10.17251/legal.2020.33.3.759

【일반 연구논문】

국제법상 사이버 간첩활동에 관한 일고찰

김 성 원*

* 원광대학교 법학전문대학원 부교수, SJD
논문 투고일: 2021. 01. 25. 논문 심사일: 2021. 02. 16. 게재 확정일: 2021. 02. 18.

Ⅰ. 서 론

정보통신기술의 비약적 발전에 따라 등장한 사이버공간은 국제사회의 구조적 변화를 가져왔다. 정보화 시대에 있어서 정보에 대한 접근, 정보의 수집, 정보의 저장 및 정보의 전송은 적지 않은 함의를 갖는바, 국제사회는 정보자산의 관리에 많은 관심을 기울이고 있다. 정보 저장의 용이함, 정보 전송의 신속함을 포함한 정보의 상호 연결성 측면에서 사이버공간은 국제사회에 많은 혜택을 주고 있지만, 동시에 사이버공간에 저장되는 정보의 관리 및 보호 측면에서 취약성 문제 또한 국제사회의 주요 관심사가 되고 있다. 특히, 사이버공간에서 발생하는 정보 관리의 심각한 위협과 관련하여 사이버 간첩활동(cyber espionage)은 국제사회의 특별한 관심사가 되고 있다.

간첩활동은 인류의 역사와 함께하여 왔다. 간첩활동의 주요 목표가 정보수집이라는 점을 감안할 때, 정보화 시대에 있어서 간첩활동은 새로운 황금기를 맞이하고 있다고 해도 과언이 아닐 것이다. Snowden 사건이 사이버 간첩활동의 고전적 사례로 언급될 만큼, 사이버 간첩활동의 규모는 더욱 커지고 있으며, 그 방법은 매우 정교하고 교묘하게 발전하고 있다. 이러한 맥락에서 사이버 간첩활동은 전통적인 간첩활동과 어떠한 차이가 있는지, 사이버 간첩활동을 규율할 수 있는 국제법규범이 존재하는지, 국제법규범의 기존 원칙들은 사이버 간첩활동에 적용 가능한 것인지 등에 대한 검토가 필요하다.

본 논문은 사이버 간첩활동에 대한 국제법적 검토를 주요 목적으로 한다. 첫째, 사이버 간첩활동의 이해를 돕기 위하여 전통적인 간첩활동에 대한 국제법적 접근을 고찰한다. 전시 간첩활동과 평시 간첩활동 각각을 규율하는 국제법규범을 살펴봄으로써 간첩활동에 대한 국제사회의 입장을 파악할 수 있을 것이다. 둘째, “사이버 작전에 적용 가능한 국제법에 관한 탈린 매뉴얼 2.0”(이하 ‘TM 2.0’ 이라 함)[1]이 규정하는 사이버 간첩

활동 관련 내용을 살펴본다. TM 2.0 또한 평시 사이버 간첩활동과 전시 사이버 간첩활동을 구분하여 다루고 있으며, 주권원칙, 국내문제 불간섭원칙 및 무력사용 금지원칙의 측면에서 사이버 간첩활동을 검토한다. TM 2.0에서 제시된 전문가그룹의 의견을 살펴봄으로써 사이버 간첩활동 관련 문제점을 파악할 수 있을 것이다. 셋째, 사이버 간첩활동을 영토주권, 국내문제 불간섭원칙 및 무력사용 금지원칙의 측면에서 고찰한다. 각 쟁점에 대하여 기존 국제법규범의 적용 시에 어떠한 문제가 있는지 살펴봄으로써 사이버 간첩활동 관련 국제법규범의 현실적 규범력을 검토한다. 결론 부분에서는 사이버 간첩활동을 보다 현실적으로 규율할 수 있는 국제법규범의 형성 가능성에 대하여 간략히 전망하도록 하겠다.

Ⅱ. 간첩활동 관련 국제법규범

1. 전시 간첩활동의 규율

간첩활동은 무력충돌법을 구성하는 다양한 조약 및 관습국제법에서 동일하게 다루어진다.[2] "육전의 법 및 관습에 관한 협약"(Convention (Ⅱ) with Respect to the Laws and Customs of War on Land and its annex; Regulations concerning the Laws and Customs of War on Land, 이하 '육전규칙'이라 함) 제24조[3]에 따라 간첩활동은 배신행위(perfidy)에 해당하지 않는 전쟁의 속임수(ruses of war)로 간주된다. 따라서 간첩활동은 전투 수행의 합법적 방법이며, 이는 군사 교범 및 국내법원의 판결로도 인정되고 있다.[4]

---

1) M. Schmitt & L. Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations/Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge Univ. Press, 2016).

2) W. Boothby, *The Law of Targeting* (Oxford Univ. Press, 2012), p. 277.

3) 육전규칙 제24조: 기계와 적정 및 지형탐지를 위하여 필요한 수단의 행사는 허용되는 것으로 본다.

육전규칙에 따르면, 간첩(spies)은 '개인'으로 규정되고 있다.[5] 따라서, 간첩활동은 군인과 민간인 모두가 수행할 수 있다. "전시에 있어서의 민간인의 보호에 관한 협약"(Geneva Convention Relative to the Protection of Civilian Persons in Time of War, 이하 '제네바 제4협약'이라 함)은 피보호인이 간첩활동을 하는 경우, 피보호인은 동협약상의 권리와 특권을 요청할 수 없음을 규정하고 있다.[6] "1949년 제네바협약에 대한 추가 및 국제적 무력충돌의 희생자 보호에 관한 의정서"(Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflict (Protocol I), 이하 '제1의정서'라 함) 제46조에 따라 충돌당사국 군대의 구성원, 즉 군인으로서 간첩활동을 수행하는 자는 간첩으로 취급될 수 있다.

제1의정서 제46조에 따라 간첩으로 취급되기 위하여 세 가지 요건이 충족되어야 한다. 첫째, 간첩활동은 소속 당사국을 위한 정보의 수집과 이의 전달과 관련된 활동을 수행하여야 한다.[7] 의사와 무관하거나 우연히 관련 정보를 누설한 개인은 간첩으로 취급되지 않는다.[8] 마찬가지로, 정보가 무력충돌과 관련이 없거나 정보를 수집한 개인이 소속 당사국에 정보를 전달하지 않는 경우, 이는 간첩활동으로 취급되지 않는다.

둘째, 간첩활동은 은밀히 또는 허위의 구실 하에 행해져야 한다. 군인이

---

4) *Flesche case* (Holland, Special Court of Cassation, 1949) [1949] 16 AD 266, 271; U.K. Ministry of Defence, *The Joint Service Manual of the Law of Armed Conflict*, 2004, section 4.9.3; Australia, *Law of Armed Conflict*, ADDP 06.4, 2006, section 7.18; US. Department of Defense, *Law of War Manual*, 2016, section 4.17.4.

5) 육전규칙 제29조: 교전자의 작전지역 내에서 상대 교전자에게 전달할 의사를 가지고 은밀히 또는 허위의 구실 하에 행동하여 정보를 수집하거나, 수집하려는 자만이 간첩으로 인정될 수 있다.

6) 제네바 제4협약 제5조: 충돌 당사국의 영역 내에서 피보호인이 동 충돌 당사국의 안전을 해하는 활동을 하였다는 혐의 또는 그러한 활동에 종사하고 있다는 사실을 확인하였을 경우에는 그러한 개인은 동인을 위하여 행사된다면 그러한 충돌 당사국의 안전에 유해할 본 협약상의 제 권리와 특권을 요청할 수 없다. 점령지역 내에서, 피보호인이 점령국에 의하여 간첩 또는... .

7) 육전규칙 제29조; 리버규칙(The Lieber Code) 제88조; 제1의정서 제46조 2항.

8) 육전규칙 제29조.

간첩이 되기 위해서는 위장한 상태에서 간첩활동을 수행해야 한다. 예를 들면, 무력충돌 상대 당사국의 군복 또는 민간인 복장을 착용한 상태에서 간첩활동을 수행해야 한다. 공개적으로 활동하는 군인 또는 민간인은 간첩으로 취급될 수 없다.[9] 따라서, 은밀하게 행해지지 않는 정보수집활동은 간첩활동으로 간주되지 않는다. 예를 들어, 군사정찰(military reconnaissance)을 공개적으로 행하는 경우, 이는 정당한 정보수집활동으로 간첩활동에 해당하지 않는다.[10]

셋째, 무력충돌법상 간첩활동은 지리적 요건을 충족하여야 한다. 즉, 특정 지역에서 정보수집활동을 행하는 자만이 간첩이 될 수 있다. 리버규칙(The Lieber Code)에 따르면, 무력충돌 상대 당사국이 체포할 수 있는 범위 내에 있거나 그 주변에 숨어있는 자만이 간첩이 된다.[11] 육전규칙, 제네바 제4협약 및 제1의정서 모두 지리적 요건을 규정하고 있다.[12] 간첩활동에 해당하기 위한 요건으로 지리적 요건은 관습국제법적 성격을 갖는다.[13]

상기에서 언급한 요건에 따라 무력충돌법상 간첩은 무력충돌 상대 당사국에 의해서 통제되는 영역 내에 물리적으로 존재하며, 자국에 유리한 무력충돌 관련 정보를 전달하기 위하여 은밀하게 정보를 수집하거나 수집하려고 시도하는 자를 의미하며, 이러한 요건을 갖춘 간첩이 수행하는 정보수집활동을 간첩활동으로 이해할 수 있다.

---

9) 육전규칙 제29조; 리버규칙(The Lieber Code) 제88조; 제1의정서 제46조 2항 및 3항.

10) O. Lissitzyn, "Electronic Reconnaissance from the High Seas and International Law," in R. Lillich & J. Moore (eds.), *Role of International Law and an Evolving Ocean Law, International Law Studies*, vol. 61 (1970), p. 563.

11) 리버규칙(The Lieber Code) 제83조. 원문은 다음과 같다 (Scouts, or single soldiers, if disguised in the dress of the country or in the uniform of the army hostile to their own, employed in obtaining information, if found within or lurking about the lines of the captor, are treated as spies, and suffer death).

12) 육전규칙 제29조는 "교전자의 작전지역"(in the zone of operations of a belligerent); 제네바 제4협약 제5조는 "충돌 당사국의 영역 내"(in the territory of a Party to the conflict); 제1의정서 제46조 2항은 "적대당사국에 의하여 지배되는 영토 내"(in territory controlled by an adverse Party)를 규정하고 있다.

13) Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, 3rd ed. (Cambridge Univ. Press, 2016), p. 280.

간첩활동을 성공적으로 수행하고 자신의 부대로 복귀한 간첩은 이후에 적에게 체포될 경우 포로로 취급되며, 이전의 간첩활동에 대하여는 어떠한 책임도 지지 않지만[14], 간첩활동 중 체포된 경우에는 전쟁포로의 지위를 향유하지 못한다.[15] 간첩 및 간첩활동에 관한 무력충돌법은 간첩활동을 수행하는 간첩과 간첩활동의 배후인 국가의 책임을 분리하여 규정한다. 즉, 간첩활동은 금지되지 않는 전쟁의 속임수로서 무력충돌법을 위반하지 않는 한, 간첩활동의 배후인 국가의 국가책임을 초래하지 않는다.[16]

2. 평시 간첩활동의 규율

(1) 평시 간첩활동의 유용성 주장 검토

전시 간첩활동과 달리, 평시 간첩활동에 관하여 국제법은 명확한 입장을 확립하지 못하고 있다. 평시 간첩활동의 법적 평가와 관련하여, 두 가지 상반된 견해가 대립한다. 즉, 평시 간첩활동을 적법한 것으로 보는 입장[17]과 위법한 것으로 보는 입장[18]이 존재한다. 평시 간첩활동에 대하여

14) 육전규칙 제31조.

15) 제1의정서 제46조 1항. 물론, 제네바 제4협약 제5조는 간첩에 대한 인간적 대우 및 공정한 재판을 받을 권리를 규정함으로써, 포로지위를 상실하게 되는 간첩에 대한 보호를 규정하고 있다.

16) U.S. "Practice Relating to Rule 57. Ruses of War," *IHL Database, Customary IHL* (https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_cou_us_rule57, 2021.1.13).

17) I. Delupis, "Foreign Warships and Immunity for Espionage," *American Journal of International Law,* vol. 78, no. 1 (1984), p. 67; M. Garcia-Mora, "Treason, Sedition and Espionage as Political Offenses under the Law of Extradition," *University of Pittsburgh Law Review,* vol. 26 (1964), pp. 79-80; Q. Wright, "Espionage and the Doctrine of Non-Intervention in Internal Affairs," in R. Stanger (ed.), *Essays on Espionage and International Law* (Ohio State Univ. Press, 1962), p. 12; R. Falk, "Space Espionage and World Order: A Consideration of the Samos-Midas Program," in Stanger, *id.*, p. 57.

18) J. Smith, "Keynote Address," *Michigan Journal of International Law,* vol. 28, no. 3 (2007), p. 544; C. Baker, "Tolerance of International Espionage: A Functional Approach," *American University International Law Review,* vol. 19, no. 5 (2003), pp. 1092, 1094; G. Sulmasy & J. Yoo, "Counterintuitive: Intelligence Operations and International Law," *Michigan Journal of International Law,* vol.

다수설은 평시 간첩활동은 위법하지도 적법하지도 않다는 것이다.[19]

간첩활동의 유용성을 긍정하는 견해는 간첩활동이 국제평화와 안전의 유지에 중요한 역할을 한다는 점을 강조한다.[20] 간첩활동의 유용성에 대한 이러한 견해는 국제관계학의 현실주의 및 기능주의에 입각한 주장이다. 현실주의 입장에서 국제사회는 무정부사회인바, 이러한 국제적 환경에서 국가의 생존은 국가 스스로가 책임져야 한다. 또한, 현실주의는 국제평화와 안전이 세력균형을 통해서 달성되는 것으로 본다.[21]

세력균형의 달성을 위해 필요한 것은 국가의 물질적 능력에 대한 정확한 평가이다. 상대국에 대한 정확한 정보는 무정부사회인 국제사회에서 국가의 생존을 보장하는데 필수적인 요소이다. 타국의 비밀정보를 많이 수집할수록 타국에 대한 전략적 평가가 가능하며, 이러한 전략적 평가를 통해서 세력균형의 쉽게 달성할 수 있다. 이러한 측면에서 간첩활동의 유용성을 주장하는 견해는 국제평화와 안전의 유지를 위해 간첩활동은 필수적이라고 주장한다.[22] 아울러, 국가들은 간첩활동을 국제관계에서 유용한 도구로 인식하며, 간첩활동은 국가의 통상적 활동이라는 견해 또한 이와 궤를 같이하는 주장이다.[23]

28, no. 3 (2007), pp. 628, 636.

19) C. Forcese, "Spies Without Borders: International Law and Intelligence Collection," *Journal of National Security Law and Policy,* vol. 5 (2011), p. 195; L. Pelican, "Peacetime Cyber-Espionage: A Dangerous But Necessary Game," *CommLaw Conspectus,* vol. 20, no. 2 (2012), p. 370; R. Williams, "(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action," *The George Washington Law Review,* vol. 79, no. 4 (2011), pp. 1164, 1175; A. Schaap, "Cyber Warfare Operations: Development and Use under International Law," *Air Force Law Review,* vol. 64 (2009), p. 140; D. Fleck, "Individual and State Responsibility for Intelligence Gathering," *Michigan Journal of International Law,* vol. 28, no. 3 (2007), p. 688.

20) M. Herman, *Intelligence Power in Peace and War* (Cambridge Univ. Press, 1996), pp. 137-220.

21) W. Wolforth, "Realim," in C. Reus-Smit & D. Snidal (eds.), *The Oxford Handbook of International Relations* (Oxford Univ. Press, 2010), pp. 131-149.

22) J. Stone, "Legal Problems of Espionage in Conditions of Modern Conflict," in Stanger, *supra* note 17, pp. 29-43.

23) W. Parks, "The International Law of Intelligence Collection," in J. Moore & R. Turner (eds.), *National Security Law* (Carolina Academic Press, 1999), pp.

그러나, 이러한 주장은 국제법상 수용되기 어렵다. 간첩활동으로 얻고자 하는 타국의 비밀정보는 통상 해당 국가의 본질적 국가 이익과 관련되는 정보에 해당한다. 국가의 본질적 이익 또는 필수적 이익에 해당하는 문제는 정치, 경제, 문화 및 사회 시스템에 관한 결정 또는 외교정책 관련 결정과 밀접히 관련되며[24], 이는 국가에 유보된 영역(domaine réservé), 소위 국가가 배타적 및 독립적으로 관할권을 행사하는 국내문제에 관련된 문제일 가능성이 크다.[25] 이러한 맥락에서 간첩활동은 타국의 주권을 침해하며 오히려 국제평화와 안전의 유지에 악영향을 줄 가능성이 크다.[26]

간첩활동 유용성 주장의 또 다른 근거는 기능주의이다. 간첩활동은 국제관계에서 유용한 국가실행인데, 왜냐하면 이는 국가 간 기능적 협력을 가능하게 하기 때문이다.[27] 세계화 시대의 국제평화와 안전은 넓게 정의되어야 하는바, 이러한 측면에서 국가 간 무력충돌의 회피와 같은 소극적 접근은 국제평화와 안전의 확보에 충분하지 않다고 Baker는 주장한다. Baker는 국제사회가 직면한 주요 문제의 해결에 국제협력은 필수적이며, 이러한 국제협력은 구속력있는 법규범을 통하여 달성될 수 있다고 주장한다.[28]

Baker는 구속력있는 법규범의 성실한 준수가 국제평화와 안전의 유지에 핵심이지만, 국가는 이를 종종 준수하지 않는다는 점을 지적한다. 국제체제는 자체 규범 준수 검증 시스템을 갖추고 있지만, 이는 한계가 있다는 점에서 Baker는 간첩활동의 유용성을 찾는다. 즉, 국가의 국제의무 이행 여부는 간첩활동으로 수집된 정보에 의해서 평가될 수 있는바, 간첩활동은 효과적 국제협력을 위해 중요한 역할을 하는 것으로 평가한다.[29]

433-434.

24) ICJ, *Nicaragua*, Judgment (1986), para. 205.

25) K. Ziegler, "Domaine Réservé," in R. Wolfrum (ed.), *The Max Planck Encyclopedia of Public International Law* (Oxford Univ. Press, 2008, online edition [www.mpepil.com]), MN 1.

26) H. Scoville Jr., "Is Espionage Necessary for Our Security?," *Foreign Affairs,* vol. 54, no. 3 (1976), pp. 482-495.

27) Baker, *supra* note 18, p. 1112.

28) *Id.*, p. 1099.

29) *Id.*, pp. 1108-1112.

기능주의에 입각한 Baker의 간첩활동 유용성 주장 또한 수용되기 어렵다. Baker가 주장한 바와 같이 국제평화와 안전의 유지에 국제사회 행위자들의 적극적 협력이 필요하다는 점은 이론의 여지가 없지만, 국제사회 행위자들의 적극적 협력은 어디까지나 신뢰를 바탕으로 전개되어야 한다. 상기에서 언급한 바와 같이 국가의 비밀정보에 대한 은밀한 수집 및 이의 폭로는 국가 주권을 존중해야 하는 실정법상 국제법과 합치되기 어렵다. 무엇보다도 간첩활동은 적극적 협력을 위한 국제협력을 오히려 방해하며, 이러한 점에서 국제평화와 안전의 확보를 방해한다.

(2) 평시 간첩활동의 적법성 주장 검토

간첩활동이 국제법상 명시적으로 허용된다고 주장하는 견해는 간첩활동이 예방적 또는 선제적 자위권 행사와 관련하여 중요한 역할을 한다는 점에 주목한다.[30] 1960년 U2기 사건 당시, 미국 국무장관은 소련 영토에서 행해진 간첩활동을 소련의 기습 위험성을 극복하는 조치로 정당화하였다.[31] 그러나, 이러한 주장은 간첩활동의 적법성을 간첩활동을 행하는 국가의 주관적 동기에서 찾는 것으로, 이는 국제법상 수용되기 어려운 주장이다.[32]

간첩활동의 적법성을 주장하는 또 다른 견해는 첩보활동과 관련된 광범위하고 만연한 국가실행(state practice)에 근거한다. 즉, 국가는 간첩활동 관련 정보기관(Intelligence Service)을 두고 있으며, 간첩활동 그 자체에 대한 공식적 항의가 제기되는 경우가 드물다는 점을 제시하며[33], 관습국제법상 적어도 국가실행의 측면에서 간첩활동의 적법성을 추론할 수

30) A. Melnitzky, "Defending America against Chinese Cyber Espionage Through the Use of Active Defenses," *Cardozo Journal of International and Comparative Law, vol. 20* (2012), p. 564; Sulmasy & Yoo, *supra* note 18, p. 636.

31) Wright, *supra* note 17, p. 17

32) Baker, *supra* note 18, p. 1097.

33) R. Buchan, "The International Legal Regulation of State-Sponsored Cyber Espionage," in A.-M. Osula & H. Rõigas (eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE Publication, 2016), pp. 83-84.

있다고 주장한다.[34] 간첩활동 관련 광범위한 국가실행은 간첩활동이 통상적이고 확립된 국가 기능의 수행으로 널리 수용된다는 명확한 증거라는 것이다.[35]

그러나, 국가실행만을 근거로 간첩활동을 적법화하는 관습국제법의 존재를 추정하는 주장은 국제법상 설득력을 갖지 못한다. 관습국제법의 형성에 요구되는 또 다른 중요 요건이 충족되지 않기 때문이다. 즉, 간첩활동의 적법성을 반영하는 관습국제법이 형성되기 위해서는 간첩활동의 적법성에 관한 법적 확신(*opinio juris*)이 충족되어야 한다. 국가는 간첩활동이 적법하다고 생각하면서 간첩활동을 수행하지 않는다. 오히려 국가는 간첩활동의 문제점을 인지하면서 간첩활동을 수행한다고 이해하는 것이 더 현실적이다. 실제로 간첩활동의 적법성을 반영하는 법적 확신이 구성될 가능성은 매우 낮은 것으로 생각된다.[36]

간첩활동은 성질상 비밀리에 행해지는바, 이러한 비밀작전이 관습국제법의 형성을 위한 국가실행이 될 수 있는지도 의문이다. 관습국제법의 확인에 관한 UN 국제법위원회 제2차 보고서를 감안할 때, 비밀리에 행해지는 국가실행은 일반 관습국제법의 형성 또는 확인에 기여하는 것으로 보기 어렵다.[37] 관습국제법의 형성에 있어서 국가실행은 공개적으로 표시되어야 하는데, 왜냐하면 국가는 긍정적 또는 부정적 의사표시를 통해 관습국제법의 형성 또는 확인에 대한 견해를 밝혀야 하기 때문이다.[38] 사실상 간첩활동은 국가실행과 법적 확신이 각각 정반대의 방향으로 진행되는 것으로 보이는바[39], 간첩활동의 적법성을 반영하는 관습국제법이 형성된

34) Smith, *supra* note 18, p. 544.

35) J. Kish, *International Law and Espionage* (ed. by D. Turns, Martinus Nijhoff Publishers, 1995), XV; G. Demarest, "Espionage in International Law," *Denver Journal of International Law and Policy,* vol. 24, no. 2 (1996), p. 321.

36) A. Radsan, "The Unresolved Equation of Espionage and International Law," *Michigan Journal of International Law,* vol. 28, no. 3 (2007), p. 596.

37) UNGA, ILC, *Second Report of the Identification of Customary International Law*, A/CN.4/672, para. 47.

38) Y. Dinstein, "The Interaction between Customary Law and Treaties," *Recueil des Cours,* vol. 322 (Brill, 2007), p. 275.

39) S. Chesterman, "The Spy Who Came in From the Cold War: Intelligence and

것으로 보기는 어렵다. 물론, 간첩활동의 위법성을 반영하는 관습국제법도 형성된 것으로 볼 수 없다는 점은 명확하다. 그러나, 적어도 간첩활동의 적법성을 반영하는 관습국제법이 존재하는 것으로 주장하기에는 많은 문제가 있다.

(3) 평시 간첩활동의 위법성 주장 검토

간첩활동에 관한 적법성 주장과 마찬가지로 간첩활동에 관한 위법성 주장 또한 적지 않은 문제점을 가지고 있다. 사실상, 간첩활동에 대한 국제법은 불완전한 상태에 있다.[40] 국제법상 간첩활동의 위법성의 근거를 국내법상 간첩활동의 처벌에서 찾는 견해가 있다.[41] 즉, 간첩활동이 적법한 것이라면 국가는 간첩을 처벌하는 국내법을 제정하지 않았을 것이라는 주장이다. 이러한 주장은 국내법상 간첩활동의 처벌을 근거로 국제법의 법원(法源)인 법의 일반원칙(general principles of law)에 의존하는 것으로 보인다. 그러나, 법의 일반원칙에 근거한 간첩활동의 위법성 주장은 법의 일반원칙의 개념을 잘 못 이해한 것으로 보이는데, 법의 일반원칙은 국가 간 관계에서 적용되는 것이기 때문이다.[42]

간첩활동이 타국의 영토보전 및 정치적 독립을 침해한다는 주장 또한 간첩활동의 위법성 주장을 뒷받침하는 주요 입장이다.[43] "영토보전" 및 "정치적 독립"이라는 표현은 매우 중요한 의미를 갖는데, 왜냐하면 이 표현은 무력위협 또는 무력사용을 포괄적으로 불법화하는 UN헌장 제2조 4항에 제시된 것이기 때문이다. 그러나, 이러한 주장은 논리적 문제가 있다. 간첩활동을 위하여 국가는 일반적으로 목표국에 항공기, 선박, 잠수함

International Law," *Michigan Journal of International Law,* vol. 27, no. 4 (2006), p. 1072.

40) J. Kraska, "Putting Your Head in the Tiger's Mouth: Submarine Espionage in the Territorial Sea," *Columbia Journal of Transnational Law,* vol. 54, no. 16 (2015), p. 172.

41) Garcia-Mora, *supra* note 17, 80; Radsan, *supra* note 36, p. 604.

42) B. Lepard, *Customary International Law: A New Theory with Practical Applications* (Cambridge Univ. Press, 2010), p. 164.

43) Wright, *supra* note 17, p. 12.

또는 간첩을 침투시킨다.

간첩활동에 있어서 목표국 영토의 "물리적 침투"는 간첩활동의 일부가 될 수 있지만, 간첩활동 그 자체는 아니다. 따라서 이러한 주장은 간첩활동의 부수적 결과와 평시 간첩활동 그 자체를 혼동하는 것이다. 아울러, 영토보전과 정치적 독립의 침해 여부는 무력위협 또는 무력사용의 맥락에서 결정되는데, 간첩활동이 무력위협 또는 무력사용과 무관한 것이라면 UN헌장 제2조 4항의 위반 여부는 제기될 수 없다.

일부 학자들은 간첩활동의 개념을 '비밀 군사지원'(covert military assistance)을 포함하는 것으로 확대해석하여 간첩활동이 국내문제 불간섭원칙을 위반하는 활동이라고 주장한다.[44] 이러한 의미에서, 1980년대 니카라과 반군을 지원한 미국의 행위를 국내문제 불간섭원칙을 위반하는 간첩활동의 명백한 사례로 제시하는 견해도 있다.[45] 사실, 이러한 견해는 미국의 군사 작전과 관련되어 주장되는 것으로 일반적인 견해는 아니다.

이러한 견해는 간첩활동을 정보기관과 밀접한 협력하에 수행되는 군대의 "전장정보분석"(preparation of the battlefield)과 혼합하는 것이다. 비밀 군사지원과 전장정보분석은 개념적으로 구별되는 간첩활동과의 차이점을 모호하게 만드는 것으로 미국의 군사 작전에 있어서 특화된 개념이다. 아울러, 국내문제 불간섭원칙이 위반되기 위해서는 '강제'(coercion)의 요건이 충족되어야 한다.[46] 간첩활동이 비록 목표국의 중요한 국내문제에 관한 정보를 수집하더라도 강제가 결여되는 경우 이는 국제법상 국내문제 불간섭원칙을 위반하는 것으로 보기 어렵다.

(4) 소결

비록 몇 차례에 걸쳐 간첩활동의 적법성 여부를 다룰 기회가 있었지만,

44) T. Gill, "Non-Intervention in the Cyber Context," in K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO CCD COE Publication, 2013), pp. 219-226.

45) Forcese, *supra* note 19, p. 198.

46) P. Kunig, "Intervention, Prohibition of," in R. Wolfrum, *supra* note 25, MN 5.

ICJ는 간첩활동 자체의 적법성 또는 위법성에 대한 판단을 보류했다.[47] 니카라과 사건에서 니카라과는 정보수집을 위한 미국 정찰기의 니카라과 영공 비행에 대하여 항의하였지만[48], 니카라과는 영공침해만을 주장했을 뿐이었다.[49] ICJ 또한 미국의 정찰행위를 니카라과 영공에 대한 침해로서 다루었고, 영토주권 위반 여부를 검토하였을 뿐, 간첩활동 자체에 관해서는 판단하지 않았다.[50] ICJ가 다룬 미국과 이란 간 인질사건에서 이란은 미국 외교관의 간첩활동을 주장하였지만, ICJ는 이란의 주장을 배척하고, 단지 외교관계법은 자기완비규범이라는 점만을 언급한 바 있다.[51] 사실상, 국가들은 간첩활동에 대한 국제법상 불확실성을 유지하고자 하는 것으로 볼 수 있다.[52] 결론적으로 간첩활동에 대하여 국제법은 확정적인 입장을 취하고 있지 않은 것으로 볼 수 있다.

Ⅲ. 사이버 간첩활동 관련 국제법규범: TM 2.0을 중심으로[53]

1. 전시 사이버 간첩활동

TM 2.0은 사이버 무력충돌법을 제4부에서 규정하고 있다.[54] 제4부는 제16장(무력충돌법 일반), 제17장(적대행위의 수행), 제18장(특정한 사람,

47) Fleck, *supra* note 19, p. 691.
48) *Nicaragua*, *supra* note 24, para. 21.
49) *Id.*, paras. 87, 250.
50) *Id.*, paras. 91, 251, 252.
51) ICJ, *Hostage case*, Judgment (1980), paras. 85-87.
52) Forcese, *supra* note 19, p. 204.
53) TM 2.0은 NATO 사이버방위협력전문센터(CCD COE)가 초빙한 국제전문가그룹이 작성한 것으로 2017년 출간되었다. 정식 명칭은 "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations"이다. NATO CCD COE는 2013년 "Tallinn Manual on the International Law Applicable to Cyber Warfare"를 발간한 바 있다 (이하 'TM'이라 함). TM이 사이버 전투에 적용되는 국제법에 초점을 두었다면, TM 2.0은 사이버 작전에 초점을 둔다.
54) Schmitt & Vihul, *supra* note 1, pp. 373-562.

대상물, 활동), 제19장(점령) 및 제20장(중립)으로 구성된다. TM 2.0 제4부에 규정된 규칙에서 간첩활동은 규칙 82(국제적 무력충돌의 정의), 규칙 89(간첩), 규칙 92(사이버 공격의 정의), 규칙 122(배신행위), 규칙 136(피구금인의 서신)에서 언급되고 있다.

사이버 간첩활동을 직접 다루는 TM 2.0 규칙 89는 무력충돌법상 간첩활동의 정의와 거의 동일하게 사이버 간첩활동을 규정한다.[55] TM 2.0은 규칙 89가 육전규칙 제29조, 제31조 및 제1의정서에 기초하여 작성되었음을 밝히고 있다.[56] 간첩활동의 세 가지 요소, 즉, 정보수집과 전달, 간첩활동의 은밀성 및 지리적 요건 모두 규칙 89에서 규정되고 있다.[57]

규칙 89는 지리적 요건을 감안하여, 사이버 간첩활동은 근접 접근 사이버 작전(close access cyber operations)의 형태로 발생할 가능성이 크다는 견해를 제시하였다. 즉, 컴퓨터 시스템에 접근하기 위하여 컴퓨터 휴대용 저장장치(flash drive)를 사용하거나, 은밀하게 행동하면서 신호를 가로채는 유형의 사이버 간첩활동이 행해질 것으로 예상하였다. 규칙 89는 적이 통제하는 영역 밖에서 행해지는 사이버 간첩활동을 본 규칙의 적용대상에서 제외한다. 따라서, 정보수집이 적이 통제하는 영역에서 발생되어도, 이러한 행위가 적이 통제하는 영토를 벗어난 곳에서 원격으로 수행되는 경우에 규칙 89는 적용되지 않는다.[58]

TM 2.0은 무력충돌법은 사이버 간첩활동 자체를 금지하지는 않지만, 무력충돌법에 규정된 모든 금지에 종속될 수 있다는 견해를 취한다. TM 2.0은 이와 관련된 사례로 특정 상황에서 사이버 간첩활동은 규칙 122에서 규정하는 배신행위에 해당할 수 있다고 설명한다.[59] TM 2.0의 작성에 참여한 전문가그룹 중 다수는 사이버 간첩활동으로 수집된 정보는 무력충돌 당사국을 위한 것이어야 한다는 점에는 합의하였지만[60], 무력충돌

55) TM 2.0 규칙 89 (간첩). 군대의 구성원으로 적 통제영역에서 사이버 간첩활동을 수행하는 자는 전쟁포로가 될 권리를 상실하며 그가 속한 군대에 복귀전에 체포될 경우 간첩으로 취급될 수 있다. *id.*, p. 409.

56) *Id.*, p. 410, para. 2.

57) *Id.*, pp. 410-411, paras. 4-7.

58) *Id.*, p. 411, para. 8.

59) *Id.*, p. 411, para. 9.

당사국을 위해 수집된 정보가 군사적 가치를 가져야 하는지에 대하여는 의견이 나뉘었다. 전문가그룹의 다수는 수집된 정보의 성격으로 사이버 간첩활동의 성격을 규정하는 것은 아니라는 견해를 밝혔지만, 소수는 수집된 정보는 반드시 군사적 가치를 가져야 한다고 주장하였다.

2. 평시 사이버 간첩활동

사이버 간첩활동은 TM 2.0 여러 부분에서 언급되고 있다.[61] 사이버 간첩활동은 TM 2.0 제1부(일반국제법과 사이버공간) 제5장(국제법에 의해 그 자체로 규율되지 않는 사이버 작전) 규칙 32에 규정되고 있다. 규칙 32는 국가가 행하는 사이버 간첩활동은 그 자체로는 국제법을 위반하지는 않지만, 수행되는 방법은 국제법을 위반할 수 있다고 설명한다.[62]

TM 2.0 규칙 32는 사이버 간첩활동을 사이버 능력을 활용하는 정보수집 또는 수집 시도로 은밀하게 또는 허위의 구실 하에 행해지는 모든 활동으로 정의한다.[63] 전문가그룹은 사이버 기술이 원격 접근 작전(remote access operations)을 가능하게 하는바, 목표국 영토에 물리적으로 존재해야 할 필요성을 경감시킨다는 점을 지적한다.[64] 전문가그룹은 비록 Snowden 사건, 위키리크스(Wikileaks) 폭로 사건 등에 따라 사이버 간첩활동을 금지하는 관습국제법이 확립되었는지에 관한 논쟁이 촉발되었지만, 관습국제법이 간첩활동 그 자체를 금지하는 것은 아니라는 점에 합의

60) *Id.*, pp. 411-412, para. 10.

61) TM 2.0 제4부 외에서 사이버 간첩활동을 언급한 규칙은 다음과 같다. 규칙 4(주권침해), 규칙 6(상당한 주의(일반원칙)), 규칙 12(관할권 행사로부터 국가 면제), 규칙 14(법집행에서 국제협력), 규칙 31(일반원칙), 규칙 35(개인이 향유하는 권리), 규칙 41(전자 문서, 서류 및 서신의 불가침성), 규칙 43(공관의 사용과 관원의 행위), 규칙 59(우주활동에 대한 존중), 규칙 65(분쟁의 평화적 해결), 규칙 66(국가에 의한 간섭), 규칙 69(무력위협 또는 무력사용의 금지), 규칙 71(무력공격에 대한 자위). Schmitt & Vihul, *supra* note 1 참조.

62) TM 2.0 규칙 32 (평시 사이버 간첩활동). 비록 국가에 의한 평시 사이버 간첩활동은 그 자체로 국제법을 위반하지는 않지만, 평시 사이버 간첩활동이 수행되는 방법은 국제법을 위반할 수 있다. *id.*, p. 168.

63) *Id.*, p. 168, para. 2.

64) *Id.*, pp. 168-169, para. 4.

하였다.[65]

TM 2.0 작성에 참여한 전문가그룹은 사이버 첩보활동 그 자체는 국제법상 금지되지 않지만, 사이버 첩보활동이 수행되는 방법은 국제법을 위반할 수 있다는 점에 동의하였다. 전문가그룹은 사이버 첩보활동이 침해할 수 있는 국제법원칙으로 주권원칙 및 국내문제 불간섭원칙을 예로 들었다. 전문가그룹은 사이버 작전을 그 자체로 위법하지 않은 사이버 간첩활동으로 주장함으로써 국제법상 적법한 것으로 주장할 수 없다는 점 또한 명확히 하였다.[66] 전문가그룹은 해저통신케이블 도청의 적법성은 작업이 수행된 지역, 즉 연안국의 영해 내 또는 외에서 수행되었는지에 따라 좌우된다는 점을 제시하며, 사이버 감시 작업은 개별적 내용에 따라 평가되어야 한다고 주장하였다.[67]

전문가그룹은 특정한 수준의 심각성을 상회하는 원격 사이버 첩보활동의 국제법 위반 여부에 대하여 총의를 도출하지 못하였다. 전문가그룹의 다수는 사이버 첩보활동은 심각성과 무관하게 어떠한 국제법상 금지도 위반하지 않는다는 견해를 밝히며, 사이버 첩보활동의 평가 쟁점은 심각성이 아니라 사용된 방법이라는 입장을 취하였다. 반면, 전문가그룹의 소수는 특정 지점에서 피해국이 겪은 결과가 심각해지면, 이는 피해국의 주권원칙을 침해하는 것이라는 입장을 취하였다.[68]

전문가그룹은 근접 접근 사이버 간첩활동(close access cyber espionage operations)에 대해서도 총의를 도출하지 못하였다. 전문가그룹 다수는 근접 접근 사이버 간첩활동이 피해국의 주권을 침해하는 것은 근접 접근 사이버 첩보활동 자체에 의한 것이 아니라, 피해국의 동의없이 근접 접근 사이버 간첩활동을 행하는 개인이 피해국 영토에 물리적으로 있었다는 사실에 의한다는 견해를 밝혔다. 전문가그룹 일부는 사이버 첩보활동은 주권원칙 및 국내문제 불간섭원칙에 대한 예외에 해당하는바, 위법하지 않은 활동이라는 입장을 취하였다.[69]

---

65) *Id.*, p. 169, para. 5.
66) *Id.*, p. 170, para. 6.
67) *Id.*, p. 170, para. 7.
68) *Id.*, pp. 170-171, para. 8.

전문가그룹 중 다수는 사이버 간첩활동 그 자체로는 국제법상 위법하지 않더라도, 국제법 위반행위의 불가결한 요소를 구성할 수 있다는 점에 합의하였다.[70] 또한 전문가그룹은 초기 단계에서 수집된 정보가 궁극적으로 국제법상 위법한 무력공격을 위해 사용되었다고 하더라도, 초기 단계의 정보수집은 그 자체로 국제법상 위법한 것은 아니라는 입장을 취하였다. 즉, 전문가그룹은 정보수집과 이에 따른 무력공격은 구분되는 행위이며, 이들의 국제법상 허용 여부는 개별적으로 평가되어야 한다는 견해를 밝혔다.[71] 아울러, 전문가그룹은 사이버 간첩활동의 수행을 위해 별개의 사이버 작전이 활용되는 경우, 비록 합법적 사이버 간첩활동을 위해 설계되었더라도 별개의 사이버 작전의 적법성 여부는 사이버 간첩활동과 분리되어 평가되어야 한다는 입장을 취하였다.[72]

국가는 허니팟(honeypot)을 활용하여 타국이 허니팟 안에서 어떠한 작전을 수행하는지 관찰할 수 있으며, 허니팟에 악성 파일을 설치하고 타국이 이를 추출할 경우에 타국의 활동을 관찰할 수 있다. 전문가그룹은 이러한 허니팟의 활용은 국제법 위반에 해당하지 않는다는 입장을 취하였다.[73] 추출된 정보가 표적 시스템에 심각한 피해를 유발하는 무기화된 허니팟에 대하여, 전문가그룹 중 소수는 허니팟의 파괴적 속성에 따라 최소한 표적국의 주권이 침해된다는 의견을 개진하였다. 반면, 전문가그룹 중 다수는 표적 시스템의 파괴는 표적국이 스스로 허니팟에 침투하여 유발된 것이라는 점을 지적하였다.[74]

---

69) *Id.*, p. 171, para. 9.
70) *Id.*, pp. 171-172, para. 10.
71) *Id.*, p. 172, para. 11.
72) *Id.*, p. 172, para. 12.
73) *Id.*, pp. 173-174, para. 15.
74) *Id.*, p. 174, para. 16.

Ⅳ. 사이버 간첩활동 관련 국제법 쟁점

1. 사이버 간첩활동과 영토주권

국가는 국제법상 주권에 따라 영토주권을 향유한다. 영토주권에 따라 국가는 자신의 영토에 대한 관할권을 행사한다. 영토주권의 행사는 국내 문제에 대하여 배타적이고 자유롭게 결정할 수 있는 국가권력의 독립과 밀접히 관련된다.[75] 국제법상 주권은 모든 것을 포섭하는 일괄적 성격을 갖는데, 영토주권의 핵심은 국가는 타국의 영토에서 자신의 권한을 행사할 수 없다는 것이다. 즉, 타국에 대한 국가의 권한 행사는 국제법상 주권의 침해로 간주된다.

사이버공간에 영토주권 개념이 어느 정도로 적용될 수 있는지에 대하여 논쟁이 있어왔다.[76] 일부 학자들은 기존 국제법은 사이버공간에 적용될 수 없다는 견해를 제시하는데, 기존 국제법은 영토에 대한 관할권의 행사에 기반한 것으로 물리적 영토와 경계를 갖지 않는 가상공간에 불과한 사이버공간에는 기존 국제법이 적용되지 않는다는 것이다.[77] 물론 사이버공간은 가상공간이지만, 사이버공간이 존재하기 위한 물리적 구조, 즉 광섬유, 구리선, 위성장치, 인터넷 등이 필요한바, 사이버공간은 물리적 공간과 분리하여 존재할 수 없다는 점에서 기존 국제법의 적용은 가능하다는 것이 다수설이다.[78]

TM 2.0 규칙 1 또한 사이버공간의 물리적, 논리적 및 사회적 층(the physical, logical, and social layers of cyberspace) 모두가 주권원칙에 포

75) H. Moynihan, "The Application of International Law to State Cyberattacks Sovereignty and Non-intervention," *Research Paper, International Law Programme* (Chatham House, 2019), p. 12.

76) N. Tsagourias, "The legal status of cyberspace," in R. Buchan & N. Tsagourias (eds.), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing, 2015), pp. 16-24.

77) D. Johnson & D. Post, "Law and Borders: The Rise of Law in Cyberspace," *Stanford Law Review,* vol. 48 (1996), p. 1367.

78) J. Goldsmith, "Against Cyberanarchy," *University of Chicago Law Review,* vol. 65, no. 4 (1998), p. 1199.

섭됨을 규정하고 있으며, 사이버 활동은 사이버 기반시설이 위치한 국가의 영토에서 행해지고, 국가는 이에 주권적 특권을 행사할 수 있다는 점을 규정하고 있다. 따라서, 영토주권을 사이버공간에 적용하기 위한 영토성 문제는 극복된 것으로 볼 수 있다.[79] 규칙 2는 또한 국가는 국제법적 의무 준수를 조건으로 자신의 영토에 있는 사이버 기반시설, 사람 및 사이버 활동에 대해 주권적 권한을 행사한다는 점을 규정한다.[80] 즉, 국가의 영토주권은 사이버 기반시설의 소유자와 무관하게 자신의 영토에 물리적으로 존재하는 모든 사이버 기반시설 및 이를 뒷받침하는 컴퓨터 네트워크 및 시스템을 대상으로 행사된다.

정보수집을 위하여 은밀히 수행되는 간첩활동은 목표국의 주권적 영역에서 수행되는바, 목표국의 허가 없는 목표국 영토로의 침입이 필요하다. 즉, 간첩활동은 그 자체로 국제법상 금지되지 않지만, 목표국의 허가 없이 목표국 영토에 침입한다는 점에서 국제법상 위법한 활동이 될 수 있다.[81] TM 2.0의 작성에 참여한 전문가그룹의 다수는 사이버 간첩활동이 목표국의 사이버 기반시설에 대한 근접 접근 작전으로 수행되는 경우, 작전을 수행하는 개인이나 플랫폼의 위치에 따라 목표국 영토주권이 침해될 수 있다고 보았다.[82] 즉, 목표국의 허가 없이 목표국에 위치하는 사이버 기반시설로 운영되는 컴퓨터 시스템 또는 네트워크에 침입하여 비밀정보를 탈취하는 경우, 이러한 사이버 간첩활동은 목표국의 영토주권을 침해할 수 있다. TM 2.0 또한 목표국의 컴퓨터 네트워크 및 시스템에 저장된 비밀정보를 수집하기 위하여 국가가 요원을 목표국 영토에 침투시키는 순간 목표국의 영토주권이 침해된다는 견해를 취한다.[83]

그러나, 사이버 간첩활동이 원격으로 수행되는 경우, 이는 복잡한 문제를 야기한다. 원격 접근 사이버 간첩활동의 경우 목표국의 영토에 인지 가능한 물리적 효과를 초래한다면, 이는 목표국의 영토주권을 위반하는

79) Schmitt & Vihul, *supra* note 1, p. 12, paras. 4-5.
80) *Id.*, p. 13, para. 1.
81) Chesterman, *supra* note 39, p. 1082.
82) Schmitt & Vihul, *supra* note 1, p. 171, para. 9.
83) *Id.*, p. 19, para. 6; p. 171, para. 9.

것으로 간주될 수 있다.[84] 그러나, 간첩활동의 본질적 특성인 비밀성을 감안할 때, 논리적으로 사이버 간첩활동은 목표국에 인지 가능한 물리적 효과를 초래하지 않을 것이다. 따라서, 목표국 사이버 기반시설에 저장된 정보를 탈취하기 위하여 침투하는 사이버 간첩활동이 목표국 영토의 물리적 침투와 같은 것이 될 수 있는지는 의문이다.[85] 목표국 영토에 허가 없이 침투하는 항공기, 선박, 잠수함 등과 같은 전통적 유형의 정보수집 플랫폼으로 사이버 간첩활동을 간주하는 것은 일견 가능한 것으로 보인다. 그러나, 사이버 간첩활동이 겨냥하는 플랫폼은 목표국의 사이버 기반시설로서 이는 목표국의 영토에 이미 설치된 것이라는 점에서 차이가 있다.

TM 2.0의 작성에 참여한 전문가그룹의 다수는 원격으로 수행되는 사이버 간첩활동이 목표국 사람 또는 사물에 대한 물리적 손해 또는 사이버 기반시설의 기능성 상실 등을 초래하는 경우에만 목표국의 영토주권을 침해하는 것으로 결정하였다. 즉, 전문가그룹의 다수는 본질상 사이버 간첩활동은 비밀정보의 수집이며, 온라인 또는 오프라인에서 파괴적 효과를 유발하지 않는다면 평시 사이버 간첩활동은 목표국의 영토주권의 침해를 구성하지 않는 것으로 보았다.[86] 전문가들이 목표국의 사람 또는 사물에 대한 물리적 손해 또는 사이버 기반시설의 기능성 상실 어느 것도 초래하지 않는 사이버 작전의 목표국 영토주권 침해 가능성에 대하여 총의를 이루지 못하였다는 점을 감안할 때[87], 단순한 비밀정보수집에 해당하는 사이버 간첩활동을 목표국의 영토주권을 침해하는 것으로 보기 어려울 것이다.

TM 2.0은 사이버 작전이 타국 정부의 본질적 기능(the inherently governmental functions of another State)의 수행에 간섭하는 경우, 주권

84) W. von Heinegg, "Legal Implications of Territorial Sovereignty in Cyberspace," in C. Czosseck, R. Ottis & K. Ziolkowski (eds.), *Proceedings of the 4th International Conference on Cyber Conflict* (NATO CCD COE Publication, 2012), pp. 11, 16; L. Greenberg, S. Goodman & K. Hoo, *Information Warfare and International Law* (U.S. National Defence Univ., 1998), p. 24.

85) Forcese, *supra* note 19, p. 208; von Heinegg, *supra* note 84, p. 11.

86) Schmitt & Vihul, *supra* note 1, p. 171, para. 8.

87) *Id.*, p. 21, para. 14.

침해가 발생할 수 있음을 규정한다.[88] 무엇이 정부의 본질적 기능의 수행인지를 결정하기는 어렵지만, 사회 서비스의 제공, 선거실시, 세금 징수, 외교의 효과적 수행, 필수 국방 활동 등과 같이 정부만이 할 수 있는 기능이 정부의 본질적 기능의 수행으로 제시된다.[89]

정부의 본질적 기능의 수행에 필수적인 정보에 대한 사이버 작전이 위법한 간섭에 해당하는지에 대하여 TM 2.0의 전문가그룹의 의견은 일치되지 않았다. 일부 전문가는 목표국 정부 기능의 수행에 관련되는 정보를 변경하거나 삭제하는 컴퓨터 작전은 위법한 간섭에 해당하는바, 목표국의 주권을 침해하는 것으로 보았다.[90] 그러나, 사이버 간첩활동이 목표국 정부 기능의 수행에 관련되는 정보를 단순히 복사하는 경우, 이는 목표국에 대한 위법한 간섭에 해당하지 않는다.

국가실행 및 법원의 판결은 사이버 간첩활동이 목표국 정부 기능의 수행에 대한 위법한 간섭에 해당하지 않음을 보여준다. 1960년 미국이 외기권에 위성을 두고 소련 영토 내의 동향을 관찰한 사건[91]에서 소련은 미국의 행위가 소련의 영토주권을 침해하며, 정부 기능의 수행에 대한 위법한 간섭이라고 주장하였다.[92] 소련의 이러한 영토주권에 관한 주장은 그 당시에도 거부된 바 있다.[93] 유럽인권법원 또한 Weber 사건에서 영토를 침범하지 않는 간첩활동은 영토주권과 양립되며, 목표국 정부 기능의 수행과 관련된 정보의 탈취를 목표국에 대한 위법한 간섭으로 간주하지 않았다.[94]

사이버 간첩활동과 정부 기능의 수행에 대한 위법한 간섭 간의 관계는 2014년 ICJ가 다룬 동티모르 사건에서 다루어졌는데, 일부 학자는 이 사

88) *Id.*, pp. 21-22, para. 15.
89) *Id.*, p. 22, para. 16.
90) *Id.*
91) Falk, *supra* note 17 참조.
92) Soviet Statement in the General Assembly, First Committee, 17th Session, 1298th Meeting, (3 Dec. 1962).
93) J. Soraghan, "Reconnaissance Satellites: Legal Characterization and Possible Utilization for Peacekeeping," *McGill Law Journal,* vol. 13, no. 3 (1964), pp. 475-483.
94) ECtHR, *Weber and Saravia v. Germany*, Decision (2006), para. 88.

건을 상기 관계에 대한 기존 견해에 대한 도전으로 평가하기도 한다.[95] 호주는 호주 주재 동티모르측 변호인 사무실에 호주 요원을 침투시켜 동티모르와 변호인 간의 서신 및 통티모르와 호주 간의 중재 관련 서신에 담겨진 정보와 문서를 탈취하였다. 이에 동티모르는 ICJ에 문서의 반환, 호주가 탈취한 정보와 문건의 파기 및 호주의 행위는 동티모르의 주권을 침해한다는 잠정조치 명령을 요청하였다.[96]

ICJ는 동티모르의 요청에 따라 잠정조치 명령을 내리며, 호주는 압수한 문건의 비밀성을 보장하고, 동티모르와 변호인 간의 통신을 어떠한 방법으로도 간섭하지 말아야 할 것을 명령했다.[97] ICJ의 잠정조치 명령에 대하여 이는 국가와 변호인 간의 비밀 서신에 담긴 문서와 정보의 수집은 정부 기능의 수행에 대한 위법한 간섭이며, 따라서 호주의 간첩활동은 동티모르의 영토주권에 위반된다는 해석이 가능하다는 주장이 있는데, 이러한 주장이 가능하다면, 매우 큰 함의를 가질 것이다. 즉, 국제법상 간첩활동의 적법성을 제한하는 사례로서 원용될 수 있기 때문이다.[98]

그러나, 동티모르의 법률 대리인 중 하나인 E. Lauterpacht는 ICJ 구두변론에서 이 사건은 간첩활동과 관련된 것이 아니라고 설명하였는바, ICJ는 간첩활동을 판단할 필요가 없었다.[99] ICJ는 잠정조치를 명령하면서 동티모르가 보호를 원하는 권리는 중재소송을 수행할 권리, 호주의 간섭없이 교섭을 진행할 권리 및 변호인과 통신의 비밀성 유지에 관한 권리를 포함한다고 언급하였다. 즉, ICJ 잠정조치 명령의 근거는 간첩활동이 정

95) N. Jupillat, "From the Cuckoo's Egg to Global Surveillance: Cyber Espionage that Becomes Prohibited Intervention," *North Carolina Journal of International Law and Commercial Regulation,* vol. 42, no. 4 (2017), pp. 960-961.

96) ICJ, *The Seizure and Detention of Certain Documents and Data*, Provisional Orders (2014), para. 2.

97) *Id.*, para. 55.

98) A. Deeks, "Can the ICJ Avoid Saying Something on the Merits About Spying in Timor-Leste vs. Australia?," *Lawfare* (12 March 2014) (http://www.lawfareblog.com/can-icj-avoid-saying-something-merits-about-spying-timor-leste-vs-australia, 2021.1.13).

99) *The Seizure and Detention of Certain Documents and Data, supra* note 96, Oral Proceeding, Verbatim Record 2014/1, CR 2014/1 (2014), 15-16.

부 기능의 수행에 대한 위법한 간섭에 근거한 것이 아니라, 주권에 따라 국가와 변호인 간의 비밀스러운 관계를 유지할 동티모르의 국제법상 권리에 근거한 것이다. 결론적으로 현행 국제법상 평시 사이버 간첩활동은 정부 기능의 수행에 대하여 위법한 간섭을 구성하지 않는바, 영토주권을 침해하는 것으로 보기 어려울 것이다.

2. 사이버 간첩활동과 국내문제 불간섭원칙

TM 2.0은 목표국에 특정한 정책 결정을 강요하는 것과 관련된 행위를 간섭금지원칙의 맥락에서 다룬다. TM 2.0은 사이버 작전을 수행하여 전자투표를 원격으로 변경함으로써 선거결과를 변조하는 것, 비-사이버 수단으로 인터넷 서비스제공자의 책임 관련 특정 국내법을 채택하거나 사이버 군축 또는 온라인 인권 관련 다자협약의 당사국이 되지 않도록 강요하는 것을 사이버 수단 및 비-사이버 수단을 통한 타국의 대내적 또는 대외적 문제의 간섭으로 제시한다.[100]

국내문제 불간섭원칙은 관습국제법의 지위를 가지며, 국제법상 확립된 원칙이다.[101] 국제법상 금지되는 간섭이 되기 위하여 간섭의 대상 및 간섭의 방법에 관한 요건이 충족되어야 한다.[102] 국내문제 불간섭원칙을 위반하기 위하여 간섭의 대상은 피간섭국에 본질적으로 유보된 영역, 즉 국제법에 따라 규율되지 아니하는, 피간섭국이 자유롭고 배타적으로 결정할 수 있는 국내사항에 관련된 것이어야 한다. 니카라과 사건에서 ICJ는 각 국가가 주권에 따라 자유롭게 결정할 수 있는 사안, 즉 정치, 경제, 사회, 문화 시스템의 선택 및 외교정책의 입안과 관련된 사안의 선택에 대하여 강제적인 방법을 사용할 때 위법한 간섭이 된다는 점을 판시한 바 있다.[103]

국가는 외교정책의 입안 및 국내 정책 목적을 결정하면서 공개할 정보

100) Schmitt & Vihul, *supra* note 1, p. 313, para. 2.
101) *Nicaragua*, *supra* note 24, para. 202.
102) M. Jamnejad & M. Wood, "The Principle of Non-Intervention," *Leiden Journal of International Law,* vol. 22, no. 2 (2009), pp. 345-347.
103) *Nicaragua*, *supra* note 24, para. 205.

와 공개를 원하지 않는 정보를 결정하는 주권적 권한을 갖는다. 정부 공무원 간의 통신은 국가의 본질적 국내사항에 속하는 대표적인 사례이다.[104] 국제법의 일반원칙에 따라 국가가 소유하거나 국가가 비상업적 목적으로 배타적으로 사용하는 물체는 국가 주권의 필수적 부분을 구성하며, 이는 국가의 배타적 관할권에 속하는 것으로 이해된다.[105]

이러한 맥락에서 사이버 기반시설에 저장되거나 이를 통해 전송되는 정보가 국가 주권에 관한 내용을 담고 있는 것이라면, 이러한 정보에 대한 사이버 간첩활동을 통한 간섭은 표적국의 유보된 영역에 대한 간섭을 구성하며, 국내문제 불간섭원칙상 간섭의 대상 관련 요건이 충족된 것으로 볼 수 있다.[106] 그러나, 국제법상 위법한 간섭은 간섭의 대상 요건은 물론 간섭의 방법, 즉 간섭의 성격상 요건 또한 충족해야 한다.

강제는 단순한 개입(interference) 또는 비우호적 행위와 국내문제 불간섭원칙을 위반하는 간섭(intervention)을 구분하는 핵심 요소이다.[107] 강제는 금지되는 위법한 간섭의 본질을 구성하며, 피강제국에 대한 압력의 부과로 이해된다.[108] 피강제국이 강제국의 압력을 거부할 수 있다면, 피강제국의 주권은 침해된 것이 아니라는 점에서 강제를 구성하기 위한 특정한 규모의 압력이 필요하다.[109] 즉, 국가가 타국의 유보된 영역에 대한 자유로운 결정에 영향을 미치고 이에 따라 타국의 의사와 무관하게 특정한 행동을 강요한다면, 이는 국제법상 금지되는 위법한 간섭을 구성하는 강제가 존재하는 것으로 볼 수 있다.

강제국의 강제는 피강제국에 영향을 미치지 못하는 경우에도 금지되는 위법한 간섭의 요건을 충족하는데, 위법한 간섭의 판단에 있어서 중요한

104) A. Peters, "Privacy, Rechtsstaatlichkeit, and the Legal Limits on Extraterritorial Surveillance," in R. Miller (ed.), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (Cambridge Univ. Press, 2017), p. 164.
105) W. von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace," *International Legal Studies,* vol. 89 (2013), p. 130.
106) K. Irion, "Government Cloud Computing and National Data Sovereignty," *Policy and Internet,* vol. 4, no. 3-4 (2012), pp. 48-54.
107) Jamnejad & Wood, *supra* note 102, p. 381.
108) Kunig, *supra* note 46, MN 5.
109) Jamnejad & Wood, *supra* note 102, p. 348.

것은 강제 그 자체이기 때문이다. 강제가 의도하는 결과의 발생은 국내문제 불간섭원칙의 전제가 아닌바, 강제국의 강제가 현실화되지 않더라도 피강제국에 대한 강제국의 강제는 국젭법상 금지되는 위법한 간섭을 구성한다. TM 2.0 또한 강제적 사이버 작전이 목표하였던 결과를 도출하지 못하였다는 사실이 간섭금지원칙의 위반 여부에 어떠한 영향을 주지 못한다는 점을 명확히 하고 있다.[110] 간섭을 구성하는 사이버 작전의 표적국이 이러한 사이버 작전을 인지해야 하는지에 대하여 TM 2.0 작성에 참여한 전문가들의 의견이 나뉘었다. 다수는 인지 여부는 간섭금지원칙 위반의 전제 조건이 아니라는 입장을 취하였지만, 소수는 표적국이 강제적 요소를 알지 못하였는바, 이는 간섭이 아니라는 견해를 취하였다.[111]

일부 학자들은 사이버 간첩활동이 목표국에 대한 강제가 될 수 있다고 주장하는데, 국가는 정보를 비밀로 유지할 권리를 갖는다는 점을 근거로 한다. 즉, 사이버 간첩활동으로 목표국의 비밀정보가 복사되는 경우, 목표국의 자율적 의사결정능력이 훼손되는데 왜냐하면 정보의 비밀성이 제거되었기 때문이다. Terry는 정보의 비밀성 훼손에서 위법한 간섭의 강제요건이 충족된다고 주장한다. 독일에 대한 미국 국가안보국(NSA)의 사이버 간첩활동에 대하여 Terry는 미국의 사이버 간첩활동으로 독일의 국내정책 및 외교정책의 목표가 공개되었는바, 이는 독일에 국내 정책 및 외교정책을 공개할 것을 강요한 것과 같은 것이며 독일은 이에 따라 정부의 비밀스러운 결정을 공유하지 않으려는 주권적 결정을 행사할 기회를 박탈당한 것이라고 설명한다.[112]

그러나, 사이버 간첩활동에 따른 표적국 비밀정보의 비밀성 제거를 표적국에 대한 강제로 직접 연결하는 것은 무리가 있어 보인다. 사이버 간첩활동의 본질은 비밀스러운 정보의 수집이며, 이러한 정보수집을 활용하여 표적국을 강제하는 금지된 간섭을 하는 것은 다른 차원의 문제이다.

110) Schmitt & Vihul, *supra* note 1, p. 322, para. 29.
111) *Id.*, p. 321, para. 25.
112) P. Terry, ""Absolute Friends": United State Espionage Against Germany and Public International Law," *Revue québécoise de droit international,* vol. 28, no. 2 (2015), p. 197.

즉, 국제법상 금지된 위법한 간섭의 요건인 강제 관련 요건이 사이버 간첩활동 그 자체로 충족된다고 보기 어렵다.[113] TM 2.0 또한 사이버 간첩활동 그 자체는 강제적 요소를 결여하는바, 간섭을 구성하지 않는다고 규정한다.[114]

사이버 작전의 맥락에서 일부 학자들은 타국의 정책 변경을 강요하는 국가의 명령적 행위로서 강제를 이해하는 것은 간섭금지원칙의 임계점을 넘기 어려운바[115], 임계점을 낮출 필요성을 주장한다. 이러한 학자들의 주장에서 주목할 쟁점은 간섭금지원칙의 임계점에 도달하는 것이 어려운바, 포괄적인 성격을 갖는 주권원칙을 적용 기준으로 설정하자는 점이다.[116] 이는 결국 사이버 간첩활동이 금지되는 간섭의 요건인 강제를 충족하기 어렵다는 점을 반증하는 것이다. 결론적으로 사이버 간첩활동은 국제법상 국내문제 불간섭원칙의 요건 중 간섭의 대상과 관련될 수 있겠지만 강제를 요하는 간섭의 방법을 충족하기 어려운바, 국내문제 불간섭원칙을 위반하는 것으로 보기 어려울 것이다.

3. 사이버 간첩활동과 무력사용 금지원칙

사이버 간첩활동이 UN헌장 제2조 4항에 규정된 금지된 무력위협 또는 무력사용에 해당하기 위해서는 적어도 사이버 간첩활동이 사람의 사망 또는 부상, 재산의 손상 또는 파괴를 유발하고, 국가의 중요한 기반시설에 대하여 대규모 및 중-장기 붕괴 사태를 초래해야 한다.[117] 사이버 간

113) K. Ziolkowski, “Peacetime Cyber Espionage - New Tendencies in Public International Law,” in Ziolkowski, *supra* note 44, p. 433.

114) Schmitt & Vihul, *supra* note 1, p. 323, para. 33.

115) I. Kilovaty, “The Elephant in the Room: Coercion,” *AJIL Unbound,* vol. 113 (4 March 2019) (https://www.cambridge.org/core/journals/american-journal-of-international-law/article/elephant-in-the-room-coercion/341847EAE494AB617E5B5899D8400C63, 2021.1.13).

116) M. Schmitt & L. Vihul, “Sovereignty in Cyberspace: Lex Lata Vel Non?,” *AJIL Unbound,* vol. 111 (22 August 2017) (https://www.cambridge.org/core/journals/american-journal-of-international-law/article/sovereignty-in-cyberspace-lex-lata-vel-non/6C6FD06E2B02B72224DF7127483A33F0, 2021.1.13).

첩활동이 금지된 무력위협 또는 무력사용에 해당하는지는 "효과-기반 접근 해석"(effects-based interpretation)에 따라 평가되어야 하는데, 효과-기반 해석은 국제법상 효과-기반 접근(effect-based approach)을 따른 것이다.[118] 효과-기반 접근에 따를 때, 사이버 작전이 재래식, 생물무기 또는 화학무기의 사용으로 야기되는 효과와 비견되는 효과를 야기할 경우, UN헌장 제2조 4항에 규정된 무력사용이나 제51조에 규정된 무력공격에 해당할 수 있다.

사이버 간첩활동이 초래하는 국가안보에 대한 손해가 일반 무기 시스템이 초래하는 물리적 파괴보다 더욱 심각하다는 견해가 있다.[119] 또한, 사이버공간에서 행해지는 정보수집의 막대한 규모와 속도를 감안할 때, 이러한 정보수집은 예전에는 오직 군사점령에 의해서만 가능했다는 점을 지적하며, 사이버공간에서 행해지는 정보수집을 매우 심각한 상황으로 평가하는 견해도 제시되고 있다. 이러한 입장은 사이버 간첩활동이 기존의 군사력에 의해서만 가능했던 심각한 피해를 초래한다는 점에서 효과-기반 접근의 요건을 충족하는 것으로 본다.[120]

그러나, 이러한 주장은 수용하기 어려운데, 본질적으로 사이버 간첩활동은 표적국의 허가 없이 정보를 수집하는 것이기 때문이다. 즉, 사이버 간첩활동은 정보의 무단 복사에 불과하며, 이는 재래식 또는 대량파괴무기가 초래하는 효과와 단정적으로 비교될 수 없으며, 더욱이 이러한 효과와 직접적인 인과관계를 형성하지 않는다. 이러한 점에서 사이버 간첩활동 자체를 무력사용 또는 무력공격으로 간주하는 것은 바람직하지 않다.

일부 학자들은 특정한 사이버 작전이 무력사용 또는 무력공격에 해당할 수 있는지에 대하여 목표-지향 접근(target-oriented approach)을 제안한다. 이들은 비밀정보와 같이 국가의 필수적 이해에 관련된 정보가 탈취

117) Ziolkowski, *supra* note 113, p. 451.
118) A. Randelzhofer & O. Dörr, "Article 2(4)," in B. Simma (ed.), *The Charter of the United Nations, 3rd ed.,* Vol. 1 (Oxford Univ. Press, 2012), p. 22.
119) T. Huntley, "Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare," *Naval Law Review,* vol. 60 (2010), p. 39
120) Melnitzky, *supra* note 30, p. 566.

되는 경우, 사이버 간첩활동은 무력사용으로 간주되어야 한다고 주장한다.[121] 나아가 군사적 성격을 갖는 모든 유형의 정보에 대한 사이버 간첩활동은 정보의 비밀성 여부와 무관하게 무력공격으로 간주될 수 있다고 주장한다.[122]

전체적으로, 무력공격 및 무력사용에 대한 목표-지향 접근은 수용될 수 없다. 이러한 접근을 따르는 경우, 국제적 무력충돌의 발생을 결정하는 임계점이 상당히 낮아지는 결과가 초래되며, 국제평화와 안전에 대한 평가가 주관적 결정에 좌우되는 결과가 유발되기 때문이다. 무엇보다도 이러한 주장은 현실적으로도 수용되기 어려운데, 왜냐하면 어떠한 국가도 사이버 간첩활동을 국제법상 금지되는 무력사용으로 간주하지 않기 때문이다.[123] 표적국 정보의 무단 복사에 불과한 사이버 간첩활동은 사실상 운동성 손해(kinetic damage)를 초래하지 않는다는 점에서 국가실행 또한 사이버 간첩활동을 UN헌장 제2조 4항과 연계시키지 않는다.[124]

사이버 간첩활동이 국방에 중요한 민감한 컴퓨터 시스템을 겨냥하는 경우, 즉 적대적 의도가 표출된다면 사이버 간첩활동을 무력공격으로 간주해야 한다는 주장도 제기된다.[125] 이러한 주장이 설득력을 갖기 위해서는 즉, 적대적 의사의 명백한 표출이 확인되어야 한다. 그러나, 이는 사이버 간첩활동의 본질적 성격상 불가능한 것인데, 사이버 간첩활동은 전통적 간첩활동과 마찬가지로 은밀하게 수행되는 비밀성을 본질적 성격으로 하기 때문이다. 설령 사이버 간첩활동이 발각되더라도 이의 배후 또는 의

121) C. Joyner & C. Lotrionte, “Information Warfare as International Coercion: Elements of a Legal Framework,” *European Journal of International Law,* vol 12, no. 5 (2001), pp. 846, 855.

122) *Id.*

123) D. Fidler, “Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies,” *ASIL Insights, vol. 17, iss. 10* (20 March 2013) (https://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving, 2021.1.12)

124) R. Buchan, “Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?,” *Journal of Conflict and Security Law,* vol. 17, no. 2 (2012), p. 211.

125) W. Sharp, Cyberspace and the Use of Force (Aegis Research Corporation, 1999), p. 130.

도가 정확히 파악되기 어렵다는 점에서 적대적 의사 표시에 근거한 이러한 주장은 용납되기 어렵다.

사이버 간첩활동이 유발할 수 있는 물리적 손해에 초점을 맞추는 견해도 제시되고 있다. 사이버 간첩활동은 컴퓨터 시스템 또는 네트워크에 침투하고, 백도어 프로그램을 설치함으로써 물리적 손해를 유발할 수 있다는 점을 지적한다. 즉, 사이버 첩보활동과 물리적 손해를 초래하려는 의도를 분리할 수 없다는 주장이다.[126] 또한, 컴퓨터 시스템에 악성 프로그램을 설치하는 것은 목표국의 주권적 영토에 정보수집을 위하여 군사적 정보수집 플랫폼을 설치하는 것과 동일하며, 이러한 플랫폼은 재래식 공격을 개시할 가능성이 있는바 자위권 행사를 유발할 수 있다고 주장한다.[127]

사이버 간첩활동을 무력사용으로 직접 연계시키는 위와 같은 주장은 국제법상 뒷받침되기 어렵다. 무엇보다도 적법하게 자위권이 행사되기 위해서는 충족해야 할 요건이 있기 때문이다. 물리적 손해를 야기할 수 있는 사이버 첩보활동을 감지한 경우, 목표국은 발견된 악성 프로그램의 정확한 의도를 파악하고, 의도된 예상 손해를 분석해야 하며, 무엇보다도 UN헌장 제51조에 규정된 무력공격에 해당하는 구체적인 효과를 확인해야 한다.[128] 상기한 주장은 어디까지나 사이버 간첩활동이 유발할 수 있는 예상적 상황에 따른 판단이라는 점에서 이는 단순한 사이버 간첩활동에 자위권을 행사함으로써 전면적인 무력충돌상황을 초래할 수 있는 위험성을 내포한다. 결론적으로 사이버 간첩활동은 재래식 무기 및 대량파괴무기가 유발하는 손해의 규모와 심각성을 유발하는 제한된 상황에서만 효과-기반 접근에 따라 UN헌장 제2조 4항에서 금지하는 무력사용 및 제51조에서 규정하는 무력공격에 해당할 것이다.

126) A. Wortham, "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?," *Federal Communications Law Journal,* vol. 64, no. 3 (2012), pp. 643, 647, 652.

127) Melnitzky, *supra* note 30, p. 565.

128) Huntley, *supra* note 119, p. 36.

V. 결 론

사이버 간첩활동은 목표국의 허락없이 목표국의 사이버 기반시설에 저장되거나 사이버 기반시설을 통해 전송되는 정보를 은밀히 복사하는 활동이다. 성질상 사이버 간첩활동은 흔적을 남기지 않는 정보의 은밀한 복사에 지나지 않는바, 사이버 간첩활동의 잠재적 위험성은 크지 않은 것으로 생각할 수 있다. 그러나, 사이버 간첩활동은 국제평화와 안전에 심각한 위협이고, 이는 생각하는 것보다 훨씬 위험한 것이다.[129]

기존 국제법과 TM 2.0은 사이버 간첩활동에 대하여 모호한 입장을 제시하고 있다. 즉, 평시 사이버 간첩활동은 그 자체로는 국제법상 위법하지 않지만, 사이버 간첩활동이 수행되는 방법에 따라 위법할 수 있다는 이중적 입장을 취하고 있다. 사실상, 사이버 간첩활동에 대한 이러한 입장은 사이버 간첩활동을 적극적으로 행하는 국가실행이 반영된 것으로 볼 수 있다. 상기에서 언급한 바와 같이 사이버 간첩활동은 이를 규제하고자 하는 인식과 이를 행하는 실행이 정반대의 방향으로 진행된다는 점에서 사이버 간첩활동 관련 국제법 체제가 어떻게 형성될 것인가에 대한 흥미를 유발한다.

상기에서 언급한 바와 같이 사이버 간첩활동은 영토주권, 국내문제 불간섭원칙 및 무력사용 금지원칙을 위반할 가능성이 있지만, 이러한 가능성이 사이버 간첩활동에 대한 일반적 평가가 될 수 없음은 명확하다. 사이버 간첩활동에 대하여 비록 TM 2.0 또는 학자들이 정의를 내리고 있지만, 현재까지 국가실행을 반영하는 법적 구속력을 가진 국제법규범은 존재하지 않는다. 이러한 맥락에서, 사이버 간첩활동에 대한 국제법적 평가는 현 상태를 반영하는 수준에 머무를 가능성이 크다.

사이버 간첩활동이 야기하는 심각성과 이를 규율하기 위하여 관련 국제법 원칙을 적용하는 것은 별개의 차원에서 파악하는 것이 필요하다. 심각한 결과를 초래하는 사이버 간첩활동에 적용할 수 있는 구체적인 국제

129) D. Fidler, "Tinker, Tailor, Soldier, Duqu: Why cyberespionage is more dangerous than you think," *International Journal of Critical Infrastructure Protection,* vol. 5, no. 1 (2015), p. 29.

법원칙이 부재하는 상황에서 영토주권, 국내문제 불간섭원칙 및 무력사용 금지원칙을 적용하고자 하는 현실적 필요성을 무시할 수는 없다. 그러나, 메타이론에 해당하는 이러한 원칙의 적용은 사이버 간첩활동 자체에 대한 국제법 체제의 형성을 사실상 방해하는 것으로 생각된다.

사이버 간첩활동 그 자체가 국제법상 위법한 것으로 간주되지 않는 이상, 사이버 간첩활동에 대한 규율의 성패는 현실적으로 국가의 사이버 역량에 좌우될 것이다. 이러한 맥락에서 국내문제 불간섭원칙에서 제시되는 국가에 유보된 영역이라는 개념에 대한 역발상이 필요하다. 즉, 사이버 간첩활동으로 간섭을 받지 않을 영역으로 국가에 유보된 영역을 이해할 것이 아니라, 국제법이 국가에 배타적으로 맡긴 영역으로 이해해야 할 것이다. 사이버 간첩활동에 자체에 대한 국제법 체제가 형성되지 않은 상태에서 국가는 스스로 자신의 사이버 기반시설의 보호에 관한 역량을 강화해야 할 것이다.

【참고문헌】

[단행본]

M. Schmitt & L. Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations/Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge Univ. Press, 2016).

Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, 3rd ed. (Cambridge Univ. Press, 2016).

[논문]

C. Baker, "Tolerance of International Espionage: A Functional Approach," *American University International Law Review,* vol. 19, no. 5 (2003).

R. Buchan, "Cyber Attacks: Unlawful Use of Force or Prohibited Interventions?," *Journal of Conflict and Security Law,* vol. 17, no. 2 (2012).

_____, "The International Legal Regulation of State-Sponsored Cyber Espionage," in A.-M. Osula & H. Rõigas (eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives* (NATO CCD COE Publication, 2016).

S. Chesterman, "The Spy Who Came in From the Cold War: Intelligence and International Law," *Michigan Journal of International Law,* vol. 27, no. 4 (2006).

D. Fleck, "Individual and State Responsibility for Intelligence Gathering," *Michigan Journal of International Law,* vol. 28, no. 3 (2007).

C. Forcese, "Spies Without Borders: International Law and Intelligence Collection," *Journal of National Security Law and Policy,* vol. 5 (2011).

W. von Heinegg, “Territorial Sovereignty and Neutrality in Cyberspace,” *International Legal Studies,* vol. 89 (2013).

M. Jamnejad & M. Wood, “The Principle of Non-Intervention,” *Leiden Journal of International Law,* vol. 22, no. 2 (2009).

A. Melnitzky, “Defending America against Chinese Cyber Espionage Through the Use of Active Defenses,” *Cardozo Journal of International and Comparative Law,* vol. 20 (2012).

A. Radsan, “The Unresolved Equation of Espionage and International Law,” *Michigan Journal of International Law,* vol. 28, no. 3 (2007).

G. Sulmasy & J. Yoo, “Counterintuitive: Intelligence Operations and International Law,” *Michigan Journal of International Law,* vol. 28, no. 3 (2007).

P. Terry, ““Absolute Friends”: United State Espionage Against Germany and Public International Law,” *Revue québécois de droit international,* vol. 28, no. 2 (2015).

Q. Wright, “Espionage and the Doctrine of Non-Intervention in Internal Affairs,” in R. Stanger (ed.), *Essays on Espionage and International Law* (Ohio State Univ. Press, 1962).

K. Ziolkowski, “Peacetime Cyber Espionage - New Tendencies in Public International Law,” in K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO CCD COE Publication, 2013).

【국문초록】

국제법상 사이버 간첩활동에 관한 일고찰

정보화의 심화에 따라 사이버공간의 활용에 관한 국제사회의 의존은 더욱 증가하고 있다. 사이버공간을 활용한 정보의 저장 및 전송은 그 크기와 속도의 측면에서 국제사회에 많은 혜택을 주고 있다. 그러나, 이러한 혜택과 함께 사이버공간은 심각한 위협 또한 국제사회에 제기하고 있다. 사이버공간과 관련하여 제기되는 심각한 위협 중 하나로 사이버 간첩활동은 국제사회의 관심의 대상이 되고 있다.

전시 간첩활동과 달리 평시 간첩활동에 대한 국제사회의 입장은 매우 복잡한 양상을 보여준다. 실제로 평시 간첩활동이 국가에 의해서 광범위하게 행해지고 있다는 점을 감안할 때, 국가가 평시 간첩활동을 금지 또는 불법화하는 국제법규범의 형성에 적극적인 자세를 보일 것으로 예상하기는 어렵다. 전통적인 평시 간첩활동에 비해 은밀성과 속도 측면에서 더욱 정교하고 교묘하게 수행되는 평시 사이버 간첩활동의 유용성을 감안할 때, 국가들의 평시 사이버 간첩활동의 수행은 오히려 더욱 증가할 것으로 예상된다.

사이버 간첩활동은 그 자체로 국제법상 위법한 활동이 아니며, 다만 사이버 간첩활동이 수행되는 방법에 따라 국제법상 위법성이 결정된다. 따라서, 영토주권, 국내문제 불간섭원칙 및 무력사용 금지원칙 측면에서 사이버 간첩활동에 대한 국제법적 규율이 시도되고 있다. 현시점에서 사이버 간첩활동은 심각한 물리적 손해를 야기하는 경우, 영토주권을 침해할 수 있다. 국가가 배타적 및 독립적으로 관할권을 행사하는 대상에 대한 강제를 수반한 간섭이 사이버 간첩활동과 관련되는 경우, 국내문제 불간섭원칙이 위반될 수 있다. 아울러, 사이버 간첩활동이 재래식 무기 또는 대량파괴무기가 초래하는 정도의 심각한 결과를 초래한다면, 무력사용 금지원칙 또한 위반될 수 있다.

그러나 이러한 평가는 사이버 간첩활동 자체에 대한 직접적인 국제법적

접근이 아니라는 점에서 문제를 노정하며, 사이버 간첩활동 자체와 관련된 사실관계의 구체적 평가 없이 국제법의 기본 원칙을 적용하는 것은 의도치 않은 심각한 결과를 초래할 수 있다. 실정법(lex lata)의 측면에서 사이버 간첩활동은 사실상 국제법의 회색지대에 있는 것으로 이해하는 것이 정확한 이해이다. 사이버 간첩활동 자체를 대상으로 하는 구체적인 국제법 체제가 형성되지 않는 한, 사이버 간첩활동에 대한 국제법적 논의는 실효성을 갖기 어려울 것으로 예상된다.

【주제어】
간섭금지, 무력사용금지, 사이버 간첩활동, 영토주권, 평시 간첩활동

【ABSTRACT】

A Review on the Cyber Espionage under International Law

Sung Won Kim
Associate Professor, School of Law, Wonkwang Univ.

The international community's dependence on the use of cybespace is ever increasing with the advent of the information revolution. Cyber capabilities concerning the storage and transmission of data and information have given many benefits to the international community in terms of its volume and rapidity. However, the international community also faces threats related to cyber exploitation. Among serious threats posed in cyberspace, cyber espionage has been regarded as the urgent issue which should be tackled with the international community.

Unlike wartime espionage, attitudes of the international community towards peacetime espionage seem to be ambivalent. Given that peacetime espionage is carried out widely by States, it is hard to expect that States will try to outlaw peacetime espionage. Considering the strategic usefulness of peacetime cyber espionage, which are more sophisticated in terms of clandestineness and rapidity compared to traditional peacetime espionage, the possibility of outlawing cyber espionage would not be easily made.

Cyber espionage is not illegal *per se* under international law. The illegality of cyber espionage is determined by the method by which it is carried out. In this context, the attempt to outlaw cyber espionage is under progress in terms of territorial sovereignty, prohibition of intervention and prohibition of the use of force. In case that cyber espionage would cause severe damages, cyber espionage would violate international legal principles such as territorial sovereignty, prohibition

of intervention and the use of force under the effect-based approach.

However, this approach poses a problem because these principles are not designed to deal with cyber espionage *per se*. Without exploring substantial issues concerning cyber espionage, the imprudent application of international legal principles such as territorial sovereignty, prohibition of intervention and the use of force to cyber espionage would exacerbate problems which cyber espionage would give rise to. In light of lex lata, cyber espionage is actually understood to be in the gray area of international law. Unless the specific international legal regime for cyber espionage is established, the debate on cyber espionage under international law will turn out to be in vain.

【Keywords】

Prohibition of Intervention, Prohibition of the Use of Force, Cyber Espionage, Territorial Sovereignty, Peacetime Espionage