DOMINIK BIERECKI, MAŁGORZATA CZURYK, CHRISTOPHE GAIE,
JEAN LANGLOIS-BERTHELOT

Sovereignty by Design: Embedding Fiscal Risk Intelligence in Europe's Defence-Digital Strategy

Abstract

The European Union confronts structural uncertainty across defence and digital sectors. Fiscal governance still relies on stability-oriented frameworks that cannot handle volatility. This paper argues that strategic autonomy requires integrating actuarial reasoning – quantification, pricing and systemic treatment of uncertainty – into existing EU budgeting and investment tools. The approach does not require new institutions or treaty changes. It requires a change in decision logic inside the Multiannual Financial Framework, the European Defence Fund, the Digital Europe Programme and the European Investment Bank. Empirical work in cyber-risk insurance, cyber-threat forecasting and development finance demonstrates that uncertainty can be modelled and priced. Actuarial governance emerges as a necessary foundation for credible European sovereignty.

KEYWORDS: defence, cyberspace, cybersecurity, fiscal risk

DOMINIK BIERECKI – associate professor, Pomeranian University in Słupsk (Poland), ORCID – 0000-0001-6993-3974, e-mail: dominik.bierecki@upsl.edu.pl
MAŁGORZATA CZURYK – associate professor, University of Warmia and Mazury in Olsztyn (Poland), ORCID – 0000-0003-0362-3791, e-mail: malgorzata.czuryk@uwm.edu.pl
CHRISTOPHE GAIE – associate researcher, Université Jean Moulin Lyon 3 (France), ORCID – 0000-0002-8252-5278, e-mail: christophe.gaie@gmail.com
JEAN LANGLOIS-BERTHELOT – PhD in applied mathematics, Center for Advanced Military Training, ORCID – 0009-0001-2397-5930, e-mail: jeanlanglois4@gmail.com

HTTPS://DOI.ORG/10.36128/2Z2K7566

1 Introduction

The issue of defence is becoming particularly important today, although it has always been a key priority in both European policy and the public policy of individual EU Member States. Defence is not only about conventional activities, but also about using cyberspace as an operational domain. An efficient army is one that makes extensive use of ICT systems for defence activities, but these systems are vulnerable to cyberattacks. Minimising cyber threats in the military sphere requires significant financial outlays as well as risk analysis, in particular forecasting the costs needed to ensure digital stability in this area.

The optimal functioning of the digital defence sphere requires adequate financial capacity, including investment in areas that may prove important for defence in the future. Therefore, it will be important to assess the fiscal risk of digital defence investments, without which defence readiness may not be at an adequate level.

Strategic thinking about defence as a highly digitised field requiring financial outlays also in high-risk areas, followed by appropriate action, will ensure military stability, which has a decisive impact on sovereignty.

In Member States that have adopted the euro as their currency, monetary policy has been federalised, but the European Union still lacks fiscal tools that could mitigate asymmetric shocks that may occur in the euro area. Member States outside the euro area are subject to fiscal constraints, and have limited capacity to respond to economic crises.[1] The European Union's common monetary policy, combining the fiscal efforts of both euro area and non-euro area countries, must take into account Europe's digital defence status.

This paper aims to emphasise the importance of fiscal risk analysis in the context of the European digital defence strategy, and its significance for sovereignty. The main research method used in this paper is the dogmatic–legal method. An analysis of the literature on the subject was also carried out.

1 Federico Fabbrini, *A Fiscal Capacity for the Eurozone: Constitutional Perspectives* (Brussels: Policy Department for Citizens' Rights and Constitutional Affairs, 2019), 6.

2 Europe's Strategic Environment and Fiscal Architecture

The European Union expands its defence-industrial and digital ambitions. The European Defence Fund consolidates cross-border research and aims to strengthen the defence technological base. The European Defence Industrial Strategy pushes industry toward readiness and resilience. The proposed Artificial Intelligence Act introduces risk-tiered governance for emerging technologies. The Digital Europe Programme and NIS2 Directive expand cybersecurity obligations.

Fiscal structures do not match these ambitions. The Stability and Growth Pact still anchors policy in deficit and debt trajectories. The Multiannual Financial Framework sets rigid ceilings that ignore the volatility of strategic sectors. Europe pursues high-risk priorities with outdated fiscal tools.

The Union disperses strategic investment across unaligned instruments. Defence projects may be financed through the EDF, Horizon Europe, InvestEU or national budgets. Digital projects follow separate pipelines under Digital Europe, cohesion funds or national recovery plans. Each instrument uses its own risk logic. Exposure becomes incoherent.

Development finance research illustrates the consequences of fragmented risk treatment. SME financing in the MENA region suffered when lenders used inconsistent evaluation processes, weakening policy transmission.[2] The analogy is straightforward: Europe cannot manage strategic investment without coherent risk assessment.[3]

Analyses of NextGenerationEU and the Recovery Facility show how the EU gained temporary fiscal capacity while leaving long-term governance fragmented[4]. Fragmentation limits predictability, discourages co-investment and undermines policy coherence.[5]

---

2 Benedikt Barthelmess, Jean Langlois, "SME Financing in MENA: A Quantitative and Qualitative Analysis of Multilateral and Bilateral Development Lenders' Intermediated Lending Practices" *Review of Middle East Economics and Finance*, No. 3 (2020): 1-32.

3 Robert Baldwin, Martin Cave, Martin Lodge, *Understanding Regulation: Theory, Strategy and Practice* (Oxford: Oxford University Press, 2012).

4 Federico Fabbrini, *EU Fiscal Capacity* (Oxford: Oxford Univerity Press, 2022); Age Bakker, Roel Beetsma, Marco Buti, "Investing in European Public Goods While Maintaining Fiscal Discipline at Home" *Intereconomics*, No. 2 (2024): 98-103.

5 Madalina Busuioc, Martin Lodge, "The Reputational Basis of Public Accountability" *Governance*, No. 2 (2015): 247-263.

Strategic sectors face uncertainty as a structural condition. Cyberattacks propagate non-linearly. Global supply chains collapse under geopolitical pressure. Emerging technologies follow irregular curves. Regulatory frameworks shift constantly. Ignoring these realities kills strategic planning.

Research supports this point. Epidemiology-inspired cyber-threat models applied to e-government systems show that propagation of digital attacks follows measurable probabilistic dynamics.[6] Cyber-risk insurance research demonstrates that organisational exposure can be decomposed, quantified and priced.[7] Climate scenario modelling used by central banks proves that long-horizon uncertainty can be integrated into institutional planning.[8] Europe must treat uncertainty as an input, not a disturbance.

3 Actuarial Governance as Fiscal Realism

Actuarial governance applies probabilistic reasoning to public investment. It quantifies uncertainty, prices exposure and identifies correlation across projects. It clarifies the fiscal implications of political choices. It replaces vague ambition with measurable risk.

This logic already exists inside European regulatory practice. Article 325 TFEU requires sound financial management. The AI Act and NIS2 Directive rely on risk-tier frameworks. Climate-related supervisory models show how systemic uncertainty can be integrated into long-term planning. Actuarial governance extends these methods to defence-digital spending.

Treaty law does not obstruct this shift. Article 173 TFEU authorises Union support for industrial competitiveness. Article 42 TEU provides the strategic basis for cooperation in defence. The Financial Regulation stresses

6 Jean Langlois-Berthelot, Christophe Gaie, Jean-Fabrice Lebraty, "Epidemiology Inspired Cybersecurity Threats Forecasting Models Applied to e-Government", [in:] *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizen's Expectations*, ed. Christophe Gaie, Mayuri Mehta (Cham: Springer, 2024): 151-174.

7 Jean Langlois, *Evaluating and Insuring Cyber Risks within Organizations*. https://hal.science/tel-04207948/ [accessed: 13.12.2025].

8 *The Future is Uncertain. The NGFS Climate Scenarios Provide a Window into Different Plausible Futures*. https://www.ngfs.net/ngfs-scenarios-portal/. [accessed: 13.12.2025].

efficiency, economy and effectiveness, which cannot be implemented without risk-based planning.

The rules for classifying high-risk artificial intelligence systems are set out in Article 6(1) of the Artificial Intelligence Act (AI Act). According to this provision, regardless of whether an artificial intelligence system is placed on the market or put into service, such a system is considered a high-risk system if two conditions are met: 1) the artificial intelligence system is intended to be used as a safety-related component of a product covered by EU harmonisation legislation, or the artificial intelligence system itself is such a product; 2) the product of which the AI system is a safety-related component, or the AI system itself as a product, is subject to third-party conformity assessment under Union harmonisation legislation in relation to its placing on the market or putting into service. In addition to these systems, artificial intelligence systems referred to in Annex III to the Artificial Intelligence Act (Article 6(2) of the AI Act) are considered high-risk system.[9]

According to Annex III of the AI Act, for safety reasons, high-risk AI systems include the following:

1. In the area of critical infrastructure: AI systems intended for use as safety-related components of critical digital infrastructure management processes, traffic management and operation processes, or water, gas, heat or electricity supply processes (paragraph 2 of Annex III to the AI Act);
2. In the area of access to and use of essential private services and essential public services and benefits:
   a) AI systems intended for use by or on behalf of public authorities to assess the eligibility of individuals for basic public benefits

[9] On the subject of artificial intelligence, see, among others: Krzysztof Kaczmarek, Mirosław Karpiuk, Claudio Melchior, "A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data" *Prawo i Więź*, No. 3 (2024): 103-121; Pierre-Alexandre Boudy, Małgorzata Czuryk, Claudio Melchior, „The Use of New Technologies in the Field of Security" *Ius et Securitas*, No. 2 (2025): 67-78; Dominik Bierecki, Christophe Gaie, Mirosław Karpiuk, "Artificial Intelligence in e-Administration" *Prawo i Więź*, No. 1 (2025): 383-407; Krzysztof Kaczmarek, Mirosław Karpiuk, Andrea Spaziani, „Use of artificial intelligence in public sector: threats and prospects" *Studia Iuridica Toruniensia*, No. 1 (2025): 29-48; Dominik Bierecki, Christophe Gaie, Mirosław Karpiuk, Jean Langlois-Berthelot, "Creating Resilient Artificial Intelligence Systems. A Responsible Approach to Cybersecurity Risks" *Prawo i Więź*, No. 5 (2025): 131-149.

and services, including healthcare, as well as to grant, restrict, withdraw or demand the return of such benefits and services;

b) AI systems intended to be used for assessing the creditworthiness of natural persons or determining their credit score, with the exception of AI systems used for detecting financial fraud;

c) AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life insurance and health insurance;

d) AI systems designed to assess and classify emergency calls made by natural persons or to be used to dispatch or prioritise the dispatch of emergency services, including police, fire and medical services, as well as in systems for assessing the health status of patients in emergency situations (paragraph 5 of Annex III to the AI Act);

3. In the area of migration management, asylum and border control, to the extent that the use of such systems is permitted under relevant European Union or national law:

a) AI systems intended for use by or on behalf of competent public authorities or by EU institutions, bodies, offices and agencies as polygraphs or similar tools;

b) AI systems intended to be used by or on behalf of competent public authorities or by institutions, bodies, offices and agencies of the European Union for the purpose of assessing the risk, including security risks, risks of irregular migration or health risks, posed by a natural person who intends to enter or has entered the territory of a Member State;

c) AI systems intended for use by or on behalf of competent public authorities or by institutions, bodies and organisational units of the EU for the purpose of supporting competent public authorities in the examination of applications for asylum, for visas or residence permits and related complaints regarding the eligibility of natural persons applying for a specific status, including the related assessment of the credibility of evidence;

d) AI systems intended for use by or on behalf of competent public authorities or by institutions, bodies, offices and agencies of the European Union in the context of migration management, asylum and border control, for the purpose of detecting, recognising or identifying natural persons, with the exception of the verification of travel documents (paragraph 7 of Annex III to the AI Act).

The risk management system, as stated in Recital 65 of the AI Act, should include a process that is planned and implemented throughout the entire life cycle of a high-risk AI system. The purpose of this process should be to identify and mitigate the risks posed by AI systems. The risk management system should be subject to regular reviews and updates to ensure its continued effectiveness. This process should ensure that the provider identifies risks or undesirable effects, and implement measures to mitigate known and reasonably foreseeable risks associated with AI systems in relation to their intended use and reasonably foreseeable misuse, including possible risks arising from interactions between the AI system and the environment in which it operates. The risk management system should adopt optimal risk management measures in light of the current state of technical knowledge in the field of AI. When determining these measures, the supplier should document and explain the choices made and, where appropriate, involve experts. When identifying reasonably foreseeable misuse of high-risk AI systems, the supplier should take into account cases of AI system use that can reasonably be expected to result from easily predictable human behaviour in relation to a given AI system (its specific characteristics and use), even if such cases are not foreseen in the intended use and operation of the AI system.

Due to the prevalence of cyber threats, particular attention should be paid to crisis management in the area of cybersecurity.[10] According to Recital 78 of the NIS2 Directive, cybersecurity risk management measures should take into account the degree of dependence of a critical or important entity on networks and information systems and should include measures aimed at identifying the risk of incidents, preventing incidents, detecting them, responding to them, and restoring normal operation after they occur, as well as mitigating their effects. Cybersecurity risk management measures should enable a systemic analysis that takes into account the human factor in order to provide a complete picture of the security of networks and information systems. [11] Due to the need to

10 Małgorzata Czuryk, „Zarządzanie kryzysowe w obszarze bezpieczeństwa" *Ius et Securitas*, No. 1 (2025): 6.

11 For more information on cybersecurity, see, among others: Małgorzata Czuryk, „Jurisdiction of the Voivode in the Field of Crisis Management" *Studia Iuridica Lublinensia*, No. 2 (2025): 94-95. Christophe Gaie, Mirosław Karpiuk, Nicola Strizzolo, "Cybersecurity of Public Sector Institutions" *Prawo i Więź*, No. 6 (2024): 359. Dominik Bierecki, Mirosław Karpiuk, Martin Kelemen, Sergii Prylipko, „The Impact of Digital Transformation on Cybersecurity in Poland, Slovakia, and

avoid imposing disproportionate financial burdens on critical and important entities, which in turn follows from Recital 81 of the NIS2 Directive, cybersecurity risk management measures should be proportionate to the risk posed to the networks and information systems concerned, taking into account the latest state of knowledge on such measures and the cost of their implementation.

Article 9(1) of the NIS2 Directive requires Member States to designate or establish at least one competent authority responsible for incident management and crisis management in the field of large-scale cybersecurity: a cybersecurity crisis management authority. If a Member State designates or establishes more than one cybersecurity crisis management authority, it shall clearly indicate which of these authorities is to act as the coordinator for incident management and large-scale cybersecurity crisis management (Article 9(2) of the NIS2 Directive). It is also possible to designate several authorities to act as coordinators, depending on the reporting entity. This is confirmed by the implementation of the NIS2 Directive in Poland (Article 26(5)-(7) of the Act of 5 July 2018 on the national cybersecurity system). Member States shall ensure that cybersecurity crisis management authorities have adequate resources to perform their tasks effectively (Article 9(3) of the NIS2 Directive). It should be recognised that this also applies to the body acting as coordinator for incident management and large-scale cybersecurity crisis management. Member States shall ensure consistency with existing general national crisis management frameworks (Article 9(3) of the NIS2 Directive). It should be recognised that this also applies to the body acting as coordinator for incident management and crisis management in large-scale cybersecurity. Member States shall ensure consistency with existing general national crisis management frameworks (Article 9(3) of the NIS2 Directive). This concerns the consistency of resources allocated to cybersecurity crisis management authorities with existing general national crisis management frameworks. Furthermore, in accordance with Article 9(4) of the NIS2 Directive, each Member State shall adopt a national plan

Ukraine" *Prawo i Więź*, No. 6 (2025): 473-495. Małgorzata Czuryk, „Cybersecurity and Protection of Critical Infrastructure" *Studia Iuridica Lublinensia*, No. 5 (2023): 43-52. Krzysztof Kaczmarek, „Bezpieczeństwo państwa wobec współczesnych zagrożeń" *Prawo i Więź* No. 5 (2025): 576-577. Małgorzata Czuryk, „Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues" *Studia Iuridica Lublinensia*, No. 3 (2022): 31-43. Dominik Bierecki, Mirosław Karpiuk, Claudio Melchior, Nicola Strizzolo, "Security in the Era of Cybersecurity Threats" *Prawo i Więź*, No. 4 (2025): 73-87.

for responding to large-scale cybersecurity incidents and crises, setting out the objectives and modalities for incident management and large-scale cybersecurity crisis management. This plan shall specify, in particular:

1) the objectives of national preparedness measures and actions;
2) the tasks and responsibilities of cybersecurity crisis management authorities;
3) cybersecurity crisis management procedures, including their integration into the overall national crisis management framework, and information exchange channels;
4) national preparedness measures, including exercises and training;
5) relevant public and private stakeholders and infrastructure;
6) national procedures and arrangements between relevant national authorities and institutions to ensure the effective participation of the Member State concerned in coordinated incident management and large-scale cybersecurity crisis management at Union level and the effective support of the Member State concerned for such coordinated management.

The use of the phrase 'in particular' in Article 9(4) of the NIS2 Directive indicates that the national plan for responding to cybersecurity incidents and crises may also contain provisions other than those required by Article 9(4) of the NIS2 Directive. This is in line with the nature of the Directive, which binds Member States as to the result to be achieved, while leaving national authorities free to choose the form and means (Article 288(3) TFEU).

Sectoral regulation strengthens this interpretation. The Digital Europe Programme links funding to performance and resilience. The EDF Regulation encourages joint risk-taking and prioritises disruptive technologies. The European Defence Industrial Strategy demands readiness and responsiveness, which require explicit treatment of technological, regulatory and geopolitical uncertainty.[12]

The objectives of the Digital Europe programme are (according to Article 3 of the programme):

12 Christopher Hood, Henry Rothstein, Robert Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes* (Oxford: University Press, 2002); Giandomenico Majone, "From the Positive to the Regulatory State: Causes and Consequences of Changes in the Mode of Governance" *Journal of Public Policy*, No. 2 (1997): 139-167.

1) to support and accelerate the digital transformation of the European economy, industry and society;
2) to deliver the benefits of the digital transformation to citizens, public administrations and businesses across the European Union;
3) to increase Europe's competitiveness in the global digital economy;
4) to reduce the digital divide across the European Union;
5) to strengthen the strategic autonomy of the European Union through comprehensive, cross-sectoral and cross-border support.

The Digital Europe programme is also implemented in close coordination with other EU funding programmes in certain situations and aims to:

1) strengthen Europe's capabilities in key areas of digital technology and promote these capabilities through large-scale implementation;
2) in the private and public sectors, to ensure greater dissemination and use of Europe's important digital technologies, supporting digital transformation and access to digital technologies.

Cyber-risk insurance research shows that internal organisational risk can be decomposed and modelled.[13] Forecasting work based on epidemiological modelling confirms that cyber-threat propagation can be anticipated.[14] Development-finance analysis demonstrates that ignoring institutional uncertainty undermines investment impact.[15] OECD research on digital governance stresses the need for explicit risk management mechanisms.[16]

These findings converge. They show that uncertainty is quantifiable and that public authorities can integrate it into fiscal decision-making.

13 Rainer Böhme, Stefan Laube, Markus Riek, "Cyber Insurance: Models, Markets, and Misconceptions" *IEEE Security & Privacy*, No. 3 (2022): 42-51.

14 Cameron Nowzari, Victor Preciado, George Pappas, "Analysis and Control of Epidemics: A Survey of Spreading Processes on Complex Networks" *IEEE Control Systems Magazine*, No. 1 (2016): 26-46.

15 Philippe Aghion, Céline Antonin, Simon Bunel, *The Power of Creative Destruction: Economic Upheaval and the Wealth of Nations* (Harvard: Harvard University Press, 2021).

16 *Government at a Glance 2023*. https://www.oecd.org/en/publications/government-at-a-glance-2023_3d5c5d31-en.html. [accessed: 15.12.2025].

4 Integration into Existing EU Fiscal Instruments

The European Defence Fund already contains language on performance and risk. Regulation (EU) 2021/697 establishes its mandate. Actuarial integration requires a classification of project risk profiles based on technological readiness, supply-chain dependencies, regulatory constraints and export-control exposures.

Funding intensity must follow exposure. High-risk, high-value projects should receive higher EU co-financing. Low-risk projects receive less. This produces a risk-adjusted strategic portfolio aligned with the objectives of the European Defence Industrial Strategy.

Programmes under the Digital Europe agenda handle high systemic cyber risk. Threat forecasting methods can support ex-ante evaluation. Epidemiology-based models identify propagation vectors and vulnerabilities within digital administrations.[17] OECD guidelines emphasise the need for economic and administrative integration of digital-security risk management.[18] Aligning funding with measurable exposure increases coherence and credibility.

The European Investment Bank already uses risk-weighted approaches in climate and infrastructure financing. Defence-digital projects can be incorporated into this system with adjusted parameters. The EIB can publish aggregate exposure to strategic-risk windows.

National finance ministries can mirror these methods in co-financing rules. Convergence around expected loss, variance and long-horizon exposure creates consistent fiscal behaviour across Member States. This supports private-sector participation and strengthens fiscal predictability.

It is also worth noting the framework for managing risks related to information and communication technologies (ICT) in the case of financial entities, which is set out in Article 6 of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the operational digital resilience of the financial sector (DORA). According to this provision, financial entities should have (as part of their overall risk management system) a robust, comprehensive and well-documented ICT risk management framework that enables them to respond quickly,

17 Langlois-Berthelot, Gaie, Lebraty, "Epidemiology Inspired Cybersecurity Threats Forecasting Models Applied to e-Government", 151-174.

18 *Digital security risk management*, https://www.oecd.org/en/topics/digital-security-risk-management.html [accessed: 15.12.2025]; *OECD Digital Government Index*, https://goingdigital.oecd.org/en/indicator/58 [accessed: 15.12.2025].

effectively and comprehensively to ICT risks and ensures a high level of operational digital resilience. ICT risk management includes at least the strategies, policies, procedures, protocols and ICT tools necessary for the proper and adequate protection of information and ICT resources, including software and hardware, servers, as well as physical elements and infrastructure such as facilities, data centres and designated sensitive areas, in order to ensure adequate protection against risks, including damage and unauthorised access or use. Financial entities shall ensure adequate separation and independence of ICT risk management, control and internal audit functions. ICT risk management shall be documented and reviewed at least annually, or periodically in the case of micro-enterprises, as well as in the event of serious ICT incidents and in accordance with supervisory instructions or conclusions resulting from relevant tests or operational digital resilience audit processes. Based on the conclusions of the audit review, financial entities shall establish a formal follow-up process, including rules for the timely verification and implementation of remedial measures following critical ICT audit findings.

It should also be noted that these general rules are modified in relation to entities for which DORA requires the proportionate application of DORA provisions on ICT risk management. Pursuant to Article 4(1) of DORA, financial entities shall apply these provisions taking into account the principle of proportionality. The factors influencing the proportionate application of these provisions are the size and overall risk profile of the financial entity and the nature, scale and complexity of its services, activities and operations. Since the application of DORA involves the exercise of supervisory powers over financial institutions, Article 4(1) of DORA sets limits on the interference of EU and national public authorities in the sphere of individual freedoms.[19] In the context of financial entities using AI systems, it should be noted that their resilience depends on ICT cybersecurity. This is confirmed by Recital 76 of the AI Act, according to which cyberattacks on AI systems may rely on exploiting vulnerabilities in the digital assets of the AI system or in the underlying ICT infrastructure. This Recital also states that in order to ensure a risk-appropriate level of cybersecurity, providers of high-risk AI systems should therefore implement appropriate measures, such as security control mechanisms,

19 Dominik Bierecki, "Zasada proporcjonalności w stosowaniu rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operational Resilience Act – DORA)" *Europejski Przegląd Prawa i Stosunków Międzynarodowych*, No. 3 (2024): 8-9.

also taking into account, where applicable, the ICT infrastructure on which the system relies. Therefore, with regard to financial market entities, there is a convergence of legal standards between the AI Act and DORA in the area of cybersecurity of ICT infrastructure intended for the operation of AI systems (including high-risk systems). The AI Act stipulates that technical solutions aimed at ensuring the cybersecurity of high-risk AI systems must be adapted to the relevant circumstances and risks (Article 15(5)(2) of the AI Act). In this context, the AI Act does not specify which circumstances should be taken into account. It therefore seems that this also concerns circumstances related to the characteristics of the financial entity, which are listed in Article 4(1) of DORA: the size and overall risk profile of the financial entity and the nature, scale and complexity of its services, activities and operations. While these characteristics do not affect the risks associated with the operation of an AI system, they do affect the framework for managing the risks associated with the ICT used to operate AI.

5 Sovereignty, Accountability and Fiscal Culture

Strategic autonomy requires fiscal tools capable of supporting long-term investment. Analyses of the Recovery and Resilience Facility and Next-GenerationEU describe these programmes as prototypes of collective fiscal capacity.[20] Europe needs to extend this logic to defence-digital investment rather than rely on crisis-driven improvisation.[21]

Risk-based governance raises concerns about opacity. Yet climate-risk supervision and digital-government metrics show that complex modelling can coexist with transparency. NGFS scenarios, OECD indicators and European Court of Auditors reviews provide accessible data for public scrutiny. Publishing strategic-risk metrics in defence-digital spending would reinforce democratic legitimacy.[22]

---

20 Fabbrini, *EU Fiscal Capacity*; Bakker, Beetsma, Buti, "Investing in European Public Goods While Maintaining Fiscal Discipline at Home", 98-103.

21 Francesco Corti, Patrik Vesan, "The Politics of the Recovery and Resilience Facility" *Journal of European Public Policy*, No. 9 (2022): 1447-1466; Zsolt Darvas, Guntram Wolff, "A Green Fiscal Pact: Climate Investment in Times of Budget Consolidation" *Bruegel Policy Contribution*, No. 18 (2021): 1-22.

22 Lucas Schramm, Ulrich Krotz, "Embedded Bilateralism, Fiscal Capacity and European Crisis Governance" *Journal of European Integration*, No. 6 (2021): 731-748;

European institutions must accept uncertainty as a baseline condition. Cyber-risk modelling, climate-scenario analysis and development-finance methodologies already show how uncertainty can be quantified. Actuarial governance is not bureaucracy; it is discipline. Europe must shift from deterministic planning to anticipatory fiscal strategy.[23]

6 Conclusion

European sovereignty in the defence-digital age depends on the ability to finance high-risk sectors under conditions of permanent uncertainty. Current fiscal governance remains tied to stability assumptions that no longer hold. Fragmented risk assessment and deterministic budgetary logic undermine Europe's strategic ambitions.

Actuarial governance provides the missing connective tissue. It requires no new institutions and no treaty change. It introduces uncertainty into fiscal planning, prices exposure and aligns strategic investment with measurable risk. Empirical evidence from cyber-risk insurance,[24] cyber-threat forecasting[25] and development finance[26] shows that complex risks can be quantified and governed.[27]

Erik Jones, Daniel Kelemen & Sophie Meunier, "Failing Forward? The Euro Crisis and the Incomplete Nature of European Integration" *Comparative Political Studies*, No. 10 (2021): 1693-1721.

23 Benedikt Barthelmess, Jean Langlois, *Tokenomics: Emerging Strands of Research*. https://ideas.repec.org/p/hal/wpaper/hal-04179572.html. [accessed: 16.12.2025].

24 Langlois, *Evaluating and Insuring Cyber Risks within Organizations*.

25 Böhme, Laube, Riek, "Cyber Insurance: Models, Markets, and *Misconceptions*, 42-51; Martin Eling, Werner Schnell, "What Do We Know About Cyber Risk and Cyber Risk Insurance?" *Journal of Risk Finance*, No. 5 (2016): 474-491.

26 Ray Berkelmans, Jason van der Merwe, "Risk-Sharing, Development Finance, and the Role of Multilateral Development Banks" *World Development*, No. 144 (2021); Chris Humphrey, "Are Credit Rating Agencies Limiting the Capital-Raising Capacity of Multilateral Development Banks?" *Review of International Political Economy*, No. 6, (2020): 1378-1407; Rishikesh Bhandary, Kelly Gallagher, Fang Zhang, "Climate Finance, Development Banks, and Blended Finance: Governance Challenges and Solutions" *Global Policy*, No. 1 (2022): 36-49.

27 Baldwin, Cave, Lodge, *Understanding Regulation: Theory, Strategy and Practice*.

If Europe embeds actuarial reasoning into its fiscal architecture, it will build strategic autonomy on a foundation of discipline instead of improvisation. Sovereignty becomes measurable. Strategy becomes financially credible. Uncertainty becomes governable.[28]

Bibliography

Aghion Philippe, Céline Antonin, Simon Bunel, *The Power of Creative Destruction: Economic Upheaval and the Wealth of Nations*. Harvard: Harvard University Press, 2021.

Bakker Age, Roel Beetsma, Marco Buti, "Investing in European Public Goods While Maintaining Fiscal Discipline at Home" *Intereconomics*, No. 2 (2024): 98-103.

Baldwin Robert, Martin Cave, Martin Lodge, *Understanding Regulation: Theory, Strategy and Practice*. Oxford: Oxford University Press, 2012.

Bannister Frank, Regina Connolly, "ICT, Public Values and Transformative Government: A Framework and Programme for Research" *Government Information Quarterly*, No. 1 (2014): 119-128.

Barthelmess Benedikt, Jean Langlois, "SME Financing in MENA: A Quantitative and Qualitative Analysis of Multilateral and Bilateral Development Lenders' Intermediated Lending Practices" *Review of Middle East Economics and Finance*, No. 3 (2020): 1-32.

Barthelmess Benedikt, Jean Langlois, *Tokenomics: Emerging Strands of Research*. https://ideas.repec.org/p/hal/wpaper/hal-04179572.html.

Berkelmans Ray, Jason van der Merwe, "Risk-Sharing, Development Finance, and the Role of Multilateral Development Banks" *World Development*, No. 144 (2021).

Bierecki Dominik, Christophe Gaie, Mirosław Karpiuk, "Artificial Intelligence in e-Administration *Prawo i Więź*, No. 1 (2025): 383-407. https://doi.org/10.36128/PRIW.VI54.1201.

28 Marijn Janssen, Haiko van der Voort, " Adaptive Governance: Towards a Stable, Accountable and Responsive Government" *Government Information Quarterly*, No. 1 (2016): 1-5; Frank Bannister, Regina Connolly, "ICT, Public Values and Transformative Government: A Framework and Programme for Research" *Government Information Quarterly*, No. 1 (2014): 119-128; Antonio Cordella, Carla Bonina, "A Public Value Perspective for ICT Enabled Public Sector Reforms: A Theoretical Reflection" *Government Information Quarterly*, No. 4 (2012): 512-520.

Bierecki Dominik, Christophe Gaie, Mirosław Karpiuk, Jean Langlois-Berthelot, "Creating Resilient Artificial Intelligence Systems. A Responsible Approach to Cybersecurity Risks" *Prawo i Więź*, No. 5 (2025): 131-149. https://doi.org/10.36128/0akf8v90.

Bierecki Dominik, Mirosław Karpiuk, Claudio Melchior, Nicola Strizzolo, "Security in the Era of Cybersecurity Threats" *Prawo i Więź*, No. 4 (2025): 73-87. https://doi.org/10.36128/PRIW.VI57.1476.

Bierecki Dominik, Mirosław Karpiuk, Martin Kelemen, Sergii Prylipko, „The Impact of Digital Transformation on Cybersecurity in Poland, Slovakia, and Ukraine" *Prawo i Więź*, No. 6 (2025): 473-495. https://doi.org/10.36128/c2xvy848.

Bierecki Dominik, "Zasada proporcjonalności w stosowaniu rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego (Digital Operational Resilience Act – DORA)" *Europejski Przegląd Prawa i Stosunków Międzynarodowych*, No. 3 (2024): 8-9.

Böhme Rainer, Stefan Laube, Markus Riek, "Cyber Insurance: Models, Markets, and Misconceptions" *IEEE Security & Privacy*, No. 3 (2022): 42-51.

Boudy Pierre-Alexandre, Małgorzata Czuryk, Claudio Melchior, „The Use of New Technologies in the Field of Security" *Ius et Securitas*, No. 2 (2025): 67-78.

Busuioc Madalina, Martin Lodge, "The Reputational Basis of Public Accountability" *Governance*, No. 2 (2015): 247-263. https://doi.org/10.1111/gove.12161.

Cordella Antonio, Carla Bonina, "A Public Value Perspective for ICT Enabled Public Sector Reforms: A Theoretical Reflection" *Government Information Quarterly*, No. 4 (2012): 512-520.

Corti Francesco, Patrik Vesan, "The Politics of the Recovery and Resilience Facility" *Journal of European Public Policy*, No. 9 (2022): 1447-1466.

Czuryk Małgorzata, „Cybersecurity and Protection of Critical Infrastructure" *Studia Iuridica Lublinensia*, No. 5 (2023): 43-52. https://doi.org/10.17951/sil.2023.32.5.43-52.

Czuryk Małgorzata, „Jurisdiction of the Voivode in the Field of Crisis Management" *Studia Iuridica Lublinensia*, No. 2 (2025): 94-95. https://doi.org/10.17951/sil.2025.34.2.87-98.

Czuryk Małgorzata, „Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues" *Studia Iuridica Lublinensia*, No. 3 (2022): 31-43. https://doi.org/10.17951/sil.2022.31.3.31-43.

Czuryk Małgorzata, „Zarządzanie kryzysowe w obszarze bezpieczeństwa" *Ius et Securitas*, No. 1 (2025): 5-12.

Darvas Zsolt, Guntram Wolff, "A Green Fiscal Pact: Climate Investment in Times of Budget Consolidation" *Bruegel Policy Contribution*, No. 18 (2021): 1-22.

Digital security risk management. https://www.oecd.org/en/topics/digital-security-risk-management.html.

Eling Martin, Werner Schnell, "What Do We Know About Cyber Risk and Cyber Risk Insurance?" *Journal of Risk Finance*, No. 5 (2016): 474-491.

Fabbrini Federico, *A Fiscal Capacity for the Eurozone: Constitutional Perspectives*. Brussels: Policy Department for Citizens' Rights and Constitutional Affairs, 2019.

Fabbrini Federico, *EU Fiscal Capacity*. Oxford: Oxford Univerity Press, 2022.

Gaie Christophe, Mirosław Karpiuk, Nicola Strizzolo, "Cybersecurity of Public Sector Institutions" *Prawo i Więź*, No. 6 (2024): 347-362, https://doi.org/10.36128/PRIW.VI53.1129.

Government at a Glance 2023. https://www.oecd.org/en/publications/government-at-a-glance-2023_3d5c5d31-en.html.

Hood Christopher, Henry Rothstein, Robert Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford: University Press, 2002.

Humphrey Chris, "Are Credit Rating Agencies Limiting the Capital-Raising Capacity of Multilateral Development Banks?" *Review of International Political Economy*, No. 6, (2020): 1378-1407.

Janssen Marijn, Haiko van der Voort, "Adaptive Governance: Towards a Stable, Accountable and Responsive Government" *Government Information Quarterly*, No. 1 (2016): 1-5.

Jones Erik, Daniel Kelemen, Sophie Meunier, " Failing Forward? The Euro Crisis and the Incomplete Nature of European Integration" *Comparative Political Studies*, No. 10 (2021): 1693-1721.

Kaczmarek Krzysztof, „Bezpieczeństwo państwa wobec współczesnych zagrożeń" *Prawo i Więź* No. 5 (2025): 567-580. https://doi.org/10.36128/.

Kaczmarek Krzysztof, Mirosław Karpiuk, Claudio Melchior, "A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data" *Prawo i Więź*, No. 3 (2024): 103-121. https://doi.org/10.36128/PRIW.VI50.907.

Krzysztof Kaczmarek, Mirosław Karpiuk, Andrea Spaziani, „Use of Artificial Intelligence in Public Sector: Threats and Prospects" *Studia Iuridica Toruniensia*, No. 1 (2025): 29-48. http://dx.doi.org/10.12775/SIT.2025.002.

Langlois Jean, *Evaluating and Insuring Cyber Risks within Organizations*. https://hal.science/tel-04207948/.

Langlois-Berthelot Jean, Christophe Gaie, Jean-Fabrice Lebraty, "Epidemiology Inspired Cybersecurity Threats Forecasting Models Applied to e-Government," [in:] *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizens' Expectations*, ed. Christophe Gaie, Mayuri Mehta. 151-174. Cham: Springer, 2024.

Majone Giandomenico, "From the Positive to the Regulatory State: Causes and Consequences of Changes in the Mode of Governance" *Journal of Public Policy*, No. 2 (1997): 139-167.

Nowzari Cameron, Victor Preciado, George Pappas, "Analysis and Control of Epidemics: A Survey of Spreading Processes on Complex Networks" *IEEE Control Systems Magazine*, No. 1 (2016): 26-46.

OECD Digital Government Index. https://goingdigital.oecd.org/en/indicator/58.

Rishikesh Bhandary, Kelly Gallagher, Fang Zhang, "Climate Finance, Development Banks, and Blended Finance: Governance Challenges and Solutions" *Global Policy*, No. 1 (2022): 36-49.

Schramm Lucas, Ulrich Krotz, "Embedded Bilateralism, Fiscal Capacity and European Crisis Governance" *Journal of European Integration*, No. 6 (2021): 731-748.

The Future is Uncertain. The NGFS Climate Scenarios Provide a Window into Different Plausible Futures. https://www.ngfs.net/ngfs-scenarios-portal/.