 임무부대를 구축할 수 있다. 물론 1개 팀의 규모는 미국의 30~60여 명보다 적은 10여 명으로 구성하지만 사이버전은 기술 집약적인 분야로 경험자들의 의견은 10여 명으로 구성된 팀을 최적의 규모로 판단할 수 있다.

인재선발시 민간기관의 전문가도 군에서 활용할 수 있도록 사이버 인재풀을 구축할 필요가 있다. 사이버전 전문 인력 획득을 위해서는 입대자원자 뿐만 아니라 우수인력의 입대를 유도하거나 민간 우수인력을 활용하는 시스템도 검토할 필요가 있다. 예를 들면 공익근무요원제도를 군 정보통신기반시설에 근무시키는 방안과 사이버전 특기병을 선발하고 사이버병과를 신설하는 방안도 있다.[286] 고려대 사이버 국방학과와 같이 민간대학과 학군협약을 통해 사이버전 학과를 설치하여 우수자에게 재학기간 중 장학금을 지급하고 국방과학연구소나 국군사이버사령부에 근무케 하여 사이버전 무기개발이나 연구업무 등을 수행하게 함으로서 군복무를 면제해 주거나 사이버전 전문 인력으로 양성하는 방안이다.[287]

---

283) 박대우(b), 앞의 논문, p.50.
284) 정시아, "사이버전쟁 선언 이스라엘의 비밀 무기는 8200부대!," 『주간조선』, 2211호, 2012년 6월 18일.
285) 부형욱, 앞의 논문, pp.117-118.
286) 박휘락, "북한의 비대칭위협에 대한 한국의 군사적 대응전략," 『전략연구』, 통권57호 (한국전략문제연구소, 2013.3), P.298.
287) 박대우(b), 앞의 논문, p.50.

실제로 우리나라 해커들 중에는 고졸 학력자가 많다. 이들이 사이버 보안 전문 인력으로 인정받지 못해 범죄자로 전락하는 경우가 적지 않다. 해킹 기술에 관심 있는 사람들보다 해킹을 즐기는 사람들에 투자할 필요가 있다. 사이버전은 기술만으로 치르는 것이 아니기 때문이다.[288] 사이버작전을 전술급 제대에서 수행할 수 있도록 전문 인력들을 편성하는 것도 중요하다. 제대별로 임무와 역할을 고려하여 사이버작전이 가능한 전문 인력을 편성 및 확보해야 한다. 국가를 위해 사이버 전쟁에 나설 인재는 사이버전에 대한 실제 경험과 이데올로기적 성향이 고도로 융합되어 있어야 하고 국가에 대한 최고 수준의 윤리의식과 책임감을 겸비해야 한다. 군은 현재의 정보보호기술병과 군 입대 조건보다 좀 더 혁신적인 방법이 필요하다.

둘째, 사이버전 기술개발 방안이다. 우리 군의 사이버전에 대한 대비는 정보보호위주의 방어적 기술위주로 수행되고 있으며 정보보호체계를 활용한 실시간 침입탐지 및 분석대응 능력 위주로 임무를 수행한다. 사이버안보 기술수집팀을 운용하여 중국과 미국뿐 아니라 북한과 소련의 해킹기술을 수집하고 아울러서 국내에서 전문가들이 사용하는 기술 보안을 위해 접근통제함으로써 관리를 철저히 할 필요가 있다. 또한 다양한 사이버 공격무기를 확충하는 노력도 병행해야 한다. 멀 웨어[289]를 장착한 프로그램과 해킹에 유리하도록 조작된 광섬유나 컴퓨터 부품을 통하여 적의 기간망과 전력망, 핵무기와 미사일 등 비대칭 수단에 이식하는 방법을 연구할 필요가 있다. 인터넷으로 연결되지 않은 시스템에 위성전화를 통해 침투하는 방법도 검토할 필요가 있다. 사이버전은 특히 평시에 준비한 기술들이 위기나 전시에 더욱 결정적인 영향을 미친다는 점에 유의할 필요가 있는 것이다.

또한 군은 대응 방식에서 새로운 패러다임의 변화가 필요하다. 우리 군은 우선 레이저빔과 고출력마이크로웨이브(HPM)탄, 전자기파(EMP)탄 등 정밀고유도에너지, 역(逆)비대칭 전력 무기를 개발할 필요가 있다. 북한의 핵과 미사일 전력에 대응할 우리의 역 비대칭무기를 정보통신기술기반으로 신개념 무기를 개발하여

288) 임채호 · 전상훈, 앞의 책, pp.71-72.

289) 바이러스나 트로이 목마와 같이 시스템에 해를 입히거나 시스템을 방해하기 위해 특별히 설계된 소프트웨어, 또는 데이터 · 컴퓨터 · 네트워크를 위험에 노출시킬 수 있는 코드를 의미함. . 악성 소프트웨어(malicious software), 또는 악성 코드(malicious code)에서 나온 말로, 남에게 피해를 입히기 위해 개발된 소프트웨어를 의미한다.

대응할 필요가 있을 것이다. e-폭탄으로 불리는 HPM탄은 탄두에서 지향성 고주파를 내보내 반경 300여m 내 모든 적 전자전 장비를 무력화하는 기술이다. EMP탄[290]은 국방과학연구소(ADD)에서 2008년부터 시험개발에 착수한 것으로 알려졌다. 사이버전 영역 중 전자기파 영역은 최근 그 중요성이 부각되고 있다. 특히 정밀 유도무기 사용시 이에 대한 교란 및 전자공격을 통한 지휘통제시스템 파괴 및 무력화는 실제 전장에서 그 효과가 입증되어 전쟁수행의 중요한 요소로 대두되고 있다.[291]

이 영역에 대한 방어 · 공격 기술개발과 공격무기체계 확보가 필요할 것이다. 미국의 경우 방어기술, GPS 재밍에 대한 보호기술과 전자공격을 위한 무기체계 개발도 꾸준히 진행시켜 일부 무기체계의 경우 실용화 단계에 이르렀다. 우리 군의 경우 전자전 수행은 대부분을 미군의 전개전력에 의존하고 있기 때문에 전자기파 영역에서의 우위를 점하기 위한 전자전 기술을 확보하고 개발을 검토할 필요가 있다. 전자전 지원관련 기술개발시 광대역 디지털 수신기술, 다중채널 디지털 수신기술, 정밀위치 탐지기술, 초정밀 방향 탐지기술, 지능형 상황인식기술, 레이저 탐지 및 기만술, 신경망을 이용한 고주파 신호식별 기술, 적외선 및 자외선 경보기술 등에 주력할 필요가 있다. 전자전 무기체계와 관련해서는 원격지원 전자교란, 지향성 적외선 방해, 전자전 교란기, 지향성 무기체계인 고주파증폭기, 탄소섬유탄 등의 전자폭탄 개발 및 보유가 우선 되어야 할 것이다. 민간 전문업체와 공동으로 사이버 기술을 개발하고 군이 요청한 기술을 제공받거나 자문을 받는 등의 방안 마련이 필요할 것이다.[292] 무엇보다도 사이버전을 위한 독립된 연구개발기관의 설립을 추진할 필요가 있다.

셋째, 해킹 방어훈련을 강화하는 방안이다. 미국의 방위고등계획국(DARPA)에는 국가사이버연습장(National Cyber Range)이 있으며 사이버전에 관한 종합연습과 훈련, 시스템의 취약성 점검, 네트워크시스템 도입시 검사 등 중요한 역할을 담당하고 있다. 러시아도 사이버사령부의 창설에 때맞춰 고등군사연구국(AMRA)의 창설을 준비하고 있다. 우리나라도 사이버전을 효과적으로 운용하기 위해서는 조직뿐만 아니라 종합연습의 실시, 장비의 점검, 개별 교육훈련을 위한 사이버연

290) EMP탄 [electromagnetic pulse bomb] : 폭발시 생기는 강한 전자기파로 적의 레이더와 항공기 방공시스템 등 전자 인프라 스트럭처 전반을 무력화시키는 미래전의 무기를 말한다.
291) 김기수, 앞의 논문, p.309.
292) 김기수, 위의 논문, pp.308-309.

습장이 필수적이다.[293] 미군은 현역에서 은퇴한 우수한 인력을 지속적으로 관리하기 위해 예비군 제도를 운용하고 있다. 육군 사이버사령부 예하에는 예비역으로 구성된 사이버부대를 운용하고 있으며 사이버 상에서 적 정보를 수집하고 있는 국가안전보장국(NSA)에서 고도의 기술력을 갖춘 600여 명 규모의 사이버 예비군 창설을 발표하는 등 다방면을 통해 우수인력을 확보하고 있다. 미국의 사이버 예비군 창설 및 의지 표명은 사회가 직면하고 있는 사이버 위협의 심각성에 맞서 더 이상 정보보안 산업에만 의지하지 않고 국가가 직접 사이버보안 문제에 적극적으로 대응하겠다는 의지로 해석할 수 있어 우리 군에 시사하는 바가 크다.

우리 군의 예비군 제도는 미국과 많은 부문에서 다른 점이 존재하지만, 사이버 인력의 부족으로 곤란을 겪고 있는 상황에서 인력 부족 문제를 해결하고 공백을 유연하고 효과적으로 메울 수 있는 대안이 될 수 있다는 점에서, 미국의 사이버 예비군 제도의 추진과 정착을 지속적으로 관심을 가질 필요가 있다. 사이버 예비군 창설을 검토하는 이유는 북한의 사이버 공격에 대응할 전문 인력의 추가 확보가 시급하기 때문이다.[294]

이상과 같이 국가와 군의 핵심요인별 사이버 안보에 대한 개선방안을 종합하면 <표 19>에서 보는 바와 같다. 이를 구체적으로 설명하면 먼저 인식과 사상적인 측면에서 살펴보면 국가는 사이버 안보에 관하여 대국민 홍보를 강화하며 민방위훈련시 사이버 훈련을 병행하고 민간의 참여를 적극적으로 유도할 필요가 있다. 군에서도 군사교육과정에 사이버전을 포함시킬 필요가 있으며 레드팀을 운용하여 수시로 사이버 훈련을 강화하여 전 장병이 경각심을 갖도록 할 필요가 있다. 국가전략 등 시스템의 관점에서 볼 때 사이버 전략은 복원력을 강화하여 북한의 공격을 억제하되 아울러 공세적인 능력을 강화할 필요가 있을 것이다.

사이버전을 효과적으로 수행하기 위해서는 컨트롤타워로 국무조정실에 '국가사이버안전처(가칭)'를 설치하고 각각의 영역별로 책임을 가지며 평시부터 민·관·군이 협력할 필요가 있다. 군에서도 제대별 사이버전 수행조직을 설치하고 특히 국군사이버사령부의 역량을 강화할 필요가 있을 것이다.

또한 법령과 제도의 발전을 위해 단일법인 '국가사이버안보기본법(가칭)'을 제정할 필요가 있으며 군에서도 통합방위법의 개정과 자위권 차원의 교전규칙과

293) 조성렬, "북한의 사이버전 능력과 대남사이버 위협평가," 『북한연구학회보』,제17권제2호(북한연구학회, 2013), p140.

294) 『이데일리』, 2015년 04월 21일 (화) 종합 03면.

전시 사이버전쟁에 관한 법률을 제정할 필요가 있을 것으로 판단하였다.

<표 19> 핵심요인별 사이버안보 개선방안

핵심요인		국 가	軍
인식과 사상		· 대국민 홍보 및 교육 · 민방위 훈련시 사이버 훈련 병행 · 민간참여 확대	· 군사교육과정에 포함 · 사이버전 훈련(RED팀)
국가전략 등 시스템	전략/정책	· 복원력 증진(억지)	· 복원력 증진(억지) · 공세적 사이버위협 대응
	콘트롤타워	· 국가사이버안전처(가칭)	· 사이버사령부 역할 강화 · 공공영역 일부역할 협의
	법령/제도	· 국가사이버안보기본법 (가칭)	· 통합방위법 개정 · 사이버전쟁에 관한 법률 제정 · 자위권 차원 교전규칙 제정
	수행체계	· 협의체별 임무/역할 정립	· 기관별 임무/역할 정립
공조체계 등 네트워크	정보보호 인프라	· 국가 차원의 사이버 방어 인프라 구축	· 유형별 다단계 정보보호 인프라 구축
	국제공조	· 국가간 협력체계 구축 * 국제법, 조직/시스템 구축	· 한미일중 공조체제 강화 * 주기적인 훈련 참여
인력과 기술	사이버 전문인력	· 정규교육 과정 확대 · 민간 전문인력 활용	· 민간 전문기관 협력 강화 · 사이버 전문직능 신설 · 사이버훈련장 확대
	기술개발	· 기술개발 전담기관 설립	· 사이버기술 연구부서 설립

수행체계도 '국가안보실'과 '국무조정실'에 협의체를 설치하고 각각의 임무와 역할을 정립할 필요가 있으며, 군에서도 각 제대별로 관련부서를 설치하고 임무와 역할을 검토할 필요가 있을 것이다. 공조체계 등 네트워크 측면에서 국가차원의 사이버 방어인프라를 구축하고 군에서도 현 체계에 유형별 다단계 인프라를 구축하여 방어를 더욱 강화할 필요가 있을 것이다. 국가간의 국제법 등 협력체계를 구축할 필요가 있으며 특히 군은 한·미·일·중과의 공조체제를 구축하고 주기적인 훈련을 강화할 필요가 있을 것이다. 인력과 기술적인 관점에서 볼 때 사이버 정규교육과정을 확대하고 화이트해커를 관리하여 적극적으로 활용하는 방안을 검토하여 활용하며, 군에서는 사이버 전문직능을 신설하고 사이버 훈련장을 강화하여 전문성을 향상시킬 필요가 있을 것이다. 국가와 군에서 운영하는 기술개발을 위한 전문연구기관의 설립이 필요할 것으로 판단된다.

제6장 결론

김정은은 전쟁계획 '7일 작전계획'를 만들어 한반도에서 7일안에 전쟁을 끝낼 수 있도록 기습남침과 동시에 속전속결로 사이버전과 물리전을 동시에 연계시키는 공격계획을 작성한 것으로 알려지고 있다.

작전계획의 골자는 북한이 기습남침과 국지전이 전면전으로 확전될 경우 미군이 본격적으로 개입하지 못하도록 7일안에 남한전역을 점령하겠다는 내용이다. 사이버 공격과 병행하여 핵·미사일 등 비대칭 전력을 사용하여 전쟁초반에 기선을 잡고 재래식 전력을 동원하여 미 증원군이 도착하기 전 늦어도 15일 안에 남한을 점령한다는 계획을 수립했다고 한다. 이를 위해서 북한은 사이버 공격으로 대한민국의 국가 핵심기반시설을 공격하여 먼저 원자력 등 전력망과 도로와 철도 등 교통시스템을 마비시킴과 동시에 금융망과 정부 기관망을 포함한 통신망을 파괴하고 이어서 수도, 의료시설 등을 통제 불능상태로 파괴하여 우리 국민을 혼란과 공항상태로 빠뜨리는 시나리오를 구상할 것이다.

이와 같이 북한의 사이버 공격이 대한민국의 국가안보에 미치는 영향은 거의 절대적인 위협이다. 그러나 대한민국의 사이버 안보에 대한 정부나 국민의 의식 수준은 이에 못 미치는 실정이다. 현실적으로 매번 공격을 당하면 관심을 보이다가 시간이 지나면 금방 잊어버리는 경향이 있고 사이버 공간이 눈에 보이지 않는 관계로 그 중요성을 심각하게 인식하지 못하는데서 비롯되는 것이라 판단된다. 국가나 군이 정책적인 차원에서 사이버 위협에 대응하려면 먼저 사이버 공격에 대한 성격과 의미를 잘 판단해 볼 필요가 있다. 특히 국가안보 차원에서 전략적으로 접근하여 우리가 어떻게 대응방향을 결정할 것인가는 매우 중요한 사항이다. 앞에서 언급한 바와 같이 한반도에서의 사이버 안보는 미국을 포함한 주요국가와 이스라엘의 사이버 안보를 참고하여 우리가 적용하고 발전시킬 필요성이 있을 것이다.

한반도의 안보 환경과 정보통신기술 발전의 추세를 고려하면 첫째, 대한민국의 사이버 안보전략의 핵심은 방어에 집중하되 공세적으로 사이버 전력을 운용하는 전략이다. 남북한의 정보통신 의존도를 고려할 때 우리가 절대적으로 불리하다. 그러나 공격받는 즉시 조기에 원상회복하여 복원한다면 북한은 공격을 계속하기가 쉽지 않을 것이며 공격해도 큰 영향이 없다면 결국 포기할 수밖에 없을 것이

다. 복원력이 중요한 이유는 이를 통하여 한반도에서 사이버전 억제가 달성될 수 있다는 의미가 되기 때문이다.

둘째, 북한의 사이버 공격 시 누가 실질적인 컨트롤타워의 역할을 할 것인가 하는 점이다. 특히 물리전과 연계하여 공격한다면 국가 안보차원에서 누가 주도를 하는 것이 효과적인지의 문제다. 현재는 청와대가 컨트롤타워의 역할을 하고 실무는 국정원이 주도하고 있다. 그러나 청와대는 국정의 최고기관으로써 상징적인 의미가 있고 국정원은 정보기관으로써 한계가 있기 때문에 국정최고 기관인 청와대와 완충역할을 할 수 있고 또한 각 부처를 조정 통제하는 국무총리실의 기능을 고려하여 국무총리실에 '국가사이버안보처(가칭)'를 설치하여 사이버전에 대한 총괄을 주도하고, 안보환경을 고려하여 군은 임무영역을 확대하여 국정원이 담당하고 있는 공공영역의 일부를 담당하는 것이 바람직하다고 판단하였다.

이를 위해서 법령과 제도의 제·개정이 필요한 실정이다. 현재 국회에서 논의하고 있는 사이버 관련 법령의 제·개정은 국정원이 주도하는 입법안으로 오래전부터 여야가 합의를 하지 못하고 계류 중에 있다. 따라서 이러한 문제점을 해결하고 국가차원에서 전·평시 사이버전에 효율적으로 대처하기 위해서는 '정보화촉진기본법', '정보통신망 이용촉진 및 정보보호 등에 관한 법률', '국가사이버안전관리규정' 등 10여개로 분산되어 있는 사이버전 관련 법령을 가능한 한 '단일법령'으로 통합해야 할 것으로 보인다. 즉 '국가사이버안전처(가칭)'가 주도하는 '국가사이버안보기본법(가칭)'을 제정하는 방안이다.

다음은 '국가사이버안보기본법(가칭)'이 제정되면 이를 근간으로 '통합방위법'을 개정하여 북한의 사이버 위협에 대비해야 한다. 현재의 '통합방위법'은 물리적인 힘을 통제하는 법으로 사이버전에서는 적용이 불가능하다. 따라서 군은 전·평시 통합방위법에 근거하여 국가 주요기반시설들이 위치하고 있는 수도권과 후방지역에서 민·관과 함께 통합방위작전을 수행하듯이 사이버전에서도 동일한 기준으로 작전을 수행하는 것이 효율적이라고 판단한다. 아울러 군은 국가를 방어할 수 있도록 충분한 사이버 역량을 갖추는 것이 필요하리라 판단된다. 군에서 방어할 목표와 범위는 군에서 운용하는 C4ISR망과 무기체계인 PGM망뿐만 아니라 국가안보에 영향을 미치는 정부기관과 국가핵심기반시설 등 공공영역의 일부를 포함하며, 이러한 국가기관과 핵심기반시설이 안전한 가운데 정상적인 운영이 가능하도록 보장하여 사이버전에서 승리하는 것이다. 또한 자위권 차원의

교전규칙을 발전시키고, 물리전과 사이버전의 연계 공격시 이에 대응할 수 있는 전시법령이 없기 때문에 이에 대한 법령도 제정할 필요가 있을 것이다.

다음은 국내 및 국제간의 공조체제 유지다. 사이버전의 특성상 네트워크를 통해 전달되는 데이터의 양과 그 처리속도는 우리의 상상을 초월하고 있기 때문에 수백만 대의 좀비 pc가 일시에 사이버 공격에 나설 경우 순간적으로 모든 상황이 종료될 수 있을 것이다. 전쟁이 일어났다는 것을 인식하는 순간 전쟁이 끝나버릴 수도 있다는 것이다. 사이버 공간은 새롭게 형성된 영역으로 국제규범이나 정책방향에 있어 아직까지 국제적으로 공감대가 형성되지 않았을 뿐만 아니라 국가 간의 이해관계로 합의점을 찾지 못한 실정이다. 그럼에도 불구하고 국내의 관련 제 기관은 물론 국제간의 공조와 협력강화를 위해 많은 노력을 할 필요가 있다. 특히 한미 간에 사이버 공조는 물론 일본, 중국과 사이버 상에서 협력을 증진시키는 것도 매우 중요하다. 사이버 국제안보 협력강화를 위해서 우선적으로 해야 할 역할은 정부 각 부처, 국군사이버사령부, 국가정보원, 경찰청 등으로 분산돼 있는 조직들을 '국가사이버안보처(가칭)'에서 총괄함으로써 여기에서 단합된 힘을 바탕으로 국제적인 공조와 협력을 강화할 필요성이 있을 것이다.

우리 사회는 모든 것이 인터넷으로 연결되는 사물인터넷 시대가 도래함에 따라 국가안보에서 사이버전은 무엇보다도 중요한 핵심요인이 되었다. 북한은 물론 대한민국을 공격하는 적대세력에 대응하기 위해 국가적인 대전략 차원에서 북한보다 강력한 사이버전 수행능력을 갖출 뿐만 아니라 주변 강대국들의 사이버 공격에도 대비할 수 있도록 역 비대칭전력으로 우위를 삼을 필요가 있다. 국가적인 대형 프로젝트를 계획하여 사이버 전력을 육성할 필요성이 있는 것이다. 이를 위해 국가예산을 과감하게 투자하여 양적이나 질적으로 우월하고 뛰어난 화이트해커인 사이버 전사양성에 최선의 노력을 다해야 한다. 방어형 사이버 무기를 지속적으로 개발하고 공격형 사이버 미사일인 한국형 스턱스넷 등을 하루빨리 개발하여 완성하도록 해야 한다. 전문가들은 사이버전에 대비해 국군사이버사령부의 현재 6백여 명 수준의 인력을 최소 3천여 명은 돼야 적절히 방호할 수 있다고 지적한다. 한미 연합작전을 위해서도 연합 사이버 전력을 강화할 필요성도 있을 것이다.

따라서 정부는 전쟁에 대비하여 국군을 설치하고 운영하는 것처럼 사이버전에서도 군의 역할을 강화하여 정부와 국민의 적극적인 지지와 협조로 사이버 전력

을 대폭적으로 보강하여 북한의 어떠한 공격에도 주도적으로 이를 해결할 수 있는 능력을 갖출 필요가 있다. 이를 위해서는 군·관·민이 총력전의 개념을 가지고 적극적인 정보공유와 협력으로 대응전략을 구축하고 대응책을 마련해야 할 것이다. 3차 세계대전은 사이버전이 될 것이라는 미래학자들의 말을 굳이 인용하지는 않아도 사이버 무기는 한반도에서 핵과 미사일과 함께 가장 위협적인 요소가 될 것이기 때문이다. 2015년 여름 북한의 DMZ 지뢰도발 사건 이후 정부는 확성기에 의한 대북방송으로 북한정권의 아킬레스 근을 끊어놓자 북한은 즉시 고위급 협상을 제안하여 대한민국에 통쾌한 승리를 맛보게 한 것처럼 사이버 전력도 우리의 역 비대칭전력으로 대한민국의 상징적인 프로젝트로 육성할 필요성이 있을 것으로 판단한다.

【참고문헌】

1. 국내문헌

가. 단행본

공진성,『테러』, 서울: 책 세상, 2010.
국방부, 『국방백서』, 서울: 기본정책과, 2014.
글렌그린월드 지음/박수민・박산호 옮김,『더 이상 숨을 곳이 없다』,
서울: 모던타임스, 2014.
김동익, 『이상한전쟁』, 서울: 중앙Books, 2012.
김종래,『CEO 칭기스칸』, 서울 : 삼성경제연구소, 2002.
김진,『2015년 김정은 급변 터질 것인가』, 서울: 늘품플러스, 2014.
김필재,『북한의 사이버 남침』, 서울: 백년동안, 2014.
네이트실버 지음/이경식 옮김,『신호와 소음』, 서울: 더퀘스트, 2014.
댄세노르・사울싱어지음/윤종록 옮김,『창업국가』, 서울: 다할미디어, 2010.
문영미, 『디퍼런트』, 서울: 살림Biz, 2011.
박세일, 『대한민국 국가전략』, 서울: 21세기북스, 2006.
박종현 외,『사물 인터넷의 미래』, 서울: 전자신문사, 2014.
배리 파커 지음/김은영 옮김,『전쟁이 물리학』, 서울: 북로드, 2014.
아브람 N, 슐스키 & 캐리 J, 슈미트 지음/신유섭 옮김, 『국가정보의 이해』,
서울: 명인문화사, 2007.
오명호 외, 『사이버전 개론』, 서울: 양서각, 2014.
오수열 외,『최신 북한사회의 이해』, 광주: 도서출판신성, 2005.
우형진, 『넷 전쟁과 인터넷 보안군』, 서울: 삼성경제연구소, 2007.
유동열,『사이버 공간과 국가안보』, 서울: 북앤피플, 2012.
육군본부, 『지상군기본교리』, 2011. 10.
이남용,『창조경제와 국가전략』, 서울: 이든북스, 2013.
이상우,『우리들의 대한민국』, 서울: 기파랑, 2012.
이정구, 『21세기프로젝트관리』, 서울: 책과 나무, 2013.
이태윤,『새로운전쟁 21세기 국제테러리즘』, 서울: 도서출판모시는사람들, 2004.

임춘택 외,『미래를 생각한다』, 서울: 비즈니스맵, 2012.
임채호, 전상훈 공저,『사이버전쟁의 위협과 대응전략』, 서울: 인포더북스, 2013.
손영동(a), 『iwar』, 서울: 황금부엉이, 2010.
손영동(b), 『0과 1의 끝없는 전쟁』, 서울: 인포더북스.
정순택,『송의 눈물』, 서울: 조갑제닷컴, 2012.
조갑제, 『한반도의 핵겨울』, 서울: 닷컴, 2015.
조희원,『해커 묵시록』, 서울: 청조사, 2013.
함유근・채승병, 『빅데이터, 경영을 바꾸다』, 서울: 삼성경제연구소, 2012.
헤이프리트 뮌클러 지음・공진성 옮김, 『새로운 전쟁』, 서울: 책 세상, 2011.
KISA, 『국가정보보호백서』, 2014.

나. 논문

강정민 외, “국가사이버역량 평가방법론 연구” 『정보보호학회논문지』, 2012.10.
권한용, “사이버테러에 대한 국제적 대응방안과 한국에의 시사점” 『동아법학』, 제65호, 2014년 11월.
김근식, “박근혜 정부 남북관계 평가: 신뢰형성의 원칙과 유연함이 필요,” 『한반도포커스』, 제25호, 2013년.
김기수, “북한의 사이버전 위협과 대비방안” 『한국정책학회』, 동계학술대회, 2013.
김도승, “사이버공간에 서의 경찰법 이론에 관한 연구”, 박사학위논문, 성균관대학교 대학원, 2009.
김동성, “북한의 통일전선 전략전술과 대남 정치심리전” 『전략연구』, 통권 제57호(한국전략문제연구소, 2013.3)
김인수, “북한 사이버전 수행능력의 평가와 전망” 『통일정책연구』, 제24권 1호, 2015.
김상배, “사이버 안보의 미국관계:안보화 이론의 시각” 『한국정치학회보』, 제49집 1호, 2015년 봄.
김승주, “세계 각국의 사이버전 수행능력과 국내 피해사례” 『군사논단』,제75호 (한국군사학회, 2013)
김흥석, “사이버 테러와 국가안보” 『전투발전』, 제137호, 2011.
김희수, “북한사이버 위협의 심각성과 사이버전 수행 발전방향” 『합참』, 제59호, 2014.4.
류창하, “작전적 수준의 사이버전 수행 발전방향” 『군사평론』, 제424호, 2013년 8월.

문순보, “북한의 사이버테러와 대화제의의 진정성,” 『세종논평』, 제217호(세종연구소, 2011.5.4.)

박찬수・박용석, “사이버전의 역량평가 개선과 역량강화방안에 관한 연구” 『한국정보통신학회논문지』, 2015. 5.

박노형・정명현, “사이버전의 국제법적 분석을 위한 기본개념의 연구” 『국제법학회논총』, 제 59권 제2호(대한국제법학회, 2014.6)

박대우(a), “국가사이버보안정책에서 해킹에 대한 소고” 『한국정보보호학회지』 제21권 5호, 2011. 10.

박대우(b), “대한민국 국군의 사이버전 대응” 『군사논단』, 제75호(한국군사학회, 2013)

박대우(c), “국가 사이버안보 관련 법률안 제안,” 『국가사이버안보정책포럼』, 2013, 5.

박환수, “북한사이버 위협대비 사이버전 발전방향” 『합참』, 제60호, 2014.7.

변상정, “쿨워시대 사이버 위협과 사이버 안보강화 방안” 『군사논단』, 제76호(한국군사학회, 2013)

부형욱, “사이버 안보의 주요이슈와 정책방향” 『국방연구』, 제56호 제2호(국방대학교 안보문제연구소, 2013.6.)

배달형(a), “국가군사전략급 수준에서 북한사이버 위협과 한국군의 대응방향” 『전략연구』, 통권 제52호(한국전략문제연구소, 2011.7)

배달형(b), “4세대전쟁 및 비대칭위협 관점의 사이버전 및 사이버 심리전 발전방향” 『전략연구』, 통권 제65호(한국전략문제연구소, 2015.3)

배병환・송은지, “주요국 사이버 보안전략 비교・분석 및 시사점” 『초점』, 2014년 11월.

안유성, “사이버 안보 대응역량 강화방안 연구” 『정보보호학회지』, 제24권 제6호(2014.12)

양무진, “장성택 처형이후 북한의 대남정책,” 『북한연구학회보』, 제18권 제1호 (북한연구학회, 2014)

양문수, “개성공단 사태와 남북경협,” 『한반도포커스』, 제25호, 2013년

오일석・김소정, “사이버 공격에 대한 전쟁법 적용의 한계와 효율적 대응방안” 『인하대학교 법학연구』, 제17지 제12호, 2014년. 6월.

오태곤・성관실, “국가 사이버 안전관리 법제의 개정방향에 대한 소고” 『조선대학교 법과대학』, 2013. 12.

이동범・곽진, “미국정부의 사이버 공격에 대한 보안 전략” 『정보보호학회지』, 제24권 제1호(2014. 2)

이미정・한승환, “사이버 공간에서의 국가안보 위협요인 및 대책방안” 『국방연구』, 제48호 제2권(국방대학교 안보문제연구소, 2005.12)

이완수, “국가 사이버 안보 구축전략에 관한 연구“, 경기대학교 대학원 박사학위 논문(2013).

이석기 외, “2012년 북한경제 종합평가 및 2013년 전망” 『통일부 정책용역과제』, 2012.

임종인 외, “북한의 사이버 전력 현황과 한국의 국가적 대응전략” 『국방정책연구』, 제29권 제4호(국방대학교 안보문제연구소, 2013)

윤규식, “북한의 사이버전 능력과 위협전망,” 『군사논단』제68호(한국군사학회, 2011.4.)

윤영준・이정희, “국가 사이버위기 관리법제정시 고려사항에 관한 연구” 『Journal of Digital Forensics』, 2014 June.

손영동, “사이버전 억지력평가모델에 관한 연구”, 숭실대학교 대학원 박사학위 논문, 2011.2.

손영동・고성훈, “사이버전 전개양상과 대응역량” 『군사논단』, 제81호(한국군사학회, 2015)

신창훈, “북한의 사이버 공격과 위협에 대한 우리의 대응”, 『글로벌거버넌스센타』, 2015년 6월.

신충근・이상진, “북한의 대남 사이버테러 전략분석 및 대응에 관한 고찰” 『경찰학 연구』, 제13권 제4호, 2013년 12월.

장노순, “사이버 안보의 국제규범에 대한 조정과 신뢰구축 제약” 『한국정치정보학회』, 2015년.

장노순・한인택, “사이버 안보의 쟁점과 연구경향” 『국제정치논총』, 제53집 3호(한국국제정치학회, 2013)

정완, “한미 사이버 보안법제 동향에 관한 고찰” 『경희법학』, 제48권 제3호, 2013년 겨울.

조성렬, “북한의 사이버전 능력과 대남 사이버 위협평가: 한국의 사이버 안보를 위한 정책적 함의” 『북한연구학회보』, 제17권 제2호(북한연구학회, 2013.11)

채재병, “안보환경의 변화와 사이버 안보” 『정치・정보연구』, 제16권 2호,

2013년 12월.

최광복, “사이버전 대비차원의 국방정보보호 관리체계 개념연구” 『군사논단』, 제70호 (한국군사학회, 2012)

한국인터넷진흥원, “주요국가별 사이버방어체제 및 대응동향” 『심층보고서』, 제4호, 2014.

한희, “사이버 공간과 국가안보“ 『국가안보전략연구소』, 2014년 4월.

한희원, “사이버 안보에 대한 국가정보기구의 책무와 방향성에 대한 고찰” 『한국경호경비학회』, 제39호, 2014.

3. 기타 자료

고경민, “북의 최후 결전은 사이버전이다” 『자주민보』, 2013년 5월 20일.

국정원, “국가 사이버 안보 종합대책”, 『ZD Korea』, 2013.

김정은, “진정으로 나라의 통일을 원하고 민족의 평화번영을 바라는 사람이라면 누구든지 손잡고 나갈 것” 『로동신문』, 2014년 1월 1일.

김정은, “7일전쟁작계 만들었다”, 『중앙일보』 , 2015년 1월 8일.

『보안뉴스 미디어』, 2014년 11월 28일.

김명자, 『중앙일보』, 2015년 01월 24일 (토)오피니언 31면

김명철,『중앙일보』, 2015년 01월 16일 금요일 29면 사설/칼럼

김정규, “사이버테러 대비 국가위기체계 시급” 『위기관리경영』, 2008년 7월 9일.

김종하, 『문화일보』, 2015년 01월 27일(화) 오피니언 31면

『LA 중앙일보』, 2015년 1월 2일.

박노형, 『조선일보』, 2015년 02월 17일 (화) 오피니언 25면

박인휘, 『세계일보』, 2015년 01월 07일 (수) 오피니언 30면 사설/칼럼

박춘식, “한수원 정보유출사고를 통한 교훈”,『파이낸셜뉴스』, 2015년 1월 15일.

백기승, “사이버 위협 분석과 전망” 『매일경제』, 2014년 12월 29일.

양정아, “북 사이버전 능력, IT강국 위협하는 세계3위권.” 『NK비전』, 2013년 5월 9일.

유동열, 『문화일보』 2015년 05월 06일(수) 오피니언 37면 사설/칼럼

임종인, “미국의 대북 사이버 응징이 주는 교훈” 『문화일보』, 2015. 1. 7.

손영동, “영화 ‘인터뷰’ 사태가 주는 안보적 함의” 『국방일보』, 2015. 1. 21.

손영동, 『국방일보』, 2015년 6월 18일.

신동주, “커지는 총성 없는 전쟁위협, 사이버군 양병론 다시 고개” 『세계일보』, 2013년 6월 24일.

정시아, “사이버전쟁 선언 이스라엘의 비밀 무기는 8200부대!” 『주간조선 2211호』, 2012년 6월 18일.

주대준, 『국민일보』, 2015년 02월 03일 화요일 026면 오피니언

주성하, “해킹을 이슈로 북한 사이버전사와 직접 나눈 대화.”, 2013년 3월 31일.

존 타식, “북한의 사이버 공격 뒤에 중국이 있다” 『미래한국 데일리』, 2011.6.26.

채인택•노진호, “빅브라더, 미국에 도전할 나라도 기술도 없다” 『중앙SUNDAY』, 2013년 6월 16일.

채인택, 『중앙일보』, 2015년 06월 25일 목요일 028면 사설/칼럼

최성주, 『세계일보』, 2015년 01월 05일 월요일 030면 오피니언

홍진수 외, “사이버 안보 위기: 한국의 사이버 대응” 『경향신문』, 2013년 4월 1일.

안철수연구소, 『보안뉴스』 2013년 6월 27일 사설/칼럼

『경향신문』, 2015년 04월 03일 금요일 029면 오피니언

『국민일보』, 2015년 08월 13일 목요일 011면 사회

『동아일보』, 2015.09.08. 화요일 A04면 종합

『로동신문』, 2014년 3월 12일. “남조선 당국자와 보수 언론매체가 함부로 입을 놀리지 말아야 하며, 당국이 추악한 인간쓰레기들을 군사적으로 비호하며 반공화국 삐라 살포에 내모는 어리석은 처사에 더 이상 매달리지 말아야 할 것이다”

『연합뉴스』, 2013년 4월 17일.

『연합뉴스』, 2014년 3월 27일. “북한이 우리 국가원수의 정상적 외교활동까지 입에 담기 어려운 말로 비방한 것은 남북간 합의에 대한 중대한 위반임은 물론 상대방에 대한 최소한의 예의마저 저버린 행위로서 매우 유감이며, 북한은 마치 우리 정부가 직접 비방 중상을 하는것처럼 주장하나 이는 사실이 아니라는 점을 다시금 강조한다.”

『영남일보』, 2011년 8월 5일. “미국 러시아에 이어 세계 3위, 북 사이버 테러 수준은?” 『채널 A』, 2013년 3월 20일.

『이데일리』, 2015년 04월 21일 (화) 종합 03면

『이마케터 조사결과』, 2014년 12월.

『세계일보』, 2014년 12월 11일 목요일 006면 종합

『세계일보』, 2015년 06월 15일 월요일 A13면 사회
『전자신문』, 2015년 05월 07 (목) 종합 02면
『전자신문』, 2015년 07월 24일 (금) 오피니언 27면
『조선일보』, 2011년 5월 20일. '북 사이버전 능력은 미국 CIA에 필적.'
『조선일보』, 2015년 07월 24일 금요일 A 03면 종합
『조선일보』, 2015년 07월 25일 토요일 A05면 종합
『중앙일보』, 2014년 12월 26일 004면 종합
『중앙일보』, 2015년 01월 08일 목요일 001면 종합
『중앙일보』, 2015년 03 18일 (수) 사설/칼럼 30면
『중앙일보』, 2015년 7월 25일 토요일 A05면 종합
『중앙일보』, 2015년 08월 27일 목요일 002면 종합
『파이낸설 뉴스』, 2015년 03월 17일 (화) 종합 08면
"구멍난 사이버안보 '컨트롤 타워' 시급하다. 미국•북한 사례로 본 우리의 방향" 『디지털타스』, 2013년 7월 3일.
"국정원 남북 사이버전 땐 우리 피해 훨씬 심각" 『머니투데이』, 2013년 5월 2일.
"긴급분석 북한의 사이버전 전투력." 『일요신문』, 2011년 5월 9일.
"미국 해킹 비판 UC 결의안에 북한도 찬성, 우리나라는?" 『미디어투데이』, 2013년 11월 23일.
"미 사이버보안 책임자가 본 한국 사이버전력" 『ZDNet Korea』, 2013년 5월 3일.
"북의 최후 결전은 사이버전이다" 『자주민보』, 2013년 5월 20일.
"북의 최후 결전은 사이버전이다" 『자주민보』, 2013년 5월 20일.
"북신문, 미•일의 사이버전쟁 준비 비난." 『통일뉴스』, 2012년 10월 11일.
"북한 사이버전 능력, 생각보다 훨씬 강력해." 『한국일보』, 2013년 10월 21일.
"북의 복합도발 경보! EMP 전차탄을 아는가?" 『뉴데일리』, 2013년 3월 26일.
"북한 사이버전법은 중국의 점혈전쟁술 모방한 것" 『중앙일보』, 2009년 7월 10일.
"북한 사이버 부대 귀순자, 3.20을 말한다" 『전자신문』, 2013년 5월 14일. 『전자신문』, 2013년 5월 14일.
"북한 사이버 부대 귀순자, 3.20을 말하다: 사이버테러, 북 귀순자의 증언." 『전자신문』, 2013년 5월 14일.
"북한의 사이버 공격 뒤에 중국이 있다" 『머니투제이』, 2013년 1월 16일.

“북한이 사이버전쟁에 투입할 수 있는 부대가 최대 1만 2,000명 수준임” 『데일리진』 2013년 8월 13일.

“북, 군사망 무력화시킬 사이버전 감행 가능” 『데일리안』, 2011년 6월 1일.

“북한군 정찰총국, 사이버 요원 해외 급파” 『자유아시아방송』, 2013년 3월 21일.

“북 사이버전 수준은 세계 3위” 『아시아경제』, 2012년 6월 7일.

“사이버전 인력, 북한의 7분의 1” 『뉴스원』, 2013년 10월 14일.

“안보강국의 길을 묻다. 한반도 주변국 사이버전력” 『세계일보』, 2013년 10월 22일.

“앞으로 북한이 노릴 사이버공격 대상은?” 『TV조선』, 2013년 10월 17일.

“전세계 컴퓨터망 해킹한 NSA도 북한은 손 못대” 『조선일보』, 2013년 10월 25일.

“6.25 남북 사이버전 어나니머스 주장 해커 실체는?” 『머니투제이』, 2013년 6월 25일.

“6.25해킹, 북한이 사용하고 있는 사이버전 전술은.” 『데일리시큐』, 2013년 6월 26일.

2. 외국문헌

가. 단행본

Martin C. Libiki, “What is Information Warfare?”, 1995.

Richard A. Clarke•Robert Knakee, “Cyber War : The Next Threat to National Security and What to Do About It” 『HarperCollins Publishers』, 2010.

“Information Operation,”, 『DoD Directive S-3600』, 1996. 12.

“International Strategy for Cyberspace” 『White house』, 2011.

나. 논문

『Cyber Commander’s eHandbook version 2.0』, The Technolytics Institute, 2011.

DoD of U.S, “Department of Defense Strategy for Operating in Cyberspace“ 『Quadrennial Defense Review Report』, July, 2011.

David Cenciotti, “Air strike on Damascus military complex shows Syrian Air Defense can do nothing against Israeli Electronic Warfare”, 2013. 2.

“In cyberarms race, North Korea emerging as a power, not a pushopver” 『The Christian Science Monitor』, 2013. 10. 19.

James A. Lewis, “Cybersecurity Two Years Later” 『CSIS』, 2011. 1.

James A. Lewis, “In cyberams race, North korea emerging as pa power, not a

pushover" 『The Christian Science Monitor』, 2013. 10. 19.

James Ball, "GCHQ captured emails of journalists from top international media" 『The Guardian』, 2015. 1. 19.

"North Korea: How the least-wired country became a hacking superpower" 『Global Post』, 2013. 5. 22.

"North Korean Newspaper hits out at U.S Cyber Warfare Polocy" 『North Korea Tech』, 2013. 8. 12.

"Q&A of the week: the current State of the Cyber Warfare Threat featuring Jeffey Carr" 『ZDNet』, 2012. 5. 11.

"Are there international rules for cyberwarfare?" 『CBC News』, 2013. 3. 21.

감사의 글

1975년에 입교하여 40년 넘게 군에 복무하고 현재는 육군정책연구위원으로 근무하고 있습니다. 군에 근무하면서 개인은 생육하고 번성하는 일이며, 국가에 대해서는 안보가 최고의 가치라는 사명감을 가지게 되었습니다. 전후방 각지에서 근무하며 군사전략과 전술에 매진하며 오직 한길 How To Fight 만을 생각하였고 앞으로도 사는 날까지 국가안보를 생명으로 알고 살아가고자 합니다. 소령 때부터 지금까지 30년 넘게 새벽 4시경에 기상하여 경건의 시간과 체력단련으로 하루 일과를 열었습니다. 지휘관을 하면서 병사들과 소통하는 것을 좋아하여 소대장시절부터 중대장, 대대장, 연대장, 여단장, 사단장, 포병학교장의 지휘관 직책을 수행하면서 장병들과 토의하는 것을 즐기고 애로사항을 들었습니다. 이런 관계로 지휘관 직책이 가장 보람이 있었고 부대원 모두가 즐겁고 해피하며 싸워 이길 수 있는 응집력이 가장 강한 부대를 만들고자 하였습니다. 지휘의 핵심은 내가 지휘하는 부대원 한사람이라도 억울한 일이 없어야 한다는 생각으로 모두가 행복한 군 생활이 되도록 최선을 다했습니다. 또한 부대원 한사람, 한사람이 생각하는 장병이 되어 병사들이 군에 오면 로봇과 같이 시키는 임무만 하지 않도록 하고 이등병도 어떠한 상황에서도 자신의 의견을 말할 수 있는 환경과 여건을 만들도록 노력하였습니다. 이는 수많은 상황들을 스스로 판단하고 행동할 수 있어야 전투에서 승리할 수 있다는 생각 때문이었습니다. 사단장 시절에 매월 2~3회씩 전 장병을 대상으로 편지를 써서 국가관을 포함한 가치관 교육을 하고 부대원들을 늘 자식과 같은 마음으로 생각하고 지휘하였습니다. 그리고 계절이 바뀔 때마다 병사들과 똑같이 위장을 하고 실탄과 수류탄으로 무장하여 디엠지를 수색하고 정찰한 경험이 있습니다. 한미연합사에서 미군 장병들과 근무시 미군방송인 AFN TV에 이라크와 아프카니스탄 전투에서 전사한 장병들을 수송기로 운구하는 장면이 나올 때마다 대통령이나 국방장관 같은 분들이 공항에 나와 예를 표하는 장면을 자주 접하게 되면서 나 자신의 군인으로서 정체성과 국가에 대한 애국심으로 스스로 신념화되는 경험도 하였습니다. 이를 통해서 국가안보가 생명보다 더 소중한 가치라는 것을 절절하게 느꼈습니다. 대한민국은 5천년 역사를 가진 위대한 나라입니다. 그러나 수많은 외침과 침략을 당해왔습니다. 그리고 아직도 우리는 북한의 대남적화통일의 위협과 주변 강대국들의 영향권 아래에 놓여있기 때문에 국민 모두는 국가안보를 생명처럼 생각하고 상무정신으로 뭉쳐

야 한다고 생각합니다. 요즘 경제가 어렵고 청년들의 일자리가 없어서 안타까운 심정입니다. 그럼에도 불구하고 안보는 죽느냐 사느냐의 생존의 문제이고 경제는 잘사느냐 못사느냐의 절박한 문제이기 때문입니다. 군대는 전쟁이 끝난 지 오래되다 보니 너무 관료적이고 행정적인 조직으로 변하고 있습니다. 국민들은 삶의 현장에서 생존을 위해 죽기 살기로 노력하고 있는 반면에 우리 군인은 안일한 자세로 근무하는 면이 있지 않나 반성합니다. 군은 전쟁경험이 없는 세대들로 구성되어 있기 때문에 한미연합사에 근무하는 미군의 전쟁교훈을 터득하고 세계 각국의 분쟁지역에 참관하여 전쟁을 간접적으로 체험하여 대비태세를 강화할 필요가 있다고 생각합니다. 이제 군도 아웃소싱을 하고 연구소, 산업체, 학교, 민간, 외국군 등과 같은 조직과 실질적인 교류를 하고 현장을 방문하여 민간과 외국의 발전된 모습을 국방개혁으로 연계할 필요가 있다고 생각합니다. 특히 정보통신기술과 정보보호 분야에 많은 투자를 하여 IT기술을 근간으로 모든 산업과 사회시스템이 이루어지도록 특단의 조치가 필요하다고 생각합니다.

늦은 나이에 조선대 대학원 정치외교학과에 입학하여 북한의 사이버 위협이 한국안보에 미치는 영향에 관한 논문을 작성하게 되었습니다. 특히 어려운 여건하에서 공부를 할 수 있도록 지도해 주시고 논문을 쓸 수 있도록 용기를 북돋아 주신 조선대학교 정책대학원장이신 오수열 교수님께 먼저 감사의 말씀을 드립니다. 같은 대학의 김재철 교수님과 한관수 교수님께도 실무차원에서 많은 지도편달을 해 주시고 격려해 주셔서 감사의 말씀을 드립니다. 또한 논문심사과정에서 지도해 주신 원광대학교의 김태웅 교수님과 건양대학교의 이종호 교수님께도 감사의 말씀을 전합니다. 특히 지난 몇 달간 주말을 반납하고 이른 새벽부터 밤늦게까지 논문에 매진할 수 있도록 돌봐주신 아내 이경자님께도 특별한 감사의 말씀을 올립니다. 그리고 논문에 관심과 격려를 보내준 딸 혜명과 혜원, 아낌없는 격려와 영문초록을 작성해 준 아주대학교 교수인 사위 허준석 군에게도 심심한 감사의 말씀을 드립니다. 또한 육군본부 정책연구위원회의 박삼득 위원장님과 위원여러분들께도 감사의 말씀을 전합니다. 그리고 연로하신 어머니와 형제들에게도 감사의 말씀을 드립니다. 마지막으로 논문을 쓸 수 있도록 다양한 자료를 제공해 주신 각주에 나와 있는 북한과 국가안보, 그리고 사이버전의 전문가이신 모든 분들께도 감사의 말씀을 전합니다. 모든 분들 감사합니다.

2015년 12월 21일(월) 계룡대 연구실에서 신동만 드림