2023-3

KERC
Issue Report

EU 디지털 관련 정책 및 전략 현황

디지털유럽을 중심으로

ISSUE REPORT
2023-3

EU 디지털 관련 정책 및 전략 현황
디지털 유럽을 중심으로

[발행일] 2023.04.04.
[발행처] 한-EU 연구협력센터
Rue de la science 14A
1040 브뤼셀, 벨기에
http://www.k-erc.eu
+32 (0)2 880 39 05
[발행인] 조 우 현 센터장
[담당자] 송 예 일 연구원
[저 자] 송 예 일 연구원

Content

Ⅰ. 개요 ····· 4
1. 분석 배경 및 목적 ····· 4
2. 디지털유럽(DIGITALEUROPE) ····· 5

Ⅱ. 주제별 주요 내용 ····· 8
1. 디지털 탄력성 ····· 8
2. 사이버 탄력성 법안(CRA) ····· 17
3. 에너지 위기 속 디지털의 역할 ····· 20
4. 유럽 사이버 거버넌스 ····· 22
5. 신뢰할 수 있는 인공지능 ····· 25
6. 유럽보건데이터공간(EHDS) ····· 26
7. 유럽 기술의 해 ····· 28

Ⅲ. 시사점 ····· 30

1. 개요

□ 분석 배경 및 목적

○ 한-EU 디지털 파트너십 체결('22.11)에 따라 11대 협력 분야에 대한 EU 정책 및 현지 동향 파악 필요

- 한-EU 연구협력센터(KERC)는 재유럽 현지 거점으로서 EU의 주요 디지털 관련 정책을 모니터링하고 이에 대한 분석을 수행하고 있음
- '23년 3월 8일 유럽의 가장 큰 디지털 정책 컨퍼런스인 Masters of Digital이 개최됨에 따라 KERC는 '23년도 디지털 관련 정책의 주요 현안을 다양한 이해관계자의 입장에서 파악하고자 현장에 참석하였음

□ 한-EU 디지털 파트너십

○ 한국과 EU는 11개 디지털 협력 과제에 대한 협력을 우선적으로 강화하고자 디지털 파트너십을 체결함('22.11.28)

- EU는 세계 주요 국가와의 디지털 협력을 강화하고 파트너십을 맺고 있음

- 일본-EU 디지털 파트너십 체결('22.05)
- 한국-EU 디지털 파트너십 체결('22.11)
- 싱가포르-EU 디지털 파트너십 체결('23.02)
- 인도-EU TTC 설립 및 디지털 협력 강화('23.02)
- 캐나다-EU 디지털 협력 강화 및 디지털 파트너십 체결 논의('23.03)

- 디지털 파트너십을 통해 한국과 EU는 반도체, 양자기술, 6G, 인공지능 등 11개 분야에서 협력할 것

한-EU 디지털 파트너십 11대 협력 과제		
공동연구	반도체	인공지능
Beyond 5G/6G	사이버보안 및 신뢰	디지털 통상
데이터 관련 법 및 체계	디지털 신원/신뢰 서비스	온라인·디지털 플랫폼 협력
초고성능컴퓨팅(HPC) 및 양자기술	인적역량-인력교류-디지털 포용	

□ DIGITALEUROPE

○ **DIGITALEUROPE(디지털유럽)은 45,000개 이상의 유럽 디지털 혁신 기업을 대표하는 선도적인 유럽 무역협회**로 102개의 글로벌 리더 기업과 유럽 전역의 41개 국가 무역협회를 포함함

- 디지털유럽은 회원들과 함께 모든 관련 입법 문제에 대한 산업 정책 입장을 협상하고 관련 EU 정책의 개발 및 이행에 기여함
- **(비전)** 디지털 기술 산업을 육성하고 지원하며, 사회적 과제를 해결하고, 일자리, 혁신 및 경제적 혜택을 제공함으로써 번영하는 유럽연합을 형성하는 것
- **(미션)** 디지털유럽은 회원을 대신하여 EU 기관, 기타 유럽 및 글로벌 기구, 그리고 국가 무역 협회를 통해 EU 회원국과의 긍정적인 파트너로 협력함으로써 디지털유럽의 상술한 비전에 맞는 유럽의 비즈니스, 정책 및 규제 환경을 형성하는 것을 목표로 함

□ Masters of Digital

○ **유럽 최대의 디지털 정책 컨퍼런스 'Masters of Digital'**

- Masters of Digital은 디지털유럽의 연례 플래그십 서밋으로 매년 2월경 EU 최고 정책 입안자, 디지털 산업 리더, 학계 및 시민 사회 대표를 모아 다가올 해의 EU 디지털 정책 의제를 형성함
- 제6회 Masters of Digital 2022에는 92개국에서 2천여 명이 온라인으로 참석하였으며, 연사 32명과 함께 104명이 현장에 참석하였음
- 이에 17개의 전시와 634개의 온라인 미팅이 진행되었고, 온라인 시청 기록은 500만 뷰에 달하였음

○ **Masters of Digital 2023 개요**

- Masters of Digital 2023는 3월 8일~9일 양일간 브뤼셀에서 온·오프라인 하이브리드 행사로 진행됨
- EU 연구혁신 집행위원, 집행위원회 총국장, 유럽의원(MEP), 네덜란드·일본·루마니아·바바리아 등 주요국 디지털 장관, NATO 관계자, 기타 EU 기관, 기업 및 협회장 등 51명이 연사로 참여함

Masters of Digital 2023 주요 프로그램

3.8	9:30~10:00	오프닝 환영인사	*Cecilia Bonefeld-Dahl (Director General, DIGITALEUROPE)* *Hilary Mine (President, DIGITALEUROPE and Vice President Strategy & Technology, CX, Nokia)*
	10:00~10:45	패널토론	• **에너지 위기 속 디지털의 역할**
	11:30~12:15	심층토론	• 'Cyber Security Everywhere' – **사이버탄력성법안** • 'Female Founders in Tech' – **성별격차 해소**
	12:15~12:25	연설	*Tomas Lamanauskas (Deputy Secretary-General, International Telecommunication Union)* • **기후 행동 및 경제 탄력성을 위한 디지털 혁신**
	14:00~14:30	패널토론	• **유럽 사이버 거버넌스 : 유럽연합 전체의 사이버보안 협력 강화**
	14:30~14:50	자유토론	• **디지털 탄력성 및 민간부문의 역할**
	15:30~15:50	시상식	• Future Unicorn Award Ceremony *Mariya Gabriel (European Commissioner for Innovation, Research, Culture, Education and Youth)*
	15:50~16:20	패널토론	EU 집행위원회 및 Future Unicorn 후보자 간 토론
	16:20~16:45	캠페인	• **우크라이나를 위한 디지털 기기 기부 캠페인**
3.9	9:00~9:10	환영인사	*Cecilia Bonefeld-Dahl (Director General, DIGITALEUROPE)*
	9:10~9:20	연설	*Sebastian Ioan Burduja (Ministry of Research, Innovation and Digitalization)*
	9:20~9:40	자유토론	• **허위정보 및 디지털 탄력성**
	9:40~9:50	연설	*Judith Gerlach (Minister for Digital Affairs, Bavaria)* • **혁신을 촉발하는 AI법안의 필요성**
	9:50~10:50	패널토론	• **사회적 탄력성을 위한 신뢰할 수 있는 AI**
	11:25~11:35	연설	*Taro Kono (Digital Minister, Japan)*
	11:35~11:45	전문리뷰	*Dr Martin McShane (Chief Medical Officer, United Health Group)* • **건강부문과 데이터 – 이해 증진 및 질병 예방**
	11:45-12:30	심층토론	• **유럽보건데이터공간 구축 : 의료분야의 단편화 해결**
	12:30~13:00	심층토론	• **2023 유럽 기술의 해**
	13:00~13:30	패널토론	• **데이터 혁명 – 건강 및 금융**
	13:30~13:35	폐회인사	*Cecilia Bonefeld-Dahl (Director General, DIGITALEUROPE)*

○ Masters of Digital 2023 주요 주제

- **(디지털 탄력성)** 올해 행사는 '위기 시대 속 탄력적인 디지털유럽'이라는 주제를 중심으로 개최되었으며, 이에 따라 코로나19, 러-우 전쟁, 터키-시리아 지진 등 잇따른 위기에 대응하기 위한 '디지털 탄력성'에 초점을 맞추어 정책 토론을 진행함
- 특히, 디지털 유럽은 '디지털 탄력성'의 4가지 필라를 설정하고 이를 위한 15가지 실행방안을 제시함

- **(디지털 규제의 쓰나미)** 지난 한 해는 수많은 새로운 디지털 규제 법안이 제안되거나 채택된 '디지털 규제의 쓰나미'의 해였음
- '24년 집행위 선출을 앞두고 올해는 현 집행위 행정부의 정책 의제 실행에 있어 매우 중요한 한 해로, 특히 인공지능법안, EU데이터전략, 유럽보건데이터공간, 사이버보안 등에 대한 정책 결정이 조만간 이루어질 것으로 예상됨에 따라 관련 토론이 활발히 이루어짐

- **(여성)** 3월 8일 세계 여성의 날을 맞이하여 디지털 부문 내 여성 참여 및 다양성의 중요성이 계속해서 강조됨
- **(EIA)** 가브리엘 연구혁신 집행위원은 '22년 7월 채택된 '신유럽혁신어젠다'의 5가지 주요 의제를 강조하였으며, 특히 퓨처유니콘상 시상식에 맞추어 딥테크 기업 지원과 인재 양성(특히, 여성)의 중요성을 역설함
- **(일본)** 고노 다로 일본 디지털 장관은 온라인으로 행사에 참여하여 EU와의 공통 주제를 중심으로 일본의 주요 디지털 현황과 정책을 공유하였으며, 최근 EU-일본 디지털 파트너십 등 같은 생각을 가진 파트너와의 국제협력의 중요성을 강조함
- **(우크라)** 디지털유럽은 회원국과 기타 기관과 협력하여 우크라이나에 노트북 등 디지털 장비 30만 대를 지원하는 캠페인을 개시한 바 있으며, 2차 지원을 위해 회원 기업 및 기관의 참여를 촉구함

※ 기타 각 세션 주제에 대한 내용은 다음 장에서 다루도록 함

2. 주제별 주요 내용

□ 디지털 탄력성

○ 디지털 탄력성의 정의 및 배경

- **(정의)** 디지털 탄력성은 우리 사회가 디지털 기술을 사용하여 재정 및 보안 자산을 유지하며 팬데믹, 자연재해, 사이버공격, 하이브리드 전쟁 등에 대처하고 예방할 수 있는 역량을 뜻함
- **(배경)** 디지털 탄력성이라는 새로운 사회적 콘셉트는 코로나19 팬데믹 동안 나타났으며, 최초의 하이브리드 전쟁이라고 할 수 있는 러-우 전쟁과 최근 터키와 시리아의 대규모 지진 등으로 인해 그 중요성이 더욱 부각되었음

디지털 탄력성의 필요성
• 글로벌 사이버공격은 **38%**('22년) 증가 • 헬스케어 부문에 대한 사이버공격은 **61%**('21년) 증가 • 공급망에 대한 공격은 **17%**('21년)에 달함 • EU 사이버보안 시장 규모는 매년 **17%** 증가하고 있으며 현재 1,300억 유로 이상 될 것으로 추정 • 유럽의 데이터 유출은 평균적으로 **440만 유로**('21년)의 재정적 피해를 입힘 • 유럽은 현재 **100만 명**의 사이버보안 전문가가 부족 • EU에는 **6만 개** 이상의 사이버보안 기업이 있으며, **660개** 이상의 사이버보안 전문 센터가 있음 • 랜섬웨어 공격은 **102%**('21년 상반기) 증가하였으며, 각 공격은 **57만 유로** 상당의 피해를 입힘 • 유럽 조직 중 **48%**만이 랜섬웨어 공격을 막을 수 있다고 답함 • 유럽 조직 중 **32%**만이 사이버보안 정책을 가지고 있음 • 유럽 중소기업 중 **28%**('21년)가 한 번 이상 사이버범죄를 겪었음 • 우크라이나의 인터넷 인프라 중 **15%**('22.06)가 러시아에 의해 파괴됨

- 위 표에서 볼 수 있듯이 하이브리드 위협은 증가하고 있으며, 이를 예방(방어)하기 위한 준비를 하는 것은 매우 중요함

○ **디지털 탄력성을 위한 민관협력의 중요성**

- 디지털 탄력성을 유지하기 위해서는 민간부문과 공공부문 간의 긴밀한 협력이 필요함
- 공공부문이 공통의 선을 위한 제도적 정책 결정 절차를 담당하는 반면, 민간부문은 심각한 혼란에서 신속히 대처하고 복구해야 할 필요가 있는 기술 혁신 및 디지털 인프라의 핵심을 쥐고 있음
- 정부는 민간 기술 부문을 포함하는 강력하고 포괄적인 거버넌스 모델을 개발하고, 안전과 시민 인식을 높이고 최첨단 디지털 도구 사용을 촉진하는 전략과 관행을 채택함으로써 디지털 탄력성 구축에 앞서 나가야 할 것임

○ **디지털유럽은 디지털 탄력성을 위한 4개의 필라를 설정하고, 각 필라에 대한 실행방안을 제시함**

- 디지털유럽은 ①강력하고 포용적인 사이버보안 및 사이버 거버넌스, ②견실하고 의지할 수 있는 중요 인프라, ③탄력성 있는 공급망, ④중요 신흥와해성기술을 위한 신속한 조달 등 4개의 요소를 디지털 탄력성을 위한 필수요소로 제시

필라	주요 내용	
①	**사이버보안 및 사이버 거버넌스**	사이버 위협에 통일된 방식으로 신속하게 대응할 수 있는 능력
②	**디지털 인프라**	사이버 위협을 감지하고 다루는 데 필요한 플랫폼과 도구를 만들고 사용할 수 있는 능력
③	**공급망 탄력성**	디지털 사회가 작동하는 데 필요한 부품과 재료에 접근할 수 있는 능력
④	**신흥와해성기술을 위한 민첩한 조달 메커니즘**	유럽과 그 동맹국이 적대국보다 한발 앞서나갈 수 있도록 혁신을 장려하는 능력

- 또한, 디지털유럽은 디지털 탄력성이 유럽의 보안에 있어 매우 중요한 부분으로 여겨져야 하며, 이를 위해서는 민관협력, 기술을 갖춘 인재 양성, 혁신, 같은 가치를 지닌 파트너와의 협력이 중요하다고 강조함

EU 회원국 별 사이버보안 기관		
아일랜드 National Cyber Security Centre(NCSC)	**프랑스** Agence nationale de la sécurité des systèmes d'information (ANSSI)	**스웨덴** Swedish Civil Contingencies Agency (MSB)
네덜란드 National Cyber Security Centre(NCSC)	**독일** Federal Office for Information Security (BSI)	**슬로베니아** Slovenian Computer Emergency Response Team (SI-CERT)
덴마크 Centre for Cyber Security(CFCS)	**이탈리아** National Cybersecurity Agency (ACN)	**키프로스** National Computer Security Incident Response Team of Cyprus (CSIRT)
벨기에 Centre for Cyber Security Belgium (CCB)	**룩셈부르크** Computer Incident Response Centre Luxembourg (CIRCL)	**체코 공화국** National Cyber and Information Security Agency (NÚKIB)
스페인 Spanish National Cybersecurity Institute (INCIBE)	**오스트리아** Cyber Crisis Management (CKM)	**그리스** Hellenic Authority for Communication Security and Privacy (ADAE)
핀란드 National Cyber Security Centre Finland (NCSC-FI)	**폴란드** Narodowe Centrum Cyberbezpieczenstwa (NCC)	**불가리아** State Agency for Electronic Governance (SEGA)
리투아니아 National Cyber Security Centre of Lithuania (NCSC)	**슬로바키아** National Agency for Network and Electronic Services (NASES)	**루마니아** Romanian National Computer Security Incidents Response Team (CERT-RO)
크로아티아 Croatian Government CERT (HG-CERT)	**에스토니아** Estonian Information System Authority (RIA)	**헝가리** National Cybersecurity Institute (NKI)
라트비아 Information Technology Security Incident Response Institution (CERT.LV)	**포르투갈** Centro Nacional de Cibersegurança (CNCS)	**몰타** Cybersecurity National Coordination Centre (NCC)

EU 수준 사이버보안 담당 기구	
• 유럽방위청(EDA) • 유럽사이버보안경쟁력센터(ECCC) • 유럽사이버보안청(ENISA) • 유럽대외관계청(EEAS) • EU CyberNet • EU컴퓨터비상대응팀(CERT-EU)	• 국가컴퓨터보안사고대응팀(CSIRTs) • EU사이버위기연락기구네트워크(CyCLONe) • 보안운영센터(SOC) • 유럽사이버범죄센터(EC3) • 상설안보 방위협력체제(PESCO)

국제 수준 사이버보안 담당 기구
• 북대서양조약기구(NATO) • NATO 사이버방위센터(CCDCOE) • EU-미국 사이버 회담

① 필라1: 사이버보안 및 사이버 거버넌스

- 러시아의 우크라이나 침공 이후 치솟는 글로벌 위협에 따라 디지털 탄력성이라는 개념은 새로운 국면에 접어듬

현황	조치
• 2021년 중소기업의 28%가 사이버 범죄를 겪음 • 병원에 대한 사이버공격으로 인해 헬스케어가 19일 가량 지연됨 • 유럽 내 100만 명의 사이버보안 전문가 필요	• 민간부문을 포함한 공동 유럽 사이버 방위팀 • 유럽 사이버 탄력성에 조언하는 민관전문가자문위원회 구성 • 공통 표준을 통한 상호운용성 • 사이버 캠퍼스 네트워크 • 모든 커리큘럼에 컴퓨터과학 의무화

- 사이버공격은 전 세계적으로 전년대비 40% 이상 증가('22년)하였으며, 헬스케어 부문은 랜섬웨어 공격의 주요 타겟이 되어 '22년에만 42개 조직이 랜섬웨어의 영향을 받은 바 있음
- 유럽 내 사이버보안은 각 회원국에 따라 27개로 나누어지고, 민간 및 군사 진영에 따라 나누어져 있는 등 매우 복잡한 양상을 띠고 있어 포용적이며 복잡하지 않은 사이버 거버넌스 모델을 만드는 것에 어려움이 있음
- 특히, 민간부문을 대표할 만한 사이버 방위 기구가 없어 사이버 정책에 대해 민간부문이 과소 대표 될 가능성이 있음
- 최근 유럽 전역에 걸쳐 각국의 컴퓨터비상대응팀(CERTs)을 연결하고 조정하는 데 큰 진전이 있었으며, EU는 공동사이버부서(Joint Cyber Unit)를 창설하여 이러한 진전을 더욱 개선하고 있음

실행방안 1 : (민간부문을 포함한) EU 공동 사이버보안 대응팀

☞ EU는 보다 구체적인 정보 공유 의무와 명확한 명령 체계를 도입하고, 민간부문 최고정보보안임원(CISO)의 역할을 강화해야 할 것임

실행방안 2 : EU 사이버방위 정책에 민관 공동 전문가 자문위원회 설치

☞ 유럽 내 주요 민간 기업의 CISO를 포함한 민관전문가부서를 통해 사이버공격에 대한 사전 준비 및 협력, 신뢰할 수 있는 제공업체 인증, '사이버 기술 아카데미' 우선순위 등에 대한 전략적 조언을 제공

실행방안 3 : 공통 표준에 기반한 상호운용성

☞ 상술한 민관전문가부서를 유럽 표준화에 관한 EU 고위급 포럼과 연결하여 정기적인 논의를 하는 등 표준 설정 기관과 협력하는 데 사용

※ 특히, NATO는 표준 채택에 있어 중요한 역할을 할 수 있음

※ 상호운용성은 같은 생각을 가진 파트너와의 사이버 방위 협력에 있어 매우 중요

실행방안 4 : 사이버 캠퍼스 네트워크 및 커리큘럼 내 컴퓨터과학 의무화

☞ 프랑스에 최근 설립된 사이버 캠퍼스를 EU 전체로 확장하고, EU 사이버 기술 아카데미에 연결함으로써 유럽의 전반적인 사이버보안 강화

※ 유럽연합 집행위원회는 이러한 네트워크를 지원하고 조정하여 범유럽 사이버방위 훈련을 제공함으로써 참가자들이 기술을 연마하고 협력하는 방법을 가르칠 수 있음

※ 또한 집행위는 모든 회원국이 컴퓨터과학을 커리큘럼에 기본 과목으로 포함하도록 장려하는 방법을 모색해야 할 것

② 필라2: 디지털 인프라

- 인프라는 사회의 번영과 보안을 위해 매우 중요한 요인이며, 특히 오늘날 위성, 5G·6G와 같은 디지털 인프라의 중요성은 더욱 커짐
- 집행위원회는 중국의 일대일로 등에 대응하여 글로벌 게이트웨이 이니셔티브를 시행함으로써 민주주의 국가와의 무역 관계를 확장하고 아프리카 및 동남아시아 등에 투자하고 있음
- 집행위는 NIS 지침을 통해 중요 인프라 네트워크 보안 문제를 해결해 왔으며, 최근 불거진 회원국 간의 격차를 해소하기 위해 새롭게 제안된 NIS2 지침이 '23년 발효되어 '24년 10월부터 적용될 예정임
- 최근 우크라이나 전쟁에서 러시아가 디지털 인프라를 주요 공격 대상으로 삼으면서 디지털 인프라의 중요성은 더욱 강조되고 있음
- 이에 디지털유럽과 집행위원회는 30만 개 이상의 노트북과 디지털 기기를 우크라이나 학교와 병원에 기증하기 위해 협력한 바 있음

현황	조치
• 러시아 공격으로 우크라이나 인터넷 인프라의 15% 파괴('22.06) • 우크라이나 학교, 병원, 지방 행정부에 30만 개 이상의 디지털 기기 필요 • 글로벌 주요 인프라에 대한 사이버 공격 40% 증가	• 연결성 강화 • NIS2 지침 이행 • 클라우드 인프라에 투자 • '데이터 대사관' 개념 수용 • 디지털 인프라 보안 및 백업 투자

실행방안 5 : 연결성 강화

- 초고속 네트워크는 위기 시대 속 디지털 운영 및 연속성 보장을 위해 필수적이며, 5G·6G 연결성 강화는 디지털 탄력성 향상에 있어 매우 중요함

실행방안 6 : 모든 회원국의 NIS2 지침 이행

- 각 회원국은 NIS2 지침을 '24년 10월까지 국가법에 적용해야 함

실행방안 7 : 클라우드 활용 가속화

- 클라우드 컴퓨팅은 사물인터넷 및 인공지능 기반 기기 등 혁신적인 상품서비스의 기반이며, 디지털 전환의 초석임
- '21년 기준 EU 기업의 50% 미만이 클라우드 컴퓨팅을 사용하고 있는 등 EU의 클라우드 활용률은 다른 지역에 비해 뒤처지고 있음

실행방안 8 : '데이터 대사관' 개념 수용

- 에스토니아는 최고 수준의 사이버보안에 따라 룩셈부르크에 정부 서버 리소스의 일부를 설치하는 데이터 대사관 이니셔티브를 주도한 바 있음
- 최근 사례로는 우크라이나 정부가 민간부문의 도움을 받아 필수 데이터를 국가 밖의 더 안전한 위치로 옮길 수 있었음

☞ 유럽 각 정부는 이러한 혁신적인 '데이터 대사관' 개념을 수용하여 대규모 공격에 대비하고, 디지털 복원력을 강화할 수 있음

실행방안 9 : 디지털 인프라 보안 및 백업에 투자

- 정부는 디지털 인프라가 전통적인 방위 산업만큼 보안에 중요하다는 것과 케이블, 서버, 장치 및 스크린과 같은 중요한 구성 요소의 탄력적인 공급망이 보안에 필수적이라는 것을 인식해야 함

③ 필라3: 공급망 탄력성

- 유럽의 디지털 탄력성은 해외에서 공급하는 특정 부품 및 원자재에 의존하고 있으며, 이러한 부품의 공급 부족은 유럽 경제와 방위에 심각한 영향을 미칠 수 있음
- EU는 최근 '반도체칩법' 및 '중요원자재법' 등을 제안하여 공급망의 탄력성을 향상하고자 함
- EU 내부적으로는 칩 제조 공장에 대한 환경 허가를 받는 데 지나치게 긴 시간(12개월 소요)이 걸리는 등 여러 가지 장벽이 있음
- 스웨덴의 기반암은 EU의 중요원자재목록에 있는 물질의 절반 이상을 포함하고 있으나, 현재 규제로 인해 채굴이 이루어지지 않고 있음
- 또한, 유럽에서는 고급 칩 제조 또는 원자재 정제 기술도 부족하며, 수많은 규제와 국가법의 파편화는 유럽의 역량 강화를 저해하고 있음
- 유럽은 생산 능력을 늘리는 것 외에도 같은 생각을 가진 파트너와의 거래를 늘리고 새로운 기회를 찾아야 할 것임

실행방안 10 : 허가 절차 간소화 및 세제 혜택 제공

- 유럽은 허가 절차와 규제 보고 부담을 완화함으로써, 칩과 같은 필수 구성 요소의 생산을 빠르게 늘리고 중요한 원자재 추출 속도를 높일 수 있을 것으로 기대
- 세금 인센티브 및 민간부문이 참여하는 맞춤형 대학 프로그램도 기술 격차를 줄이는 데 도움이 될 것임

실행방안 11 : 무역 파트너 글로벌 네트워크 구축

- EU-미국 무역기술위원회(TTC)는 글로벌 정부 참여의 새로운 모델이 될 모든 요소를 갖추고 있으므로 이를 벤치마킹하도록 권장
- EU-미국 TTC는 칩 부문에서 높은 예상 수요를 따라잡고 시장 역학에 대한 EU-US 공통 이해를 심화하기 위해 공공 지원 조치를 조정할 수 있는 기회를 제공함
- 원자재와 관련하여 최근 나미비아 및 그린란드와 EU 간의 전략적 파트너십은 무역 다각화를 위한 길을 제시할 수 있으며, 지리적으로 집중된 지역에 대한 EU의 과도한 의존도를 완화할 수 있음

④ 필라4: 신흥와해성기술(EDTs)을 위한 민첩한 조달 메커니즘

- 유럽의 디지털 복원력을 강화하기 위해서는 기업 및 중소기업의 연구 혁신을 위한 지원이 충분히 제공되어야 함
- 보안 부문을 위한 연구혁신에 대한 투자는 유럽이 잠재적 적대국에 대항하여 기술적 우위를 점하는 데 가장 중요한 기회를 제공함
- 보안 및 방위 분야의 현재 조달 관행을 재검토할 필요가 있으며, 특히 신흥와해성기술과 관련하여 중소기업이 최신 기술 혁신을 제공할 수 있도록 빠른 경로를 열어주어야 할 것임

중소기업을 위한 펀딩 프로그램		
유럽방위기금(EDF)	2021-2027	80억 유로
디지털 유럽 프로그램(DEP)	2021-2027	75억 유로
내부보안기금(ISF)	2021-2027	19억 유로
망명이주기금(AMF)	2021-2027	100억 유로
유럽방위청 그랜트	-	-
유럽연결프로젝트(CEF)	2021-2027	337억 유로
코로나회복기금(RRF)	2021-2026	6,725억 유로
유럽방위산업강화 공동조달법(EDIRPA)	2022-2024	5,000억 유로
사회를 위한 시민 보안	2021-2027	16억 유로
유럽지역개발기금 및 결속기금	2021-2027	2,430억 유로
호라이즌 유럽(HE)	2021-2027	955억 유로
유럽평화시설(EPF)	2021-2027	50억 유로
InvestEU 기금	2021-2027	262억 유로
EU 우주 프로그램	2021-2027	150억 유로

- 디지털 탄력성 및 방위 분야에는 중소기업을 위한 많은 펀딩 프로그램이 있으나 대부분 잘 알려지지 않았으며, 일반적으로 그 신청 절차가 매우 길고 복잡함

A. **(정보과부하)** 수많은 웹 플랫폼을 탐색하며 펀딩 기회를 찾아보는 것이 중소기업에게는 어려우며, 새로운 펀딩 메커니즘이 생길 경우, 중소기업은 이에 새롭게 적응해야 하는 등 부담이 있음

B. **(규모격차)** EU는 학계와 기업 간의 대규모 컨소시엄을 선호하는 경향이 있어 유럽방위기금과 같은 주요 펀딩 프로그램에 중소기업이 참여하는 것은 어려움

C. **(파편화)** EU 내 27개 회원국에 따라 규칙이 파편화 되어 있다 보니 때로는 유럽 내에서 국경을 넘어 확장하는 것보다 다른 대륙으로 이동하는 것이 쉬운 경향이 있음

실행방안 12 : 간소화된 자금 지원 시스템

- 행정적 부담을 줄이는 것을 포함하여 간소화된 자금 조달을 통해 더 많은 소규모 기업이 디지털 복원력을 위해 마련된 자금에 액세스할 수 있도록 할 필요 있음

☞ 중소기업이 접근할 수 있는 자금 모델로 DIANA(북대서양 방위혁신 액셀러레이터)를 참고하여 유사한 자금 지원 시스템을 구축할 것

실행방안 13 : 디지털 및 사이버보안 기술에 대한 자금 배정

☞ GDP의 1%를 이중용도 와해성기술에 지출하는 등 미래의 방어에 투자할 것

실행방안 14 : 중소기업에 방위 자금의 25% 할당

- EU는 전통적인 방위 산업체 외부에서 일하고 있는 혁신가들이 디지털 복원력을 위한 유럽의 공적 자금을 얻을 수 있도록 보장해야 함

실행방안 15 : 유럽단일시장의 디지털 장벽 제거

- EU는 규제의 복잡성을 줄이고 장벽을 제거하여 혁신 기업이 유럽에서 성장하고 수익을 낼 수 있도록 지원해야 함

☞ 집행위원회는 성장에 대한 장벽을 해결하기 위해 기존 규정을 다시 살펴보고, 새로운 규정이 국가 간의 조화를 우선시하도록 해야 할 것임

□ 사이버 탄력성 법안

○ 유럽 사이버탄력성법안(CRA) 개요

- **(개요)** 집행위원회는 디지털 요소가 있는 제품에 대한 사이버보안 관련 요구사항을 설정하는 새로운 규정에 대한 제안을 발표함('22.09)
- **(배경)** 디지털 제품 대상 사이버공격으로 인한 연간 사이버범죄 비용은 5조 5천억 유로에 달할 것으로 추산('21년 기준)
- 대부분의 하드웨어 및 소프트웨어 제품은 현재 EU 사이버보안 법률의 적용을 받지 않고 있음
- 현 디지털 제품에는 두 가지 주요 문제가 있으며, 이에 대한 해결방안이 요구됨

문제점	해결방안
낮은 수준의 사이버보안 광범위한 취약점 및 이를 해결하기에 불충분하며 일관되지 않은 업데이트	☞ 하드웨어 및 소프트웨어 제품이 더 나은 보안성을 가지고 시장에 출시될 수 있도록 지원 ☞ 보안에 대한 인식 제고를 통해 제조업체가 제품 수명 주기 전반에 걸쳐 안전한 디지털 제품을 개발할 수 있는 조건 형성
정보에 대한 사용자의 이해 및 접근성 부족 사이버보안이 잘 갖춰진 제품의 선택과 안전한 방식의 사용 저해	☞ 사용자가 디지털 제품을 선택하고 사용할 때 사이버보안을 고려할 수 있도록 조건 형성

- **(목표)** 위 문제점과 해결방안에 따라 네 가지 구체적 목표가 제시됨

사이버탄력성법안 주요 목표
1. 제조업체가 설계 및 개발 단계부터 전체 수명 주기 동안 디지털 제품의 보안을 개선하도록 보장 2. 일관된 사이버보안 프레임워크를 보장하여 하드웨어 및 소프트웨어 생산자의 규정 준수 촉진 3. 디지털 제품의 보안 속성에 대한 투명성 향상 4. 기업과 소비자가 디지털 제품을 안전하게 사용할 수 있도록 지원

- **(내용)** CRA는 하드웨어와 소프트웨어를 포함하여 디지털 요소가 있는 제품의 제조업체, 개발자 및 유통업체에 대한 사이버보안 규칙을 도입

CRA는 다음 세 가지 사항을 보장:
1. EU 시장에 출시된 커넥티드 제품 및 소프트웨어의 안정성 2. 제품 수명 주기 전반에 걸친 사이버보안에 대한 제조업체의 책임 3. 소비자에게 디지털 제품과 관련된 사이버보안에 대한 정보 제공

- **(특징)** CRA는 '23년 1월 발효된 'NIS2' 지침을 보완함

○ CRA에 따른 필수 사이버보안 요구사항

- 디지털 제품은 CRA 부록에 명시된 '필수 사이버보안 요구사항'을 충족하는 경우에만 시장에 출시될 수 있음
- 제품 제조업체는 CRA 부록에 명시된 취약성 처리와 관련된 다양한 요구사항을 준수해야 하며, 이를 위한 정책과 절차를 마련해야 함
- CRA 범위의 모든 제품은 자체 인증 적합성 평가 절차를 거쳐야 하나, '핵심 제품'의 경우 회원국의 국가 당국이 선택한 중앙 EU 기관을 통해 보다 공식적인 평가 절차가 필요함

핵심 제품(Critical products)	
1등급 (Class 1)	2등급 (Class 2)
• ID 관리 시스템 소프트웨어 • 권한 있는 액세스 관리 소프트웨어 • 암호 관리 및 네트워크 트래픽 관리 시스템	• 서버 • 데스크톱 • 모바일 장치용 운영 체제

- CRA 3장은 CRA 범위에 속하는 제품의 제조업체가 준수해야 하는 다양한 적합성 요구사항을 제공함
- 제품은 EU 적합성 신고서와 함께 제공되어야 하고, 제품 자체나 제품 라벨에는 CE 마크가 부착되어야 함
- CRA 부록II는 '사용자에게 제공되는 정보 및 지침'에 포함되어야 하는 내용을 명시하며, 제조업체는 해당 정보를 명확하고 이해하기 쉬운 언어로 제공해야 함
- 제조업체는 제품의 취약점이나 보안에 대해 사용자 및 유럽사이버보안청(ENISA)에 보고해야 할 의무가 있음
- 유통업자와 수입업자는 해외의 비준수 제품을 EU 시장에 들이지 않도록 해야 할 의무가 있음

○ **CRA에 대한 유럽 산업계(디지털유럽)의 주요 입장**

- '28년까지 전 세계적으로 커넥티브 디바이스는 347억 개에 도달할 것으로 예상되며, 이러한 장치를 보호하는 것의 중요성은 더욱 높아짐
- 최근 몇 년 동안 다양한 EU 법률에 따라 단편적인 사이버보안 요구사항이 확산됨에 따라 기업과 당국의 규정 준수는 더욱 어려워지고 있으며, 이는 EU 내 사이버보안 능력을 저해하고 있음
- CRA는 제조업체, 사용자 및 당국이 전반적으로 사이버보안을 강화하는 데 도움이 되는 장기적인 솔루션이 될 것으로 기대되며, 이를 위해서는 규정 준수를 명확하고 실행 가능하게 만드는 조치가 필요함

☞ CRA가 EU 전체의 높은 공통 수준의 사이버보안을 위한 조치에 대한 새로운 지침인 **NIS2와 과도하게 겹치지 않도록** 원격 데이터 처리·전송·저장에 사용되는 하드웨어, 소프트웨어 및 서비스를 제외할 것

- 또한 CRA로 인해 불필요해진 **무선장비지침(RED)을 폐지**하고, 둘 중 하나를 준수할 수 있는 전환 기간을 제공할 것

☞ 완제품에 통합되어야 하는 소프트웨어·하드웨어의 보다 정확한 적합성 평가를 허용하는 **'디지털 요소가 있는 부분 완성 제품'*의 개념 도입**할 것

* RAM 칩, 마이크로프로세서 등 그 자체로 기능할 수 없고 다른 제품에 통합되어 디지털 요소가 있는 제품을 형성하도록 의도된 제품을 뜻함

☞ 유럽 및 전 세계적으로 이미 시행 중인 사이버보안 표준을 활용하여 **조화된 표준을 개발하고 사용함으로써** 기업의 CRA 준수를 지원하고 **자체 평가를 극대화**할 것

☞ 중소기업 및 신생기업의 규정 준수를 지원하고 CRA 향후 개정을 위한 규제 학습에 기여하기 위해 유럽 **규제 샌드박스 생성**

- 디지털 요소가 포함된 제품의 설계, 개발 및 생산을 지원하는 환경을 제공하고, CRA에 대한 증거 기반 평가 및 검토에 기여할 수 있도록 규제 학습 프로세스를 도입해야 함

□ 에너지 위기 속 디지털의 역할

○ 쌍둥이 전환(Twin Transition, 녹색 및 디지털 전환)을 위한 디지털 부문과 에너지 부문 간 협력의 필요성

- 디지털 기술은 유럽의 화석 에너지 의존도를 줄이고 에너지 효율성을 개선하고 소비자와 비즈니스의 비용 부담을 줄이는 재생에너지로의 전환을 가속함으로써 유럽이 에너지 주권을 확립하는 것을 도울 수 있음
- 특히, 러·우 전쟁으로 촉발한 에너지 위기는 에너지 부문과 디지털 부문 간의 협력을 위한 기회로 사용되어야 할 것임
- 디지털 기술은 탄소 배출을 줄이는 데에 있어 필수적인 요소이며, EU는 이를 인지하고 적극적으로 활용하여 그 잠재력을 극대화해야 함

○ 쌍둥이 전환을 위한 핵심 액셀러레이터

- 디지털유럽은 유럽 에너지 생태계의 디지털화를 위한 고위급 포럼을 개최('22.10)하였으며, 이를 통해 핵심 4가지 액셀러레이터를 선별함

①	**데이터 협력**	지속가능성 데이터의 활용 및 액세스 향상
②	**녹색 네트워크 인프라**	연결성 가속화
③	**투자 증대**	녹색기술 연구개발 및 혁신 강화
④	**규제 활성화**	디지털 및 녹색 정책 간의 시너지 형성

① **(데이터 협력)** 인공지능(AI) 및 사물인터넷(IoT)과 같은 기술은 고품질의 상호운용 가능한 데이터에 대한 접근에 의존함

☞ EU의 '공동데이터공간' 계획은 지속가능성 데이터의 풀링을 증진함으로써 에너지 사용을 줄이고 지능적인 의사 결정을 내리는 데 있어 좋은 기회가 될 것으로 기대

② **(연결성 및 인프라 강화)** AI와 IoT 같은 전략적인 디지털 솔루션은 빠른 속도의 고품질 연결성에 의존함

☞ EU와 회원국은 5G 등 고품질 네트워크 인프라의 출시를 가속화하고 이에 대한 자금 지원을 증대해야 할 것

③ **(투자 증대)** 2050 기후 중립을 달성하기 위해서는 기후 관련 ICT 솔루션과 획기적인 기술의 극적인 스케일업이 필요함

☞ EU 및 국가 펀딩 프로그램은 청정기술 이니셔티브를 강화하기 위해 중소기업과 스타트업에 더 많은 자원을 투자하고, 기술적 혁신을 촉진하기 위한 민관 파트너십을 구축해야 함

④ **(정책 간의 시너지)** 최근의 여러 입법 제안 사례는 디지털 기술의 광범위한 활용 가능성을 인식하지 못하고 있음

※ 예를 들어 한 패널은 fit to 55 패키지가 디지털 부문을 전혀 포함하지 않는다고 지적하며, 현재 에너지 부문이 풍력 발전기나 태양전지판 등 거대한 하드웨어에만 익숙해져 있고 보이지 않는 디지털 부문을 경시하는 경향이 있다고 언급함

☞ 유럽은 정책 솔루션 간의 상호보완적 본질을 인지하고 디지털 전환을 각 부문의 전략에 포함해야 할 것임

○ 에너지 전환을 위한 핵심 디지털 기술

- 더하여, 동 포럼은 유럽이 주도할 수 있는 디지털 기술로 ▲클라우드, 인공지능 및 머신러닝과 ▲사물인터넷 및 엣지 컴퓨팅을 선별함

유럽이 선도할 수 있는 디지털 기술 세트	클라우드·인공지능·머신러닝
	사물인터넷 및 엣지 컴퓨팅

- 이러한 디지털 기술은 2030년까지 자원 집약적 산업의 글로벌 탄소 배출을 20%까지 절감할 수 있음
- 이러한 기술들을 잘 활용하면 디지털 트윈, 유연성 향상, 최종사용자 시스템 및 플랫폼 활성화 등 중요한 결과를 만들어 낼 수 있음
- **(디지털 트윈)** 에너지 자산의 디지털 모델을 구축함으로써 잠재적 위협을 모니터링하고 프로세스를 시각화할 수 있으며, 이는 에너지 생태계의 수행 능력을 개선할 수 있을 것
- **(유연성 향상)** 디지털 기술은 서로 다른 에너지원의 효율적인 연결 및 운영을 가능하게 하는 등 전력 그리드에 유연성을 더할 수 있음

※ 예) 특정 에너지원이 가장 효율적인 시간대를 식별하여 사용하도록 지원

- **(플랫폼 및 시스템)** 데이터 기반 디지털 기술은 소비자를 위한 새로운 시장을 계속해서 창출해 낼 것

※ 예) 무료 모바일 앱을 통해 소비자는 자신의 일간 에너지 소비를 모니터링하고 에너지 소비를 줄일 수 있는 맞춤형 솔루션을 받을 수 있음

□ 유럽 사이버 거버넌스

○ EU 사이버방위 정책 개요

- **(개요)** 집행위원회와 EU 고위대표는 EU 사이버 정책에 대한 공동 커뮤니케이션을 발표함('22.11)
- **(목적)** 우크라이나 전쟁 이후 악화되는 안보 환경을 개선하고, 시민과 인프라를 보호하며, EU의 역량을 강화하기 위함
- **(구조)** EU 사이버방위 정책은 네 가지 필라를 중심으로 구축됨

1	더 강력한 EU 사이버방위를 위한 협력
2	EU 방위 생태계 보호
3	사이버방위 능력을 위한 투자
4	공동 과제 해결을 위한 파트너십

- **(내용)** 네 가지 필라에 따른 주요 이니셔티브는 다음과 같음

1	국가 및 EU 사이버 방위 플레이어 간의 조정 메커니즘을 강화하여 군사 및 민간 사이버보안 커뮤니티 간의 정보 교환 및 협력을 강화하고 군사 CSDP(공동안보방위정책) 임무 및 운영을 추가로 지원할 것
2	군사 및 민간 영역 모두를 보호하기 위해 사이버보안 표준화 및 인증에 대한 추가 작업을 개시할 것
3	EU 회원국은 PESCO, 유럽방위기금(EDF), 호라이즌유럽(HE), 디지털유럽 프로그램(DEP) 등과 같은 EU 수준의 협력 플랫폼 및 자금 조달 메커니즘을 사용하여 사이버방위 능력에 대한 투자를 크게 늘릴 것
4	파트너 국가와의 사이버 대화에 더하여 EU는 기존의 안보 및 방위를 기반으로 사이버 방위 분야에서의 맞춤형 파트너십을 구축할 것

- **(배경)** 집행위와 외교안보정책 고위대표가 '20년 12월 발표한 EU 사이버보안 전략은 EU의 사이버방위 정책 프레임워크를 검토할 필요성을 강조하였으며, 집행위원장은 '21년 연두교서에서 EU 사이버방위 정책 개발을 촉구함
- 사이버방위 정책은 EU 이사회가 '22년 3월 승인한 안보 및 방위를 위한 전략 나침반의 목표 중 하나이며, EU의 사이버 태세 개발에 관한 이사회 결론('22.05)은 EU 사이버방위에 대한 제안을 환영함

○ EU 사이버보안 전략 개요

- (개요) 집행위와 EU 외교안보정책 고위대표는 새로운 EU 사이버보안 전략을 발표함('20.12)
- (목표) ▲사이버공격에 대응할 수 있는 집단적 역량 및 사이버 위협에 대한 탄력성 구축, ▲신뢰할 수 있는 디지털 기술, 글로벌하고 개방된 인터넷 보장을 위한 안전장치 제공, ▲사이버 공간의 국제 보안과 안정성을 보장하기 위한 전 세계 파트너와의 협력
- (내용) 전략은 사이버보안을 위한 EU의 세 가지 활동 영역을 설정함

EU의 사이버보안을 위한 세 가지 활동 영역	
1	회복력, 기술 주권 및 리더십
2	예방, 억제 및 대응을 위한 운영 능력
3	글로벌하고 열린 사이버 공간 발전을 위한 협력

- 세 가지 활동 영역에 따른 구체적 실행방안은 다음과 같음

1	• **네트워크 및 정보 시스템 보안에 관한 규칙 개혁 (NIS2)** - 공공·민간 부문(병원,데이터센터,공공행정,연구소 등)의 사이버 회복력 수준 향상 • **사이버보안 방패** - 인공지능으로 구동되는 EU 전역의 보안 운영 센터 네트워크 - 사이버 공격 징후 조기 감지 및 사전 예방 • **디지털혁신허브를 통한 중소기업 지원** - 전담 지원, 인력 향상, 사이버보안 인재 유치 및 유지, 개방된 연구혁신
2	• **공동사이버부서(Joint Cyber Unit) 설립** - 사이버보안에 대한 책임이 있는 회원국 간의 협력 강화 • **EU 사이버외교 툴박스** - 악의적 사이버 활동의 방지, 억제 및 대응 목표 • **최첨단 사이버 방위 능력 개발** - 유럽방위청(EDA)의 작업을 기반으로 회원국이 구조적 협력과 유럽 방위를 활용하도록 장려
3	• **EU 외부사이버 역량 구축 의제 개발** - 제3국에 대한 사이버 역량 구축 노력 확대 (서부발칸반도, 6개유럽동부국가 등 지원) - 제3국, 지역 및 국제기구, 다중이해관계자 커뮤니티와의 사이버 대화 강화 • **EU 사이버외교 네트워크 구성** - 전 세계를 대상으로 EU의 사이버 공간에 대한 비전 홍보

○ **EU 전체의 사이버보안 협력 강화를 위한 '유럽 사이버 거버넌스'**

- 사이버 군대와 정보 전쟁이 증가함에 따라 EU, 회원국, NATO 및 동맹국은 디지털 보안 문제에 대한 협력을 강화해야 할 필요가 있음
- 유럽의 디지털 탄력성을 지원하기 위해 설립된 '디지털유럽 탄력성집행위원회(Resilience Executive Council)'는 EU 사이버방위 정책에 대한 권장사항을 제시함

※ 여기서 제시된 권장사항은 앞서 서술한 '디지털 탄력성'을 위한 15가지 실행 방안에도 반영됨

☞ 사이버 탄력성에 대한 **'민관 합동 자문위원회' 구성**

- 민간부문은 상당한 양의 중요 인프라를 소유하고 운영하고 있으며, 보안의 취약성 해결 방법과 소프트웨어 관련 업데이트 및 수정 사항에 대한 전문 지식을 제공하고, 중요한 사이버보안 사고를 예방·감지·대응하는 데 가장 적합함
- 따라서 사이버 탄력성에 있어 민간부문의 참여는 매우 중요하며, 공동의 민관 거버넌스 구조는 EU 수준의 기존 이니셔티브 및 민간부문의 관련 이니셔티브를 연결할 수 있을 것임
- 자문위원회는 하이브리드 민방위 표준을 촉진하고 개발하기 위해 유럽 표준화에 관한 고위급 포럼과 협력해야 하며, 사이버보안 전문가를 양성하기 위한 사이버 기술 아카데미 이니셔티브에도 참여해야 함

☞ **NATO의 DIANA 모델을 적용한** EU 수준의 프레임워크 구축

- EU 기관은 민간부문, 학계 및 회원국과의 협력을 통해 DIANA와 유사한 EU 수준의 프레임워크를 구축하여 스타트업, 연구원 및 기술회사 사이에서 신뢰할 수 있는 사이버보안 혁신가를 모아 중소기업 혁신을 촉진할 수 있을 것임
- 이러한 프레임워크는 회원국 간 디지털 및 사이버보안 기술의 공동조달을 촉진하는 동시에 신흥 플레이어가 디지털 방위 분야의 혁신을 위한 EU 프로그램에 대해 더 잘 알 수 있도록 도울 것으로 기대

□ 신뢰할 수 있는 인공지능

○ 사회적 탄력성을 위한 '신뢰할 수 있는 AI'

- AI 정책의 목표는 유럽 시민과 기업의 이익을 위해 인간 중심 가치에 기반한 신뢰할 수 있는 AI의 광범위한 활용을 촉진하고 장려하는 것임
- **(투명성)** AI의 사용과 응용에 대한 투명성은 인간 중심적인 신뢰할 수 있는 AI를 위한 핵심 요소임

☞ 사용자에게 맞게 조정된 정보를 제공하여 기술에 대한 사용자의 신뢰를 높이고 전반적인 이해를 촉진해야 함

- **(데이터)** AI는 알고리즘, 딥러닝 등을 위한 데이터의 가용성에 의존하므로, 충분한 양의 데이터에 대한 접근이 공급자에게 있어 매우 중요함

☞ EU 정책은 보다 광범위한 디지털 전환 및 인프라 개발을 통해 데이터 생성 및 사용을 늘리고 장려해야 할 것임

- **(책임·안전)** EU는 제조물책임 및 기계 지침 등을 포함하여 신제품이나 신기술의 책임 및 안전에 대해 견고하고 효과적인 프레임워크를 갖추고 있음

☞ 기존 규제의 적절성 판별을 위한 분석이 필요하며, 정보에 입각한 증거 기반 방식으로 책임, 태만 및 과실 위험 등에 추가 분석이 수행되어야 함

○ AI책임지침 개요

- **(개요)** 집행위는 AI에 대한 비계약적 민사 책임 규칙(AI책임지침)을 제안('22.09)
- **(목적)** AI 시스템에 의해 피해를 입은 사람이 EU의 다른 기술로 피해를 입은 사람과 동일한 수준의 보호를 받을 수 있도록 하기 위함
- **(목표)** ▲신뢰할 수 있는 AI의 출시 촉진 ▲AI를 개발하거나 사용하는 기업의 법적 불확실성 감소 ▲국가 민사 책임 규칙 간의 분열 방지
- **(특징)** AI책임지침은 EU에서 추진 중인 AI법을 보완하기 위해 제안됨

※ AI법안은 AI로 인한 위험을 줄이고 사고를 미연에 방지하는 데 목표를 두고 있으며, AI책임지침은 AI법안에도 불구하고 발생할 수 있는 사고에 대해 사용자의 피해를 보상하기 위한 안전망으로써 제안됨

- **(내용)** AI책임지침은 AI 시스템으로 인한 피해자에게 보다 합리적인 입증 책임과 성공적인 책임 청구의 기회를 제공하는 인과 관계 추정을 만드는 등 피해자의 권리를 강화하고 피해 입증의 부담을 덜어줌

□ 유럽보건데이터공간

○ 유럽보건데이터공간(EHDS) 개요

- (개요) 유럽연합 집행위원회는 '22년 5월 유럽보건데이터공간을 제안함
- (배경) 코로나19 확산으로 의료분야 디지털 서비스의 중요성이 부각됨
- EU 회원국 전반에 걸친 규칙, 구조 및 절차의 복잡성으로 인해 국가 간 보건데이터에 접근하고 공유하는 것은 매우 까다로움
- 유럽데이터전략('20)은 특정 분야별 공동유럽데이터공간의 구축을 제안하였으며, EHDS는 그중 첫 번째 공동데이터공간
- (목표) ▲디지털 의료 상품서비스의 진정한 단일 시장의 육성을 통한 데이터 경제 활성화 ▲연구혁신, 정책 결정 및 규제 활동을 목적으로 하는 보건 데이터의 2차 사용에 대한 규칙 설정 ▲개인 보건데이터에 대한 더 나은 디지털 액세스 제공
- (내용) 시민들은 무료로 전자보건데이터에 쉽게 액세스할 수 있게 되며, 이러한 데이터를 회원국 안팎의 다른 의료 전문가와 공유함으로써 헬스케어를 개선할 수 있음
- 회원국은 전자 처방, 이미지, 보고서, 검사 결과, 퇴원 보고서 등이 유럽의 공통 형식으로 발행되고 승인되도록 관리하게 되며, 전자 건강 기록 시스템 제품의 상호 운용성 및 보안은 필수 요구사항이 될 것
- EHDS는 연구혁신 공중 보건, 정책 결정 및 규제 목적의 보건데이터 사용에 대한 강력한 법적 프레임워크를 만들고, 엄격한 조건하에 연구원, 혁신가, 공공 기관 및 산업체가 보건 데이터에 접근할 수 있게 함

○ 유럽보건데이터공간이사회(EHDS Board)

- 디지털 보건 당국 대표, EU 회원국, 집행위원회 및 새로운 보건 데이터 액세스 기관으로 구성된 EHDS 이사회가 설립되어 EU 전역에서 규칙을 일관성있게 적용하는 데 기여하기 위해 다른 EU 기관 및 조직과 협력하고 집행위원회에 조언을 제공할 것

○ **EHDS에 대한 유럽 산업계(디지털유럽)의 주요 입장**

- EHDS는 의료 서비스 제공에 사용되는 건강 데이터에 대해 더 잘 관리된 접근 방식을 확립하고 건강 데이터의 광범위한 2차 사용 목적을 규정함으로써 보건 부문의 연구혁신에서 유럽의 역량과 경쟁력을 높이고 건강 시스템과 공중 보건의 탄력성을 강화할 것으로 기대
- 확립된 법적 권리와 개념을 훼손하지 않으면서 규제 조정과 일관성을 보장할 수 있다면 EHDS는 유럽 내 의료 혁신을 향상하고 절실히 필요한 투자를 촉발할 수 있을 것임
- 그러나, EHDS만으로는 의료분야의 모든 데이터 관련 규제 문제를 해결할 수 없다는 점에 주의해야 할 것
- 특히 의료 데이터의 1차적 및 2차적 사용 모두에 대한 GDPR의 해석 및 적용에 있어 EU 회원국들은 분열되어 있으며, 이는 유럽의 보건 분야 연구혁신을 계속해서 저해하고 있음

☞ EHDS는 일반데이터보호규정(GDPR), 의료기기규정(MDR), AI법, 사이버 탄력성법, 데이터거버넌스법 등을 포함한 **모든 관련 유럽 법률과 일치**해야 함

- 전자보건데이터의 주요 사용과 관련하여 자연인의 권리 범위를 명확히 하고, 이러한 권리와 GDPR 및 데이터법안에 따른 해당 권리와의 관계를 명확히 필요성 있음
- 전자보건데이터와 상호작용하는 모든 상품서비스를 포함하지 않도록 '전자보건기록(EHR)' 시스템의 정의를 명확하게 제시할 필요 있음

☞ **원격 의료 서비스**를 위해 **디지털 단일 시장**을 발전시켜야 함

- EU 회원국 전체에 걸쳐 환급 규칙을 조정하는 등 분열을 줄임으로써 디지털 의료 서비스의 진정한 유럽 단일 시장을 촉진해야 함

☞ 전자보건데이터의 **2차 사용**에 대한 일반적인 조건과 거버넌스 및 메커니즘을 명확히 해야 함

- 데이터 보유자와 사용자에 대한 요구사항을 지정하여 의료데이터 액세스 기관에 명확하고 조화된 프로세스를 제공하고, 데이터 허가 신청을 지연하거나 거부할 수 있는 기준이 무엇인지, 어떤 데이터가 전자보건 데이터의 범주에 포함되는지 명확하게 설명할 필요 있음

□ 유럽 기술의 해

○ 유럽 기술의 해(European Year of Skills) 개요

- **(개요)** EU는 '22년 10월 집행위원회가 제안한 '유럽 기술의 해'에 대한 정치적 합의에 도달함('23.03)
- **(배경)** 녹색 전환은 '30년까지 EU에서 최대 100만 개의 추가 일자리를 창출할 것으로 보이나, 기업은 일자리에 맞는 올바른 기술을 갖춘 근로자를 찾는 데 어려움을 겪고 있음
- 디지털경제사회지수(DESI)에 따르면 성인 10명 중 4명, 유럽 근로자의 3분의 1이 기본적인 디지털 기술이 부족한 것으로 나타남
- EU는 디지털 나침반을 통해 '30년까지 모든 성인의 최소 80%가 기본적인 디지털을 보유하는 것과 EU 내 ICT 전문가 2천만 명을 달성하는 것을 목표로 삼고 있음
- **(목표)** 유럽 기술의 해의 주요 4가지 목표는 다음과 같음

• 교육 및 숙련도 향상에 대한 투자 촉진을 통해 사람들이 직장을 유지하거나 새로운 일자리를 찾을 수 있도록 지원 • 사회적 파트너 및 회사와 긴밀히 협력하여 기술이 고용주의 요구에 부합하도록 보장 • 녹색 및 디지털 전환과 경제 회복을 위해 사람들의 열망과 기술을 취업 시장의 기회와 매치 • 필요한 기술을 갖춘 해외 인재 유치

- **(내용)** 유럽 기술의 해는 국가적 노력과 EU 자금 지원을 포함한 EU 이니셔티브를 통해 기술 격차를 해소하고 EU 전역에서 기술 관련 활동 및 행사의 조직을 촉진할 것
- European Digital Skills and Jobs Platform은 디지털 기술 자체 평가 도구, 교육 및 자금 조달 기회와 같은 디지털 기술에 대한 정보를 제공함
- EU Digital Skills and Jobs Coalition은 회원국, 기업, 비영리 기관 및 교육 제공자를 모아 디지털 기술을 향상시키고, 교육을 장려하기 위해 다양한 조치를 취하여 디지털 기술 격차를 해소하는 데 기여하고 있음

- 디지털유럽프로그램(DEP)은 고급 디지털 기술 개발을 위해 5억 8천만 유로를 지원하며, 디지털 전문가의 숙련된 인재풀의 개발을 지원함
- 호라이즌유럽(HE)은 특히 마리퀴리 프로그램(MSCA), 유럽혁신위원회(EIC) 및 유럽혁신기술연구소(EIT)를 통해 연구원, 기업가 및 혁신가를 위한 기술을 지원함
- 유럽 기술의 해는 기존 이니셔티브의 이행에 중점을 둘 것이나 이를 뒷받침하고 회원국 전체의 기술 개발을 더욱 강화하기 위해 다수의 새로운 EU 제안도 채택될 예정

계획된 새로운 이니셔티브 예시
디지털 교육 및 기술 패키지 채택
European Quality Framework for Traineeships 업데이트 제안
EU Talent Pool 개시 (제3국 인재 채용)
Learning mobility framework
해외 기술자 유치를 위한 비EU 국가 학력/기술 자격 인정 향상
선별된 비EU 파트너 국가와의 인재 파트너십 출시
Pact for Skills의 일환으로 근로자의 재교육 훈련 및 투자를 위해 더 많은 파트너십 구축
Net-Zero Industry Academy 설립 제안
사이버보안 전문가 증대를 위한 사이버 기술 아카데미 설립
연구 경력을 위한 새로운 프레임워크 도입
'25년까지 딥테크 인재 100만 명을 양성하기 위한 Deep Tech Talent Initiative
Making Skills Count Conference(6.8~9)
European Digital Skills Awards 2023(우승자 6월 발표)
European Vocational Skills Week 2023(10.23~27.)
EU Code Week(10.7~22)

3. 시사점

□ 한-EU 디지털 파트너십에 따른 협력 방안

○ 유럽 디지털 정책 주요 현안 및 한국과의 협력

- 대규모 사이버공격에 대한 공동 대응 능력을 구축하는 등 EU의 전반적인 디지털 탄력성을 개선하기 위해서는 회원국 간의 정보 공유를 강화하고 규제를 조정할 수 있는 조화된 프레임워크가 필요함
- EU의 정책입안자 및 주요 이해관계자는 이러한 점을 인지하고 통일된 프레임워크를 제공하는 것을 주요 현안으로 설정하고 이를 해결하기 위해 여러 노력을 기울이고 있음
- 예를 들어, EU는 회원국 간의 정보 공유를 활성화하고 국가 규제 간의 조정을 위해 공동사이버부서, EU사이버보안청(ENISA) 등의 조정 기관을 설립 및 활용하고 있으며,
- 디지털 기술에 대한 유럽 표준화 개발을 통해 회원국 간 규제의 상호 운용성을 확보하고 이를 제3국에 홍보함으로써 글로벌 표준 개발에까지 확장하고자 함

☞ 한-EU 디지털 파트너십은 과기정통부(MSIT)와 EU사이버보안청(ENISA) 간 MoU 체결 등을 통해 사이버보안 역량 강화에 협력할 수 있음을 명시하고 있음

☞ 한-EU 디지털 파트너십은 반도체 분야에서 반도체 및 칩 보안에 대한 국제 표준화에 있어 시너지를 모색할 것과 고성능컴퓨팅(HPC) 및 양자기술 분야에서 학회, 세미나 또는 포럼 등을 통해 국제 표준화에 대한 협력을 증진할 것, 그리고 3GPP에 대한 단일 글로벌 6G 표준 개발을 위해 기술 협력을 심화할 것임을 명시함

- 최근 급격히 고조된 지정학적 긴장으로 인해 EU는 러시아 및 중국과 같은 국가에 대한 공급망 의존도를 줄이기 위해 '반도체칩법', '중요 원자재법' 등 다양한 정책을 통해 공급망의 탄력성을 개선하고자 함
- 반도체칩법은 EU 내 반도체 공급에 대한 위험을 평가하는 위기 대응 메커니즘을 수립하여 특정 제품에 대한 공급을 우선적으로 처리하거나 회원국에 대한 공동 구매를 수행하는 등의 긴급 조치를 제시함

- 더하여, EU는 한국과 같이 '같은 생각을 가진 민주주의 국가'와의 협력을 강화하고 있음

☞ 한-EU 디지털 파트너십은 양측이 조기 경보 체계 구축 등을 통해 글로벌 공급망 격차 및 잠재적 공급망 차질 파악에 협력할 것과 관련 산업 정책 정보 공유 및 관련 당국 간 수출통제 조정의 가능성을 모색하기 위해 협력할 것임을 명시함

ㅇ 협동연구

- 한-EU 디지털 파트너십은 양측이 디지털 분야에서 한국의 국가연구개발사업과 EU의 호라이즌 유럽의 연계를 통해 한-EU 협력 연구 협력 활동을 지원할 수 있음을 명시함
- 특히 디지털 파트너십을 통해 양측은 호라이즌 유럽 내 민관 파트너십인 공동사업단(Joint Undertaking) 등을 통해 추가적 협동 연구활동 수행 기회를 제공할 수 있음

☞ 한국의 연구 기관 및 기업은 관심 분야에 대한 호라이즌 유럽 공동연구의 기회를 모색하고, 관련 분야의 공동사업단 참여 가능성을 검토하도록 장려됨

ㅇ 인적역량(Skills)-인력교류-디지털 포용

- 한-EU 디지털 파트너십은 양측이 ICT 분야에서 젊은 연구자 교류 프로그램을 개시할 수 있으며, 한국의 학교 및 직업교육훈련(VET) 기관들이 EU 이니셔티브인 CodeWeek에 참여할 수 있다고 언급함
- EU는 '23년 '유럽 기술의 해'를 맞아 다양한 이니셔티브를 개시하고 있으며, 특히 필요한 기술을 갖춘 해외 인재를 유치하는 것에 많은 노력을 기울일 것으로 예상됨

☞ 한국의 기관 및 개인은 유럽 기술의 해 기간동안 EU의 인력교류 기회를 탐색하고 적극적으로 이용하도록 장려되며, 한-EU 협력 기관은 활발한 정보 공유를 통해 이를 지원하도록 권장됨

□ 참고문헌

[문헌]

DIGITALEUROPE - “THE DIGITAL FRONT LINE: 15 actions to boost Europe’s Digital Resilience” (2023)

DIGITALEUROPE - “Creating a proportionate Product Liability Directive” (2023)

DIGITALEUROPE - “DIGITALEUROPE RESILIENCE COUNCIL: Public, Civil and Private Cooperation for an ambitious EU Cyber Defence” (2023)

DIGITALEUROPE - “Digitalisation as a key enabler for a resilient and sustainable energy ecosystem” (2023)

DIGITALEUROPE - “DIGITALEUROPE’s recommendations for a more ambitious EU Cyber Defence Policy” (2023)

DIGITALEUROPE - “Cybersecurity everywhere: deciphering the Cyber Resilience Act” (2023)

DIGITALEUROPE - “DIGITALEUROPE’s Position Paper on the European Health Data Space proposal” (2023)

DIGITALEUROPE - “Initial reactions to the European Health Data Space proposal” (2022)

DIGITALEUROPE - “DIGITALEUROPE’s Recommendations on Artificial Intelligence Policy” (2019)

DIGITALEUROPE - “Event Report: Digital Resilience Roundtable on Supply Chains” (2023)

DIGITALEUROPE - “DIGITALEUROPE’s recommendations for the Critical Raw Materials Act” (2022)

DIGITALEUROPE - “Critical digital technologies for European digital resilience” (2022)

DIGITALEUROPE - “Why it is time to move digital skills to the top of the EU’s agenda” (2022)

Tambiama Madiega - “EU Legislation in Progress: Artificial intelligence liability directive”, European Parliamentary Research Service (2023)

Korea-EU Research Centre - “EU 디지털 관련 정책 및 전략” (2022)

NIS2 Directive (EU) 2022/2555

EUROPEAN COMMISSION - “The Data Act (COM/2022/68 final)”

EUROPEAN COMMISSION - “The AI Act (COM/2021/206)”

EUROPEAN COMMISSION - “Fostering a European approach to Artificial Intelligence(COM/2021/205)”

EUROPEAN COMMISSION - “Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics(COM/2020/64)”

EUROPEAN COMMISSION - “Factsheet: European Health Data Space(FS/22/2713)”

EUROPEAN COMMISSION - “The Cyber Resilience Act (COM/2022/454)”

European Commission, Consumers, Health, Agriculture and Food Executive Agency, Hansen, J., Wilson, P., Verhoeven, E., et al., Assessment of the EU Member States’ rules on health data in the light of GDPR, Publications Office, 2021, https://data.europa.eu/doi/10.2818/546193

[웹페이지]

Regan, J. (2022, October 25). The proposed EU Cyber Resilience Act: what it is and how it may impact the supply chain ¦ Data Protection Report. https://www.dataprotectionreport.com/2022/10/the-proposed-eu-cyber-resilience-act-what-it-is-and-how-it-may-impact-the-supply-chain/

https://www.european-cyber-resilience-act.com/

https://year-of-skills.europa.eu/index_en

https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en

https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

https://www.european-cyber-defence-policy.com/

https://www.digitaleurope.org/

https://mastersofdigital.org/