▣ 논 단

커넥티드 차량의 사이버-물리 위협과 GATT 제XXI조(b)(iii) 안보예외의 적용 한계

- 미국 상무부의 2025년 커넥티드 차량 최종규칙에 대한 '국제관계상 긴급상황' 요건의 적용을 중심으로 -

고려대학교 대학원 법학과 박사과정(국제통상법 전공) 박 자 혜*

*논문접수 : 2026. 7. 13. *심사개시 : 2026. 7. 22. *게재확정 : 2026. 8. 8.

〈목 차〉

* 저자: 현대차그룹 전략기획담당 글로벌정책기획팀장, 고려대학교 법학과 박사과정생.

Ⅰ. 서론

1. 문제의 제기

오늘날 자동차 산업은 고도화된 소프트웨어, 통신 모듈 및 센서 기반 데이터 처리가 결합된 커넥티드 차량(connected vehicle) 중심으로 재편되고 있다. 이러한 기술적 전환은 운행 안전성과 사용자 편의성을 향상시켰으나, 동시에 차량연결시스템(vehicle connectivity system, 이하 “VCS”), 자율주행시스템(automated driving system, 이하 “ADS”), 무선 업데이트 및 텔레매틱스 데이터 흐름을 통하여 외부 침투, 원격 접근·조작, 민감정보 탈취 등 새로운 유형의 사이버-물리적(cyber-physical) 안보 위험을 구조적으로 수반한다.

이와 같은 위험 인식 아래, 미국 상무부 산업안보국(Bureau of Industry and Security, 이하 “BIS”)은 2025년 1월 16일 「Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles」 최종규칙을 공포하였다.[1] 동 규칙은 2025년 3월 17일 발효하였고, 중국 또는 러시아가 소유·통제하거나 그 관할 또는 지시를 받는 주체가 설계·개발·제조·공급한 VCS 하드웨어 및 대상 소프트웨어(covered software)를 탑재한 특정 커넥티드 차량 관련 거래를 금지·제한하는 구조를 취한다. 금지의 적용은 대상 소프트웨어에 관하여는 모델연도(Model Year) 2027부터, VCS 하드웨어에 관하여는 모델연도 2030부터 단계적으로 개시된다.[2]

BIS 최종규칙 발효 이후에도 미국 내에서는 Connected Vehicle Security Act of 2026, Motor Vehicle Modernization Act of 2026 및 2027 회계연도 국방수권법안 등을 통하여 커넥티드 차량 공급망을 국가안보 규제의 대상으로 다루려는 후속 입법 움직임이 계속되고 있다.[3] 다만 본 논문의 분석 대상은 이러한 입법 동향의 정책적 타당성이 아니라, BIS 최종

E-mail: nuniknaii@hanmail.net.
본고의 내용은 필자의 개인적인 견해이며, 현대차그룹의 공식적인 입장과는 무관함을 밝힙니다.

1) Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 90 Fed. Reg. 5360, 2025.1.16. (15 C.F.R. pt. 791; 이하 “BIS 최종규칙”).

2) BIS 최종규칙, 90 Fed. Reg. 5360, 5379, 5415-5417, 5420; 15 C.F.R. §§ 791.301-791.304, 791.308 참조. 규제 대상 주체에 관한 작동 문언은 “owned by, controlled by, or subject to the jurisdiction or direction of”이며, 규칙 전문(preamble)은 이를 “sufficient nexus”로 축약하여 표현한다(90 Fed. Reg. 5397, 5411).

3) Connected Vehicle Security Act of 2026, S. 4429, 119th Cong. (2026.4.29. 상원 발의; 2026.7.22. 상원 상무·과학·교통위원회 수정대안 가결); Connected Vehicle Security Act of 2026, H.R. 8730, 119th Cong.

규칙이 국제통상법상 안보예외 법리와 형성하는 긴장 관계이다.

BIS 최종규칙은 국가안보 목적을 전면에 내세우고 있으나, 특정 국가와 연계된 차량 소프트웨어·하드웨어의 수입·판매 및 관련 거래 자체를 금지하거나 제한하는 방식을 취한다는 점에서 GATT 제XI조의 수량제한금지 원칙과의 저촉이 문제된다.[4] 미국으로서는 GATT 제XXI조(b)(iii)의 안보예외, 즉 "국제관계에 있어서의 그 밖의 긴급상황(emergency in international relations)"의 원용이 예상된다. 특히 미국은 종래 GATT 제XXI조의 원용이 WTO 패널의 실질심사 대상이 되지 아니한다는 자기판단(self-judging) 입장을 견지하여 왔다는 점에서, 해당 조항의 원용 방식 자체도 별도의 쟁점이 된다.[5]

그러나 WTO 패널은 *Russia – Traffic in Transit* 사건에서 GATT 제XXI조(b)(iii)의 적용 여부가 전적으로 회원국의 자기 판단에 맡겨져 있지 않다고 보면서, "국제관계에 있어서의 긴급상황"을 무력충돌, 잠재적 무력충돌, 고조된 긴장 또는 위기, 국가를 둘러싼 일반적 불안정 상황 등으로 해석하였다.[6] 다만 이러한 해석은 주로 전통적인 군사·외교적 사태를 통하여 긴급상황을 식별하여 온 것으로서, 커넥티드 차량과 같이 디지털 네트워크에 내재하여 장기간 잠재·누적되는 구조적 취약성을 어떠한 객관적 기준으로 평가할 것인지는 여전히 불명확하다.

WTO 안보예외와 디지털 통상의 교차 영역에 관한 기존 연구는 통신 인프라 보안, 사이버 스파이 행위, 안보예외의 자기판단성 및 고위험 IoT 상품에 대한 수입규제를 중심으로 전개되어 왔다. 2021년 이후의 연구는 GATT 제XXI조(a)의 정보제공 거부, 안보예외의 입증 구조, US-Steel 패널보고서의 중대성 기준 및 상소기구 기능 정지가 규칙 기반 통상체제에 미치는 영향을 검토한다.[7] 그러나 이러한 연구도 BIS 최종규칙의 두 수입금지를 제

(2026.5.11. 하원 발의); Motor Vehicle Modernization Act of 2026, H.R. 7389, 119th Cong. § 301 (2026.5.21. 하원 에너지·상무위원회 수정안 가결·보고 명령); National Defense Authorization Act for Fiscal Year 2027, S. 4784, 119th Cong. § 353 (2026.6.15. 상원 군사위원회 보고) 참조.

4) GATT 1994 art. XI:1 참조. 분석 범위를 GATT 제XI조 및 제XXI조로 한정하는 이유는 제Ⅱ장 제2절에서 밝힌다.

5) GATT 1994 art. XXI(b)(iii); United States, Third-Party Oral Statement, *Russia – Measures Concerning Traffic in Transit,* WT/DS512, 2018.1.25., paras. 1, 5, 10-12, 18, 33, 35-36 참조.

6) Panel Report, *Russia – Measures Concerning Traffic in Transit,* WT/DS512/R and Add.1, adopted 26 April 2019 (이하 "Russia 패널보고서"), paras. 7.70-7.77, 7.82, 7.100-7.104 참조.

7) 김경우, "안보예외에서의 정보제공 거부 조항(GATT XXI(a))의 기원과 진화에 대하여", 『국제경제법연구』 제23권 제1호 (2025), 25-35면; Mona Pinchis-Paulsen, Kamal Saggi & Petros C. Mavroidis, "The National

1·제2·제3요건에 따라 각각 분석하거나, 지속적·구조적 취약상태와 국제관계상 긴급상황을 구별하면서 이를 심사에 반영할 누적적 기준을 제시하지는 않는다. 본고는 이 적용상 공백을 분석 대상으로 삼는다. 현행 WTO 패널 해석 기준에 따를 때, 사이버-물리 위협은 '국제관계상 긴급상황'으로 포섭되기 어렵다. 본 논문은 이 한계를 출발점으로 삼아, 외부에서 확인 가능한 중대한 사실관계가 충분하지 않은 디지털 인프라 환경에서 장기간 잠재·누적되는 기술적 취약상태를 향후 규범 형성론상 어떠한 보충적 표지에 따라 평가할 수 있는지를 검토한다.

본고는 위험 자체를 '사건형'과 '상태형'으로 분류하지 않는다. 다만 관련 패널보고서가 국제관계상 긴급상황의 존재를 확인할 때 의존한, 외부에서 확인할 수 있는 사실적 표지와 공급망 안에서 장기간 존속하는 기술적 취약상태를 분석상 구별한다. 관련 보고서들은 긴급상황을 단일한 사건으로 한정하지 않고 잠재적 무력충돌, 고조된 긴장이나 위기, 일반적 불안정과 같은 계속적 상황도 포함하였다.[8] 따라서 본고가 다루는 간극은 사건과 상태의 형식적 이분법이 아니라, 국가 간 관계의 중대한 악화를 외부에서 확인할 표지가 충분하지 않은 기술적 취약상태를 현행 기준에 따라 어떻게 평가할 것인가에 있다.

이를 위하여 본 연구는 커넥티드 차량 규제와 같이 구체적 사이버 공격이나 무력충돌이 현실화되기 이전 단계의 상시적·누적적 취약성에 대응하는 국가조치가 GATT 제XXI조의 해석상 정당화될 수 있는지를 규명한다. 구체적으로는 BIS 최종규칙이 필수적 안보이익의 충분한 특정성, 국제관계상 긴급상황의 존재, 그리고 조치와 안보이익 사이의 선의 및 최소한의 개연성[9]이라는 요건을 충족하는지를 순차적으로 분석한다. 나아가 이를 통해 기

Security Exception at the WTO: Should It Just Be a Matter of When Members Can Avail of It? What About How?", 23(3) *World Trade Review* 271, pp. 285-294 (2024); Klint W. Alexander, "The 2022 U.S. Steel/Aluminum Tariff Ruling: A Legal Reckoning for the United States and the WTO over the National Security Exception in International Law", 72(4) *American University Law Review* 1137, pp. 1168-1172 (2023); Stephen S. Kho, Yujin K. McNamara, Sarah B. W. Kirwin & Brooke Davies, "The Conundrum of the Essential Security Exception: Can the WTO Resolve the GATT Article XXI Crisis and Save the Dispute Settlement Mechanism?", 40(1) *American University International Law Review* 127, pp. 127-133, 187-195 (2024) 참조.

8) *Russia* 패널보고서, paras. 7.75-7.76; Panel Report, *United States – Certain Measures on Steel and Aluminium Products (China),* WT/DS544/R, circulated 9 December 2022, appeal notified 26 January 2023, not adopted (이하 "*US-Steel* 패널보고서"), paras. 7.138-7.149 참조.

9) *Russia* 패널보고서, paras. 7.53-7.58, 7.70-7.77, 7.100-7.104, 7.130-7.139 참조. 본 논문에서 말하는 "최소한의 개연성"은 GATT 제XX조식 필요성 심사 또는 대체수단 심사의 이식을 의미하는 것이 아니라, GATT 제XXI조(b)의 문언상 회원국에게 인정되는 판단재량이 선의(good faith) 원칙에 의해 제한되며, 조치가 제

존 GATT 제XXI조 해석론이 주로 '발생·존속을 객관적으로 식별할 수 있는 국제관계상 긴급상황'을 중심으로 형성되어 있어 '지속적·구조적 취약상태'를 평가하는 데 한계가 있음을 밝히고, 이를 보완하기 위하여 '상시적 취약성(Persistent Vulnerability)' 개념을 제안한다. 그 정의와 네 요소는 제Ⅳ장 제2절에서 제시한다. 본고는 이하에서 현행법 해석(*de lege lata*)과 향후 규범 형성론(*de lege ferenda*)을 구분한다. GATT 제XI조 제1항의 문언과 관련 WTO 보고서의 해석을 현재 공개된 사실관계에 적용하면, BIS 최종규칙의 두 수입금지는 제XI조 제1항을 위반할 가능성이 크며 제XXI조(b)(iii)에 따른 정당화도 성립하기 어렵다. 이는 현행법상 결론이다.

상시적 취약성은 위 결론을 뒤집기 위한 확장해석이 아니다. 지속적·구조적 취약상태는 현행 조문 아래에서 이미 존재하는 국제관계상 긴급상황을 뒷받침하는 사실 자료가 될 수 있을 뿐, 그 자체만으로 독립된 긴급상황을 구성한다고 보기 어렵다. 이러한 취약상태를 독립된 식별 근거로 인정하려면 협정 개정이나 WTO 설립협정 제IX조 제2항에 따른 권위 있는 해석 등 회원국의 제도적 합의를 거쳐야 한다.[10] 본고의 네 요소는 그 논의를 위한 향후 규범 형성론상의 제안이다.

2. 연구의 범위 및 방법

본 연구의 분석 대상은 2025년 공포된 미국 BIS 최종규칙과 GATT 제XI조 및 제XXI조이다. 우선 해당 조치가 GATT 제XI조상 수입금지 또는 수량제한 조치로 평가될 수 있는지를 검토한 후, GATT 제XXI조(b)(iii)에 따른 안보예외에 의하여 정당화될 수 있는지를 분석한다.

본고가 GATT 제XXI조(b)(iii)에 집중하는 이유는 BIS 최종규칙이 원격 접근·조작과 민감정보 탈취를 포함한 공급망 위험을 근거로 장래 적용되는 두 수입금지를 도입하였기 때문이다. (b)(ii)는 무기·탄약·전쟁도구의 거래 및 군사시설에 공급하기 위한 목적으로 직접 또는 간접적으로 이루어지는 그 밖의 상품·재료의 거래에 관한 조치를 대상으로 한다. 일

시된 필수적 안보이익의 보호수단으로서 최소한의 개연성(minimum requirement of plausibility)을 갖추어야 한다는 의미로 사용한다.

10) Vienna Convention on the Law of Treaties, 23 May 1969, 1155 U.N.T.S. 331 (이하 "VCLT"), art. 31; Marrakesh Agreement Establishing the World Trade Organization, art. IX:2 참조.

부 VCS·ADS 구성요소가 군사·민간 양쪽에 사용될 수 있더라도, 일반 상용 커넥티드 차량에 관한 두 수입금지 전체를 동목으로 정당화하기는 어렵다. 한편 (a)는 공개가 필수적 안보이익에 반한다고 회원국이 판단하는 정보의 제공을 거부할 수 있게 할 뿐, 수입금지 자체를 정당화하는 조항은 아니다. 따라서 이들 조항의 적용 가능성은 각주에서 한정적으로 언급하고, 본문은 두 수입금지가 '전쟁 또는 국제관계상 긴급상황 시에 취하여진' 조치인지에 관한 (b)(iii)의 해석과 적용에 집중한다.[11] 다만 커넥티드 차량 규제가 제품의 기술적 요건 또는 적합성 평가 절차와 관련될 수 있다는 점에서 TBT 협정의 적용 가능성을 완전히 배제하지는 않되, TBT 협정 및 GATS 제XIVbis조에 대한 본격적 분석은 후속 연구 과제로 남긴다.

방법론적으로 본 연구는 조약법에 관한 비엔나협약(이하 "VCLT") 제31조에 따라 해당 조문의 문언, 문맥 및 대상과 목적을 분석한다.[12] 특히 본 연구는 VCLT 제31조 제3항(c)가 예정하는 체계적 통합(systemic integration)의 문제의식을 고려하되, UN 정부전문가그룹(GGE) 보고서·개방형 실무그룹(OEWG) 최종보고서와 ISO/SAE 21434 등 사이버 안보 관련 자료는 직접 구속규범이 아니므로 그 법적 성격을 구분하여, GGE·OEWG 문서는 VCLT 제31조 제3항(c)의 관련 국제법 규칙이 아니라 사이버 공간에 대한 국제법 적용과 책임 있는 국가행동에 관한 국가들의 규범적 인식을 보여 주는 자료로, ISO/SAE 21434는 차량 사이버 위험의 기술적 구조를 확인하는 사실 자료로 각각 한정하여 원용한다.[13]

한편 안보예외의 해석 확대는 국가의 자의적 남용 가능성을 수반한다. 이에 본 연구는 국제법상 상당한 주의(due diligence) 원칙을 검토하되, 이를 제XXI조의 해석규칙이나 독립된 정당화 근거가 아니라, 현실화 이전의 인식 가능한 위험 상태에 규범적 의미가 부여될 수 있음을 보여 주는 제한적인 구조적 유비 자료로만 한정한다. 국제사법재판소는 *Corfu*

11) GATT 1994 arts. XXI(a), XXI(b)(ii); 김경우, 앞의 주 7, 25-35면; Joel P. Trachtman, "The Internet of Things Cybersecurity Challenge to Trade and Investment: Trust and Verify?", SSRN Working Paper No. 3374542, pp. 25-27 (18 April 2019), https://ssrn.com/abstract=3374542 참조.

12) VCLT arts. 31(1)-31(2) 참조.

13) VCLT art. 31(3)(c); Joost Pauwelyn, *Conflict of Norms in Public International Law: How WTO Law Relates to Other Rules of International Law,* Cambridge University Press, 2003, pp. 244-270; Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc. A/76/135, 2021.7.14., paras. 15, 69-72; Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021-2025, Final Report, UN Doc. A/80/257, 2025.7.24., annex, paras. 32-34, 39-41; ISO/SAE 21434:2021, *Road Vehicles — Cybersecurity Engineering,* cl. 8 참조.

Channel 사건에서 국가가 자국 영역이 타국의 권리에 반하는 행위에 사용되는 것을 알고도 허용하여서는 아니 된다는 일반적 의무를 확인한 바 있다.[14]

상소기구의 기능 정지는 WTO 협정상 실체적 의무를 정지시키지 않으며, 회원국은 협의와 패널절차를 계속 이용할 수 있다.[15] 따라서 WTO 합치성 검토는 보고서의 최종 채택 가능성만을 예측하기 위한 것이 아니라, 한국 정부와 기업이 규제 설계·통상협의·분쟁해결절차 선택에 활용할 법적 기준을 제시한다.

3. 논문의 구성

본 논문은 서론과 결론을 포함하여 총 5개의 장으로 구성된다. 제Ⅱ장에서는 BIS 최종규칙의 입법 배경, 규제 구조 및 통상법적 성격을 규명한다. 제Ⅲ장에서는 GATT 제XXI조(b)(iii)의 기존 해석론과 긴급상황 개념의 역사적 맥락을 검토한다. 제Ⅳ장에서는 BIS 최종규칙의 GATT 제XXI조(b)(iii) 합치성을 요건별로 분석하고, 현행 해석론의 한계를 바탕으로 상시적 취약성 개념을 구체화한다. 마지막으로 제Ⅴ장에서는 연구 결과를 종합하고 디지털 인프라 시대의 안보예외 해석에 관한 규범적 제언을 제시한다.

Ⅱ. 미국 BIS 커넥티드 차량 최종규칙의 내용과 통상법적 성격

1. BIS 최종규칙의 입법 배경과 규제 구조

가. 규제 연혁

BIS 최종규칙은 정보통신기술·서비스(ICTS) 공급망 안보를 위한 일련의 규제 체계의 연장선에서 성립하였다. 그 수권의 출발점은 2019년 5월의 행정명령 제13873호이다. 동 명령은 국제비상경제권한법(IEEPA)에 근거하여 국가비상사태를 선포하고, 외국 적대세력(foreign adversary)의 소유·통제·관할·지시하에 있는 자가 관여한 ICTS 거래가 국가안보 또는 미국인의 안전 등에 과도한 위험을 초래하는 경우 이를 금지·제한할 권한을 상무장

14) *Corfu Channel (United Kingdom v. Albania),* Judgment, I.C.J. Reports 1949, p. 4, at p. 22 참조.

15) Understanding on Rules and Procedures Governing the Settlement of Disputes, arts. 3.2, 16.4, 17 and 19.2; Kho et al., supra note 7, pp. 127-133, 187-195 참조.

관에게 위임하였다.[16]

이러한 위임에 기초하여 2021년 1월 ICTS 거래 일반에 관한 심사 규정이 제정되었고,[17] 그 틀 위에서 BIS는 커넥티드 차량에 특화된 규범을 단계적으로 형성하였다. 즉 2024년 3월 1일 사전규칙제정예고(ANPRM)를 통하여 규제의 필요성과 범위에 관한 의견을 수렴하고, 같은 해 9월 26일 규칙제정예고(NPRM)를 거쳐, 2025년 1월 16일 최종규칙을 공포하였으며, 동 규칙은 2025년 3월 17일 발효하였다.[18] 특히 ANPRM 단계에서는 ADS를 포함한 여섯 개 차량 시스템이 잠재적 규제 대상으로 검토되었으나, 전 시스템에 대한 규제는 과도하게 광범위하다는 공중 의견과 BIS의 자체 분석을 반영하여 최종규칙은 규제 대상을 VCS와 ADS 중심으로 축소하였다. 약 1년에 걸쳐 의견 수렴과 수정을 거듭한 이 행정절차와 그에 따른 규제 범위의 축소는, 동 조치가 통상 이익의 은폐적 보호가 아니라 특정된 안보 위험에 대응하기 위하여 설계되었다는 선의 판단에 유리한 자료가 된다.

나. 규제 대상의 정의와 적용 범위

최종규칙의 물적 적용 범위는 세 개의 정의로 획정된다. 첫째, VCS는 450MHz를 초과하는 주파수 대역에서 차량의 차외 통신을 직접 가능하게 하는 하드웨어·소프트웨어 품목을 말한다.[19] 둘째, ADS는 완성 커넥티드 차량에서 동적 운전작업 전체를 수행할 수 있는 하드웨어·소프트웨어의 총체로 정의되며, 이는 SAE J3016 분류상 레벨 3 내지 5의 자동화 수준에 대체로 상응한다.[20] 셋째, 대상 소프트웨어는 차량 수준에서 VCS 또는 ADS의 기

16) Exec. Order No. 13873, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689 (2019.5.17.), § 1(a). 동 명령은 IEEPA(50 U.S.C. § 1701 이하)에 근거하여 발령되었으며, § 1(a)(ii)는 금지 대상 거래가 미국 내 ICTS의 설계·완전성·제조·운영 등에 사보타주 또는 전복의 과도한 위험을 초래하거나, 핵심 기반시설 또는 디지털 경제의 안보·복원력에 파국적 효과를 미칠 과도한 위험을 초래하거나, 그 밖에 국가안보 또는 미국인의 안전에 수인할 수 없는 위험을 초래하는 경우를 규정한다.

17) Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909 (2021.1.19.). 동 규정은 행정명령 제13873호의 일반적 이행 규범으로서 ICTS 거래의 심사 절차와 기준을 정하였고, 현행 15 C.F.R. pt. 791에 편제되어 있다.

18) Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 89 Fed. Reg. 15066 (2024.3.1.) (ANPRM); 89 Fed. Reg. 79088 (2024.9.26.) (NPRM); BIS 최종규칙, 90 Fed. Reg. 5360 (발효일 2025.3.17.은 5360면 DATES 항목). ANPRM 단계의 여섯 개 검토 대상 시스템의 열거와 VCS·ADS 중심으로의 축소 경위는 90 Fed. Reg. 5362 참조.

19) 15 C.F.R. § 791.301 (“Vehicle Connectivity System (VCS)”), 90 Fed. Reg. 5415. 자동차 센싱(LiDAR·레이더·영상·초광대역) 전용의 송수신·변환·처리만을 가능하게 하는 품목 등은 정의에서 제외된다.

능을 직접 가능하게 하는, 외국의 이해관계가 존재하는 소프트웨어 기반 구성요소(응용·미들웨어·시스템 소프트웨어)를 말한다. 다만 펌웨어는 대상 소프트웨어의 정의에서 제외된다. 오픈소스 소프트웨어도 원칙적으로 제외되지만, 독점적 목적으로 수정되고 그 수정본이 재배포 또는 공유되지 않은 경우에는 제외되지 않는다. 2026년 3월 17일은 최종규칙의 발효일인 2025년 3월 17일과 구별되는, 이른바 레거시(legacy) 소프트웨어 제외의 기준일이다. 그 기준일 전에 설계·개발·제조·공급된 소프트웨어 하위 구성요소라도, 이후 중국·러시아 관련 주체가 이를 유지·보강하거나 그 밖의 방식으로 변경하면 해당 제외를 적용받지 못한다.[21]

인적 적용 범위는 서론에서 확인한 작동 문언에 따라 획정된다. 즉 규제는 중국(홍콩 및 마카오 특별행정구 포함) 또는 러시아가 소유·통제하거나 그 관할 또는 지시를 받는 주체가 설계·개발·제조·공급한 VCS 하드웨어와 대상 소프트웨어에 미친다.[22] 이러한 물적·인적 획정이 전제하는 기술 구조에 주목할 필요가 있다. 커넥티드 차량은 V2X 통신, 무선(OTA) 업데이트 및 텔레매틱스를 통하여 외부 네트워크와 상시적 데이터 흐름으로 결합되어 있으며, 규제 대상인 VCS와 ADS는 바로 이 결합의 통로이자 차량 제어의 중핵이다.

다. 규제 메커니즘과 단계적 시행 일정

규제 메커니즘은 세 유형의 금지로 구성된다. 제791.302조는 VCS 하드웨어 수입자가 위 주체 요건에 해당하는 자가 설계·개발·제조·공급한 VCS 하드웨어를 고의로 수입하는 행위를, 제791.303조는 커넥티드 차량 제조자가 위 주체 요건에 해당하는 자가 설계·개발·제조·공급한 대상 소프트웨어를 탑재한 완성 커넥티드 차량을 고의로 미국에 수입하거나 미

20) 15 C.F.R. § 791.301 (“Automated Driving System (ADS)”), 90 Fed. Reg. 5415; SAE International, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles,* SAE J3016_202104 (2014.1. 최초 제정, 2021.4. 개정), pp. 31-32 (§§ 5.4-5.6: 레벨 3 내지 5). BIS는 최종규칙 전문에서 동 표준(pp. 31-32)을 인용하면서도(90 Fed. Reg. 5364-5365), 규정상 ADS 정의에 특정 판본의 J3016을 명시적으로 편입하는 것은 거부하고, 레벨 3·4·5에 관한 동 표준의 세부 내용이 적용 범위 판단에 유용한 지침(useful guidance)이 된다고 밝혔다. 90 Fed. Reg. 5373. 본문의 “대체로 상응한다”는 서술은 이러한 전문상의 설명에 따른 것이다.

21) 15 C.F.R. § 791.301 (“Covered software”), 90 Fed. Reg. 5415. 제외 요건의 상세는 앞의 주 2 및 해당 본문 참조.

22) 15 C.F.R. § 791.301 (“Person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary” 및 “PRC”), 90 Fed. Reg. 5415. 작동 문언 전반은 앞의 주 2 참조.

국 내에서 판매하는 행위를 각 금지한다. 이와 달리 제791.304조는 위 주체 요건에 해당하는 커넥티드 차량 제조자 자신을 수범자로 하여, 그러한 제조자가 그 하드웨어·소프트웨어의 공급 주체를 불문하고 VCS 하드웨어 또는 대상 소프트웨어를 탑재한 완성 커넥티드 차량을 미국 내에서 고의로 판매하는 행위와 ADS 탑재 차량을 이용한 상업적 서비스를 제공하는 행위를 금지한다.[23] 금지의 경직성은 이행·통제 장치로 보완된다. 규제 대상 사업자는 적합성선언(Declaration of Conformity)을 통하여 규제 준수를 증명하여야 하고, 일반허가(general authorization)와 BIS의 심사·승인을 거치는 특정허가(specific authorization) 및 면제 제도가 금지의 경직성을 완화하는 안전판으로 기능한다.[24]

시행 시기는 단계적으로 설계되어 있다. 규칙 자체는 2025년 3월 17일 발효하였으나, 대상 소프트웨어 관련 금지와 적합성선언 의무는 모델연도 2027부터, VCS 하드웨어 관련 금지는 모델연도 2030부터(모델연도와 결부되지 아니하는 부품은 2029년 1월 1일부터) 적용되며, 2026년 3월 17일은 대상 소프트웨어의 'legacy software' 해당 여부를 가르는 기준일로 기능한다. 이와 같은 유예 구조는 제소국의 입장에서 위협의 절박성을 다투는 논거가 될 수 있는바, 그 통상법적 평가는 제Ⅳ장 제3절에서 다룬다.

끝으로 최종규칙이 스스로 밝힌 위협 인식을 정리한다. 규칙 전문은 중국 또는 러시아 관련 주체가 VCS 하드웨어와 대상 소프트웨어에 대한 접근 제공을 강제당할 수 있고, 그 결과 커넥티드 차량이 수집한 민감정보의 탈취("exfiltration of sensitive data")와 차량에 대한 원격 접근·조작("remote access and manipulation")이 가능하게 된다는 점을 적시하면서, 이를 긴급한 국가안보 위험("urgent national security risk")으로 성격 규정한다.[25] 정리하면 최종규칙은 중국·러시아 관련 주체에 대한 접근 제공 강제를 위험의 전제로 삼고, 그로부

23) 15 C.F.R. §§ 791.302 (금지되는 VCS 하드웨어 거래), 791.303 (금지되는 대상 소프트웨어 거래), 791.304 (관련 금지 거래), 90 Fed. Reg. 5416. 세 조문 모두 고의(knowingly)를 요건으로 하며, § 791.303은 (a)항에서 수입을, (b)항에서 미국 내 판매를 구분하여 규정하는 반면 § 791.304는 항의 구분이 없는 단일 조문이다.

24) 15 C.F.R. §§ 791.305 (적합성선언), 791.306 (일반허가), 791.307 (특정허가), 90 Fed. Reg. 5416-5418. 적합성선언은 대상 소프트웨어를 탑재한 완성 커넥티드 차량의 경우 각 모델연도별 최초 수입 또는 최초 판매의 최소 60일 전에, VCS 하드웨어의 경우 각 모델연도별(모델연도와 결부되지 아니하는 부품은 역년별) 최초 수입의 최소 60일 전에 제출되어야 하며(§ 791.305, 90 Fed. Reg. 5417), 공급망 실사(due diligence)의 수행에 관한 증명을 포함하여야 하고, 관련 기록은 IEEPA상 시효에 상응하는 10년간 보존되어야 한다.

25) BIS 최종규칙, 90 Fed. Reg. 5361 (위협 열거 및 "urgent national security risk" — 열거부 원문은 동사형: "(1) exfiltrate sensitive data … (2) allow remote access and manipulation …"), 5363-5371 (위험 분석) 참조. 접근 제공 강제와 두 위협의 결합 서술 및 "exfiltration of sensitive data" 명사구는 90 Fed. Reg. 5388. 시행일정 전반은 90 Fed. Reg. 5360, 5379, 5415-5417, 5420; 15 C.F.R. §§ 791.301-791.304, 791.308 참조.

터 민감정보 탈취와 차량에 대한 원격 접근·조작의 가능성을 도출하는 구조를 취한다.

<표 1> BIS 최종규칙상 금지·완화 구조

구분	근거 조문	대상 거래	적용 개시
대상 소프트웨어	15 C.F.R. § 791.303(a)·(b)	대상 소프트웨어 탑재 완성 커넥티드 차량의 수입(a)·미국 내 판매(b)	모델연도 2027
VCS 하드웨어	§ 791.302	VCS 하드웨어의 수입	모델연도 2030 (모델연도 비결부 부품은 2029.1.1.)
관련 금지 거래	§ 791.304	규제 대상 주체인 제조자의 완성차 판매 및 ADS 탑재 차량 상업적 서비스 제공	모델연도 2027(대상 소프트웨어 탑재) / 모델연도 2030(VCS 하드웨어 탑재)
완화 장치	§§ 791.305-791.307	적합성선언·일반허가·특정허가	–
예외	§ 791.308	수리·보증용 부품 등 단계적 면제	–

출처: 90 Fed. Reg. 5360, 5379, 5392, 5415-5420; 15 C.F.R. §§ 791.301-791.308을 바탕으로 필자 작성.

2. BIS 최종규칙의 통상법적 성격 규명

가. GATT 제XI조상 수입제한 조치로서의 성격

GATT 제XI조 제1항은 관세·조세 또는 그 밖의 과징금 이외의 금지 또는 제한을 그 시행 형식과 관계없이 규율한다.[26] 관련 보고서가 '그 밖의 조치'를 포괄적 범주로, '제한'을 수입에 제약적 조건이나 제한적 효과를 부과하는 조치로 해석해 온 점에 비추어 보면,[27] 제791.302조의 VCS 하드웨어 수입금지와 제791.303조(a)항의 대상 소프트웨어 탑재 완성 커넥티드 차량 수입금지는 각각 제XI조 제1항의 '금지'에 해당할 가능성이 크다.[28] 공급주체의 소유·통제·관할·지시 관계를 기준으로 한다는 사정은 수입 자체를 차단하는 법적 효과를 바꾸지 않는다. 일반허가와 특정허가는 금지를 예외적으로 해제하는 절차이지, 일정한 수입 수량을 배분하거나 통상적인 수입 조건을 설정하는 제도가 아니다. 또한 이 규칙은 관세·조세 또는 그 밖의 과징금이 아니므로, 그 통상법적 성격은 관세양허가 아니라

26) GATT 1994 art. XI:1 ('No prohibitions or restrictions other than duties, taxes or other charges, whether made effective through quotas, import or export licences or other measures, shall be instituted or maintained by any contracting party on the importation of any product of the territory of any other contracting party ⋯').

27) Appellate Body Reports, *China – Measures Related to the Exportation of Various Raw Materials,* WT/DS394/AB/R, WT/DS395/AB/R, WT/DS398/AB/R, adopted 22 February 2012, paras. 319-320; Appellate Body Reports, *Argentina – Measures Affecting the Importation of Goods,* WT/DS438/AB/R, WT/DS444/AB/R, WT/DS445/AB/R, adopted 26 January 2015, para. 5.217 참조.

28) 앞의 주 27 참조.

수량제한 금지의 문제로 귀착된다.[29]

제791.303조(b)항과 제791.304조에 따른 완성차 판매 금지는 미국 내 판매에 관한 국내 조치이므로, 수입상품이 동종 국내상품보다 불리하게 대우되는 범위에서 GATT 제III조 제4항의 쟁점을 제기할 수 있다.[30] 다만 동종성, 수입상품에 대한 불리한 대우 및 규제 대상 주체의 지배관계가 경쟁조건을 어떻게 변경하는지는 별도의 사실관계 심사가 필요하다. 제791.304조의 ADS 상업 서비스 제공 금지는 상품 판매와 구별하여 GATS 관련 각주에서 다룬다. 본고는 두 수입금지에 대한 제XXI조(b)(iii)의 적용에 초점을 두므로, 제III조 제4항의 위반 여부를 확정하는 것은 분석 범위에서 제외한다.

나. TBT 협정 적용 가능성 검토 및 분석 범위의 한정

TBT 협정과 GATT 제XI조는 각 협정의 요건에 따라 병존하여 적용될 수 있다.[31] TBT 협정상 기술규정은 상품의 특성 또는 그와 관련된 공정·생산방법을 규정하고 그 준수가 강제되는 문서이지만, BIS 규칙은 상품의 기술적 특성보다 공급 주체의 소유·통제·관할·지시 관계를 기준으로 거래를 금지하므로 기술규정 해당성에는 다툼의 여지가 있다. *EC-Seal Products* 상소기구보고서의 판단도 상품 외적 기준에 따른 시장접근 규율이 곧바로 기술규정에 해당하는 것은 아님을 보여 준다.[32] 기술규정에 해당한다면 제2.1조의 비차별의무, 제2.2조에 따라 국가안보상 요건이라는 정당한 목적을 달성하는 데 필요한 이상으로 무역제한적인지 여부 및 제2.4조의 국제표준 관련 의무를 각각 검토하여야 하며, GATT 제XXI조의 원용이 그 위반을 자동으로 정당화하지는 않는다. 제791.304조의 상업 서비스 제공 금지는 GATS의 쟁점을 제기할 수 있으나, 본고에서는 별도 본문을 두지 않고 각주로 한정한다.[33]

---

29) 앞의 주 26 및 해당 본문 참조.

30) GATT 1994 art. III:4. 수입 상품에 대하여 국경에서 집행되는 국내 조치의 성격 구분에 관하여는 GATT 1994 제III조에 관한 주해(Ad Article III) 참조. 제791.303조(b)항 및 제791.304조가 미국 내에서 생산된 커넥티드 차량에 적용되는 범위에 따라 제III조 제4항과 제XI조 제1항의 적용 영역이 달라질 수 있으나, 이 쟁점의 상세는 본 논문의 범위를 벗어난다.

31) TBT 협정 부속서 1 제1항; Appellate Body Report, *European Communities – Measures Affecting Asbestos and Asbestos-Containing Products,* WT/DS135/AB/R, adopted 5 April 2001, paras. 66-70 참조.

32) Appellate Body Reports, *European Communities – Measures Prohibiting the Importation and Marketing of Seal Products,* WT/DS400/AB/R, WT/DS401/AB/R, adopted 18 June 2014, paras. 5.45, 5.58-5.59 참조.

33) GATS arts. I:2(a), XIVbis:1(b)(iii) 참조. 제XIVbis조 제1항(b)호(iii)목은 GATT 제XXI조(b)(iii)와 동일한

Ⅲ. GATT 제XXI조(b)(iii)의 해석론

1. 관련 WTO 패널보고서의 법적 지위와 제XXI조(b)(iii)의 해석 구조

이하에서 검토하는 네 패널보고서는 동일한 법적 지위를 갖지 않는다. *Russia – Traffic in Transit* 패널보고서는 2019년 4월 26일 채택되었지만, 채택된 보고서도 후속 분쟁을 형식적으로 구속하는 선례는 아니다. *Saudi Arabia – IPRs* 패널보고서는 상소 중 분쟁이 종료되어 채택되지 않았고, *US-Origin Marking*과 *US-Steel* 패널보고서도 미국의 상소로 채택되지 않았다. 따라서 본고는 이들 보고서를 국내법상 판례와 같은 구속적 선례가 아니라, 조문의 문언·문맥에 관한 해석 자료와 향후 판단을 예측하기 위한 설득적 자료로 사용한다.[34)]

해석의 출발점은 제XXI조(b)의 'which it considers necessary'라는 문언이 원용국의 판단에 맡기는 범위를 확정하는 데 있다. 이 문언은 필수적 안보이익의 정의와 그 보호에 필요하다고 보는 조치의 선택에 상당한 판단 여지를 부여한다. 그러나 (i)목부터 (iii)목까지 열거된 상황의 존재까지 원용국의 일방적 판단에 맡기는지는 별개의 문제이다. GATT 제XXI조(b) 또는 이에 상응하는 TRIPS 협정 제73조(b)를 검토한 네 패널은 모두 각 세부목이 객관적 한계를 설정한다고 판단하였다.

다만 그 결론에 이르는 논증은 구분하여 서술하여야 한다. *Saudi Arabia* 패널은 *Russia* 패널의 긴급상황 정의와 선의·최소한의 개연성에 관한 분석을 직접 활용하였다. 반면 *US-Origin Marking*과 *US-Steel* 패널은 *Russia* 보고서에 구속된다는 전제 없이 VCLT에 따라 자기판단적 문언과 (iii)목을 독자적으로 해석하였다. 특히 *US-Steel* 패널은 긴급상황의 존재를 부정한 단계에서 심사를 마쳤으므로, 네 보고서가 모두 동일한 최소한의 개연성 심사를 적용하였다고 서술해서는 안 된다.[35)]

'taken in time of war or other emergency in international relations'라는 문언을 사용한다.

34) *Russia* 패널보고서; Panel Report, *Saudi Arabia – Measures concerning the Protection of Intellectual Property Rights,* WT/DS567/R, circulated 16 June 2020, not adopted; dispute terminated 21 April 2022 (이하 "*Saudi Arabia* 패널보고서"); Panel Report, *United States – Origin Marking Requirement (Hong Kong, China),* WT/DS597/R, circulated 21 December 2022, appeal notified 26 January 2023, not adopted (이하 "*US-Origin Marking* 패널보고서"); *US-Steel* 패널보고서 참조.

35) *Russia* 패널보고서, paras. 7.70-7.77, 7.100-7.104, 7.130-7.139; *Saudi Arabia* 패널보고서, paras. 7.244-7.246, 7.257-7.294; *US-Origin Marking* 패널보고서, paras. 7.259-7.264, 7.306-7.308; *US-Steel* 패널보고서, paras.

이에 따라 본고는 공통적으로 확인되는 객관적 상황 요건과 각 보고서의 독자적인 논증을 먼저 제시한 뒤, 필수적 안보이익의 특정, 국제관계상 긴급상황과 시간적 관련성, 선의와 최소한의 개연성을 분석상 구분한다. 이 구분은 패널들이 동일한 공식 심사 순서를 확립하였다는 뜻이 아니라, 서로 다른 보고서의 판단과 BIS 규칙에 대한 적용을 비교하기 위한 본고의 분석틀이다.

2. *Russia — Traffic in Transit* 관련 WTO 패널보고서의 심사 구조와 분석적 재구성

첫 번째 단계는 (iii)목이 정하는 상황의 존부와 조치의 시간적 관련성에 대한 객관적 심사이다.[36] 아울러 패널은 회원국 간의 정치적 또는 경제적 이견은 그것이 국방·군사적 이익 또는 법질서·공공질서 유지 이익을 발생시키지 아니하는 한 그 자체로 (iii)목의 긴급상황을 구성하지 못한다고 하였다. 패널은 2014년 이래 러시아와 우크라이나 사이에 존재한 사태가 국제관계상 긴급상황에 해당하는지를 판단하면서 두 가지 특징적 태도를 보였다. 첫째, 사태 발생의 원인이 어느 행위자에게 귀속되는지, 그 사태가 일반국제법상 어떻게 성격 규정되는지는 판단에 필요하지 아니하다고 보았다.[37] 긴급상황 심사를 책임 귀속의 문제로부터 절연함으로써 심사의 객관성을 확보하는 동시에, 패널이 정치적 쟁점의 판정자가 되는 부담을 회피한 것이다. 둘째, 패널은 사태의 중대성을 뒷받침하는 자료로 국제연합 총회 결의와 다수 국가의 대러시아 제재 부과 사실을 원용하였다.[38] 이때 패널은 총회 결의를 사태의 중대성을 확인하는 하나의 참고 요소로 활용하였을 뿐, 이를 긴급상황

7.127-7.149 참조.

36) *Russia* 패널보고서, paras. 7.75-7.76 및 7.111 참조. 패널은 국제관계상 긴급상황을 무력충돌, 잠재적 무력충돌, 고조된 긴장 또는 위기, 국가를 둘러싼 일반적 불안정 상황을 지칭하는 것으로 해석하고, 적용 단계에서 이 해석을 재확인하였다. 정치적 또는 경제적 이견에 관한 판단은 para. 7.75 참조.

37) *Russia* 패널보고서, para. 7.121 참조. 다만 이러한 태도는 다른 국제기구가 해당 사태의 위법성에 관하여 일반국제법적 판정을 내리기 이전의 상황에서만 타당성을 가지며, 위기를 자초한 국가의 원용은 자초한 위험을 정당화 사유로 원용할 수 없다는 법의 일반원칙과 긴장을 이룬다는 비판으로 정찬모, "WTO 안보예외 —「러시아-통과운송 제한 사건」 패널결정의 법리와 한국에의 함의",『국제법평론』 통권 제54호(2019), 39면 참조.

38) *Russia* 패널보고서, paras. 7.119-7.123 참조(러시아가 원용 사태를 특정한 다섯 요소 — 발생·계속 시기, 우크라이나 관련성, 국경 안보에 대한 영향, 대러시아 제재, 공지성 — 의 정리는 para. 7.119). 패널이 원용한 자료는 UN 총회 결의 제68/262호(2014.3.27.), 1949년 제네바협약을 명시적으로 언급함으로써 무력충돌 관련성을 확인한 UN 총회 결의 제71/205호(2016.12.19.) 및 2014년 이래 다수 국가가 동 사태와 관련하여 대러시아 제재를 부과한 사실이다.

인정의 필수 요건으로 명시하지는 않았다. 그럼에도 이 증거 구조는 1단계 심사가 국제적으로 가시화된 사건의 존재와 그에 대한 국제공동체 차원의 인식 자료에 의존하여 수행되었음을 보여 주며, 바로 이 지점에서 가시적 사건을 결여한 위협 유형에 대하여 동 심사가 어떻게 작동할 것인지의 문제가 예고된다. 시간적 관련성 심사는 각 조치의 도입 시점이 긴급상황의 계속 중이었음을 확인하는 것으로 충족되었다.[39]

두 번째 단계는 필수적 안보이익의 특정에 대한 심사이다. 패널은 필수적 안보이익을 일반적 안보이익보다 좁은 개념으로서 외부 위협으로부터의 영토와 국민의 보호 및 대내적 법질서·공공질서의 유지라는 국가의 본질적 기능에 관련된 이익으로 파악하고, 그 정의는 원칙적으로 각 회원국에 맡기되 원용국에게 그 진실성을 보일 수 있을 정도로 이익을 특정할 의무를 부과하였다.[40] 요구되는 특정성의 수준은 고정되어 있지 아니하다. 패널에 따르면 원용된 긴급상황이 무력충돌 또는 법질서·공공질서 붕괴라는 전형에서 멀어질수록 그로부터 발생하는 국방·군사적 이익 또는 법질서 유지 이익은 덜 자명해지므로, 원용국은 자국의 필수적 안보이익을 그만큼 더 구체적으로 특정하여야 한다.[41] 실제 적용에서 패널은 2014년 사태가 전쟁 또는 무력충돌이라는 전형적 상황에 매우 근접한 사태라는 이유로, 러시아의 암시적 서술만으로도 특정성 요건이 최소한으로 충족되었다고 보았다.[42] 이러한 적용에 대하여는 통상적인 입증책임의 분배에 비추어 원용국의 입증 부담을 사실상 완화한 것이라는 지적이 제기된다.[43] 여기서 추출되는 심사 기준은 다음과 같다. 필수적 안보이익의 특정성 요구 수준은 긴급상황의 성격과 분리되어 판단되지 아니하며, 전쟁·무력충돌 등 전형적으로 긴급상황에 해당한다고 이해되어 온 사태와 거리가 있는 위협을 원용할수록 원용국의 특정 부담은 가중된다.

세 번째 단계는 선의 및 최소한의 개연성 심사이다. 패널은 선의 의무가 필수적 안보이익의 정의뿐만 아니라 그 이익과 문제된 조치 사이의 관련성에도 미친다고 보고, 이를 조치가 제시된 안보이익의 보호수단으로서 최소한의 개연성을 갖출 것, 즉 그러한 보호수단

39) *Russia* 패널보고서, paras. 7.124-7.126 참조.

40) *Russia* 패널보고서, paras. 7.130-7.131, 7.134 참조.

41) *Russia* 패널보고서, para. 7.135 참조.

42) *Russia* 패널보고서, paras. 7.136-7.137 참조("Despite its allusiveness, Russia's articulation of its essential security interests is minimally satisfactory in these circumstances.").

43) 정찬모, 앞의 주 37, 39면 참조.

으로서의 개연성이 전적으로 결여되지 아니할 것이라는 요구로 구체화하였다.[44] 그 심사 방식은 조치가 긴급상황으로부터 너무 동떨어져 있거나 무관하여(so remote from, or unrelated to) 안보이익 보호조치로서의 개연성이 부정되는지를 검토하는 것이다.[45] 적용 단계에서 패널은 문제된 조치들이 국경의 안보에 영향을 미치는 2014년 긴급상황과 무관하다고 볼 수 없다고 판단한 뒤, 그렇다면 조치의 필요성 판단은 원용국의 몫으로 남으며 이것이 "which it considers"라는 문언에 법적 효과를 부여하는 논리적 귀결이라고 보았다.[46] 이 단계의 심사는 조치와 상황 사이의 명백한 단절만을 배제하는 소극적 심사에 그친다.

3. 국제관계상 긴급상황의 인정례·부정례 비교와 시사점

앞 절에서 확인한 심사 구조가 무력충돌 이외의 사태에 적용된 사례가 *Saudi Arabia - IPRs* 패널보고서이다. 2017년 6월 5일 사우디아라비아는 카타르가 테러리즘과 극단주의를 지원한다고 주장하면서 — 카타르는 이를 강하게 부인하였다 — 카타르와의 외교·영사 관계를 단절하고 경제 관계의 단절을 포함하는 포괄적 조치를 취하였다(이하 '2017년 단교 사태'). 카타르는 사우디아라비아의 지식재산권 보호에 관한 조치와 부작위가 TRIPS 협정에 위반된다고 제소하였고, 사우디아라비아는 GATT 제XXI조(b)(iii)와 동일한 문언을 가진 TRIPS 협정 제73조(b)(iii)를 원용하였다.[47] 따라서 동 보고서는 미채택 상태라는 한계에도 불구하고 제XXI조(b)(iii)의 긴급상황 요건을 해석하는 데 중요한 참고자료가 된다.[48]

패널은 *Russia* 패널의 긴급상황 정의를 채택한 뒤,[49] 2017년 단교 사태가 늦어도 2017년

44) *Russia* 패널보고서, paras. 7.132-7.133, 7.138 참조. 본 논문이 사용하는 '선의 및 최소한의 개연성'의 용어법에 관하여는 앞의 주 9 참조.

45) *Russia* 패널보고서, para. 7.139 참조.

46) *Russia* 패널보고서, paras. 7.144-7.146 참조.

47) *Saudi Arabia* 패널보고서, para. 7.258 참조(단교 조치와 그 공표 경위). 동 보고서의 미채택 경위와 그 전거에 관하여는 앞의 주 34 참조.

48) TRIPS 협정 제73조(b)(iii). 동 호는 GATT 제XXI조(b)(iii)와 동일한 문언을 두고 있으므로, 본 논문에서 양 조항의 해석은 상호 참조된다.

49) *Saudi Arabia* 패널보고서, paras. 7.244-7.246 참조. 패널은 (iii)목 상황의 객관적 심사 기준(para. 7.244)과 Russia 패널의 긴급상황 정의(para. 7.245)를 채택하였고, 양 당사국 모두 위 정의에 이의를 제기하지 아니하였음을 확인하였다(para. 7.246).

6월 5일부터 계속되는 긴급상황에 해당한다고 판단하였다. 패널은 개별 요소가 아니라 요소들의 결합이 이 결론을 지탱한다고 밝혔는데, 그 요소는 세 가지로 정리된다. 첫째, 외교·영사·경제 관계의 전면적 단절이라는 조치 자체가 둘 이상의 국가 간 관계의 예외적이고 중대한 위기로 성격 규정될 수 있다는 점이다. 둘째, 패널은 사우디아라비아가 제기한 주장의 진위에 관하여 어떠한 입장도 표명하지 아니하면서도, 그러한 주장의 성격 자체가 양국 관계의 악화와 파탄의 중대성을 보여 주는 추가 증거이며 원용국의 안보이익과 명시적으로 관련된다고 보았다. 셋째, 패널은 이 사태를 단순한 정치적 또는 경제적 이견으로 볼 수 없다고 하였다.[50] 이 판단은 (iii)목의 외연이 무력충돌 상황에 한정되지 아니함을 실제 인정례로서 보여 준다.[51] 다만 인정된 사태의 시간적 구조는 별도로 살펴볼 필요가 있다. 긴급상황의 기산점은 단교 선언이라는 특정 시점의 공식적 행위로 특정되었고, 그 존속 역시 공지의 사실로 확인되었다. 결국 무력충돌을 수반하지 아니한 사태에 대한 인정례이면서도, 그 인정은 특정 시점에 발생한 가시적이고 전면적인 관계 파탄 사건을 근거로 이루어진 것이다.

US-Origin Marking 패널은 홍콩을 둘러싼 사태와 미·중 관계의 악화를 독자적으로 검토하였으나, 그 사태가 국가 간 또는 국제관계 참여자 간 관계의 파탄이나 그에 준하는 수준에 이르렀다고 보지 않아 국제관계상 긴급상황의 존재를 부정하였다. *US-Steel* 패널도 경제·정치적 긴장만으로는 부족하다고 보고, 문제된 상황이 국제관계에 미치는 영향이 전쟁과 적어도 비견될 정도로 중대하거나 심각할 것을 요구하였다. 두 부정례는 무력충돌이나 단교가 없는 양자 긴장의 법적 중대성을 별도로 입증하여야 한다는 비교기준을 제공한다.

TRIPS 협정 제73조(b)의 도입문은 GATT 제XXI조(b)와 마찬가지로 회원국이 필수적 안

50) *Saudi Arabia* 패널보고서, paras. 7.257-7.264 참조. 요소들의 결합이 결론을 지탱하며 어느 하나가 단독으로 결정적인 것은 아니라는 판단과 인정의 결론은 para. 7.257, 단교의 사실관계와 공표는 para. 7.258, 전면적 단절의 '둘 이상의 국가 간 관계의 예외적이고 중대한 위기' 성격 규정은 paras. 7.259-7.262, 주장의 진위에 대한 판단 유보·주장의 성격의 증거 가치·'단순한 정치적 또는 경제적' 분쟁 반론의 배척은 para. 7.263 참조. 단교가 (iii)목의 상황과 도입문의 조치를 겸한다는 순환 논증 반론에 대하여는, 도입문 심사의 대상이 되는 조치가 단교 자체가 아니므로 판단이 필요하지 아니하다고 하였다. 같은 보고서, para. 7.264 참조. 시간적 관련성 판단은 paras. 7.269-7.270 참조.

51) 구모란, "WTO 안보예외 분쟁의 유형화와 대응전략에 관한 연구", 『통상법무정책』 2026년 제1호(통권 제11호), 95면(단교 조치를 '이례적인 상황으로서 국제관계에 있어서의 비상사태'에 해당한다고 인정한 판단의 정리) 및 97면(안보예외 항변이 인정된 전통안보 사례(DS512·DS567)와 긴급상황 요건이 부정된 경제안보 사례(DS544)의 대비) 참조.

보이익의 보호를 위하여 필요하다고 판단하는 조치를 규정한다. Saudi Arabia 패널은 국제관계상 긴급상황이 인정되었다는 이유만으로 문제된 모든 조치를 일괄적으로 정당화하지 않고, 각 조치가 제시된 안보이익과 지나치게 동떨어져 있거나 무관한지를 조치별로 검토하였다. 카타르 권리자가 사우디아라비아 변호인을 선임할 수 없게 된 사정에 대하여는, 그것이 단교에 수반하는 상호작용 차단 정책의 결과로서 원용된 안보이익 보호와의 개연성이 인정된다고 본 반면, 방송 해적행위 주체인 beoutQ에 대한 형사 절차와 제재의 미적용에 대하여는 그것이 위 차단 정책과 시간적으로도 논리적으로도 연결되지 아니하여 긴급상황으로부터 너무 동떨어져 있거나 무관하다는 이유로 최소한의 개연성을 부정하고 정당화를 배척하였다.[52] 이처럼 조치별로 달라진 결론은 두 가지를 시사한다. 하나는 긴급상황이 인정되더라도 선의 및 최소한의 개연성 심사가 조치 단위로 작동하여 실질적 통제 기능을 수행할 수 있다는 점이고, 다른 하나는 그 통제의 기준 역시 조치와 사태 사이의 관련성이라는 점이다. 전자는 BIS 최종규칙의 수입금지들을 조치 단위로 나누어 심사하여야 함을, 후자는 각 조치와 원용된 위협 사이의 관련성이 그 심사의 척도임을 뜻한다.

<표 2> '국제관계상 긴급상황' 관련 WTO 패널 판단 비교

사건 (채택 여부)	원용된 사태	긴급상황 판단	핵심 판단
Russia – Traffic in Transit, DS512 (2019.4.26. 채택)	2014년 이래 우크라이나 관련 사태	인정	paras. 7.75–7.76(정의), 7.119–7.123(적용)
Saudi Arabia – IPRs, DS567 (분쟁 종료로 미채택)	2017년 공표된 단교	인정	paras. 7.257–7.264, 7.269–7.270
US – Origin Marking, DS597 (상소로 미채택)	홍콩을 둘러싼 사태	부정 (중대성 기준 미충족)	paras. 7.306–7.308(정의), 7.353–7.358(적용)
US – Steel and Aluminium, DS544 (상소로 미채택)	글로벌 과잉설비를 둘러싼 긴장	부정 (전쟁에 비견될 중대성 불비)	paras. 7.138–7.139, 7.147–7.149

출처: 각 패널보고서를 바탕으로 필자 작성(세부 서지는 각주 6·49·52·81).

따라서 BIS 규칙의 사실관계를 인정례 또는 부정례와 단순히 동일시해서는 안 된다. 다만 공개된 규제 기록이 공급망 위험의 실재성을 보여 주더라도, 미·중 관계와 미·러 관계

52) *Saudi Arabia* 패널보고서, paras. 7.286-7.288(변호인 선임을 차단하는 결과를 낳은 조치들은 카타르 국민과의 모든 상호작용을 차단하는 포괄적 정책의 일환으로 볼 수 있어 최소한의 개연성을 충족한다는 판단), paras. 7.289-7.293(형사 절차·제재의 미적용은 위 정책과 시간적·논리적 관련이 없어 긴급상황으로부터 너무 동떨어져 있거나 무관하므로 개연성이 부정된다는 판단) 및 para. 7.294(결론: TRIPS 협정 제42조·제41조 제1항 비합치 부분은 제73조(b)(iii)의 원용 요건 충족, 제61조 비합치 부분은 불충족) 참조.

가 관련 시점에 각각 제XXI조(b)(iii)가 요구하는 국제관계상 중대성 기준을 충족하였다는 점은 별도로 입증하여야 한다. 이러한 점에서 BIS 규칙은 *US-Origin Marking*과 *US-Steel*이 제시한 중대성 판단과 비교하여 평가할 필요가 있다.[53]

4. GATT 제XXI조(b)(iii) '긴급상황' 개념의 역사적 맥락과 디지털 시대의 도전

앞의 세 절에서 확인한 사건 중심성은 제XXI조(b)(iii)의 문언 구조와 초기 운용 맥락 속에서 형성된 것으로 볼 수 있다. 제XXI조의 원형은 1947년 제네바 회의에서 ITO 헌장 초안의 상업정책 장에 속하여 있던 예외 조항을 헌장 전체에 적용되는 독립 조항으로 재배치하면서 성안되었다.[54] 그 기초 과정을 지배한 문제의식은 안보 필요와 남용 통제 사이의 균형이었다. 심의에 참여한 미국 대표가 정리한 바와 같이, 조항은 순수하게 안보상 필요한 조치를 금지할 수 없으므로 지나치게 좁게 설계될 수 없으나, 안보를 구실로 상업적 목적의 조치가 취하여질 만큼 넓게 설계되어서도 아니 된다는 요청 위에 서 있었다.[55] 이 균형의 조문상 해법이 각 목에 의한 재량의 한정이었고, (iii)목이 채택한 한정 방식은 조치가 전쟁 또는 긴급상황 '시에 취하여진' 것이어야 한다는 시간적 한정이었다. 그 문언이 주로 상정한 전형적 준거는 제2차 세계대전 직후의 전쟁과 그에 준하는 국제위기, 곧 시점을 특정할 수 있는 사건이었다. 따라서 (iii)목의 문언은 단순한 절차적 시점 요건이 아니라, 조치가 특정 가능한 국제위기와 시간적으로 결부되어야 한다는 구조를 내포한다.

GATT 시대의 원용례도 대체로 같은 경향을 보인다. 미국의 수출통제를 둘러싼 1949년 체코슬로바키아의 이의 제기 이래, 1961년 포르투갈령 문제, 1982년 포클랜드 분쟁 등 제

53) *Russia* 패널보고서, paras. 7.75-7.76, 7.111-7.126; *Saudi Arabia* 패널보고서, paras. 7.257-7.270; *US-Origin Marking* 패널보고서, paras. 7.306-7.308, 7.353-7.361; *US-Steel* 패널보고서, paras. 7.138-7.149; Alexander, *supra* note 7, pp. 1168-1172 참조.

54) 이하의 교섭사 검토는 VCLT 제32조상 보충적 해석수단으로서, 제1절부터 제3절까지 확인한 문언·문맥·관련 보고서상 해석을 보완하는 범위에서 원용한다. 성안 경위는 Mona Pinchis-Paulsen, "Trade Multilateralism and U.S. National Security: The Making of the GATT Security Exceptions", 41(1) *Michigan Journal of International Law* 109, pp. 110-116, 152-153 (2020) 참조(1947년 제네바 회의에서 상업정책 장의 예외 조항이 헌장 전체에 적용되는 독립 조항으로 재배치된 경위).

55) Roger P. Alford, "The Self-Judging WTO Security Exception", 2011 *Utah Law Review* 697, pp. 699-700; 이동은, "이중용도 물품 수출통제에 관한 국제통상법적 고찰 — GATT 제21조(b)(ii)의 해석 및 적용을 중심으로",『통상법률』2024년 제3호, 125면 참조. Alford는 UN Doc. E/PC/T/A/PV/33, 1947.7.24., p. 21의 미국 대표 Leddy 발언을 인용한다.

XXI조가 실제로 원용된 국면은 무력충돌 또는 그에 준하는 급성 위기와 관련되어 있었고,[56] *Russia* 패널 역시 (iii)목 원용 사례의 유의미한 다수가 무력충돌 내지 급성 국제 위기 상황이었음을 관행 조사를 통하여 확인한 바 있다.[57] 관련 패널보고서가 외연을 넓힌 지점 — 무력충돌(Russia)에서 전면적 단교(Saudi Arabia)로 — 역시 사건성 표지의 완화가 아니라 긴급상황으로 포섭될 수 있는 사건 유형의 확장이었음은 앞 절에서 확인한 바와 같다.

외교부 공식 번역본은 제XXI조(b)(iii)를 '전시 또는 국제관계에 있어서의 그밖의 비상시에 취하는 조치'라고 옮긴다. 'emergency'의 통상적 의미는 긴급한 주의를 요하는 중대하고 예기치 않은 상황을 가리키지만, 그 발생이 반드시 순간적일 것을 요구하지는 않는다. 'in international relations'는 문제된 상황이 국내의 기술적 위험이나 기업 간 분쟁에 머물지 않고 국가 간 또는 국제관계 참여자 간 관계의 차원에 존재하여야 한다는 한계를 부과한다. 또한 'taken in time of'는 조치와 그 상황 사이의 시간적 관련성을 요구하지만, 계속적 상황을 문언상 배제하지는 않는다.

그러나 'other emergency'의 'other'는 긴급상황이 전쟁과 병렬되는 범주임을 나타내므로 중대성 기준을 완화하는 근거가 될 수 없다. 비군사적·계속적 상황도 문언상 포함될 수 있지만, 그 상황이 국제관계에 미치는 영향은 US-Steel 패널보고서가 제시한 수준으로 중대하거나 심각하여야 하고 조치도 그 상황이 존속하는 동안 취하여져야 한다. 따라서 지속적·구조적 취약상태가 문언상 당연히 배제되는 것은 아니지만, 통상적인 기술적 위험이나 특정 국가에 대한 일반적 불신만으로는 (iii)목을 충족하지 못한다.[58] 본고의 향후 규범형성론상 제안은 이 기준을 완화하는 것이 아니라, 계속적 상황에서 그 충족 여부를 객관적으로 확인할 표지를 제시하는 데 한정된다.

---

56) J. Benton Heath, "The New National Security Challenge to the Economic Order", 129 *Yale Law Journal* 1020, p. 1053 (2020); Dapo Akande & Sope Williams, "International Adjudication on National Security Issues: What Role for the WTO?", 43 *Virginia Journal of International Law* 365, pp. 373-374, 400 (2003) 참조.

57) *Russia* 패널보고서, para. 7.81 참조. 다만 패널은 GATT 시대의 관련 기록에 관하여 제XXI조의 의미에 대한 공통의 이해가 부재하였다고 보아, 이를 VCLT 제31조 제3항(b)의 의미에서 해석상 합의를 형성하는 후속관행으로 취급하지 아니하였다. 같은 보고서, para. 7.80 참조. 본문이 확인하는 것도 해석상 합의가 아니라 원용 양태의 역사적 경향이다.

58) 대한민국 외교부, 「1947년도 관세 및 무역에 관한 일반협정」 공식 국문 번역본, 제21조(b)(iii); *US-Steel* 패널보고서, paras. 7.138-7.149 참조.

Ⅳ. BIS 최종규칙의 GATT 제XXI조(b)(iii) 합치성 분석

이하에서는 제Ⅲ장에서 추출한 심사 기준을 BIS 최종규칙에 적용한다. 분석은 제XXI조(b)(iii)의 조문 구조에 따라 필수적 안보이익의 특정성(제1절), 국제관계상 긴급상황(제2절), 선의 및 최소한의 개연성(제3절)의 순서로 진행하고, 제4절에서 예상 가능한 패널 판단을 종합한다.

1. '필수적 안보이익'의 충분한 특정성 분석

가. BIS 최종규칙상 위협 논거의 추출

BIS 최종규칙은 커넥티드 차량의 VCS 하드웨어와 대상 소프트웨어가 외국 적대세력과 연계될 경우 발생할 수 있는 사이버-물리 위험을 국가안보 위험으로 구성한다. 특정성 심사의 직접 대상은 위험 시나리오 그 자체가 아니라, 그 위험에 대응하여 보호하려는 필수적 안보이익이다. 다만 BIS 위험 분석부는 그 안보이익이 추상적 구호가 아니라 구체적 위험에 결부되어 있는지를 판단하는 자료가 된다.[59]

BIS가 제시한 위협 논거는 네 갈래로 정리할 수 있다. 제Ⅱ장에서 정리한 세 범주가 규제의 인과구조를 요약한 것이라면, 여기의 네 갈래는 이를 보호되는 안보이익의 특정성 관점에서 재분류한 것이다. 첫째는 민감정보 탈취 위험이다. 최종규칙은 커넥티드 차량이 운전자와 탑승자의 위치정보, 이동 패턴, 생체정보, 개인식별정보 및 건강정보를 수집할 수 있고, 이 정보가 외국 적대세력에 의해 탈취될 경우 핵심기반시설의 위치 파악, 정보활동, 협박 또는 감시 수단으로 사용될 수 있다고 본다.[60] 이 위험은 단순한 개인정보 보호의 문제가 아니라, 국가 기능과 핵심기반시설 보호, 방첩 및 법집행 기능과 연결될 때 필수적 안보이익의 특정성을 뒷받침할 수 있다.

둘째는 군사·치안 관련 정보의 수집 위험이다. BIS는 커넥티드 차량이 군사기지, 법집

59) BIS 최종규칙, 90 Fed. Reg. 5363-5371 참조. 위험 분석부는 VCS·ADS 취약성 분석(5363-5365), 중국·러시아 관련 위협 분석(5365-5369), 결과 분석(5370-5371)으로 구성된다. 위협 논거의 총괄 서술은 앞의 주 25 및 해당 본문 참조.

60) BIS 최종규칙, 90 Fed. Reg. 5370(기반시설의 위치·기능·운용 경향 정보의 도출과 공격 정밀성 제고) 및 5371(개인식별정보·건강정보의 수집과 협박 위험) 참조.

행기관, 응급대응기관 및 기타 민감 시설 주변에서 이동하면서 차량군의 규모, 구성, 이동 경로, 대응 시간 및 지리공간 정보를 수집할 수 있다고 본다. 또한 ADS 소프트웨어가 차량 센서와 내부 네트워크에 접근함으로써 주변 환경에 관한 정보를 수집할 수 있다는 점도 지적한다.[61] 이 논거는 군사·치안 기능의 보호라는 전통적 안보이익과 직접 연결되므로, 필수적 안보이익의 특정성 측면에서 가장 강한 부분이다.

셋째는 원격 접근 및 조작 위험이다. 최종규칙은 외국 적대세력이 차량 시스템에 접근할 경우 차량의 기능 정지, 오작동, 다수 차량의 동시 교란, 주요 교통축 차단 또는 충돌 유발이 가능하다고 본다. 또한 ADS가 차량 내부 네트워크에 직접 접근한다는 점에서, ADS 침해는 데이터 탈취뿐 아니라 차량 조작 위험으로 이어질 수 있다고 설명한다.[62] 이 위험은 물리적 피해 가능성을 수반한다는 점에서 가볍게 볼 수 없으나, 특정한 군사·치안 기능과 연결되지 아니할 경우 일반 교통안전 또는 공공안전 위험과 국가안보 위험의 경계가 흐려질 수 있다.

넷째는 공급망 백도어 및 강제 접근 위험이다. BIS는 중국 및 러시아 관련 법제와 정책 환경상 관련 기업이 정부의 접근 제공 요구를 거절하기 어렵고, 그 결과 VCS 하드웨어·펌웨어 또는 대상 소프트웨어에 백도어, 취약점 또는 악성 기능이 삽입될 수 있다고 본다.[63] 이 논거는 단독으로는 넓은 ICT 공급망 안보 일반론에 가까우므로 필수적 안보이익의 특정성을 충분히 뒷받침하기 어렵다. 그러나 앞서 본 민감정보 탈취, 군사·치안 관련 정보 수집 및 원격 조작이 가능해지는 인과적 통로로 기능한다는 점에서는 조치와 안보이익 사이의 관련성을 설명하는 보조 논거가 될 수 있다.

나. 패널 기준과의 대조 분석

결국 본 절의 쟁점은 BIS 최종규칙이 국가안보를 표방하였는지가 아니라, 그 주장이 어

61) BIS 최종규칙, 90 Fed. Reg. 5370-5371(군·법집행·긴급대응 차량 데이터로부터의 조직 규모·구성·능력과 대응 시간·절차 정보의 도출) 및 5365(ADS 소프트웨어 조작을 통한 특정 지리 영역 정보의 탐지·수집·보존) 참조.

62) BIS 최종규칙, 90 Fed. Reg. 5370(주행 중 차량의 무력화, 다수 차량의 동시 장애를 통한 주요 교통로의 차단과 충돌 유발) 참조. ADS 침해가 데이터 탈취를 넘어 차량 조작 위험으로 이어진다는 서술은 ADS의 차량 내부 네트워크(IVN) 직접 접근 구조를 전제로 한 것이다. 같은 규칙, 90 Fed. Reg. 5365 참조.

63) BIS 최종규칙, 90 Fed. Reg. 5364(공급망 단계에서 하드웨어·펌웨어 변조를 통한 백도어 삽입) 및 5366-5367(중국 국가안보 법제에 따른 협조 강제와 취약점 보고·비축 제도) 참조.

떠한 위험 유형에서는 국가의 본질적 기능 보호와 구체적으로 연결되고 어떠한 위험 유형에서는 공급망 안보 일반론에 머무는지를 구별하는 데 있다. *Russia* 패널의 기준에 따르면 필수적 안보이익은 회원국이 일차적으로 정의할 수 있으나, 그 정의는 선의 원칙에 의해 제한된다. 특히 원용된 상황이 전쟁 또는 무력충돌과 같은 전형적 상황에서 멀어질수록, 원용국은 보호하려는 필수적 안보이익을 보다 구체적으로 특정하여야 한다.[64] 커넥티드 차량의 사이버-물리 위험은 무력충돌이나 외교관계 단절처럼 특정 시점에 외부적으로 확인되는 사건이 아니라, 기술 인프라에 내재한 구조적 취약성을 전제로 한다. 따라서 미국이 제시하는 필수적 안보이익은 *Russia* 사건에서보다 더 높은 정도의 특정성을 요구받을 가능성이 크다.

이 기준에서 보면, BIS 최종규칙의 위협 논거 중 민감정보 탈취와 군사·치안 관련 정보 수집은 필수적 안보이익의 특정성 요건을 비교적 충족하기 쉽다. 위치정보, 이동 패턴, 핵심기반시설 주변의 운행 정보, 군·법집행·응급대응기관의 차량 운용 정보는 단순한 상업 정보나 일반 개인정보를 넘어 국가 기능, 방첩, 핵심기반시설 보호와 연결될 수 있다. *US – Origin Marking Requirement* 패널도 긴급상황이 반드시 국방 또는 군사적 이익과 관련되어야 한다고 보지는 않았다.[65] 따라서 데이터 보안, 방첩 및 핵심기반시설 보호가 전통적 군사 이익이 아니라는 이유만으로 필수적 안보이익에서 배제된다고 보기는 어렵다.

반면 원격 조작 및 대규모 사고 위험은 특정성 판단에서 다소 불안정하다. 차량 기능 정지나 다수 차량의 동시 교란은 현실화될 경우 중대한 물리적 피해를 초래할 수 있다. 그러나 BIS의 설명은 상당 부분 장래 위험을 전제로 하며, 구체적 공격 사례나 특정 국가 기능의 침해 양상을 직접 제시하기보다는 가능한 피해 시나리오를 제시하는 방식에 가깝다.[66] 따라서 이 논거는 필수적 안보이익의 특정성을 전적으로 결여한다고 볼 수는 없으나, 단독으로는 일반 공공안전 위험과 구별되는 국가안보 이익을 충분히 특정하였는지에 관하여 다툼의 여지가 남는다.

---

64) *Russia* 패널보고서, paras. 7.130-7.131, 7.134-7.135 참조. 특정성 요구 수준과 긴급상황의 성격 사이의 연동 구조는 앞의 주 41 및 해당 본문 참조.

65) *US-Origin Marking* 패널보고서, para. 7.301 참조. 동 보고서의 관련 해석에 관하여는 앞의 주 53 및 해당 본문 참조.

66) BIS 최종규칙, 90 Fed. Reg. 5363 참조("many of the risks laid out in the NPRM and final rule are forward-looking").

공급망 백도어 및 강제 접근 논거는 더욱 조심스럽게 취급되어야 한다. 외국 적대세력 관련 기업이 정부의 접근 요구에 노출될 수 있다는 주장은 ICT 공급망 안보 조치에서 반복적으로 제시되는 일반 논거이다. 이를 그대로 필수적 안보이익으로 승인하면, 특정 국가와 연계된 광범위한 기술 제품 전반이 안보예외의 대상으로 확장될 위험이 있다. 따라서 이 논거는 독립된 필수적 안보이익으로 보기보다는, VCS·ADS를 매개로 한 데이터 탈취 및 차량 조작 위험이 왜 특정 국가와의 인적·관할적 연계에서 문제 되는지를 설명하는 보조적 연결고리로 한정하는 편이 타당하다.

한편 특정성 판단과 별도로, BIS 최종규칙이 위장된 산업정책이라는 반론에 대하여는 선의 심사 차원의 재반론이 가능하다. *Russia* 패널은 필수적 안보이익의 정의와 조치의 관련성 모두가 선의 원칙의 제한을 받는다고 보았고, 조치가 제시된 안보이익의 보호수단으로서 최소한의 개연성을 갖추어야 한다고 보았다.[67] 국가안보 개념의 외연이 확장되는 오늘날의 환경에서도 원용국의 전적인 자기 판단이 허용되는 것은 아니므로, 관건은 원용국 판단의 존중과 남용 통제 사이의 균형이다.[68] 제Ⅱ장에서 확인한 바와 같이 BIS 최종규칙은 약 1년의 의견 수렴 절차를 거쳐 규제 대상을 여섯 개 차량 시스템에서 VCS와 ADS 중심으로 축소하였다.[69] 또한 단순한 상품 원산지 기준의 전면 수입금지가 아니라, 중국 또는 러시아와의 소유·통제·관할·지시 관계라는 인적 연계와 VCS·ADS라는 기능적 범위에 결부된 복합적 금지 구조를 취한다. 이 사정들은 조치가 통상 이익의 은폐적 보호가 아니라 특정된 안보 위험에 대응하기 위해 설계되었다는 점을 뒷받침한다. 다만 이러한 선의 관련 사정은 조치와 안보이익 사이의 최소한의 개연성을 뒷받침할 뿐, 불충분하게 특정된 안보이익을 사후적으로 보완하지는 아니한다.

따라서 안보이익 주장의 설득력은 위협 유형별로 불균등하나 적어도 일부 논거에는 충분한 특정성을 인정할 여지가 있으며, 문제는 그것이 제XXI조(b)(iii)의 '국제관계상 긴급상황'이라는 별도의 객관적 요건과 결부될 수 있는지에 있다.

---

67) *Russia* 패널보고서, paras. 7.132-7.133, 7.138-7.139 참조.

68) 김보연, "국가안보 예외조항의 '자기판단' 범위 — 국제법상 의미와 WTO 협정에의 적용", 『국제경제법연구』 제17권 제2호 (2019), 204면 참조(회원국 판단의 존중과 남용 통제 사이의 균형).

69) BIS 최종규칙, 90 Fed. Reg. 5362-5363 참조(ANPRM이 검토 대상으로 열거한 6개 차량 시스템 전부를 규율하는 것은 과도하게 광범위하다는 판단에 따른 축소). 절차 경과는 앞의 주 18 및 해당 본문 참조.

2. '국제관계상 긴급상황' 요건과 사이버-물리 위협

앞 절의 결론은 BIS 최종규칙이 제시하는 안보이익 가운데 적어도 일부가 충분한 특정성을 갖추고 있다는 것이었다. 그러나 제XXI조(b)(iii)의 정당화가 성립하려면, 그와 별도로 조치가 '전시 또는 국제관계상 그 밖의 긴급상황'에 취하여졌다는 요건이 객관적으로 확인되어야 한다.[70]

가. 현행 해석론의 적용과 한계

제Ⅲ장에서 확인한 긴급상황의 정의와[71] 인정례·부정례의 의 판단 구조를[72] 종합하면, 관련 WTO 판정례는 무력충돌, 관계 파탄에 준하는 중대한 사태, 특정 시점에 공표된 단교와 같이 그 존재와 존속을 외부에서 확인할 수 있는 사실관계를 중심으로 긴급상황을 식별하여 왔다.

커넥티드 차량의 사이버-물리 위협은 이 식별 구조에 부합하지 아니한다. BIS 최종규칙이 제시하는 위험은 특정 시점에 개시되어 공지의 사실로 확인되는 사태가 아니라 VCS·ADS라는 기술 인프라에 내재하여 장래에 현실화될 수 있는 잠재적 위험이며, BIS 스스로 그 상당 부분이 장래지향적임을 밝히고 있다.[73] 또한 사이버 침투는 은닉성을 본질로 하므로, *Russia* 사건에서 원용 사태의 특정에 기여한 요소들 — 발생과 계속의 시기, 관련성, 공지성 — 을 사이버-물리 위협에 관하여 동일한 정도로 확정하기 어렵고, 여기에 사실확정과 증거 수집의 곤란이 더해진다.[74]

---

70) *Russia* 패널보고서, paras. 7.70-7.71 참조. 긴급상황의 객관적 심사 구조에 관하여는 앞의 주 36 및 해당 본문 참조.

71) *Russia* 패널보고서, paras. 7.75-7.76 참조. 긴급상황 정의와 그 적용상 재확인에 관하여는 앞의 주 36 및 해당 본문 참조.

72) *Saudi Arabia* 패널보고서, paras. 7.257-7.258 및 7.269-7.270 참조. 인정 구조와 시간적 관련성 판단의 상세는 앞의 주 50 및 해당 본문 참조.

73) BIS 최종규칙, 90 Fed. Reg. 5363 참조("many of the risks laid out in the NPRM and final rule are forward-looking").

74) 원용 사태 특정의 다섯 요소에 관하여는 Russia 패널보고서, para. 7.119 및 앞의 주 38 참조. 사이버 안보 사안에서 사실 확정과 증거 수집이 제XXI조 원용 심사의 가장 곤란한 국면이라는 지적으로 Shin-yi Peng, "Cybersecurity Threats and the WTO National Security Exceptions", 18(2) *Journal of International Economic Law* 449, pp. 458-459 (2015) 참조.

제소국의 관점에서는 미·중 간 사이버 안보 긴장을 무력충돌에 준하는 관계 파탄이 아니라 경제·기술 경쟁의 산물로 성격 규정하는 반론이 유력하다. 실제로 *US – Steel and Aluminium Products* 패널은 경제적 성격의 안보 원용에 대하여 긴급상황이 국제관계에 미치는 영향의 측면에서 전쟁에 적어도 비견될 중대성 또는 심각성을 갖추어야 한다고 해석한 뒤, 글로벌 과잉설비를 둘러싼 긴장에 관하여 국제사회가 이를 협력적 정책 대상으로 다루고 있다는 사정 등을 들어 긴급상황의 존재를 부정하였다.[75] 사이버 안보 역시 UN 차원의 다자 협의가 계속되고 있는 영역이므로, 제소국은 적어도 형식상 유사한 논리 구조를 원용할 수 있다. 여기에 미국 통상법제 일반에서 안보를 이유로 한 예외적 권한 행사가 확대되어 왔다는 평가가 더해지면,[76] 제소국은 개별 조치의 진정성과 무관하게 미국의 원용을 안보예외의 확장적 원용 사례로 성격 규정할 수 있다.

BIS 규칙은 완성품의 국적·원산지만이 아니라, VCS 하드웨어와 대상 소프트웨어를 설계·개발·제조·공급한 주체가 중국 또는 러시아에 의하여 소유·통제되거나 그 관할 또는 지시를 받는지를 기준으로 삼는다.[77] 따라서 한국 등 제3국에서 생산된 차량도 핵심 부품·소프트웨어의 공급자가 중국 또는 러시아와 이러한 방식으로 연계되어 있으면 수입금지 대상이 될 수 있다. 그러나 이러한 소유·통제·관할·지시 관계만으로 제XXI조(b)(iii)의 국제관계상 긴급상황이 입증되는 것은 아니다.[78]

또한 미·중 관계와 미·러 관계는 긴장의 원인·강도·시기가 다르므로 하나의 추상적인 '외국 적대국 위험'으로 묶어서는 안 된다. 원용국은 중국·러시아 각각과 연계된 공급망에 관하여 행위자의 능력과 접근 가능성뿐 아니라, 문제된 조치와 관련된 시점에 존재한 양

---

75) *US-Steel* 패널보고서, paras. 7.138-7.139 참조(국제관계에 미치는 영향의 측면에서 전쟁에 "at least comparable in its gravity or severity to a war"일 것을 요구). 적용상 배척 판단은 paras. 7.147-7.149 참조(글로벌 과잉설비 문제가 국제적 관심과 협력적 정책 논의의 대상으로 다루어져 왔음을 확인하면서도, 그러한 증거만으로는 국제관계에 미치는 영향의 중대성 내지 심각성이 입증되지 아니한다고 판단). 전통안보 인정례와 경제안보 부정례의 대비 정리로 구모란, 앞의 주 51, 92면 및 97면; 동 사건 패널보고서 전반의 국문 평석으로 윤여현(이재민 감수), "United States–Certain Measures on Steel and Aluminium Products (WT/DS544)", 『통상법무정책』 2024년 제2호(통권 제8호), 107-109면 참조.

76) Kathleen Claussen, "Trade's Security Exceptionalism", 72 *Stanford Law Review* 1097, p. 1097 (2020) 참조(미국 통상법이 안보를 이유로 한 예외적 권한 행사를 구조화하여 왔다는 분석). 최근 상호관세 협상 국면에서 경제안보 논리가 통상 의제와 연계·확장되는 양상의 국내 분석으로 류예리, "미국 상호관세 협상에서의 경제안보와 지식재산권 보호 연계에 관한 연구", 『국제거래와 법』 통권 제51호 (2025), 189면 이하 참조.

77) BIS 최종규칙, 90 Fed. Reg. 5365-5369, 5387-5390, 5415-5416; 15 C.F.R. §§ 791.301-791.303 참조.

78) BIS 최종규칙, 90 Fed. Reg. 5365-5369 참조(중국·러시아 관련 위협 분석).

자 관계의 객관적 상황과 그 상황이 국제관계에 미친 영향의 중대성을 각각 제시하여야 한다. 공개된 BIS 규제 기록에서 두 관계가 충분히 구별되지 않은 점은 상황의 특정성과 시간적 관련성에 관한 입증을 약화한다.

US-Steel 패널보고서가 제시한 객관적 중대성 기준은 국제관계상 긴급상황이 국제관계에 미치는 영향이 전쟁과 적어도 비견될 정도로 중대하거나 심각하여야 한다는 것이다.[79] 무력충돌, 단교 또는 관계의 전면적 파탄은 이 기준의 충족을 보여 줄 수 있는 강한 사실적 표지이지만, 그중 어느 하나가 반드시 존재하여야 하는 것은 아니다. 반대로 차량의 원격 조작이나 민감정보 탈취가 기술적·사회적으로 중대한 위험이라는 사실만으로 이 기준을 충족하지는 않는다. 원용국은 그러한 위험을 둘러싼 국제관계상 상황의 영향이 이 정도에 이르렀음을 별도로 입증하여야 한다.

공개된 BIS 규제 기록은 VCS·ADS의 공격 표면과 중국·러시아 관련 주체의 접근 가능성에 관하여 상당한 자료를 제시한다. 그러나 미·중 관계와 미·러 관계의 악화 정도를 각각 구분하여, 관련 조치의 채택·발효 및 실제 적용 시점에 각 관계가 위 중대성 기준을 충족하였음을 보여 주는 자료까지 제시하지는 않는다. 따라서 본고가 제안하는 보충적 식별틀을 적용하더라도 현재 공개된 기록만으로는 제2요건을 충족하기 어렵다. 이는 상시적 취약성이 미국 조치의 정당화를 전제로 한 기준이 아니라, 기술적 위험의 중대성과 국제관계상 긴급상황의 법적 중대성을 구별하여 과잉 포섭을 막는 기준임을 보여 준다.

나. 목적론적 해석의 한계와 향후 규범 형성의 단서

VCLT 제31조 제1항에 따르면 '긴급상황'은 문맥과 조약의 대상·목적에 비추어 성실하게 해석되어야 한다.[80] 그 통상적 의미가 무력충돌만을 가리키는 것도 아니다. 실제로 Saudi Arabia 패널은 무력충돌을 수반하지 아니한 단교 사태를 긴급상황으로 인정하였고, US – Origin Marking Requirement 패널은 앞 절에서 본 바와 같이 긴급상황과 국방·군사적 이익의 필연적 연계를 요구하지 아니하였다.[81]

---

79) *US-Steel* 패널보고서, paras. 7.138-7.149; Alexander, *supra* note 7, pp. 1168-1172 참조.

80) VCLT art. 31(1) 참조.

81) *US-Origin Marking* 패널보고서, para. 7.301 참조. 동 판단의 원용 수위에 관하여는 앞의 주 53 및 주 65와 해당 본문 참조. 무력충돌을 수반하지 아니한 사태에 대한 인정례는 *Saudi Arabia* 패널보고서, para. 7.257 및 앞의 주 50 참조.

GGE의 2021년 보고서와 OEWG의 2025년 최종보고서는 사이버 작전과 국제안보의 관련성에 관한 동시대 국가들의 규범적 인식을 보여 주는 자료이다. 그러나 별도의 당사국 합의나 후속 관행이 입증되지 않는 한 이들 보고서를 VCLT 제31조 제3항(a) 또는 (b)의 자료라고 단정할 수 없고, 보고서 자체가 같은 항 (c)의 '당사국 간 관계에 적용되는 국제법 규칙'에 해당하는 것도 아니다.[82] ISO/SAE 21434와 EU NIS2 지침도 같은 항 (c)의 국제법 규칙이 아니라, 사이버 위험이 상시적 위험 관리의 대상으로 표준화·법제화되고 있음을 보여 주는 기술적·비교법적 자료이다.[83] 따라서 이들 자료는 현행 조문의 독립적 확장해석 근거가 아니라, 향후 규범 형성의 필요성과 방향을 뒷받침하는 보조적 자료로 한정하여 원용하여야 한다.[84]

이처럼 비군사적·계속적 상황이 문언상 배제되는 것은 아니지만, 현행 판정례의 해석 아래에서는 지속적·구조적 취약상태가 이미 존재하는 국제관계상 긴급상황을 뒷받침하는 사실 자료가 될 수 있을 뿐, 그 자체로 독립된 긴급상황을 구성한다고 보기 어렵다. 이를 독립된 식별 근거로 인정하려면 협정 개정이나 WTO 설립협정 제IX조 제2항에 따른 권위 있는 해석 등 회원국의 제도적 합의가 필요하다. 다음 항의 상시적 취약성 개념과 네 요소는 그러한 향후 규범 형성을 위한 제안이다.

다. Persistent Vulnerability 개념의 제안

UN GGE의 2021년 보고서는 유엔헌장을 비롯한 국제법이 국가의 ICT 사용에도 적용되며 국가가 ICT 사용에 있어 무력의 위협 또는 사용 금지 원칙을 준수하여야 함을 재확인하였고, ISO/SAE 21434는 차량 사이버보안 위협을 일회적 사건이 아니라 상시적 위험 관리의 대상으로 국제 표준화하였다.[85] 이 토대 위에서 본 논문은 다음의 개념을 제안한다.

---

82) UN Doc. A/76/135, paras. 70-71; UN Doc. A/80/257, annex, paras. 32-34, 39-41. 서지는 앞의 주 13 참조. 후자의 국제법 적용 관련 문언이 협상 과정에서 절제된 수준으로 정리된 점을 고려하여, 본 논문은 이를 해석상 합의가 아니라 국가들의 규범적 인식과 실행의 축적으로만 원용한다.

83) ISO/SAE 21434:2021, cl. 8(서지는 앞의 주 13 참조); Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union (NIS 2 Directive), OJ L 333, 27.12.2022, art. 21.

84) Pauwelyn, *supra* note 13, pp. 252-256 참조. 제31조 제3항(c)에 따라 참조될 수 있는 규칙은 '당사국 간 관계에 적용되는 국제법 규칙'에 한정되며, 그 경우에도 해석의 대상인 조약이 일차적 지위를 유지한다.

85) UN Doc. A/76/135, paras. 70-71; ISO/SAE 21434:2021, cl. 8. 앞의 주 82 및 주 83 참조.

상시적 취약성(Persistent Vulnerability)이란 “특정 기술 인프라에 내재된 구조적 취약성으로 인하여 외부 행위자의 의도적 개입이 현실화되기 이전 단계에서도 국가 기능에 대한 중대한 위험이 상존하는 상태”를 의미한다. 관련 WTO 판정례는 긴급상황을 외부에서 확인 가능한 중대한 사실관계를 통하여 식별하여 왔다. 이에 비하여 상시적 취약성은 그러한 사실적 표지가 뚜렷하지 않은 채 기술 인프라 안에서 장기간 잠재·누적되는 취약상태를 가리킨다.

상시적 위험 관리라는 사실적 전제 자체는 새로운 것이 아니다. 이를 제XXI조(b)(iii)의 긴급상황 식별 논의에 연결하는 것이 본고의 규범적 제안이다. 우선 EU NIS2 지침 제21조는 필수 기관 및 중요 기관에 상시적 사이버보안 위험 관리 조치를 법적 의무로 부과함으로써, 지속적 사이버보안 위험이 EU 법제에서 이미 관리 대상이 되었음을 보여 준다.[86]

국제법상 기존 논의와의 구조적 유비도 확인된다. 국제사법재판소는 Corfu Channel 사건 이래, 국가가 자국 영역이 타국의 권리에 반하는 행위에 사용되는 것을 알고도 허용하여서는 아니 된다는 상당한 주의(due diligence) 의무를 확인하여 왔는바, 이 법리는 국가의 의무가 위해의 현실화 이후에만 문제 되는 것이 아니라 국가가 알았거나 알 수 있었던 위험 상태를 전제로 작동할 수 있음을 보여 주며, 전문가 집단의 비구속적 정리인 Tallinn Manual 2.0은 이를 사이버 작전에 관한 원칙으로 정리하였다.[87] 위험이 현실화되기 이전 단계의 규범적 대응이라는 구조는 WTO 협정 내부에도 낯선 것이 아니어서, SPS 협정 제5조 제7항은 과학적 증거가 불충분한 상황에서의 잠정 조치를 명문으로 허용한다. 다만 동 조항은 별도 협정의 명문 규정이므로, 여기서는 제XXI조(b)(iii)의 직접적 해석 근거가 아니라 위험의 불확실성에 대한 WTO 체계 내 대응방식의 비교사례로 한정하여 원용한다.[88] 나아가 사이버 작전이 기존 규범의 경계 불확실성을 이용하여 명확한 위반으로 평가되지 않을 정도로 지속될 수 있다는 관찰은,[89] 가시적 사건이 발생할 때까지 기다리는

86) Directive (EU) 2022/2555, art. 21. 서지는 앞의 주 83 참조.

87) *Corfu Channel, supra* note 14, p. 22; Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Cambridge University Press, 2017, Rule 6 및 그 해설, pp. 30-31 참조.

88) Agreement on the Application of Sanitary and Phytosanitary Measures, art. 5.7. 결국 *Corfu Channel* 법리, Tallinn Manual 및 SPS 협정 제5조 제7항은 위험이 완전히 현실화되기 이전 단계에서도 객관화 가능한 위험 상태가 규범적 판단의 대상이 될 수 있다는 구조적 유비를 제공할 뿐, 제XXI조(b)(iii)의 문언을 직접 변경하는 해석 근거는 아니다.

89) Michael N. Schmitt, “Grey Zones in the International Law of Cyberspace”, 42 Yale Journal of International

식별 구조가 사이버 위협을 충분히 포착하지 못할 수 있음을 시사한다. 상시적 취약성은 기존 법리를 직접 이식한 것이 아니라, 인식 가능한 위험 상태에 규범적 의미를 부여하여 온 여러 규율의 구조를 참고하여 구성한 본 논문의 규범적 제안이다.

다만 관련 WTO 판정례가 가시적 사건의 존재를 독립된 법적 요건으로 요구하였다고 단정하기는 어렵다. Russia 패널 스스로 긴급상황을 고조된 긴장 또는 일반적 불안정과 같은 상황으로 정의하였으므로, 무력충돌이나 단교는 그 존재를 입증한 사실적 표지였을 뿐 지속적·구조적 취약상태를 원천적으로 배제하는 요건이라고 볼 수는 없다. 따라서 본고가 향후 규범 형성론으로 제안하는 것은 긴급상황을 사건에서 상태로 전환하여 재정의하는 것이 아니라, 일정한 지속적·구조적 취약상태를 평가할 수 있는 보충적 식별 표지를 마련하는 것이다. 상시적 취약성의 네 요소는 제2요건의 객관적 상황을 식별하기 위한 보충적 표지이지만, 제1·제3요건의 심사와 일부 동일한 사실 자료에 의존할 수 있다. 중복을 피하려면 '어떤 사실을 보는가'가 아니라 '그 사실을 통하여 어떤 법적 질문에 답하는가'를 기준으로 각 요건을 구분하여야 한다. 제1요건은 원용국이 보호하려는 필수적 안보이익과 그에 관련된 국가 기능을 충분히 특정하였는지를 묻는다. 이에 비하여 아래의 네 요소는 그 이익의 중요성을 다시 평가하는 것이 아니라, 그 이익을 둘러싼 객관적 상황이 제XXI조(b)(iii)의 국제관계상 긴급상황으로 식별될 수 있는지를 묻는다. 제3요건은 그러한 상황이 별도로 인정된 뒤, 각 수입금지가 특정된 안보이익의 보호수단으로서 그 이익과 지나치게 동떨어져 있거나 무관한지를 조치별로 심사한다.

첫째, '객관적으로 확인할 수 있는 기술적 취약상태'는 독립적인 기술 자료, 공격 표면과 접근 권한 및 현실적인 악용 가능성을 토대로 상황의 사실적 기초를 확인하는 요소이다. 둘째, '국제관계상 연계'는 공급자의 국적 자체가 아니라 외국 국가 또는 국가 연계 행위자의 능력·의도·접근 가능성을 토대로 해당 위험이 국가 간 긴장 또는 일반적 불안정 속에서 객관화되었는지를 묻는다. 셋째, '국제관계상 중대성'은 예상 피해가 소비자 안전이나 상업적 손실을 넘는다는 데 그치지 않고, 그 상황이 국제관계에 미치는 영향이 *US-Steel* 패널보고서가 제시한 중대성 기준을 충족하였는지를 묻는다. 넷째, '지속성과 시간적

Law Online 1, pp. 1-3 (2017) 참조(사이버 작전이 기존 규범의 경계 불확실성을 이용하여 명확한 위반으로 평가되지 않는 수준에서 수행되는 양상의 분석). 국내 실무계에서도 사이버 안보 위기 등 새로운 위기 유형이 제XXI조가 적용되는 국가안보 상황에 해당할 가능성이 커지고 있으며 조항의 현대화가 필요하다는 평가로 윤여현(이재민 감수), 앞의 주 75, 110-111면 참조.

관련성'은 객관화된 상황이 조치의 채택·발효뿐 아니라 실제 적용·유지 시점에도 존속하여, 해당 조치가 '그러한 때에 취하여진' 것인지에 필요한 시간적 연결을 형성하는지를 묻는다. 본고가 제안하는 주기적 재검토는 이 네 번째 요소와 구별되는 별도의 통제장치로서, 장기 조치의 유지 단계에서도 원용된 상황과 조치 사이의 시간적 관련성 및 각 조치와 안보이익 사이의 최소한의 개연성이 존속하는지를 확인하기 위한 것이다.[90]

따라서 동일한 규제 기록이 여러 단계에서 증거로 사용되더라도 각 단계에서 제기되는 법적 질문과 도출되는 결론은 서로 다르다. 필수적 안보이익이 구체적으로 특정되더라도 전쟁과 비견되는 중대성의 객관적 상황이 없다면 제2요건을 충족하지 못한다. 그러한 상황이 인정되더라도 특정 수입금지와 그 안보이익 사이에 최소한의 개연성이 없다면 제3요건에서도 정당화되지 않는다. 첫째 요소와 관련하여, ISO/SAE 21434는 법적 의미의 국제관계상 긴급상황을 정의하는 규범이 아니라 기술적 취약상태의 존재와 위험 관리의 필요성을 확인하는 사실 자료로 원용될 수 있다. 그 충족 여부는 표준의 적용 여부만으로 결정되지 않으며, 독립적인 시험·취약점 자료, 원격 접속 권한 및 현실적인 악용 경로를 함께 검토하여야 한다. 이 기준에 비추어 보면, 공개된 BIS 규제 기록은 VCS·ADS의 기술적 취약성과 중국·러시아 관련 주체의 접근 가능성에 관하여 비교적 구체적인 자료를 제시한다. 그러나 미·중 관계와 미·러 관계가 관련 시점에 각각 *US-Steel* 패널보고서가 요구한 국제관계상 중대성 기준을 충족하였다는 점과 각 수입금지가 그러한 상황과 시간적으로 연결된다는 점까지 충분히 보여 주지는 못한다. 현재 공개된 자료만으로는 제2요건의 충족을 인정하기 어렵다.

라. 입증책임과 심사강도

현행법상 제소국은 문제된 조치가 GATT 제XI조 제1항의 금지 또는 제한에 해당함을 일응 입증하고, 제XXI조(b)를 원용하는 회원국은 원용한 세부목을 특정하여 그 객관적 요건이 충족되었음을 입증한다. 패널은 DSU 제11조에 따라 제출된 자료를 객관적으로 평가하되, 원용국을 대신하여 안보정책의 최적 수단을 선택하거나 GATT 제XX조와 같은 필요성 심사를 수행하지 않는다. 제3요건에서는 조치의 선택에 상당한 판단 여지를 인정하면

90) *Russia* 패널보고서, paras. 7.119, 7.145-7.146; US-Steel 패널보고서, paras. 7.138-7.149 참조. 두 보고서는 주기적 재검토 의무를 직접 정한 것이 아니며, 본문은 그 시간적 관련성 및 개연성 판단에서 도출한 향후 규범 형성론상의 제안이다.

서도, 각 조치가 특정된 안보이익과 지나치게 동떨어져 있거나 무관한지를 최소한의 개연성 기준에 따라 심사한다.

본고의 향후 규범 형성론에서는 원용국이 기술 자료와 취약점 정보, 접근 권한과 현실적인 악용 경로, 외국 국가와 공급 주체 사이의 소유·통제·관할·지시 관계, 문제된 상황이 국제관계에 미친 영향 및 그 상황과 조치 사이의 시간적 관련성을 제시하여야 한다. 제XXI조(a)는 공개가 필수적 안보이익에 반한다고 회원국이 판단하는 정보의 제공을 거부할 수 있게 하지만, 수입금지를 독립적으로 정당화하거나 제XXI조(b)(iii)의 객관적 요건이 충족된 것으로 간주하게 하지는 않는다.[91] 패널은 비기밀 자료와 검증 가능한 요약을 포함하여 제출된 자료를 종합하고, 두 수입금지를 각각 심사하여 네 표지의 누적적 충족 여부를 판단하여야 한다.

3. 단계적 시행 구조와 선의·최소한의 개연성 심사

본 절은 규칙의 단계적 시행 구조가 제XXI조(b)의 선의 및 최소한의 개연성 통제에서 어떻게 평가될 것인지를 검토한다. *Russia* 패널에 따르면 어떠한 조치가 필수적 안보이익의 보호에 필요한지는 원칙적으로 원용국의 판단에 맡겨지되, 그 재량은 선의 원칙에 따라 조치가 제시된 안보이익으로부터 너무 동떨어져 있거나 무관하지 아니할 것, 곧 최소한의 개연성을 갖출 것을 요구받는다. 따라서 본 절의 쟁점은 단계적 시행 그 자체가 조치의 필요성을 부정하는지가 아니라, 수년에 걸친 적용 시차가 조치와 안보이익 사이의 개연성을 부정할 정도에 이르는지에 있다.[92]

가. 장기 유예와 절박성 결여의 반론

규칙의 금지는 일시에 적용되지 아니한다. 대상 소프트웨어를 탑재한 완성 커넥티드 차량에 관한 금지는 모델연도 2027부터, 모델연도와 결부되지 아니하는 VCS 하드웨어에 관한 금지는 2029년 1월 1일부터, 모델연도와 결부된 VCS 하드웨어에 관한 금지는 모델연

91) *US-Origin Marking* 패널보고서, paras. 7.259-7.260; 김경우, 앞의 주 7, 25-35면; Pinchis-Paulsen, Saggi & Mavroidis, *supra* note 7, pp. 285-294 참조.

92) *Russia* 패널보고서, paras. 7.132-7.138 참조. 용어법의 상세는 앞의 주 9, 단계적 시행 일정의 상세는 앞의 주 24 및 주 25와 해당 본문 참조.

도 2030부터 적용된다. 제소국은 이 구조를 근거로, 미국이 위험의 절박성을 스스로 인정하지 아니하였다고 주장할 수 있다. 규칙 전문이 해당 위험을 "긴급한 국가안보 위험(urgent national security risk)"으로 규정하고 그 상당 부분을 장래를 향한(forward-looking) 것으로 설명하면서도,[93] 금지가 실질적으로 작동하기 전까지 해당 위험을 발생시키는 거래를 수년간 허용한 것은 즉각적 대응을 요하는 사태의 현존과 양립하기 어렵다는 논리이다.

최종규칙은 행정명령 제13873호에 따라 선포·연장된 미국 국내법상 국가비상사태를 수권 배경으로 하고, 커넥티드 차량 관련 위험을 별도로 'urgent national security risk'라고 평가한다. 그러나 이러한 국내법상 비상사태의 선포와 위험의 긴급성에 관한 행정부의 평가는 GATT 제XXI조(b)(iii)의 '국제관계에 있어서의 긴급상황(emergency in international relations)'과 동일한 법적 판단기준이 아니다. *US-Steel* 패널 역시 미국 국내법상 제232조 결정은 상이한 법적 기준과 근거에 기초하므로 (iii)목의 상황 요건 판단에 직접 전용될 수 없다고 보았는바, 이는 국내법상 안보 판단과 WTO상 상황 요건을 구별하여야 한다는 점을 뒷받침하는 유추 근거가 된다. 따라서 본 절은 양자의 등가성을 전제하는 것이 아니라, 위험의 긴급성을 강조한 규칙의 설명과 장기간에 걸친 단계적 시행 사이의 내적 정합성을 선의·최소한의 개연성 심사의 정황으로 검토한다.[94]

나. 단계적 시행의 기술적·규범적 근거

그러나 절박성과 개연성은 구별되어야 한다. 선의 심사에서 핵심은 조치가 언제 전면적으로 시행되는지가 아니라, 조치가 제시된 필수적 안보이익으로부터 너무 동떨어져 있거나 무관하여 그 보호수단으로서의 개연성이 부정되는지 여부이다.[95] *Russia* 패널은 이 기준에 따라 조치가 긴급상황과 너무 요원하거나 무관하다고 볼 수 없는 한 최소한의 개연

93) BIS 최종규칙, 90 Fed. Reg. 5361 ("urgent national security risk"); 5363 ("many of the risks laid out in the NPRM and final rule are forward-looking") 참조. 위협 열거부의 원문 표현과 장래지향성 서술은 앞의 주 25 및 주 66과 해당 본문 참조.

94) *US-Steel* 패널보고서, para. 7.143 참조. 패널은 미국 국내법상 제232조 판단이 GATT 제XXI조(b)(iii)와 상이한 법적 기준에 기초하므로 그 상황 요건에 직접 전용될 수 없다고 보았다. 본고는 이를 동일 사안의 판단이 아니라 국내법상 안보 판단과 WTO상 상황 요건의 구별을 뒷받침하는 유추 근거로 원용한다. 동 보고서의 미채택 경위는 앞의 주 8 참조.

95) *Russia* 패널보고서, paras. 7.138-7.139 참조. '선의 및 최소한의 개연성'의 용어법은 앞의 주 9 참조.

성이 인정된다고 보았을 뿐, 즉각적·전면적 거래 중단이나 덜 무역제한적인 대체수단의 부재를 요구하지 아니하였다.[96] '시에 취하여진'이라는 문언이 요구하는 시간적 연결에 관하여도, 적어도 규칙의 채택·발효 시점을 기준으로 보면 구체적 금지의 적용 개시가 단계화되었다는 사정만으로 그 연결이 당연히 단절된다고 보기는 어렵다.[97] 다만 모델연도 2027 또는 2030 이후 실제 금지의 적용·유지·집행이 분쟁의 대상이 되는 경우에는, 원용된 국제관계상 긴급상황이 그 시점에도 계속되고 있었는지와 조치와의 시간적 연결이 유지되고 있었는지가 별도로 심사될 수 있다.

나아가 유예를 정당화할 수 있는 사정은 위험의 경미함이 아니라 규제 대상의 기술적·산업적 구조에서 찾을 수 있다. 차량 사이버보안은 개념 단계의 위험 평가에서 출발하여 제품 개발과 검증에 이르는 수명주기 전반에 통합되는 활동이므로, 공급자 및 소프트웨어 구조의 변경은 차량의 개발·검증 일정과 밀접하게 결부될 수 있고, 충분히 검증되지 아니한 대체의 급조는 오히려 새로운 취약성을 들여올 수 있다.[98] 이러한 단계화에는 규칙 자체가 제시한 보다 직접적인 근거도 존재한다. BIS는 하드웨어에 대하여 대상 소프트웨어와 같은 legacy 제외를 두기를 거부하면서, 하드웨어와 완성차의 장기 사용성으로 인하여 관련 안보 위험이 차량 세대에 걸쳐 장기간 지속될 수 있고 하드웨어에 내재한 취약점은 소프트웨어 취약점보다 탐지·완화하기 어렵다고 설명하였다. 이에 비모델연도 하드웨어에는 2029년 1월 1일, 모델연도 연계 하드웨어에는 모델연도 2030을 기준으로 설정하고 모델연도 2030 이전 차량의 수리·보증용 부품 수입을 허용하는 방식을 위험 통제와 공급망 조정 사이의 합리적 중간선으로 제시하였다.[99] 이러한 동시대적 규제 설명이 그 자체

---

96) *Russia* 패널보고서, para. 7.145 참조. 패널은 러시아의 통과운송 제한이 2014년의 긴급상황과 너무 요원하거나 무관하다고 볼 수 없다고 보아 최소한의 개연성을 인정하였고, 긴급상황 중 일부 거래가 계속되었다는 사정에 관계없이 이러한 결론에 이르렀다.

97) *US-Steel* 패널보고서, paras. 7.139-7.140 참조. 패널은 (iii)목의 긴급상황이 국제관계에 미치는 영향의 측면에서 전쟁에 준하는(at least comparable) 중대성을 갖추어야 한다고 보고(para. 7.139), '시에 취하여진(taken in time of)'이라는 문언이 회원국이 취한 조치와 긴급상황 사이의 시간적 연결(temporal link)을 서술한다고 하였다(para. 7.140). 상황의 존재와 그 시기가 객관적으로 확정될 수 있는 사실의 문제라는 점은 *Russia* 패널보고서, paras. 7.70-7.71 및 앞의 주 36 참조.

98) ISO/SAE 21434:2021, cl. 8 및 cls. 9-11 참조. Cl. 8은 지속적 사이버보안 활동을, cls. 9-11은 개념·제품개발·차량 수준 검증 단계에서 사이버보안 위험과 요건을 도출·구현·검증하는 구조를 다룬다. 다만 동 표준은 공급망 전환에 필요한 구체적인 기간을 정하지 아니하므로, 여기서는 다년간의 유예기간 자체의 직접 근거가 아니라 공급자 또는 소프트웨어 구조의 변경이 개발·통합·검증 절차에 반영되어야 한다는 기술적 배경으로 원용한다. 서지는 앞의 주 13 참조.

로 조치의 정당성을 입증하는 것은 아니지만, 장기 유예가 위험의 부재를 자인한 것이라기보다 장기적으로 잔존할 수 있는 하드웨어 위험의 차단과 공급망 전환 가능성을 함께 고려한 이행 설계였다는 점을 뒷받침하는 정황이 될 수 있다. 나아가 지속적·구조적 취약 상태에 대한 적절한 대응은 위험이 현실화된 뒤의 일회적 금지보다 취약성이 차량군 전체에 축적되기 이전에 구조 전환을 개시하는 데 있을 수 있으므로, 단계적 시행을 위험의 비절박성을 보여 주는 사정으로만 평가하기는 어렵다.[100]

다. 수입금지 조치별 개연성 심사

다만 이러한 개연성 판단은 규칙 전체를 하나의 조치로 뭉뚱그려서가 아니라 조치별로 이루어져야 한다. 본 논문이 GATT 제XI조 분석의 대상으로 삼은 수입금지 부분에 한정하면, 제791.302조의 VCS 하드웨어 수입금지와 제791.303조(a)항의 대상 소프트웨어 탑재 완성 커넥티드 차량 수입금지가 각각 별도의 조치로서 심사될 필요가 있다.[101] *Saudi Arabia* 패널은 하나의 긴급상황을 전제하면서도, 권리자의 민사적 구제 접근을 차단한 조치에 대하여는 최소한의 개연성을 인정한 반면, 해적 방송에 대한 형사절차와 제재의 부작위에 대하여는 긴급상황과의 시간적·논리적 관련성이 인정되지 아니한다는 이유로 이를 부정함으로써, 개연성 심사가 조치별로 분할될 수 있음을 보였다.[102] 같은 방식으로 보면, 모델연도 2027부터 적용되는 대상 소프트웨어 탑재 완성차 수입금지는 제1절에서 필수적 안보이익의 특정성이 비교적 강하게 인정된 데이터 탈취 및 원격 조작 위험에 직접 대응하고 적용 시차도 상대적으로 짧으므로 개연성을 부정하기 어렵다. 반면 VCS 하드웨어 수입금지는 동일한 위험과 기능적으로 연결되면서도 가장 긴 유예를 수반하므로, 위험 인식과 조치 설계 사이의 정합성에 관한 다툼은 여기에 집중될 수 있다. 그러나 하드웨어가 VCS의 통신 기능을 직접 가능하게 하고 그 교체가 차량의 개발·검증 주기 및 다층적 공

99) BIS 최종규칙, 90 Fed. Reg. 5392 참조. BIS는 하드웨어와 완성차의 장기 사용성, 하드웨어 취약점의 탐지·완화 곤란 및 공급망 조정의 필요성을 이유로 2029년 1월 1일과 모델연도 2030의 적용 기준을 설정하고, 모델연도 2030 이전 차량의 수리·보증용 부품 수입을 허용하는 방식을 “reasonable middle ground”라고 평가하였다. 단계적 면제 구조는 15 C.F.R. § 791.308; 90 Fed. Reg. 5420 참조.

100) 앞의 주 98 및 주 99와 해당 본문 참조.

101) 15 C.F.R. §§ 791.302, 791.303(a), 90 Fed. Reg. 5416 참조. § 791.303이 (a)항에서 수입을, (b)항에서 미국 내 판매를 구분하여 규정하는 구조는 앞의 주 23 참조. 미국 내 판매 금지(§ 791.303(b))와 관련 금지 거래(§ 791.304)는 제Ⅱ장 제2절의 분석 범위 획정에 따라 본 절의 심사 대상에서 제외한다.

102) *Saudi Arabia* 패널보고서, paras. 7.285, 7.288, 7.291-7.294 참조. 채택 여부에 관하여는 앞의 주 34 참조.

급망의 전환과 결부된다는 점을 고려하면, 공개된 규제 기록만으로 하드웨어 수입금지가 제시된 안보이익과 너무 동떨어져 있거나 무관하다고 단정하기는 어렵다.

단계적 시행은 제2요건에서 국제관계상 긴급상황의 존재를 직접 부정하는 법적 기준은 아니다. 다만 규칙이 장래지향적 위험에 대응하면서 수년간 거래를 허용한다는 사정은, 관련 시점의 상황이 국제관계에 미친 영향이 전쟁과 비견될 정도로 중대하였다는 주장과 규제 기록의 정합성을 평가할 때 반대 정황이 될 수 있다. 국내 규제 기록의 '긴급한 국가안보 위험'이라는 표현만으로 WTO법상 긴급상황이 입증되는 것도 아니다.

제3요건에서는 단계적 시행과 레거시 소프트웨어·수리용 부품의 제외가 차량의 개발·검증 주기와 공급망 전환을 고려한 규제 설계라는 점이 각 수입금지와 안보이익 사이의 최소한의 개연성을 뒷받침할 수 있다. 다만 실제 금지가 적용·유지되는 단계에서도 원용된 국제관계상 상황과 조치 사이의 시간적 관련성이 존속하는지는 별도로 평가하여야 한다.[103]

4. 자기판단 항변의 적용 한계와 예상 가능한 패널 판단

이러한 해석 구조를 BIS 최종규칙에 적용하면, 미국이 커넥티드 차량의 공급망 위험을 필수적 안보이익으로 판단하였다는 사정만으로 제XXI조(b)(iii)의 심사가 배제되지는 않는다. 미국의 필요성 판단에는 상당한 판단 여지가 인정될 수 있으나, 관련 시점에 객관적 긴급상황이 존재하였는지와 두 수입금지가 각각 그러한 때에 취하여졌는지는 별도로 입증되어야 한다. 행정명령 제13873호에 따른 미국 국내법상 국가비상사태의 선포와 BIS의 위험 평가는 패널이 고려할 사실 자료가 될 수 있다. 그러나 *US-Steel* 패널보고서가 국내법상 안보 판단과 (iii)목의 법적 기준을 구별한 점에 비추어 보면, 그러한 국내법상 판단이 제XXI조(b)(iii)의 국제관계상 긴급상황을 대체하지는 못한다.

앞 세 절의 분석을 종합하면 예상 가능한 패널 판단의 윤곽은 다음과 같다. 필수적 안보이익의 특정성(제1요건)은 민감정보 탈취와 군사·치안 관련 정보 수집 위험을 중심으로 일부 충족될 수 있다. 조치별로 분할된 선의·최소한의 개연성 심사(제3요건)에서도 대상

103) BIS 최종규칙, 90 Fed. Reg. 5360, 5379, 5392, 5415-5420; *Russia* 패널보고서, paras. 7.138-7.146; *US-Steel* 패널보고서, paras. 7.138-7.149 참조.

소프트웨어 탑재 완성차 수입금지의 개연성은 부정하기 어렵고, 가장 긴 유예를 수반하는 VCS 하드웨어 수입금지는 상대적으로 다툼의 여지가 크지만 공개된 규제 기록만으로 그 개연성을 부정하기도 어렵다. 그러나 세 요건은 누적적으로 충족되어야 하므로, 제2요건이 충족되지 아니하는 이상 제1·제3요건에 관한 긍정적 판단만으로 정당화는 성립하지 아니한다.[104] 공개된 규제 기록은 상시적 위험 관리의 구조를 제시할 뿐, 긴급상황의 존재와 조치의 시간적 관련성을 객관화할 수 있는 사태의 발생·계속 시기와 공지성에 관한 자료를 충분히 제시하지 아니한다. 현행 WTO 패널 해석 기준에 따를 때, 사이버-물리 위협은 '국제관계상 긴급상황'으로 포섭되기 어렵다. 따라서 BIS 최종규칙에 대한 제XXI조(b)(iii)의 정당화는 제2요건의 단계에서 실패할 가능성이 높다.

이상의 분석에서 우선 도출되는 것은 현행법상 결론이다. BIS 최종규칙의 두 수입금지는 GATT 제XI조 제1항의 금지 또는 제한에 해당할 가능성이 크고, 현재 공개된 규제 기록은 미·중 관계와 미·러 관계가 관련 시점에 제XXI조(b)(iii)의 국제관계상 긴급상황에 이르렀다는 점을 충분히 뒷받침하지 못한다. 따라서 필수적 안보이익의 특정성과 조치의 최소한의 개연성이 일부 인정되더라도 현행법상 정당화는 성립하기 어렵다.

상시적 취약성에 관한 제안은 이러한 판단을 달리하지 않는다. 지속적·구조적 취약상태는 현행 조문 아래에서 이미 존재하는 국제관계상 긴급상황을 뒷받침하는 사실 자료로 기능할 수 있을 뿐, 그 자체만으로 제XXI조(b)(iii)의 긴급상황이 되지는 않는다. 이를 독립된 식별 근거로 인정하려면 회원국의 제도적 합의를 거쳐야 한다.

Ⅴ. 결론 및 한국에 대한 시사점

1. 연구 결과와 규범적 함의

본 연구는 미국 상무부 산업안보국(BIS)의 2025년 커넥티드 차량 최종규칙을 대상으로, 구체적인 사이버 공격이나 무력충돌이 현실화되기 이전의 사이버-물리 위험에 대응하는 예방적 공급망 규제가 GATT 제XXI조(b)(iii)에 의하여 정당화될 수 있는지를 검토하였다.

104) 본고가 Russia 패널의 판단을 분석 목적상 세 심사항목으로 재구성한 방식과 그 누적적 적용에 관하여는 앞의 주 9 및 주 36 내지 주 46과 해당 본문 참조.

이 규칙이 제기하는 핵심 문제는 커넥티드 차량의 사이버 위험이 중대한지 여부 자체가 아니다. 문제는 장기간 잠재·누적되는 기술적 취약성이 관련 WTO 판정례의 해석상 요구되는 '국제관계상 긴급상황'의 객관적 표지에 해당할 수 있는지, 그리고 그러한 상황과 수입금지 조치 사이의 시간적 관련성이 인정될 수 있는지에 있다.

분석 결과, BIS 최종규칙 중 제791.302조의 VCS 하드웨어 수입금지와 제791.303조(a)항의 대상 소프트웨어 탑재 완성 커넥티드 차량 수입금지는 GATT 제XI조 제1항에 비합치될 가능성이 높다. 공개된 규제 기록만을 전제로 할 때, 이들 조치는 제XXI조(b)(iii)에 의하여 정당화되기도 어렵다.[105] 다만 그 이유는 BIS가 제시한 안보이익이 모두 추상적이거나, 수입금지가 안보 목적과 무관하기 때문은 아니다.

요건별 결론은 제Ⅳ장 제4절에서 확정한 바와 같다. 필수적 안보이익의 특정성과 조치별 선의·최소한의 개연성은 부분적으로 인정될 수 있으나, 그것만으로 정당화가 성립하지는 아니한다.

정당화의 가장 큰 장애는 제2요건인 '국제관계상 긴급상황'의 존재이다. BIS는 VCS·ADS에 내재한 기술적 취약성, 중국과 러시아 정부가 자국 관할 기업에 행사할 수 있는 법적·제도적 영향력, 민감정보 탈취와 원격 조작의 가능성을 비교적 구체적으로 제시하였다. 공개된 자료 중에는 중국의 미국 핵심기반시설 침투 활동과 양국 간 고조된 전략적 긴장을 뒷받침할 수 있는 내용도 존재한다. 그러나 BIS는 그러한 사태가 어느 시점에 제XXI조(b)(iii)상 국제관계상 긴급상황으로 발생하였고 계속되고 있는지, 그 사태가 중국뿐 아니라 러시아 관련 거래까지 함께 규율하는 각 수입금지의 시간적 기반이 되는지를 규칙의 정당화 구조 안에서 충분히 특정하지 아니하였다. 미국 국내법상 국가비상사태의 선포와 BIS의 국가안보 평가는 중요한 사실 자료가 될 수 있으나, 그 자체가 GATT 제XXI조(b)(iii)의 객관적 상황 요건을 대체하지는 않는다.[106]

따라서 본 연구의 결론은 "커넥티드 차량의 사이버 위험은 안보 위험이 아니다"라는 것이 아니다. 보다 정확한 결론은, 위험의 사실적 중대성과 제XXI조(b)(iii)상 긴급상황의 존

105) 앞의 주 104 및 제Ⅳ장 제1절 내지 제4절 참조.

106) BIS 최종규칙, 90 Fed. Reg. 5366-5369 참조(중국 정부의 기업 통제·취약점 보고 체계, Volt Typhoon의 미국 핵심기반시설 침투 활동 및 러시아 관련 위협 분석). 미국 국내법상 안보 판단과 GATT 제XXI조(b)(iii)의 객관적 상황 요건의 구별은 앞의 주 94, 시간적 관련성은 앞의 주 97 참조.

재는 서로 다른 법적 문제이며, BIS의 공개 기록은 전자를 상당 부분 설명하였지만 후자를 충분히 객관화하지 못하였다는 것이다. 필수적 안보이익의 특정성과 조치의 최소한의 개연성이 일부 인정되더라도, 누적적으로 요구되는 객관적 상황 요건이 충족되지 않는 이상 안보예외에 의한 정당화는 성립하지 않는다.

그러나 이 결론만으로는 예방적 안보규제가 직면한 문제를 해결할 수 없다. 관련 WTO 판정례가 긴급상황을 무력충돌, 외교관계의 단절 또는 공개적으로 식별되는 위기와 같이 발생·계속 시기를 특정할 수 있는 사실관계를 통하여 확인하여 왔다면, 커넥티드 차량의 위험은 외부 행위자가 활용할 수 있는 접근 경로와 취약성이 공급망과 차량 수명주기 전반에 장기간 존재하는 상태로 나타난다. 이러한 위험에 대하여 가시적인 공격의 발생만을 요구하면 예방적 대응은 피해가 현실화된 뒤에야 가능해진다. 반대로 잠재적인 기술적 취약성만으로 긴급상황을 인정하면 일상적인 사이버 위험이나 산업정책적 이해가 안보예외로 포장될 수 있다. 현행 법리가 직면한 과제는 예방적 규제를 전면적으로 배제하거나 안보예외의 적용 요건을 무제한으로 완화하는 것 중 하나를 선택하는 데 있지 않다. 예방적 조치의 필요성을 인정하면서도 그 발동 요건을 객관적으로 심사할 수 있는 기준을 마련하는 데 있다.

본고가 제안한 상시적 취약성(Persistent Vulnerability)은 향후 규범 형성론상의 식별틀이며, 객관적으로 확인할 수 있는 기술적 취약상태, 국제관계상 연계, 국제관계상 중대성, 지속성과 시간적 관련성의 네 요소가 누적적으로 충족되어야 한다. 주기적 재검토는 이 네 요소와 구별되는 별도의 통제장치로서, 장기 조치의 적용·유지 단계에서 원용된 상황과 조치 사이의 시간적 관련성이 존속하는지를 확인한다.

이러한 관점에서 단계적 시행과 예외의 존재는 위험의 부재를 자인한 것으로만 평가되어서는 아니 된다. 자동차와 같이 개발·검증 주기가 길고 공급망이 다층적인 제품에서는 즉시 대체가 새로운 취약성이나 공급망 혼란을 야기할 수 있다. 특정허가, 위험완화 조치, 수리·보증용 부품에 대한 예외와 합리적인 전환기간은 조치가 실제 위험에 맞추어 설계되었는지를 보여 주는 자료가 될 수 있다. 다만 시행 유예가 길어질수록 긴급상황과 실제 조치 적용 사이의 시간적 관련성이 유지되는지를 재평가할 필요성도 커진다. 예방적 안보규제의 정당성은 조치 채택 당시의 위험 설명만으로 고정되는 것이 아니라, 그 조치가 실제로 적용되고 유지되는 기간에도 계속 입증되어야 한다.

상시적 취약성은 안보예외의 적용범위를 확대할 위험을 내포한다. 회원국이 일반적인 기술적 취약성이나 특정 국가에 대한 불신을 국가 기능에 대한 중대한 위험으로 포장할 가능성을 배제할 수 없기 때문이다. 본고가 제시한 네 요소는 이러한 남용을 제한하기 위한 출발점이지만, 기밀성이 높은 사이버안보 자료를 패널이 어떠한 증명 수준과 절차에 따라 평가하여야 하는지까지 완결적으로 제시한 것은 아니다. 아울러 실제 분쟁에서는 공개되지 아니한 안보 관련 자료나 추가적인 국제관계상 사태에 관한 증거가 제출될 수 있으므로, 본고의 결론은 현재 공개된 규제 기록에 기초한 예상 판단이라는 한계를 갖는다. 또한 본 연구는 GATT 제XI조와 제XXI조(b)(iii)에 분석을 한정하였으므로, TBT 협정, GATS 제XIVbis조, 서비스·데이터 규제 및 디지털무역협정상 안보예외와의 관계는 후속 연구가 필요하다.[107]

결국 BIS 최종규칙 사례의 의미는 특정한 미국 조치가 현행 GATT 법리상 정당화되기 어렵다는 결론에 그치지 않는다. 이 사례는 디지털 인프라에 대한 예방적 보호의 필요성과 사건 중심으로 형성된 현행 안보예외 법리 사이의 간극을 보여 준다. 디지털 공급망의 보호를 위하여 실제 공격이 발생할 때까지 대응을 유보할 필요는 없지만, 국가안보라는 명칭만으로 특정 국가와 연계된 상품의 수입금지가 면책되어서도 아니 된다. 예방적 규제가 국제통상법상 정당성을 확보하기 위해서는 위험의 존재, 외국 국가와의 연계, 국제관계상 상황, 조치별 기능적 관련성 및 적용기간을 객관적으로 기록하고 주기적으로 재검토하여야 한다. 본 연구의 규범적 기여는 예방적 안보규제를 허용할 것인지에 관한 추상적 찬반이 아니라, 그러한 규제를 법적으로 심사 가능한 형태로 설계하고 입증하기 위한 기준을 제시하는 데 있다.

2. 한국에 대한 시사점

이상의 분석은 한국에 이중적인 의미를 갖는다. 한국은 커넥티드 차량과 관련 부품·소프트웨어를 생산·수출하는 국가인 동시에, 자국의 교통·통신 기반시설과 디지털 공급망을 보호하여야 하는 규제국이다. 따라서 안보예외의 적용범위를 일률적으로 확대하는 입장과 가시적인 공격이 발생하기 전에는 예방적 규제를 인정하지 않는 입장 중 어느 하나만을

107) GATS art. XIVbis:1(b)(iii) 참조. 동 조항은 GATT 제XXI조(b)(iii)와 동일하게 “taken in time of war or other emergency in international relations”라는 문언을 사용한다.

취하기 어렵다. 안보예외가 과도하게 확대되면 외국 정부가 불명확한 공급망 위험이나 기업의 국적을 이유로 한국산 제품과 한국 기업을 배제할 가능성이 커진다. 반대로 사건 발생 이전의 지속적·구조적 취약상태를 전혀 고려하지 않으면 한국도 핵심 디지털 인프라에 내재한 취약성에 적시에 대응하기 어렵다.

먼저 한국이 외국의 국가안보 규제에 대응하는 경우, 상대국의 국내법상 안보 판단이나 국가비상사태 선포를 그대로 WTO상 긴급상황의 존재로 받아들여서는 아니 된다. 규제국이 보호하려는 필수적 안보이익을 구체적으로 특정하였는지, 한국산 제품 또는 한국 기업이 외국 정부의 소유·통제·관할·지시와 어떠한 방식으로 연결되는지, 그 연계가 실제 데이터 접근이나 원격 통제 능력으로 이어지는지, 조치의 채택과 적용 시점에 어떠한 국제관계상 상황이 존재하는지를 구분하여 확인할 필요가 있다. 특히 하나의 국가안보 목적 아래 소프트웨어, 하드웨어, 완성차와 서비스에 대한 제한을 일괄적으로 정당화하는 경우, 각 조치가 해당 위험에 대응하는 기능적 수단인지와 그 적용시점이 개별적으로 심사되어야 한다는 점을 제기할 수 있다.

이는 한국산 완성차가 최종적으로 한국에서 생산되었다는 사실만으로 외국 규제의 적용에서 자동으로 제외된다는 의미는 아니다. BIS 최종규칙과 같은 규제는 완성차의 원산지만이 아니라, 핵심 하드웨어와 소프트웨어를 설계·개발·제조·공급한 주체가 중국 또는 러시아에 의하여 소유·통제되거나 그 관할 또는 지시를 받는지, 업데이트·원격 접속 권한과 데이터 접근 가능성이 누구에게 있는지를 문제 삼는다. 한국 기업은 하드웨어·소프트웨어 구성 명세, 공급자의 소유·통제·관할·지시 관계, 원격 접속 및 업데이트 권한, 데이터의 저장·전송 경로와 취약점 대응체계를 문서화하여 기업의 국적 자체와 국가 연계에서 비롯되는 기능적 위험을 구별할 수 있는 자료를 확보하여야 한다. 이러한 자료는 특정허가나 위험완화 조치를 신청하고 규제 적용의 과도성을 다투거나 한국 정부가 통상협의에 나서는 과정에서 입증 자료로 활용될 수 있다.

한국이 향후 커넥티드 차량이나 다른 디지털 공급망에 대하여 유사한 안보규제를 도입하는 경우에도 같은 기준이 적용되어야 한다. 국내법상 국가안보 필요성의 판단과 GATT 제XXI조(b)(iii)상 긴급상황의 판단을 구분하고, 규제 입안 단계에서부터 보호하려는 국가기능, 기술적 취약성, 외국 국가와의 구체적 연계, 국제관계상 상황 및 각 조치의 대응방식을 별도로 기록하며, 규제 범위는 기업의 국적이나 생산지보다 원격접속 권한, 업데이트

통제, 데이터 접근, 공급망 지위와 같은 기능적 위험 요소를 중심으로 설정하여야 한다. 특정허가, 위험완화 조치, 합리적인 전환기간과 정기적 재검토 절차를 함께 설계하면, 이러한 규제 기록은 사후에 안보예외를 원용하기 위한 자료에 그치지 않고, 조치의 범위가 실제 위험에 상응하는지를 정부 스스로 검토하고 산업정책적 목적이 안보규제로 전환되는 것을 통제하는 기능을 한다. 단계적 시행과 예외가 규제의 불성실성이 아니라 위험과 산업 현실을 조정한 설계라는 설명력을 갖는 것도 이러한 절차가 마련될 때이다.

WTO법상 검토와 함께, 한국 기업의 상품이 미국의 안보규제 대상이 되는 경우에는 한미 FTA 제23.2조의 필수적 안보예외와 제22.6조의 분쟁해결절차 선택 규정도 고려하여야 한다. 제23.2조는 GATT 제XXI조(b)와 달리 적용 상황을 세 개의 목으로 열거하거나 '전시 또는 국제관계에 있어서의 그 밖의 비상시'라는 시간적 한정을 두지 않으며, 각주 2는 제11장 또는 제22장에 따른 절차에서 당사국이 이 조항을 원용하면 중재판정부 또는 패널이 그 예외가 적용됨을 판정하도록 정한다. 동일 사안이 한미 FTA와 WTO 협정 모두에서 발생하면 제22.6조에 따라 제소 당사국이 절차를 선택할 수 있으나, 어느 한 협정에 따라 패널 설치를 요청하거나 사안을 패널에 회부한 뒤에는 선택된 절차가 다른 절차를 배제하므로 청구 원인과 심사 기준을 함께 고려하여야 한다.[108]

아울러 한국은 관련 국제규범의 형성에도 능동적으로 참여할 필요가 있다. WTO 위원회와 통상협의, 자유무역협정 및 디지털무역협정의 논의에서 국가 연계 디지털 공급망 규제가 갖추어야 할 최소한의 투명성, 위험의 객관적 식별, 기밀정보의 취급, 특정허가와 위험완화, 시행 유예 및 주기적 재검토에 관한 공통원칙을 제안할 수 있다. 기술표준은 취약성의 존재와 관리 필요성을 확인하는 사실 자료로 활용하되, 특정 표준상 위험 관리 대상이라는 사실이 곧바로 국제관계상 긴급상황의 존재를 입증하는 것은 아니라는 구별도 유지하여야 한다.

한국의 이해는 안보예외의 범위를 단순히 넓히거나 좁히는 데 있지 않다. 한국 기업이 외국의 국적 중심적·포괄적 규제로부터 보호받을 수 있도록 객관적 심사기준을 요구하는 동시에, 한국이 실제 디지털 공급망 위험에 대응할 수 있는 합리적인 규제공간도 확보하여야 한다. 이를 위하여 필요한 것은 국가안보라는 추상적 명분이 아니라, 위험의 기술적

108) 대한민국과 미합중국 간의 자유무역협정 제22.6조, 제23.2조 및 각주 2 참조.

구조와 국제적 연계를 개별 조치 및 적용기간에 맞추어 입증하는 규제체계이다. BIS 최종 규칙 사례는 한국이 향후 수출국과 규제국의 양 지위에서 어떠한 법적 기준을 요구하고 스스로 준수하여야 하는지를 보여 준다.

참고문헌

1. 국내문헌

구모란, “WTO 안보예외 분쟁의 유형화와 대응전략에 관한 연구”, 「통상법무정책」 2026년 제1호(통권 제11호), 산업통상자원부, 2026.

김경우, “안보예외에서의 정보제공 거부 조항(GATT XXI(a))의 기원과 진화에 대하여”, 「국제경제법연구」 제23권 제1호, 한국국제경제법학회, 2025.

김보연, “국가안보 예외조항의 ‘자기판단’ 범위 — 국제법상 의미와 WTO 협정에의 적용”, 「국제경제법연구」 제17권 제2호, 한국국제경제법학회, 2019.

류예리, “미국 상호관세 협상에서의 경제안보와 지식재산권 보호 연계에 관한 연구”, 「국제거래와 법」 통권 제51호, 동아대학교 법학연구소, 2025.

윤여현(이재민 감수), “United States–Certain Measures on Steel and Aluminium Products (WT/DS544)”, 「통상법무정책」 2024년 제2호(통권 제8호), 산업통상자원부, 2024.

이동은, “이중용도 물품 수출통제에 관한 국제통상법적 고찰 — GATT 제21조(b)(ii)의 해석 및 적용을 중심으로”, 「통상법률」 2024년 제3호, 법무부, 2024.

정찬모, “WTO 안보예외 —「러시아-통과운송 제한 사건」 패널결정의 법리와 한국에의 함의”, 「국제법평론」 통권 제54호, 국제법평론회, 2019.

대한민국 외교부, 「1947년도 관세 및 무역에 관한 일반협정」 공식 국문 번역본.

2. 외국단행본·논문

Akande, Dapo & Sope Williams, “International Adjudication on National Security Issues: What Role for the WTO?”, 43 *Virginia Journal of International Law* 365 (2003).

Alexander, Klint W., “The 2022 U.S. Steel/Aluminum Tariff Ruling: A Legal Reckoning for the United States and the WTO over the National Security Exception in International Law”, 72(4) *American University Law Review* 1137 (2023).

Alford, Roger P., “The Self-Judging WTO Security Exception”, 2011 *Utah Law Review* 697 (2011).

Claussen, Kathleen, “Trade’s Security Exceptionalism”, 72 *Stanford Law Review* 1097 (2020).

Heath, J. Benton, “The New National Security Challenge to the Economic Order”, 129 *Yale Law Journal* 1020 (2020).

Kho, Stephen S., Yujin K. McNamara, Sarah B. W. Kirwin & Brooke Davies, “The Conundrum of the Essential Security Exception: Can the WTO Resolve the GATT Article XXI Crisis and Save the Dispute Settlement Mechanism?”, 40(1) *American University International Law Review* 127-195 (2024).

Pinchis-Paulsen, Mona, “Trade Multilateralism and U.S. National Security: The Making of the GATT Security Exceptions”, 41 *Michigan Journal of International Law* 109 (2020).

Pinchis-Paulsen, Mona, Kamal Saggi & Petros C. Mavroidis, “The National Security Exception at the WTO: Should It Just Be a Matter of When Members Can Avail of It? What About How?”, 23(3) *World Trade Review* 271-295 (2024).

Pauwelyn, Joost, *Conflict of Norms in Public International Law: How WTO Law Relates to Other Rules of International Law,* Cambridge University Press, 2003.

Peng, Shin-yi, “Cybersecurity Threats and the WTO National Security Exceptions”, 18(2) *Journal of International Economic Law* 449-478 (2015).

Schmitt, Michael N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Cambridge University Press, 2017.

Schmitt, Michael N., “Grey Zones in the International Law of Cyberspace”, 42 *Yale Journal of International Law Online* 1 (2017).

Trachtman, Joel P., “The Internet of Things Cybersecurity Challenge to Trade and Investment: Trust and Verify?”, SSRN Working Paper No. 3374542, 18 April 2019, https://ssrn.com/abstract=3374542.

3. 판정례·재판자료

ICJ, *Corfu Channel (United Kingdom v. Albania)*, Judgment, I.C.J. Reports 1949, p. 4.

United States, Third-Party Oral Statement, *Russia – Measures Concerning Traffic in Transit,* WT/DS512, 25 January 2018.

WTO, Appellate Body Reports, *Argentina – Measures Affecting the Importation of Goods,* WT/DS438/AB/R, WT/DS444/AB/R, WT/DS445/AB/R, adopted 26 January 2015.

WTO, Appellate Body Reports, China – *Measures Related to the Exportation of Various Raw Materials,* WT/DS394/AB/R, WT/DS395/AB/R, WT/DS398/AB/R, adopted 22 February 2012.

WTO, Appellate Body Report, European Communities – *Measures Affecting Asbestos and Asbestos-Containing Products,* WT/DS135/AB/R, adopted 5 April 2001.

WTO, Appellate Body Reports, *European Communities – Measures Prohibiting the Importation and Marketing of Seal Products,* WT/DS400/AB/R, WT/DS401/AB/R, adopted 18 June 2014.

WTO, Panel Report, *Russia – Measures Concerning Traffic in Transit,* WT/DS512/R and Add.1, adopted 26 April 2019.

WTO, Panel Report, *Saudi Arabia – Measures concerning the Protection of Intellectual Property Rights,* WT/DS567/R, circulated 16 June 2020, not adopted; dispute terminated 21 April 2022.

WTO, Panel Report, United States – *Certain Measures on Steel and Aluminium Products (China),* WT/DS544/R, circulated 9 December 2022, appeal notified 26 January 2023, not adopted.

WTO, Panel Report, United States – *Origin Marking Requirement (Hong Kong, China),* WT/DS597/R, circulated 21 December 2022, appeal notified 26 January 2023, not adopted.

4. 미국 법령·행정자료

United States, International Emergency Economic Powers Act, 50 U.S.C. § 1701 et seq. 15 C.F.R. pt. 791.

U.S. President, Executive Order No. 13873, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689, 17 May 2019.

U.S. Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909, 19 January 2021.

U.S. Department of Commerce, Bureau of Industry and Security, Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles (ANPRM), 89 Fed. Reg. 15066, 1 March 2024.

U.S. Department of Commerce, Bureau of Industry and Security, Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles (NPRM), 89 Fed. Reg. 79088, 26 September 2024.

U.S. Department of Commerce, Bureau of Industry and Security, Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 90 Fed. Reg. 5360 (15 C.F.R. pt. 791), 16 January 2025.

U.S. Congress, Connected Vehicle Security Act of 2026, S. 4429, 119th Cong. (2026).

U.S. Congress, Connected Vehicle Security Act of 2026, H.R. 8730, 119th Cong. (2026).

U.S. Congress, Motor Vehicle Modernization Act of 2026, H.R. 7389, 119th Cong. § 301 (2026).

U.S. Congress, National Defense Authorization Act for Fiscal Year 2027, S. 4784, 119th Cong. § 353 (2026).

[국문초록]

커넥티드 차량의 사이버-물리 위협과 GATT 제XXI조(b)(iii) 안보예외의 적용 한계

- 미국 상무부의 2025년 커넥티드 차량 최종규칙에 대한 '국제관계상 긴급상황' 요건의 적용을 중심으로 -

박자혜

미국 상무부 산업안보국(BIS)의 2025년 커넥티드 차량 최종규칙은 중국 또는 러시아에 의하여 소유·통제되거나 그 관할 또는 지시를 받는 주체가 설계·개발·제조·공급한 차량 연결시스템(VCS) 하드웨어와 대상 소프트웨어의 수입 및 거래를 제한한다. 이 규칙이 겨냥하는 위험은 구체적인 사이버공격이 현실화되지 않더라도 공급망 안에서 장기간 존속할 수 있는 기술적 취약성이다. 본고는 규칙에 포함된 두 수입금지를 각각 GATT 제XI조 제1항에 따라 검토한 뒤, 관련 WTO 패널보고서의 해석을 바탕으로 제XXI조(b)(iii)의 적용 가능성을 요건별·조치별로 분석한다.

현행 WTO 패널보고서의 해석 기준에 따를 때, 현재 공개된 규제 기록만으로는 두 수입금지가 제XXI조(b)(iii)에 따라 정당화되기 어렵다. BIS 자료는 민감정보 탈취와 군사·치안 관련 정보 수집의 위험을 근거로 필수적 안보이익을 일정 부분 특정하고, 각 수입금지와 그 이익 사이의 최소한의 개연성을 뒷받침할 수 있다. 그러나 관련 패널보고서는 국제관계상 긴급상황을 단일한 사건으로 한정하지 않으면서도, 국가 간 관계의 중대한 악화가 객관적으로 확인되고 그 상황이 국제관계에 미치는 영향이 전쟁과 적어도 비견될 정도로 중대하거나 심각할 것을 요구하였다. BIS 자료는 사이버-물리 위협의 기술적·사회적 중대성을 구체적으로 설명하지만, 관련 시점의 미·중 관계와 미·러 관계가 각각 이 중대성 기준을 충족하였다는 점까지 입증하지는 못한다. 따라서 위험의 사실적 중대성과 제XXI조(b)(iii)상 국제관계상 긴급상황의 존재는 구별되어야 한다.

본고는 이러한 현행법상 결론과 별도로, 지속적·구조적 취약상태를 장래의 안보예외 심사에 반영하기 위한 상시적 취약성(Persistent Vulnerability)을 향후 규범 형성론상의 분석틀로 제안한다. 이는 현행 조문의 확장해석을 통하여 미국 조치를 정당화하려는 기준이 아

니다. 이 개념을 적용하려면 객관적으로 확인할 수 있는 기술적 취약상태, 국가 연계 행위자의 능력·의도·접근 가능성에 기초한 국제관계상 연계, 전쟁과 적어도 비견될 정도의 국제관계상 중대성, 객관화된 상황의 지속성과 문제된 조치와의 시간적 관련성이 누적적으로 확인되어야 한다. 원용국은 각 표지를 입증하여야 하며, 주기적 재검토는 긴급상황의 식별 요소가 아니라 장기 조치의 지속적 적용을 통제하는 별도의 장치로 기능한다. 이러한 구분은 한국이 외국의 안보규제에 대응하고 국내 디지털 공급망 규제를 설계할 때 WTO 협정과 한미 FTA의 서로 다른 심사·분쟁해결 구조를 검토할 기준을 제공한다.

주제어: GATT 제XXI조, 안보예외, 국제관계상 긴급상황, 커넥티드 차량, 사이버-물리 위협, 상시적 취약성, BIS 최종규칙, 공급망 안보, 한미 FTA, 디지털 통상

[Abstract]

Cyber-Physical Threats Posed by Connected Vehicles and the Limits of the Security Exception under GATT Article XXI(b)(iii)

- The 2025 U.S. BIS Connected Vehicles Final Rule and the 'Emergency in International Relations' Requirement -

Jahye Park

The 2025 Connected Vehicles Final Rule issued by the U.S. Department of Commerce, Bureau of Industry and Security (BIS), restricts imports and transactions involving vehicle connectivity system (VCS) hardware and covered software designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of China or Russia. The Rule addresses technological vulnerabilities that may persist within a supply chain even when no discrete cyberattack has materialized. This article examines the Rule's two import prohibitions separately under GATT Article XI:1 and then assesses, requirement by requirement and measure by measure, whether they can be justified under Article XXI(b)(iii), using the relevant WTO panel reports as interpretative materials of differing procedural status.

Under current law, the two prohibitions are likely inconsistent with Article XI:1 and are unlikely to be justified under Article XXI(b)(iii) on the basis of the public regulatory record. The BIS record may identify certain essential security interests, particularly the prevention of sensitive-data exfiltration and the collection of military- or law-enforcement-related information, and may support a minimum degree of plausibility between each prohibition and those interests. The relevant panel reports do not confine an emergency to a single event, but they require an objectively observable grave deterioration in international relations. Under the threshold articulated in US–Steel, the impact on international relations must be at least comparable to that of war in gravity or severity. The BIS record explains the technical and social gravity of the cyber-physical threats, but it does not establish that U.S.–China and U.S.–Russia relations, considered separately at the relevant times, met that threshold. The factual gravity of a risk must therefore be dis-

tinguished from the legal existence of an emergency in international relations.

Separately from that conclusion, this article proposes Persistent Vulnerability as a framework for future rule development, not as an expansive interpretation that would justify the U.S. measures under existing law. Four cumulative indicia would be required: an objectively verifiable technological vulnerability; a nexus to international relations based on a state-linked actor's capability, intent, and access; an impact on international relations comparable to war in gravity or severity; and the persistence of the situation and a temporal connection between that situation and the measure at the relevant stages of adoption, application, and maintenance. The invoking Member would bear the burden of substantiating each indicium. Periodic review would operate not as an element identifying an emergency, but as a separate safeguard for the continuing application of a long-term measure. This distinction also provides a basis for Korea to compare the different review and dispute-settlement structures of the WTO agreements and the KORUS FTA when responding to foreign security regulation or designing its own digital-supply-chain measures.

Keywords: GATT Article XXI; security exception; emergency in international relations; connected vehicles; cyber-physical threats; persistent vulnerability; BIS Connected Vehicles Final Rule; supply chain security; KORUS FTA; digital trade