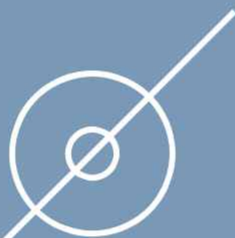


사이버 안보와 윤리



2023

〈요 약〉

인터넷의 등장과 사이버 공간의 확장은 사회의 발전과 인류의 진보를 그리는 낙관적 기대를 일부 실현하는 한편 사이버 위협에 대한 노출을 증가시키는 결과도 낳았다. 사이버 안보 문제가 국가 안보화되는 경향은 보편적으로 발견되며, 그 결과 정부가 사이버 위협에 대응하기 위해 취하는 조치는 국민의 프라이버시를 침해하거나 민주주의 가치를 훼손할 소지가 있어 논란을 일으킨다. 사이버 안보, 프라이버시, 민주주의 등은 모두 인간의 좋은 삶을 뒷받침하는 가치로서 이들이 충돌할 때 간단히 어느 하나를 선택하기는 어렵다. 즉, 다양한 가치를 평가하고 그 우열을 판단할 수 있도록 하는 윤리학이 사이버 안보에 적용될 필요가 있다.

본 연구는 주요한 윤리적 관점인 덕 윤리, 의무론, 결과론을 사이버 안보에 적용하여 특히 개인과 국가의 관계를 규정하는 원칙을 도출하는 데에 따르는 문제를 살펴보았다.

덕 윤리는 인간 품성과 지성의 훌륭한 상태인 덕, 다시 말해 중용을 기르고 실천하도록 가르치는 윤리이다. 이를 국가 지도자에 적용해 보면, 국가의 행복을 목표로 지혜, 용기, 관대함, 절제, 정의 등을 함양하고 행하는 것이 덕스러운 국가 지도자의 자세라고 할 수 있다. 특히 국가의 행복과 이를 구성하는 국가 구성원 개개인의 행복의 관계를 고려할 때, 사이버 안보, 프라이버시, 민주주의 등의 가치가 국가와 개인의 관계 속에서 충돌하는 경우에 지나치지도 모자라지도 않는 중용을 파악하고 실천하는 것이 주요한 과제일 것이다.

국가의 행복을 추구하는 국가 지도자의 덕과 개인의 행복을 추구하는 개인의 덕을 구분하는 덕 윤리와 달리 인간에게 보편적인 이성에 의해 절대적인 법칙이 도출될 수 있다고 주장하는 의무론적 윤리학은 모든 인간이 동일한 도덕적 의무를 진다고 본다. 거짓말을 하지 않거나 모든 인간을 목적으로 대하는 행동의 고결함은 분명하지만 그 결과의 선택이 보장되지 않는다는 점에서 국가 지도자가 의무론에 따라 사이버 안보 조치를 결정하고 실행해도 되는지 여부는 논의의 여지가 있다.

반면 결과론적 윤리학은 원칙이 아닌 예상되는 결과의 좋고 나쁨을 기준으로 삼는다. 가령功利주의는 최대 다수의 최대 행복을 기준으로 삼으며, 이는 기본적으로 개인의 행복을 염두에 두고 덕의 함양과 실천을 주장하는 덕 윤리와 달리 다수의 행복을 우선한다는 특징을 가진다. 따라서 소수의 희생이 수반되는 경우가 많으며, 다수의 행복을 위해 수용할 수 있는 희생의 범위나 정도를 판단하는 과제가 있다.

I. 서론

인터넷이 대중화되고 그에 따라 사이버 공간이 형성되던 시기에 적지 않은 이들이 새로운 정보통신 기술로 인해 사회가 발전하리라고 생각하였다.¹⁾ 소통의 방식과 수단이 변화하면서 인간의 삶이 달라지고 진보를 이루었던 역사적 경험을 고려할 때 이러한 낙관론은 당연했는지도 모른다. 문자의 발명과 인쇄술의 보급이 시대와 지역을 넘은 지식의 전파를 가능하게 하고 우편·전신·전화 기술과 제도의 발달이 정보의 교환을 촉진하였듯이, 온라인 네트워크를 통한 디지털 통신은 오프라인 공간이 지닌 지리적 거리나 정부의 규제와 같은 제약을 상당히 극복함으로써 사람들 사이의 연계를 확장할 수 있는 기회로 여겨졌다. 시공간의 한계로부터 비교적 자유로운 통신에 다수의 사람이 쉽게 참여하게 되면 정보의 양이 폭발적으로 증가할 것이고 그 결과 배우고 지식을 습득하며 새로운 정보를 생산하는 기회도 증가할 것이다. 또한 사회적 관계가 지리적으로 근접한 영역 내에 머물지 않고 확대됨으로써 공동체의 의미와 모습이 변화함과 동시에 대형 언론사나 정치권력의 도움 없이 개인이 대중에게 생각을 전달하거나 다수가 의견을 나눌 수 있게 되고 게다가 익명으로 소통하는 것이 가능해지면서 사회적 토론과 교류가 활발해지고 시민민주주의가 활성화하는 여건이 마련될 것이라는 기대가 있었다.

인터넷의 등장과 활용이 우리의 삶과 사회를 크게 바꾸었음은 분명하다. 지난 수십 년간 우리가 인식하고 사고하고 배우고 가르치고 소통하고 교류하고 생산하고 소비하고 일하고 즐기고 협력하고 경쟁하고 대립하는 방식과 범위는 급격히 달라졌고, 이러한 변화는 사이버 공간이 확장되는 과정과 서로 영향을 주고받으며 진행되었다. 사이버 공간은 우리 일상의 거의 모든 영역에 침투하였고, 특히 최근의 코로나19 위기로 인해 정보통신 기술을 활용하고 온라인 공간에 의존하는 정도가 급증하면서 디지털 대전환이 가속화되었다.

변화는 기대하던 발전과 번영만을 가져오진 않았다. 사이버 공간이 인간의 주된 활동 영역으로 자리 잡고 정보통신 기반 시설의 사회적 중요성이 증대함에 따라 인간의 삶은 사이버 위협에 더욱 취약해졌고 사이버 안보는 개인과 개별 기관의 디지털 기기와 네트워크, 데이터를 보호하는 문제에서 국가적 과제로 확대되었다. 에스토니아 주요 공공기관의 전산망을 대상으로 광범위하게 벌어진 2007년의 테러, 스텝스넷을 이용하여 이란의 핵 시설을 파괴한 2010년의 공격, 2016년 미국 대선을 겨냥하여 이루어진 러시아의 미국 민주당 이메일 계정 해킹과 문건 유출, 2022년 우크라이나에 대한 전면 침공 전부터 시작되어 이어지고 있는 러시아의 사이버 공격과 우크라이나의 대응은 국가 간 대립과 경쟁이 사이버 공격과 분쟁으로 표출된, 즉 사이버 공간이 군사안보 영역이 되고 사이버 안보가 국가적 사안이 되었음을 일깨우고 보여주는 사례 일부이다. 사이버 안보 문제의 국가 안보화는 여러 양상을 통해 보편적인 경향으로 확인된다. 많은 국가가 사이버 안보 기관을 설립하고, 사이버 안보 법 제정과 전략 및 정책 수립에 노력을 기울이며, 점점 더 많은 예산을 사이버 공간의 방어를 위해 사용하여 사이버 안보 정책 연구와 기술 개발을 지원하고 있다. 그 결과 촉발된 사이버 군비경쟁은 더욱 치열해지고 있고, 국가 안보 개념이 사이버 안보 담론을 장악하였다.

1) Kevin Kelly, *Out of Control: The New Biology of Machines, Social Systems, and the Economic World* (1992; repr., New York: Basic Books, 1995); Nicholas Negroponte, *Being Digital* (New York: Alfred A. Knopf, 1995); William J. Mitchell, *City of Bits: Space, Place, and the Infobahn*, rev. ed. (Cambridge, MA: MIT Press, 1996); Virginia Postrel, *The Future and Its Enemies: The Growing Conflict over Creativity, Enterprise, and Progress* (New York: Free Press, 1998); James Surowiecki, *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations* (New York: Doubleday, 2004).

국가 안보 차원에서 이루어지는 사이버 안보 활동이 실재하는 위협에 대응하는 필요한 조치임은 부인할 수 없다. 하지만 이러한 대처는 동시에 또 다른 위협을 초래하는 문제를 안고 있다. 가령 사이버 공격에 대처하고 네트워크 환경의 안전을 지키기 위한 사이버 검열과 감시는 프라이버시를 침해하고 사이버 공간에서의 익명성과 기밀성을 해침으로써 오히려 국민이 안심하고 누릴 수 있는 사이버 환경을 위태롭게 만들 소지가 있다. 국가 안보를 위한 조치가 안전을 도모하는 위험한 수단이 될 수 있다는 역설적 문제는 새로운 것이 아니다. 『국가』를 통해 플라톤은 풍요로운 국가를 만들고 침략을 막기 위해서는 전쟁을 전문적으로 수행할 수 있는 수호자가 필요하나 적에게 발휘되어야 하는 그들의 기개와 공격성이 동료 시민에게 향할 수 있음을 지적한다.²⁾

그렇다면 플라톤은 이 문제를 어떻게 해결할까. 훌륭한 수호자란 동료 시민에게는 온순하면서도 적에게는 사나워야 하고 따라서 친구와 적을 분별하는 지혜를 가져야 하며, 국가는 이를 위한 교육을 시행해야 한다고 그는 주장한다.³⁾ 국민에게 안전한 사이버 환경을 제공한다는 궁극적인 목적에 부합하는 훌륭한 사이버 안보 정책의 시행 역시 분별력을 요구한다. 우리는 안보 조치의 혜택과 잠재적인 해악을 파악하고 각각의 경중을 따져 적절한 방안을 모색할 수 있어야 한다. 그리고 이는 곧 득실의 경중을 가늠하는 데 적용할 기준의 수립, 다시 말해 사이버 안보와 관련된 가치를 고찰하고 이해하는 윤리적 논의가 필요함을 의미한다.

II. 사이버 안보 분야의 주요 가치와 가치 간 갈등

가치를 단순하고 간략하게 정의하면 좋은 것 또는 좋다고 여겨지는 것이라고 할 수 있다.⁴⁾ 가령 건강, 아름다움, 지혜, 정의와 같이 보편적으로 좋다고 생각되는 것들 말이다. 또한 바람직하기에 추구해야 하는 것으로서 많은 경우 특정한 개인이나 집단이 이상으로 좇는 것도 가치라고 불린다. 서구적 가치로 흔히 꼽히는 자율성, 민주주의, 자본주의 등을 예로 들 수 있다.

가치와 연관된 분야 중 하나는 규범적 영역, 즉 있는 그대로의 사실을 서술하는 실증적 분석과 대조적으로 무엇을 해야 하는지에 관한 주장에 관계된 영역이다. 일반적으로 규범적 영역은 가치를 포괄하는 것으로 여겨진다.⁵⁾ 분명 우리가 해야 하는 것 또는 하지 말아야 하는 것에 관한 규정의 다수는 무엇이 좋거나 또는 나쁘다는 가치 판단에 기초한다. 정직은 좋은 것이기에 진실을 말해야 하고 거짓말은 하지 말아야 한다는 식으로 말이다. 그리고 해야 하는 것과 하지 말아야 하는 것에 대한 논란이 지속되는 데에는 가치 판단에서의 합의가 부재한 문제가 일부 작용한다. 일견 좋고 나쁜 것은 명백한 듯하지만, 설사 그 명백함을 받아들인다 해도 좋은 것도 나쁜 것도 적지 않기 때문에 그중 더 좋은 것과 더 나쁜 것을 가리는 과정에 이견이 발생하게 마

2) 372e-75c

3) 375c-76c. 로크의 표현을 빌리자면, 족제비와 여우의 해악을 피하겠다고 온갖 궁리를 하면서 사자에게 삼켜지는 걸 안전하다고 여기며 태평할 만큼 인간은 어리석지 않기에 안전을 위한 특정한 조치가 가지고 있는 위험을 배제하기 위한 노력을 할 것이다(Second Treatise, §93).

4) Christine Tappolet and Mauro Rossi, "What Is Value? Where Does It Come From? A Philosophical Perspective," in *Handbook of Value: Perspectives from Economics, Neuroscience, Philosophy, Psychology, and Sociology*, ed. Tobias Brosch and David Sander (Oxford: Oxford University Press, 2016).

5) Jonathna Dancy, ed., *Normativity* (Oxford, UK: Blackwell, 2000); Michael J. Zimmerman, "Value and Normativity," in *The Oxford Handbook of Value Theory*, ed. Iwao Hirose and Jonas Olson (Oxford: Oxford University Press, 2015).

런이다. 결국 가장 좋은 것을 해야 하고 가장 나쁜 것을 피해야 한다고 말할 수 있지만, 최선과 최악에 관한 보편적 합의를 도출하는 것은 물론 개인적으로 판단을 내리는 것조차 쉽지 않다. 만약 어느 독재자가 내 부모를 감금한 채 무고한 이를 붙잡아 오지 않으면 부모를 해치겠다고 위협하며 명령한다면, 이 상황에는 가족, 정의, 생명 등 여러 가치가 걸려 있으며 생명에 있어서도 가족의 생명과 무고한 타인의 생명을 동등하게 여겨야 하는지, 그렇지 않다면 그 차이는 어느 정도인지 판단하여 최종적으로 가장 좋은 가치는 무엇인지 가려내야 하는 과제를 안게 된다.⁶⁾

이미 시사하였듯이 사이버 안보와 관련된 가치도 한 가지가 아니다. 우선 위험과 위협으로부터의 자유를 의미하는 안보를 가치라고 할 수 있으며, 안보는 생명과 안전 등의 가치를 내포하거나 이에 연관된다. 사이버 공간에서의 안보에 한정하여 보아도 이를 개인의 사이버 안보, 기업 등 기관의 사이버 안보, 국가의 사이버 안보로 나눌 수 있으며, 정보 안보, 데이터 안보 등과 연관된다. 사이버 안보를 정보통신 서비스와 시스템을 보호하고 이에 대한 해를 막는 것이라고 정의하고⁷⁾ 정보 안보를 정보와 정보 시스템을 보호함으로써 정보의 가용성, 무결성, 기밀성을 유지하는 것이라고 할 때,⁸⁾ 사이버 안보는 사이버 공간에 저장되거나 사이버 공간을 통해 전송되는 정보의 안보와 겹치는 부분이 있을 것이다.

게다가 정보 안보가 정보의 가용성, 무결성, 기밀성 유지를 목적으로 함을 고려할 때, 사이버 안보와 관련된 또 다른 가치, 프라이버시에 주목하게 된다. 프라이버시는 사이버 테러 및 공격 방지를 위해 정보를 수집하거나 사이버 위협을 감시하는 과정에서 침해될 수 있는 가치로서 흔히 거론되며, 세계인권선언을 비롯한 여러 인권 조약에 의해 기본적인 권리로 인정받고 있다.⁹⁾ 특히 유엔 총회나 인권이사회는 여러 차례 「디지털 시대 프라이버시 권리에 관한 결의」를 채택한 바 있고, 이에 따르면 프라이버시는 인간이 타인, 타 기관, 정부 등의 간섭 없이 자유롭게 영위하고 교류할 수 있는 사적 영역으로 이해된다.¹⁰⁾ 그리고 이중 어떤 종류의 간섭과 침해를 우려하고 경계하느냐에 따라서 프라이버시는 각기 다른 가치와 연계되는 모습을 보인다. 즉, 정부의 침해로부터 시민의 사적 영역을 지키려는 이들에게 프라이버시는 자유와 자율성의 문제로 이해되고, 개인들 간의 교류나 회사와 같은 사기관과 개인 사이의 관계 속에서 사적 영역이 위축되는 문제에 집중하는 이들에게 프라이버시는 인간 존엄과 깊이 연관된 가치로 여겨진다.¹¹⁾ 또한 사적 영역의 부문 또는 유형에 따라서도 각각의 프라이버시와 연관되는 가치는 다르다. 쿽스 등에 따르면 프라이버시는 신체 프라이버시(bodily privacy), 지적 프라이버시(intellectual privacy), 공간 프라이버시(spatial privacy), 결정 프라이버시(decisional privacy), 소통 프라이버시(communicational privacy), 결사적 프라이버시 (associational privacy), 재산 프라이버시(proprietary privacy), 행동 프라이버시(behavioral privacy)로 나눌 수 있으며, 이들을 모두

6) Plato, *Apology*, 32c-e; Aristotle, *Nicomachean Ethics*, 3.1.1110a6-8.

7) <https://csrc.nist.gov/glossary/term/cybersecurity>

8) <https://csrc.nist.gov/glossary/term/infosec>

9) 세계인권선언 12조; 시민적 및 정치적 권리에 관한 국제규약 17조; 유럽인권조약 8조; American Convention on Human Rights 11조; 유엔아동권리협약 16조; 모든 이주노동자와 그 가족의 권리보호에 관한 국제협약 14조

10) U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (Dec. 18, 2014); U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/28/L.27 (Mar. 24, 2015); U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/71/199 (Dec. 19, 2016).

11) Ibo van de Poel, "Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security," in *The Ethics of Cybersecurity*, eds. Markus Christen, Bert Gordijn, and Michele Loi (Cham, Switzerland: Springer Open, 2020), 55.

관통하면서 별도의 영역을 가진 정보 프라이버시(informational privacy)가 있다.¹²⁾ 이중 사이버 안보와 가장 연관된 것으로 보이는 정보 프라이버시의 핵심은 개인정보의 보호, 다시 말해 개인정보의 기밀성을 유지하고 개인정보에 대한 통제를 확보하는 것이다.¹³⁾ 즉, 프라이버시와 사이버 안보는 기밀성이라는 공통의 가치를 가지면서 때론 대립하는 셈이다.

정부 활동에 의한 프라이버시와 자유의 침해 문제는 사이버 안보와 연관된 또 다른 가치가 있음을 시사한다. 바로 민주주의다. 가령 사이버 폭력과 테러에 대응하는 방안으로 논의되는 인터넷 실명제와 같은 조치는 표현의 자유와 정치 참여의 자유를 비롯한 시민적 자유와 정치적 자유를 침해할 소지가 있다. 그리고 사이버 안보, 특히 국가 사이버 안보를 도모하기 위한 정부의 활동이 종종 비밀스럽게 이루어지는 점을 고려할 때, 이는 법적·제도적 절차를 어긴, 민주적으로 정당하지 못한 행위일 가능성이 있다. 요컨대 말이 주목하고 탐구했던 자유와 공적 권위 사이의 다툼이 디지털판으로 이어지고 있는 셈이다.¹⁴⁾ 한편 사이버 안보가 훼손됨으로써 민주주의가 위협받는 일도 있다. 2016년 미국 대선 기간에 일어난 민주당 이메일 계정 해킹과 가짜뉴스의 광범위한 유포가 대표적인 사례다. 즉, 안전한 디지털 공간의 조성은 우리가 표현의 자유와 결사의 권리를 누릴 수 있는 민주적인 환경을 만들기 위함이기도 하지만, 안보 조치가 민주주의를 해치기도 한다.

민주주의와 사이버 안보의 이같이 복잡한 관계는 사이버 안보를 둘러싼 가치 갈등의 문제를 해결하기 어려운 이유 중 하나를 보여준다. 표현의 자유를 억압한다고 해서 인터넷상의 발언과 활동에 아무런 제약을 두지 않는다면 가짜뉴스와 흑색선전이 판치면서 도리어 민주적 절차를 왜곡할 수 있기에, 민주주의와 사이버 안보의 갈등은 두 가치를 비교하고 어느 가치가 더 좋은 것인지 가늠하는 것만으로 해결할 수 없다. 사이버 안보와 프라이버시의 관계 역시 이러한 복잡한 성격을 지닌다. 위에서 예로 든 인터넷 실명제는 개인정보의 기밀성과 개인정보에 대한 통제권을 모두 위협하는 한편 무분별한 폭로와 허위 유포로부터 개인의 존엄과 명예, 프라이버시를 보호하는 측면도 있다. 게다가 인터넷 실명제의 사례는 사이버 안보와 관련된 가치 갈등이 일대일의 형태로만 일어나지 않음을 드러낸다. 이 사안에서 사이버 안보, 민주주의, 프라이버시가 모두 복합적인 관계로 얽혀 있고, 추측건대 두 가치를 비교하고 가늠하기보다 셋 이상의 가치를 고려하여 최선과 차선을 가려내기는 더 어려울 것이다.

그런 한편 사이버 안보와 관련 가치의 관계는 하나의 가치, 즉 안심하고 살아가는 삶으로 귀결된다고도 볼 수 있다. 프라이버시와 민주주의는 그 자체로 좋은 가치이지만 우리가 평온하게 사는 데 필요한 가치이기도 하기 때문이다. 우리의 생존과 안전을 해치는 위험은 여러 근원에서 비롯되어 다양한 형태로 나타나며, 따라서 그 대처도 다양한 방식으로 이루어진다. 범죄, 테러, 외침으로부터 우리를 지키는 데에는 경찰과 군대가 유용하지만, 폭력적이고 부당한 공권력에 맞서 우리의 생명과 재산을 보호하려면 스스로 생각하고 판단하며 행동할 수 있는 자율성과 자유가 중요한 힘이 된다. 그렇다면 사이버 안보 조치에 의해 프라이버시와 민주주의가 침해되는 경우, 이는 세 가치의 갈등과 충돌인 동시에 우리의 평안한 삶이라는 가치를 구성하는 여러 가치의 균형이 깨어진 문제이기도 하다. 즉, 사이버 검열과 감시로 인해 디지털 공간에서의 프라이버시와 시민적 자유가 위축될 때 우리는 사이버 안보를 위한 활동이 오히려 우리의 사이버 안보를 저해하는 사이버 안보 딜레마에 직면한다.

12) Bert-Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tomislav Chokrevski, and Maša Galič, "A Typology of Privacy," *University of Pennsylvania Journal of International Law* 38, no. 2 (Spring 2017).

13) Van de Poel, "Core Values and Value Conflicts in Cybersecurity," 53.

14) John Stuart Mill, *On Liberty*.

사이버 안보 딜레마는 국제적 수준의 문제이기도 하다. 일반적인 안보 딜레마가 발생하는 과정과 마찬가지로 한 국가가 취하는 사이버 안보를 위한 노력과 행동은 다른 국가의 불안을 자극하여 사이버 안보 활동을 하게끔 유도하고 결과적으로 두 국가 사이의 불안과 안보 조치의 연쇄를 일으키면서 사이버 안보를 저해하는 역설적 결과를 낳는다. 더욱이 위에서 언급했듯이 국가 사이버 안보를 위한 정부 활동이 비밀스러운 경우가 많다는 점을 고려하면, 사이버 안보 딜레마는 국민이 지지하거나 승인하기는커녕 알지도 못했던 정책의 비용과 결과를 감당해야 하는 불의의 소지를 안고 있으며 투명성, 민주적 책임성 등의 가치와도 연결된다.¹⁵⁾

III. 사이버 안보 윤리의 필요

여러 가치의 충돌 또는 하나의 가치를 뒷받침하는 세부 가치들 사이의 불균형은 가치에 대한 탐구로서 윤리학이 필요함을 의미한다. 윤리학은 인간의 행위와 인간 사이의 관계에 있어서 옳고 그름을 규정하는 문제를 다루며, 자연히 규범적 논의가 포괄하는 가치에 관해서 연구한다.

가치 갈등과 연관해서 우리가 고찰할 수 있는 점 하나는 가치의 유형이다. 위의 서술에서 드러나듯이 가치는 그 자체로서 좋은 내재적 가치와 다른 좋은 것을 성취하는 데에 유용한 도구적 가치로 나뉜다. 그리고 많은 가치가 내재적 가치인 동시에 도구적 가치의 성격도 갖는다. 가령 건강과 진리는 그로부터 파생되는 결과와 관계없이 그 자체로 좋은 것이지만 행복한 삶에 이바지하는 가치이기도 하다. 일반적으로 내재적 가치가 도구적 가치보다 더 좋고 귀중한 것으로 여겨지며, 따라서 도구로서가 아니라 어느 경우에도 오직 그 자체로만 좋은 것, 즉 내재적 가치이기에 한 것을 최상의 가치이자 최고선이라고 할 수 있다. 아리스토텔레스에 따르면, 행복은 언제나 그 자체로 좋고 선택되는 가장 가치 있는 최고선이고, 명예, 즐거움, 미덕 등은 그 자체로 좋으면서도 행복을 위해 선택되는 가치이다.¹⁶⁾ 요컨대 순수한 내재적 가치, 유용하기도 한 내재적 가치, 도구로서 유용하기만 한 가치의 순서로 가치의 등급을 매길 수 있다.

이 등급을 사이버 안보와 이에 연관된 가치에 적용하면 어떨까. 일단 각각의 등급을 판단해보자. 사이버 안보의 경우 도구적으로 유용한 가치로 보인다. 안전한 네트워크 환경과 기기는 그 자체로 좋은 것이라기보다 그것이 개인의 활동과 삶, 기관의 운영과 이익, 사회의 유지와 작동에 이바지할 수 있기에 가치로 간주된다. 범죄자의 휴대전화에 접근하거나 테러 조직의 네트워크를 공격한다고 해서, 이를 침범해서는 안 되는 절대적인 가치를 훼손한 행위, 가령 인간 존엄을 부정하는 고문과 같은 것으로 보기는 어렵다. 하지만 사이버 안보를 도구적 가치로 간단히 결론 내리기 전에 추가로 고려해야 할 점이 있다. 앞서 언급했듯이 사이버 안보는 개인 사이버 안보, 기관 사이버 안보, 국가 사이버 안보 등으로 나뉜다. 그리고 사이버 안보의 세부 유형도 모두 수단으로서 유용한 것으로 판단한다 해도 각 가치의 경중은 같지 않을 수 있다. 특히 개인 사이버 안보와 기관이나 국가 사이버 안보를 비교하면, 기관 및 국가 사이버 안보의 가치는 결국 개인의 삶과 안전을 지키는 데에서 비롯되기에 개인 사이버 안보가 우선한다고 여겨진다. 그러나 개인 사이버 안보의 우위가 절대적이라고 할 수는 없다. 개개인의 안전과 사회적 질서를 위해서 개인의 자유가 일정 부분 제한되듯이, 개인적 가치와 사회적 가치는 적절한 조율을 통해 균형을

15) Andrew N. Liapopoulos, "Reconceptualising Cyber Security: Safeguarding Human Rights in the Era of Cyber Surveillance," in *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*, by Information Resources Management Association, vol. 1 (Hershey, PA: IGI Global, 2018), 18-19.

16) Aristotle, *Nicomachean Ethics*, 1.1.1094a1-1.2.1094a23, 1.7.1097a32-b7.

이루어야 하는 관계로 볼 수 있다.

프라이버시의 경우, 앞서 언급했듯이 내재적 가치인 동시에 도구적 가치인 양면적 성격을 지니며, 프라이버시가 인간의 자유, 자율성, 존엄과 관련된 가치임을 고려할 때 그 관련성을 어떻게 이해하느냐에 따라서 어느 측면이 강한지에 관한 판단이 달라진다. 즉, 자유롭고 존엄한 존재로서 자율적으로 살아가는 인생을 위한 수단으로 간주한다면 프라이버시는 도구적 가치에 가깝다고 할 수 있지만 이를 대체할 수단이 마땅치 않다는 점을 생각하면 존엄하고 자율적인 삶을 구성하고 성립시키는 내재적 가치로 볼 수도 있다.

민주주의 가치 역시 비슷하다. 정부를 구성하고 국가를 통치하는 다양한 방식 중 하나로서 민주주의는 (비록 비효율적이고 다수의 폭정으로 왜곡될 수 있는 단점을 갖고 있지만) 국민 개개인의 자유롭고 평등한 삶을 가장 잘 보장할 수 있는 제도라고 할 수 있다. 그런 한편 자신의 공동체를 다스리는 규율을 만들고 집행하는 과정에 참여하는 활동이 인간다운 삶의 본질이라고 한다면 민주주의는 분명 내재적 가치기도 하다.

사이버 안보가 유용함이 두드러지는 가치인 것과 달리 프라이버시와 민주주의가 도구적 가치이면서 내재적 가치라는 점은 이들의 관계가 기본적으로 프라이버시와 민주주의를 위해서 사이버 안보가 필요한 구도임을 시사한다. 물론 개인 사이버 안보와 프라이버시가 중첩되고 사이버 안보, 프라이버시, 민주주의의 목적이 안전하고 평온한 삶으로 수렴된다는 것을 상기하면 사이버 안보에 대한 다른 두 가치의 절대적 우위를 주장하기는 어려우며, 따라서 여러 가치에 관한 더욱 세밀한 윤리적 논의가 필요하다.

그러나 국가 안보화되고 있는 사이버 안보 영역에서 윤리적 논의와 원칙이 필요한지에 대해 의문을 제기하는 이들도 있을 것이다. 특히 “어떤 방법이든 방어에 성공했다면 적절하다”라는 마키아벨리의 주장에 동조하는 이들이라면 국가 안보를 위한 정책과 활동에 대해서 윤리적 원칙에 근거한 제약이 가해지는 것은 온당치 못하며 그렇기에 윤리적 고찰은 무의미하다고 주장할 법하다.¹⁷⁾ 하지만 흔히 현실주의라고 칭해지는 이러한 관점에도 가치 판단이 함축되어 있다. 방어를 강조하는 마키아벨리가 지향하는 목표는 정치적 공동체의 생존과 번성인데 같은 이유로 그는 자유에도 주목한다. “오직 자유로운 상태에서만 도시가 영토와 부의 증대를 이룩한다”라는 신념으로 그는 도시의 생존과 자유란 절대적인 가치이며 이를 지키기 위해서라면 수단의 정당함과 고귀함은 제쳐 두어야 한다고 주장한다.¹⁸⁾ 마찬가지로 홉스가 리바이어던에 막강한 권한을 부여하고 그 권위에 대한 국민의 저항을 부정할 데에는 리바이어던의 부재가 생존에 가하는 위협이 리바이어던이 끼치는 위해보다 더 크며 생존은 절대적인 가치라는 판단이 자리한다.¹⁹⁾ 다시 말해, 이들은 가치를 가능하고 옳고 그름을 가리는 윤리적 논의를 전적으로 부정하기보다는 특정한 가치(생존 또는 생존과 자유)를 침범할 수 없는 것으로 여기는 관점을 지녔다고 할 수 있다. 그리고 홉스나 마키아벨리의 관점을 단순히 거부하는 대신 그들과 같은 견해를 가진 이들을 향해 우리가 지켜야 하는 삶의 모습과 그 삶을 지키는 좋은 수단이 무엇인지를 질문함으로써 다양한 가치관과 윤리적 관점을 비교하는 논의를 시작할 수 있을 것이다.

IV. 윤리적 관점과 적용

17) Niccolò Machiavelli, *Discourses on Livy*, 3.41.

18) Machiavelli, *Discourses*, 2.2, 3.41.

19) Thomas Hobbes, *Leviathan*, chap.18.

본 장에서는 주요한 윤리적 관점인 덕 윤리, 의무론, 결과론을 각각 사이버 안보 영역의 국가와 개인의 관계에 적용하고자 한다.

1. 덕 윤리

덕 윤리학의 흐름을 거슬러 올라가면 아리스토텔레스에 이른다. 아리스토텔레스는 모든 행위에 목적이 있으며 인간의 모든 행위가 궁극적으로 지향하는 목표가 있다고 보았다. 인간의 궁극적 목표, 다시 말해 최고선이 행복임은 대부분 동의할 수 있을 것이다. 문제는 행복이 무엇인지에 관해 제각각 다른 견해를 갖고 있다는 점이다. 기존의 견해가 부분적으로 타당하지만 충분하지 않다고 본 아리스토텔레스는 행복을 영혼의 덕스러운 행위라고 정의하였다. 즉, 행복하게 잘 살 고자 한다면 우리는 영혼의 덕을 함양해야 한다. 덕은 영혼의 훌륭한 상태, 지나치지도 모자라지도 않은 중용으로 용기, 관대함, 절제, 정의, 정직 등을 들 수 있다. 그리고 아리스토텔레스에 따르면, 행복하다고 일컬을 수 있는 덕스러운 사람의 덕스러운 행위는 용기, 관대함, 절제, 정의, 정직을 그저 행하는 것이 아니라 덕 그 자체를 목적으로 삼아 올바른 방식으로 이루어지는 행위다. 가령 타인의 칭찬을 바라고 또는 비난을 두려워해서 전투에 적극적으로 나선다면 이는 용기 있는 사람의 용기 있는 행위가 아니다. 요컨대 행위를 하는 사람의 마음가짐과 행위의 방식이 행위의 성격에 영향을 미친다.²⁰⁾

덕 윤리는 덕을 기르고 실천하도록 유도하는 최종적인 목적이 개인의 행복에 있다는 점에서 강력하고 현실적인 관점이다. 또한 중용의 덕이라는 개념은 해당 상황에서 지나치지도 모자라지도 않는 적절함을 찾게끔 하는 유연함과 실용성을 가진다.

기본적으로 개인의 윤리인 덕 윤리를 사이버 안보 영역의 국가와 개인의 관계에 어떻게 적용할 수 있을까? 아마도 국가 지도자의 덕을 고려해볼 수 있을 것이다. 즉, 국가 지도자는 국가의 행복을 목적으로 지혜, 용기, 절제, 정의를 함양하고 올바르게 실천해야 하며, 사이버 안보와 프라이버시가 충돌하는 것과 같은 상황에서 중용을 파악하고 행해야 한다고 볼 수 있다. 그리고 궁수가 활을 정확히 쏘기 위해서는 과녁을 바르게 알아야 한다는 아리스토텔레스의 말처럼 중용을 파악하려면 목적을 바르게 이해해야 한다. 특히, 안보, 자유, 민주주의와 같이 우리 삶에 중대한 가치들이 국가와 개인의 관계 속에서 충돌할 때는 더욱 그러하다. 국가의 행복이란 결국 국가 속에 사는 개개인의 안녕과 복으로 귀결되는데, 국가 안보적 조치가 개인의 권리와 충돌한다면 어떤 선택이 국가의 행복에 기여하는 것일까? 요컨대 덕스러운 국가 지도자의 역할이란 국가의 행복을 구성하는 본질이 무엇인지 이해하고 이를 달성하기 위한 올바른 방식과 수단을 파악하여 실행에 옮기는 것이다.

2. 의무론

의무론적 윤리학을 펼친 대표적인 학자는 칸트다. 그는 인간이 공통으로 가지고 있는 이성을 활용하여 도덕 법칙, 다시 말해 의무로서 수행해야 하는 절대적인 법칙인 정언명령을 도출할 수 있다고 믿었다. 정언명령은 그 자체로 선행하고 옳은 행동을 지시하기 때문에 행동의 결과와 관계 없이 따라야 하며, 그런 점에서 행동의 결과를 가늠하여 선택해야 한다는 결과론적 윤리학의 가

20) Aristotle, *Nicomachean Ethics*.

르침과 대조된다.²¹⁾

정언명령은 절대적이고 무조건적인 의무이기에 모든 이에게 동일하게 적용된다. 즉, 덕 윤리의 경우, 국가 지도자의 덕과 평범한 시민의 덕이 (각각이 처한 위치와 맡은 역할이 다르기에) 다르다고 주장할 수도 있지만, 의무론은 공직을 수행하는지 여부가 우리가 마땅히 선택하고 실천해야 하는 행위가 무엇인지를 결정하지 않는다고 본다.

이성으로 도출한 보편적 법칙에 대해 일단 합의가 이루어진다면, 의무론에 따라 우리가 해야 하는 바는 명확하며 이는 분명 의무론의 장점 중 하나이다. 하지만 추상적인 도덕 법칙 몇 가지만을 토대로 사이버 안보, 프라이버시, 민주주의가 얹히고 충돌하는 다양한 상황들을 헤쳐 나갈 방안을 모색하기란 쉽지 않을 것이다. 그리고 이상적인 원칙을 엄격하게 적용한 결과의 선택이 보장되지 않는 점도 간과할 수 없다. 국가를 이끄는 지도자가 자신의 이성과 양심에 따라 행동한 대가를 다수의 국민이 치르는 것은 옳은 일일까? 오히려 그가 지도자의 의무를 다하지 못했다고 할 수 있지 않을까?

3. 결론론

반면 결론론은 행동에 결과에 주목하고 결과의 좋음을 적절한 행동이 무엇인지 판단할 기준으로 삼는다. 결론론적 윤리학의 잘 알려진 유형 중 하나인 공리주의는 최대 다수의 최대 행복을 가장 좋은 결과로 여기는 관점이다. 행복을 추구한다는 점에서 덕 윤리와 유사하면서도 기본적으로 개인의 행복을 염두에 둔 덕 윤리와 달리 다수의 행복을 목적으로 한다는 특징이 있다.²²⁾

그렇기에 공리주의자는 자신의 행복만이 아니라 타인의 행복도 추구할 것이다. 예를 들어 적절한 사이버 안보 조치를 결정해야 하는 상황에서 공리주의자인 국가 지도자라면 해당 조치의 영향을 받는 국민 모두의 행복을 고려할 테고, 이는 의무론을 따르면서 국민이 피해를 당할 가능성을 감수하는 지도자에 비해 책임감 있는 태도를 취하는 것으로 여겨질 수 있다. 또한 다양한 대안의 효용과 비용을 가늠하여 최적의 결과를 도출하는 윤리적 사고는 인공지능도 배우고 실천할 수 있을 것으로 보인다. 사이버 위협을 측정하고 이에 대응할 윤리적인 방안을 채택하는데에 인공지능을 활용할 수 있다는 뜻이다.

하지만 다수의 행복을 목적으로 삼는다는 것은 다수의 효용을 위해 소수의 희생을 요구할 수 있음을 내포한다. 이는 절대적인 의무를 지시하고 인간을 수단으로 취급해서는 안 된다고 주장하는 의무론에 의해서는 발생하지 않는 문제이다. 물론 공동체를 구성하여 살아감으로써 모든 개인은 자신의 권리에 대한 일정한 제약을 받아들일 수밖에 없으며, 이러한 맥락에서 다수의 행복을 위한 소수의 희생도 어느 정도 납득할 수 있을지 모른다. 그러나 수용할 수 있는 희생의 범위는 어디까지일까? 그 범위가 명확하지 않다면 여러 가치가 충돌하는 상황에서 자신의 행복과 아울러 다수의 행복을 고려해야 하는 통치자가 중립적인 입장을 유지하며 적절한 판단을 내리기란 쉽지 않을 것이다.

V. 결론

21) Immanuel Kant, *Groundwork of the Metaphysics of Morals*.

22) John Stuart Mill, *Utilitarianism*.

사이버 안보 문제가 국가 안보화되는 경향은 보편적으로 발견되며, 그 결과 정부가 사이버 위협에 대응하기 위해 취하는 조치는 국민의 프라이버시를 침해하거나 민주주의 가치를 훼손할 소지가 있어 논란을 일으킨다. 사이버 안보, 프라이버시, 민주주의 등은 모두 인간의 좋은 삶을 뒷받침하는 가치로서 이들이 충돌할 때 간단히 어느 하나를 선택하기는 어렵다. 즉, 다양한 가치를 평가하고 그 우열을 판단할 수 있도록 하는 윤리학이 사이버 안보에 적용될 필요가 있다. 본 연구는 주요한 윤리적 관점인 덕 윤리, 의무론, 결과론의 특징과 장단점을 분석함으로써 각각이 사이버 안보 윤리로서 기능할 수 있는 가능성을 살펴보았다.

〈참고문헌〉

- Arisototle. *Nicomachean Ethics*. Translated by C. D. C. Reeve. Indianapolis: Hackett, 2014.
- Chatterjee, Deen K., ed. *The Ethics of Preventive War*. New York: Cambridge University Press, 2013.
- Christensen, M., B. Gordijn, and M. Loi, eds. *The Ethics of Cybersecurity*. New York: Springer Open, 2021.
- Dancy, Jonathan, ed. *Normativity*. Oxford, UK: Blackwell, 2000.
- Demy, T., and George Lucas. *Military Ethics and Emerging Technologies*. London: Routledge, 2013.
- Douglas, D. M. "Toward a Just and Fair Internet: Applying Rawls's Principles of Justice to Internet Regulation." *Ethics of Information Technology* 17, no. 1 (2015): 57-64.
- Eberle, Christopher. "Just War and Cyber War." *Journal of Military Ethics* 12, no. 1(2013): 54-67.
- Fabre, Cecile, and Seth Lazar, eds. *The Morality of Defensive War*. Oxford: Oxford University Press, 2014.
- Floridi, L. *The Ethics of Information*. Oxford: Oxford University Press, 2013.
- Graham, David E. "Cyber Threats and the Law of War." *Journal of National Security Law* 4, no. 1 (2010): 87-102.
- Gross, Michael, and Tami Meisels. *Soft War: The Ethics of Unarmed Conflict*. Cambridge: Cambridge University Press, 2016.
- Hobbes, Thomas. *Leviathan*. Edited by Richard Tuck. Cambridge: Cambridge University Press, 1991.
- Kant, Immanuel. *Groundwork of the Metaphysics of Morals*. Translated by Mary Gregor. Cambridge: Cambridge University Press, 1998.
- Kelly, Kevin. *Out of Control: The New Biology of Machines, Social Systems, and the Economic World*. 1992. Reprint, New York: Basic Books, 1995.
- Koops, Bert-Jaap, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tomislav Chokrevski, and Maša Galič, "A Typology of Privacy," *University of Pennsylvania Journal of International Law* 38, no. 2 (Spring 2017).
- Liaropoulos, Andrew N. "Reconceptualising Cyber Security: Safeguarding Human Rights in the Era of Cyber Surveillance." In *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*. By Information Resources Management Association. Vol. 1 Hershey, PA: IGI Global, 2018.
- Locke John. *Two Treatises of Government*. Cambridge: Cambridge University Press, 1988.
- Lucas, George. *The Ethics of Cyber Warfare*. New York: Oxford University Press, 2017.
- Machiavelli, Niccolò. *Discourses on Livy*. Translated by Harvey C. Mansfield and Nathan Tarcov. Chicago: University of Chicago Press, 1996.

-
- Manjikian, M. Cybersecurity Ethics: An Introduction. London: Routledge, 2017.
- Mill, John Stuart. On Liberty, Utilitarianism, and Other Essays. Edited by Mark Philp and Frederick Rosen. Oxford: Oxford University Press, 2015.
- Miller, S., and T. Bossomaier. Ethics and Cyber Security. Oxford: Oxford University Press, 2019.
- Mitchell, William J. City of Bits: Space, Place, and the Infobahn. rev. ed. Cambridge, MA: MIT Press, 1996.
- Moore, A. D., ed. Privacy, Security, and Accountability: Ethics, Law, and Policy. London: Rowman & Littlefield International, 2016.
- Negroponte, Nicholas. Being Digital. New York: Alfred A. Knopf, 1995.
- Nissenbaum, H. "Where Computer Security Meets National Security." Ethics and Information Technology 7, no. 2 (2005): 61-75.
- Nissenbaum, H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford University Press, 2009.
- O'Meara, Richard M. Governing Military Technologies in the 21st Century: Ethics and Operations. New York: Palgrave Macmillan, 2014.
- Plato. Complete Works. Edited by John M. Cooper. Indianapolis: Hackett, 1997.
- Postrel, Virginia. The Future and Its Enemies: The Growing Conflict over Creativity, Enterprise, and Progress. New York: Free Press, 1998.
- Surowiecki, James. The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations. New York: Doubleday, 2004.
- Taddeo M., and L. Glorioso, eds. Ethics and Policies for Cyber Operations. Cham: Springer, 2017.
- Tappoloet, Christine, and Mauro Ross., "What Is Value? Where Does It Come From? A Philosophical Perspective." In Handbook of Value: Perspectives from Economics, Neuroscience, Philosophy, Psychology, and Sociology, edited by Tobias Brosch and David Sander. Oxford: Oxford University Press, 2016.
- Tripodi, Paolo, and Jessica Wolfendale, eds. New Wars and New Soldiers. London: Ashgate, 2011.
- Van de Poel, Ibo. "Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security." In The Ethics of Cybersecurity, edited by Markus Christen, Bert Gordijn, Michele Loi. Cham, Switzerland: Springer Open, 2020.
- Van den Hoven, J. A., ed. Information Technology and Moral Philosophy. New York: Cambridge University Press, 2008.
- Zimmerman, Michael J. "Value and Normativity." In The Oxford Handbook of Value Theory, edited by Iwao Hirose and Jonas Olson. Oxford: Oxford University Press, 2015.

*이 글의 내용은 필자 개인의 견해이며
한국사이버안보학회의 공식 입장이 아닙니다.*