

학제 통합논술 II

2014년도 외교관후보자 선발 제2차시험

응시번호 :

성명 :

※ 다음 제시문을 읽고 물음에 답하시오.

<제시문 1>

☐ 제네바협약 제1추가의정서 (일부 발췌)

채택일자 1977년 06월 08일, 발효일자 1978년 12월 07일, 당사국 수 174개국(2014년 5월 1일 현재)

제48조 기본규칙

민간주민과 민간물자의 존중 및 보호를 보장하기 위하여 충돌당사국은 항시 민간주민과 전투원, 민간물자와 군사목표물을 구별하며 따라서 그들의 작전은 군사목표물에 대해서만 행하여지도록 한다.

제51조 민간주민의 보호

4. 무차별공격은 금지된다. 무차별공격이라 함은,
- 가. 특정한 군사목표물을 표적으로 하지 아니하는 공격,
 - 나. 특정한 군사목표물을 표적으로 할 수 없는 전투의 방법 또는 수단을 사용하는 공격 또는,
 - 다. 그것의 영향이 본 의정서가 요구하는 바와 같이 제한될 수 없는 전투의 방법 또는 수단을 사용하는 공격을 말하며, 그 결과 개개의 경우에 있어서 군사목표물과 민간인 또는 민간물자를 무차별적으로 타격하는 성질을 갖는 것을 말한다.

제52조 민간물자의 일반적 보호

1. 민간물자는 공격 또는 보복의 대상이 되지 아니한다. 민간물자라 함은 제2항에 정의한 군사목표물이 아닌 모든 물건을 말한다.
2. 공격의 대상은 엄격히 군사목표물에 한정된다. 물건에 관한 군사목표물은 그 성질·위치·목적·용도상 군사적 행동에 유효한 기여를 하고, 당시의 지배적 상황에 있어 그것들의 전부 또는 일부의 파괴, 포획 또는 무용화가 명백한 군사적 이익을 제공하는 물건에 한정된다.



<제시문 2>

정보통신 기술의 발달과 함께 다양한 국내외 사안들이 사이버 공간에 활발하게 등장하고 있다. 이러한 변화는 많은 혜택도 제공하지만 개인정보 유출에서부터 사이버 테러에 이르기까지 심각한 피해를 입히기도 한다. 사이버 공간은 “컴퓨터의 네트워크화로 컴퓨터 내에 번져 나가는 정보 세계이며, 정보화 사회를 상징하는 개념으로서 물리적인 실체와 떨어진 가상공간”으로 정의된다.

사이버 공간을 안보의 측면에서 보면 사이버 안보(cyber security)라는 용어로 집약되며 비전통적 안보에 포함된다. 이 안보 영역에서는 정치, 경제, 사회에 걸쳐서 모든 요소들이 사이버 공격의 대상이 될 수 있다. 예를 들어, 스텍스넷(Stuxnet) 워ม 바이러스의 이란 핵시설 공격, 우리나라의 2009년 분산서비스거부(DDos) 공격, 2011년 농협 전산망 마비 사태 등과 같은 사이버 공격은 단순히 사이버 공간에만 한정된 문제가 아니라 직접적으로 국가, 기업, 개인에게 영향을 미치고 있다.

<제시문 3>

☐ Tallinn Manual on the International Law Applicable to Cyber Warfare

○ 규칙2 관할권

적용 가능한 국제의무를 침해함이 없이, 국가는 다음 사항에 대해 관할권을 행사한다.

- (a) 자국의 영토 내에서 사이버 활동을 행하는 자
- (b) 자국의 영토 내에 소재하는 사이버 기반시설
- (c) 국제법에 따른 역외 사항

○ 규칙6 국가의 법적 책임

국가는 자신에게 귀속 가능하며 국제의무 위반을 구성하는 사이버 작전에 대하여 국제법적 책임을 진다.



○ 규칙7 정부의 사이버 기반시설에서 착수된 사이버 작전

사이버 작전이 정부의 사이버 기반시설에서 착수되었거나 또는 그로부터 비롯되었다는 사실만으로는 당해 작전을 그 국가에게 귀속시키는 충분한 증거가 될 수 없고, 다만 문제의 국가가 그 작전에 관련되어 있음을 보여준다.

○ 규칙8 어떤 국가를 경유한 사이버 작전

사이버 작전이 어떤 국가에 소재한 사이버 기반시설을 경유하여 이루어졌다는 사실은 당해 작전을 그 국가에 귀속시키기 위한 충분한 증거가 되지 못한다.

○ 규칙39 민간 및 군사적 목적을 위해 사용되는 물건

민간 및 군사적 목적 모두를 위하여 사용되는 물건(컴퓨터, 컴퓨터 네트워크 및 사이버 기반시설 포함)은 군사목표물이 된다. (이상 일부 발췌)

The Tallinn Manual, prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence in 2013, was designed to produce a non-binding document applying existing law to cyber warfare. The group was composed of twenty renowned international law scholars and practitioners.

The Manual “identifies the international law applicable to cyber warfare and sets out ninety-five ‘black-letter rules’ governing such conflicts. It addresses topics including sovereignty, State responsibility, the *jus ad bellum*, international humanitarian law, and the law of neutrality. An extensive commentary accompanies each rule, which sets forth each rule’s basis in treaty and customary law, explains how the Group of Experts interpreted applicable norms in the cyber context, and outlines any disagreements within the group as to each rule’s application.”

<제시문 4>

사회적으로 최적 수준의 사이버 안보는 사회적 한계 편익이 한계 비용과 일치하는 수준에서 결정된다. 그러나 만약 사이버 안보의 공급을 시장에 맡긴다면, 민간 소비자들 간에 무임승차의 문제가 발생하게 될 것이다. 이와 같은 상황에서는 사회적 한계 편익이 사적 한계 편익을 초과하기 때문에, 민간 공급자들이 사회적으로 최적 수준의 사이버 안보 서비스를 제공할 충분한 금전적 유인을 얻지 못하게 된다. 정부는 이러한 문제를 개선하기 위하여 정책적 개입을 추구할 수 있다.

<제시문 5>

미국은 사이버 공격으로 유출되고 있는 기밀이 중국의 군사 및 경제적 경쟁력을 빠르게 신장시키고 있고, 이러한 위협이 계속된다면 군사적 우위와 지배력이 급격하게 약화될 것을 우려한다. 오바마 행정부는 중국의 사이버 위협이 한계를 넘어서고 있다고 보고, 사이버 안보 문제를 중국과의 정상회담에서 정식 의제로 설정하였다. 오바마 대통령은 중국의 사이버 위협이 미중관계를 악화시킬 것이라고 중국을 압박했고, 중국은 자국도 사이버 공격의 피해자라고 주장하기도 했다. 중앙정부가 존재하지 않는 국제 체제에서 미국과 중국은 사이버 영역에서 기선을 잡기 위하여 적극적인 탐색전에 돌입했다. 미국은 현재의 사이버 우위를 유지하기 위하여 사이버 안보에 있어서 국제법과 레짐의 조성을 선점하고, 중국이 이 국제규범을 수용하도록 만들 필요성이 있다고 보고 있다. 한편, 중국은 미국 주도의 국제규범을 지키면서 미국과 경쟁하여 세력균형에 도달하기는 어렵다고 보면서 자국에 유리한 방안을 모색하고 있다.

<문 제>

제 1 문. <제시문 1>과 <제시문 2>를 참조하여 전통적인 안보와 사이버 안보의 차이를 서술한 후, <제시문 3>의 문서가 <제시문 1>과의 관계에서 어떠한 규범적 지위와 가치를 갖는지를 설명하고, 이 문서가 사이버 안보를 둘러싼 국제레짐의 확산에 있어서 어떻게 기여하고 영향을 줄 수 있는지에 대하여 논하시오.

(총 35점)

제 2 문. <제시문 4>와 <제시문 5>는 사이버 위협에 대처하고 안보를 확보하기 위한 노력을 보여주고 있다. <제시문 4>에서 서술하고 있는 사회적으로 최적 수준의 사이버 안보의 결정을 사회적 한계 편익과 한계 비용이라는 개념을 적용하여 정부 개입의 근거를 설명하시오. 그리고 이러한 정부의 기능이 국제관계에서는 제한적일 수 있음을 국제정치 이론을 사용하여 논하시오.

(총 35점)

제 3 문. <제시문 4>에 따라 사이버 안보 서비스의 시장공급량이 사회적으로 바람직한 수준에 미치지 못한다고 가정하자. 정부는 이를 해결하고자 경쟁력 있는 해외 업체에게 사이버 안보 시장을 개방하는 방안을 고려하고 있다. 그러나 안보 서비스의 특성상 해외업체에 대한 정부 규제에 어려움이 가중될 우려가 제기된다. 먼저, 사이버 안보 서비스 시장을 해외업체에게 개방하였을 경우 경제적 관점에서 장단점을 논하시오. 그리고 <제시문 3>에 기초하여, 위법한 행위를 한 해외 사이버 업체에 대한 국가의 관할권 행사의 근거 및 한계를 논하시오.

(총 30점)

안전행정부 시험출제과장

