



www.turkishstudies.net/economy

Turkish Studies - Economics, Finance, Politics

eISSN: 2667-5625

Research Article / Araştırma Makalesi



Organizational Immunity Architecture: A Preventive Early Warning Model Proposal

Örgütsel Bağışıklık Mimarisi: Önleyici Bir Erken Uyarı Model Önerisi

Osman Kara*

Abstract: Organizations often discuss crises through their visible outcomes; however, many organizational breakdowns deepen because weak signals, delayed decisions, disrupted information flows, and normalized minor deviations that emerge before the crisis are not recognized in time. The existing literature makes strong contributions to this debate through organizational resilience, dynamic capabilities, weak signals, organizational learning, and organizational memory. Nevertheless, these approaches remain limited in offering an integrated explanation of how organizations diagnose pre-crisis vulnerabilities, at which thresholds they generate alarms, how they initiate preventive intervention, and how they transform these experiences into organizational learning. This study reconceptualizes organizational immunity not as a defensive capacity activated after a crisis, but as a cyclical architecture that connects early warning, weak-link diagnosis, risk thresholds, preventive intervention, and organizational learning processes. The proposed organizational immunity architecture is built on four panels: leadership/structure, adaptation, integration, and intellectual capital. These panels treat organizational weaknesses not as general performance problems, but as diagnostic domains that can be read through decision clarity, responsiveness to change, systemic coherence, and the preservation and use of knowledge. In this respect, the model is not a new label for resilience, dynamic capabilities, or organizational learning; rather, it is an original theoretical framework that integrates the explanatory power of these literatures within a cycle of early diagnosis and preventive regulation. The study contributes to organizational immunity research by shifting the focus from post-crisis reaction to pre-crisis diagnosis, threshold assessment, and learning-oriented intervention. The model can be tested in future longitudinal, multi-source, and event-based studies; it also provides a conceptual basis for designing early warning panels, weak-link analyses, and preventive governance mechanisms in organizations.

Keywords: Organizational Immunity Architecture, Early Warning Systems, Weak Signal Detection, Pre-crisis Diagnosis, Preventive Intervention, Management and Organization, Organizational behavior

Öz: Örgütler krizleri çoğu zaman görünür sonuçları üzerinden tartışır; oysa birçok örgütsel kırım, krizden önce beliren zayıf işaretlerin, geciken kararların, kopan bilgi akışlarının ve olağanlaşan küçük sapmaların

* Dr., Independent Researcher

Dr., Bağımsız Araştırmacı

ORCID <https://orcid.org/0009-0008-9313-4150>

osmkara@msn.com

Cite as/ Atıf: Kara, O. (2026). Organizational immunity architecture: A preventive early warning model proposal / Örgütsel bağışıklık mimarisi: Önleyici bir erken uyarı model önerisi. *Turkish Studies – Economics, Finance, Politics*, 21(Ö1), 1759-1810. [Special Issues Dedicated to Prof. Dr. Mahmut Özer], Ankara Bilim University Publications. <https://dx.doi.org/10.7827/TurkishStudies.94479>

Received/Geliş: 20 May/ Mayıs 2026

Accepted/Kabul: 15 September/Eylül 2026

Published/Yayın: 20 September/Eylül 2026

Checked by plagiarism software



zamanında okunamamasıyla derinleşir. Mevcut literatür örgütsel dayanıklılık, dinamik yetenekler, zayıf sinyaller, örgütsel öğrenme ve örgütsel hafıza üzerinden bu tartışmaya güçlü katkılar sunmaktadır. Bununla birlikte bu yaklaşımlar, örgütlerin kriz öncesi kırılma noktaları nasıl teşhis ettiği, hangi eşiklerde alarm ürettiği, önleyici müdahaleyi nasıl başlattığı ve bu deneyimi nasıl kurumsal öğrenmeye dönüştürdüğü konusunda bütüncül bir açıklama sunmakta sınırlı kalmaktadır. Bu çalışma, örgütsel bağışıklık kavramını kriz sonrasında devreye giren savunmacı bir kapasite olarak değil, erken uyarı, zayıf halka teşhisi, risk eşiği, önleyici müdahale ve örgütsel öğrenme süreçlerini birbirine bağlayan döngüsel bir mimari olarak yeniden kavramsallaştırmaktadır. Önerilen örgütsel bağışıklık mimarisi, liderlik/yapı, adaptasyon, entegrasyon ve entelektüel sermaye panelleri üzerine kuruludur. Bu paneller, örgütsel zayıflıkları genel performans sorunları olarak değil; karar açıklığı, değişime yanıt verme kapasitesi, sistem içi bütünlük ve bilginin korunup kullanılabilmesi üzerinden okunabilen teşhis alanları olarak ele almaktadır. Bu yönüyle model, dayanıklılık, dinamik yetenekler ya da örgütsel öğrenmenin yeni bir adı değildir; bu literatürlerin açıklayıcı gücünü erken teşhis ve önleyici düzenleme döngüsünde birleştiren özgün bir kuramsal çerçevedir. Çalışma, örgütsel bağışıklık çalışmalarına kriz sonrası tepki yerine kriz öncesi tanı, eşik değerlendirmesi ve öğrenen müdahale mantığını eklemektedir. Model, ileride boylamsal, çok kaynaklı ve olay-temelli araştırmalarla test edilebilir; ayrıca örgütlerde erken uyarı panelleri, zayıf halka analizleri ve önleyici yönetim mekanizmalarının tasarlanması için kavramsal bir zemin sunar.

Anahtar kelimeler: Örgütsel Bağışıklık Mimarisi, Erken Uyarı Sistemleri, Zayıf Sinyal Tespiti, Kriz Öncesi Tanı, Önleyici Müdahale, Yönetim ve Organizasyon, Örgütsel Davranış.

Structured Abstract:

This study conceptualizes the organizational immunity architecture not as a defensive reflex activated after a crisis emerges, but as a cyclical diagnosis and learning architecture capable of reading the early signs that generate the possibility of crisis, distinguishing the sources of vulnerabilities, assessing risk thresholds, initiating preventive intervention, and transforming this experience into organizational learning and memory. The main question of the study is how organizations recognize weak signals before a crisis becomes visible, how they diagnose vulnerable points within the organization, at which thresholds they generate alarms, and how they transform this diagnosis into preventive managerial action. Contemporary organizations face not only competitive pressure and technological change, but also supply chain disruptions, workforce mobility, reputational risk, deterioration in information flows, and sudden environmental fluctuations. Under these conditions, explaining organizational success solely through how rapidly an organization recovers after a crisis remains insufficient. The truly critical issue is whether the weak signals that emerge before a crisis becomes visible are noticed, whether vulnerable points within the organization are diagnosed in time, and whether this diagnosis can be transformed into preventive managerial action.

Although the organizational immunity architecture shares the same field of debate with the literatures on resilience, dynamic capabilities, risk management, weak signals, organizational learning, organizational memory, and intellectual capital, it is not a simple sum of these concepts. The resilience literature explains the capacity of organizations to maintain functionality in the face of unexpected events, adapt under pressure, and establish a new equilibrium after disruption. The organizational immunity architecture, however, approaches how resilience becomes possible from an earlier point: through which indicators is deterioration within the organization noticed before it turns into performance loss, crisis behavior, or visible collapse, and how is it connected to preventive decisions? While the dynamic capabilities approach focuses on the ability of organizations to integrate, reconfigure, and transform their resources in changing environments, the organizational immunity architecture discusses how the need for such reconfiguration is diagnosed and under which conditions it gains priority. Risk management offers a systematic framework for identifying, classifying, monitoring, and controlling uncertainties; however, within the organizational immunity architecture, the issue is not merely to identify or reduce risks. The more fundamental issue is the organization's ability to recognize immunity losses occurring within itself in time, to interpret these losses managerially, and to transfer the information obtained into learning and memory processes.

This study is based on a conceptual model development approach. Therefore, no quantitative or qualitative population, sample, field data, data collection instrument, or scale was used in the study. The main methodological basis is the analytical integration of the literatures explaining the organizational immunity architecture and their rearticulation within the processes of early warning, weak-link diagnosis, risk threshold, preventive intervention, organizational learning, and organizational memory. The proposed model is built on four main panels: leadership/structure, adaptation, integration, and intellectual capital. These panels are not independent measurement headings, but complementary diagnostic domains that help explain where the organization weakens, through which channels this weakness spreads, and what kind of intervention it requires. If the model is empirically tested in the future, employee surveys, error reports, project delays, employee turnover rates, customer complaints, internal audit findings, and meeting records can be used together.

As a result of the conceptual study, it is concluded that the organizational immunity architecture is not a control activity conducted at certain intervals, but a continuously operating cycle of early warning and preventive intervention. The organization collects signals from the environment and from its own internal order, interprets them, distinguishes the source of weakness, intervenes when necessary, and transfers this experience to its subsequent decisions. The diagnostic quality of the model stems from its evaluation of early warning indicators within the organization not as isolated symptoms, but as patterns associated with organizational functions. The unusual prolongation of decision-making processes, the blurring of role and authority boundaries, delayed or incomplete circulation of information among units, coordination weaknesses, the concentration of critical knowledge in a few individuals, the repetition of the same mistakes, or employees' inability to express problems openly do not, by themselves, mean crisis. However, when such indicators are monitored together and over time, they may provide important clues about the area in which the organization is experiencing immunity loss. The Challenger and Columbia examples show why the organizational immunity architecture should focus not only on technical risks, but also on organizational interpretation, culture, communication, and decision-making structure.

In conclusion, the organizational immunity architecture builds its claim to make organizations more resilient against crises on the capacity to perceive earlier, interpret more accurately, and intervene in a more timely manner. The model does not promise a flawless control system; it reminds us that vulnerabilities often appear before visible outcomes, in the form of small deviations and neglected signals. Therefore, how early, how honestly, and how learning-oriented organizations can read their own weaknesses should be at the center of management and organization research, as much as how strong they are. For practitioners, early warning panels, weak-link analyses, risk threshold indicators, and preventive governance mechanisms can be developed. For researchers, it is recommended that the model be tested through longitudinal, multi-source, and event-based designs, and through the panels of leadership/structure, adaptation, integration, and intellectual capital.

Keywords: Organizational Immunity Architecture; Early Warning Systems; Weak Signal Detection; Pre-crisis Diagnosis; Preventive Intervention; Organizational Learning; Management and Organization; Organizational Behavior.

الملخص المنظم:

تقدم هذه الدراسة تصوراً لمعمارية المناعة التنظيمية، لا بوصفها رد فعل دفاعياً يُفعل بعد نشوء الأزمة، بل بوصفها معمارية دورية للتشخيص والتعلم، قادرة على قراءة العلامات المبكرة التي تُفضي إلى احتمال نشوء الأزمات، والتميز بين مصادر مواطن الهشاشة، وتقييم عتبات المخاطر، والشروع في التدخل الوقائي، وتحويل هذه الخبرة إلى تعلم تنظيمي وذاكرة تنظيمية. ويتمثل السؤال الرئيس للدراسة في كيفية تعرف المنظمات على الإشارات الضعيفة قبل أن تصبح الأزمة ظاهرة، وكيفية تشخيص مواطن الهشاشة داخل المنظمة، وتحديد العتبات التي تُطلق عندها الإنذارات، وكيفية تحويل هذا التشخيص إلى إجراءات إدارية وقائية. فالمنظمات المعاصرة لا تواجه الضغوط التنافسية والتغير التكنولوجي فحسب، بل تواجه أيضاً اضطرابات سلاسل الإمداد، وحركية القوى العاملة، ومخاطر السمعة، وتدهور تدفقات المعلومات، والتقلبات المفاجئة في البيئة المحيطة. وفي ظل هذه الظروف، يظل تفسير النجاح التنظيمي استناداً حصرياً إلى سرعة تعافي المنظمة بعد الأزمة تفسيراً غير كافٍ. وتكمن المسألة الحاسمة في مدى رصد الإشارات الضعيفة التي تظهر قبل أن تصبح الأزمة مرئية، وتشخيص مواطن الهشاشة داخل المنظمة في الوقت المناسب، وإمكان تحويل هذا التشخيص إلى إجراءات إدارية وقائية.

وعلى الرغم من أن معمارية المناعة التنظيمية تشترك في الحل النقاشي ذاته مع أدبيات الصمود التنظيمي، والقدرات الديناميكية وإدارة المخاطر، والإشارات الضعيفة، والتعلم التنظيمي، والذاكرة التنظيمية، ورأس المال الفكري، فإنها لا تمثل مجرد حاصل جمع لهذه المفاهيم فأدبيات الصمود التنظيمي تفسر قدرة المنظمات على الحفاظ على وظائفها في مواجهة الأحداث غير المتوقعة، والتكيف تحت الضغط، وإرساء توازن جديد بعد الاضطراب. أما معمارية المناعة التنظيمية فتتناول كيفية التي يصبح بها الصمود ممكناً انطلاقاً من مرحلة أسبق: فمن خلال أي مؤشرات يُرصد التدهور داخل المنظمة قبل أن يتحول إلى تراجع في الأداء، أو سلوك أزموي، أو انهيار ظاهر، وكيف يُربط هذا الرصد بالقرارات الوقائية؟ وبينما يركز مدخل القدرات الديناميكية على قدرة المنظمات على دمج مواردها وإعادة تشكيلها وتحويلها في البيانات المتغيرة، تناقش معمارية المناعة التنظيمية كيفية تشخيص الحاجة إلى إعادة التشكيل هذه، والظروف التي تكتسب فيها الأولوية. وتوفر إدارة المخاطر إطاراً منهجياً لتحديد أوجه عدم اليقين وتصنيفها ورصدها وضبطها؛ غير أن المسألة، ضمن معمارية المناعة التنظيمية، لا تقتصر على تحديد المخاطر أو الحد منها. بل تتمثل المسألة الأكثر جوهرية في قدرة المنظمة على التعرف، في الوقت المناسب، على ما يطرأ داخلها من تراجع في المناعة التنظيمية، وتفسيره إدارياً، وإدماج المعلومات المستخلصة منه في عمليات التعلم والذاكرة التنظيمية.

تستند هذه الدراسة إلى مقارنة تطوير نموذج مفاهيمي. ومن ثم، لم تعتمد على مجتمع بحث أو عينة ضمن تصميم كمي أو نوعي، ولم تستخدم بيانات ميدانية أو أداة لجمع البيانات أو مقياساً. ويتمثل مرتكزها المنهجي الرئيس في التكامل التحليلي للأدبيات المفسرة لمعمارية المناعة التنظيمية، وإعادة صياغة الروابط بينها ضمن عمليات الإنذار المبكر، وتشخيص الحلقات الضعيفة، وتحديد عتبات المخاطر، والتدخل الوقائي والتعلم التنظيمي، والذاكرة التنظيمية. ويقوم النموذج المقترح على أربع لوحات رئيسية: القيادة/الهيكل التنظيمي، والتكيف، والتكامل، ورأس المال الفكري. ولا تمثل هذه اللوحات محاور قياس مستقلة، بل مجالات تشخيصية متكاملة تساعد على تفسير مواضع ضعف المنظمة، والقنوات التي ينتشر عبرها هذا الضعف، ونوع التدخل الذي يستلزمه. وفي حال اختبار النموذج تجريبياً في المستقبل، يمكن الجمع بين استبانات العاملين وتقارير الأخطاء، وبيانات تأخر المشاريع، ومعدلات دوران العاملين، وشكاوى العملاء، ونتائج التدقيق الداخلي، ومحاضر الاجتماعات.

وتخلص الدراسة المفاهيمية إلى أن معمارية المناعة التنظيمية ليست نشاطاً رقابياً يُنفذ على فترات محددة، بل دورة مستمرة من الإنذار المبكر والتدخل الوقائي. فالمنظمة تجمع الإشارات من بيئتها ومن نظامها الداخلي، وتفسرها، وتميز مصدر الضعف، وتتدخل عند الضرورة، وتنقل هذه الخبرة إلى قراراتها اللاحقة. وتتبع القيمة التشخيصية للنموذج من تقييمه مؤشرات الإنذار المبكر داخل المنظمة بوصفها أنماطاً مرتبطة بالوظائف التنظيمية، لا أعراضاً منعزلة. فاستطالة عمليات اتخاذ القرار على نحو غير معتاد، وضبابية حدود الأدوار والصلاحيات، وتأخر تداول المعلومات بين الوحدات أو عدم اكتماله، وأوجه القصور في التنسيق، وتركز المعارف الحرجة لدى عدد محدود من الأفراد، وتكرار الأخطاء ذاتها، أو عدم قدرة العاملين على التعبير عن المشكلات بصراحة، لا تعني، كلٌ منها على حدة، وجود أزمة. غير أن رصد هذه المؤشرات مجتمعة وعلى امتداد الزمن قد يوفر قرائن مهمة على المجال الذي تشهد فيه المنظمة تراجعاً في مناعتها التنظيمية.

وُتَظْهَرُ حَالَتَا «تَشَالَنْجَر» و«كُولُومْبِيَا» لِمَاذَا يَنْبَغِي أَنْ تَرْكُزَ مَعْمَارِيَّةُ الْمَنَاعَةِ التَّنْظِيمِيَّةِ، إِلَى جَانِبِ الْمَخَاطِرِ التَّقْنِيَّةِ، عَلَى التَّفْسِيرِ التَّنْظِيمِيِّ وَالثَّقَافَةِ، وَالِاتِّصَالِ، وَبِنِيَّةِ اتِّخَاذِ الْقَرَارِ

وختامًا، تؤسس معمارية المناعة التنظيمية طرحها بشأن تعزيز صمود المنظمات في مواجهة الأزمات على القدرة على الاستشعار المبكر، والتفسير الأكثر دقة، والتدخل في التوقيت الأنسب. ولا يعد النموذج بنظام رقابي خالٍ من العيوب؛ بل يلفت الانتباه إلى أن مواطن الهشاشة غالبًا ما تظهر قبل نتائجها المرئية، في صورة انحرافات طفيفة وإشارات مُهمَّلة. ولذلك، ينبغي أن يحتل مدى قدرة المنظمات على قراءة مواطن ضعفها مبكرًا وبصدق وبمنظور موجه نحو التعلُّم موقعًا محوريًا في بحوث الإدارة والتنظيم، بقدر ما يحتلّه مدى قوتها. وعلى مستوى الممارسين، يمكن تطوير لوحات للإنذار المبكر، وتحليلات للحلقات الضعيفة، ومؤشرات لعتبات المخاطر، وآليات للحوكمة الوقائية. أما على مستوى الباحثين، فتوصي الدراسة باختبار النموذج باستخدام تصاميم بحثية طويلة، ومتعددة المصادر، وقائمة على الأحداث، ومن خلال لوحات القيادة/الهيكل التنظيمي، والتكيف، والتكامل، ورأس المال الفكري

الكلمات المفتاحية: معمارية المناعة التنظيمية؛ نظم الإنذار المبكر؛ رصد الإشارات الضعيفة؛ التشخيص السابق للضرورة؛ التدخل الوقائي؛ التعلُّم التنظيمي؛ الإدارة والتنظيم؛ السلوك التنظيمي

Résumé Structuré:

Cette étude conceptualise l'architecture de l'immunité organisationnelle non comme un réflexe défensif activé après l'émergence d'une crise, mais comme une architecture cyclique de diagnostic et d'apprentissage, capable de déceler les signes précoces susceptibles de conduire à une crise, de distinguer les sources de vulnérabilité, d'évaluer les seuils de risque, d'engager une intervention préventive et de transformer cette expérience en apprentissage et en mémoire organisationnels. La question centrale de l'étude consiste à déterminer comment les organisations repèrent les signaux faibles avant qu'une crise ne devienne manifeste, comment elles diagnostiquent leurs points de vulnérabilité internes, à partir de quels seuils elles déclenchent des alertes et comment elles traduisent ce diagnostic en actions managériales préventives. Les organisations contemporaines sont confrontées non seulement à la pression concurrentielle et au changement technologique, mais également aux perturbations des chaînes d'approvisionnement, à la mobilité de la main-d'œuvre, au risque réputationnel, à la dégradation des flux d'information et aux fluctuations soudaines de leur environnement. Dans ces conditions, expliquer la réussite organisationnelle uniquement par la rapidité du rétablissement après une crise demeure insuffisant. L'enjeu véritablement déterminant est de savoir si les signaux faibles qui apparaissent avant qu'une crise ne devienne manifeste sont repérés, si les points de vulnérabilité internes sont diagnostiqués en temps utile et si ce diagnostic peut être traduit en actions managériales préventives.

Bien que l'architecture de l'immunité organisationnelle s'inscrive dans le même champ de discussion que les travaux sur la résilience, les capacités dynamiques, la gestion des risques, les signaux faibles, l'apprentissage organisationnel, la mémoire organisationnelle et le capital intellectuel, elle ne constitue pas une simple addition de ces concepts. La littérature sur la résilience explique la capacité des organisations à maintenir leur fonctionnement face à des événements imprévus, à s'adapter sous pression et à établir un nouvel équilibre après une perturbation. L'architecture de l'immunité organisationnelle examine toutefois les conditions de possibilité de cette résilience à un stade plus précoce : au moyen de quels indicateurs la dégradation interne est-elle repérée avant de se traduire par une baisse de performance, des comportements de crise ou un effondrement manifeste, et comment ce repérage est-il relié aux décisions préventives ? Alors que l'approche des capacités dynamiques se concentre sur l'aptitude des organisations à intégrer, à reconfigurer et à transformer leurs ressources dans des environnements changeants, l'architecture de l'immunité organisationnelle examine la manière dont le besoin de reconfiguration est diagnostiqué et les conditions dans lesquelles il devient prioritaire. La gestion des risques fournit un cadre systématique pour identifier, classer, surveiller et maîtriser les incertitudes ; cependant, dans l'architecture de l'immunité organisationnelle, l'enjeu ne se limite pas à identifier ou à réduire les risques. Il concerne, plus fondamentalement, la capacité de l'organisation à reconnaître en temps utile les pertes d'immunité qui se produisent en son sein, à les interpréter sur le plan managérial et à intégrer les informations obtenues aux processus d'apprentissage et de mémoire organisationnels.

Cette étude repose sur une démarche de développement d'un modèle conceptuel. Elle ne mobilise donc ni population ni échantillon relevant d'un dispositif quantitatif ou qualitatif, ni données de terrain, ni

instrument de collecte de données, ni échelle de mesure. Son principal fondement méthodologique réside dans l'intégration analytique des travaux permettant d'expliquer l'architecture de l'immunité organisationnelle et dans leur réarticulation autour des processus d'alerte précoce, de diagnostic des maillons faibles, de détermination des seuils de risque, d'intervention préventive, d'apprentissage organisationnel et de mémoire organisationnelle. Le modèle proposé s'articule autour de quatre volets principaux : leadership/structure, adaptation, intégration et capital intellectuel. Ces volets ne constituent pas des rubriques de mesure indépendantes, mais des domaines diagnostiques complémentaires permettant d'expliquer où l'organisation s'affaiblit, par quels canaux cet affaiblissement se propage et quel type d'intervention il requiert. Si le modèle fait ultérieurement l'objet d'une mise à l'épreuve empirique, les enquêtes auprès du personnel, les rapports d'erreurs, les retards de projets, les taux de rotation du personnel, les réclamations des clients, les constats d'audit interne et les comptes rendus de réunion pourront être exploités conjointement.

L'analyse conceptuelle conduit à conclure que l'architecture de l'immunité organisationnelle ne constitue pas une activité de contrôle menée à intervalles déterminés, mais un cycle continu d'alerte précoce et d'intervention préventive. L'organisation recueille des signaux issus de son environnement et de son propre fonctionnement interne, les interprète, distingue la source de l'affaiblissement, intervient lorsque cela s'avère nécessaire et mobilise cette expérience dans ses décisions ultérieures. La qualité diagnostique du modèle tient au fait qu'il évalue les indicateurs d'alerte précoce internes non comme des symptômes isolés, mais comme des configurations associées aux fonctions organisationnelles. L'allongement inhabituel des processus décisionnels, le brouillage des délimitations des rôles et de l'autorité, la circulation tardive ou incomplète de l'information entre les unités, les déficiences de coordination, la concentration des connaissances critiques entre les mains de quelques individus, la répétition des mêmes erreurs ou l'incapacité des membres du personnel à exprimer ouvertement les problèmes ne signifient pas, pris isolément, qu'une crise est en cours. Toutefois, lorsque ces indicateurs font l'objet d'un suivi conjoint dans le temps, ils peuvent fournir des indices importants sur le domaine dans lequel l'organisation subit une perte d'immunité. Les exemples de Challenger et de Columbia montrent pourquoi l'architecture de l'immunité organisationnelle doit porter son attention non seulement sur les risques techniques, mais également sur l'interprétation organisationnelle, la culture, la communication et la structure décisionnelle.

En conclusion, l'architecture de l'immunité organisationnelle fonde son ambition de rendre les organisations plus résilientes face aux crises sur leur capacité à percevoir plus tôt, à interpréter avec davantage de justesse et à intervenir au moment opportun. Le modèle ne promet pas un système de contrôle sans faille ; il rappelle que les vulnérabilités apparaissent souvent avant leurs conséquences visibles, sous la forme d'écarts mineurs et de signaux négligés. Dès lors, la précocité, la franchise et l'orientation vers l'apprentissage avec lesquelles les organisations parviennent à discerner leurs propres faiblesses devraient occuper une place centrale dans la recherche en management et en organisation, au même titre que leur degré de solidité. Pour les praticiens, des tableaux de bord d'alerte précoce, des analyses des maillons faibles, des indicateurs de seuils de risque et des mécanismes de gouvernance préventive peuvent être développés. Pour les chercheurs, il est recommandé de mettre le modèle à l'épreuve au moyen de dispositifs longitudinaux, multisources et fondés sur les événements, en examinant les volets leadership/structure, adaptation, intégration et capital intellectuel.

Mots-clés: Architecture de l'immunité organisationnelle ; systèmes d'alerte précoce ; détection des signaux faibles ; diagnostic précoce ; intervention préventive ; apprentissage organisationnel ; management et organisation ; comportement organisationnel.

Resumen Estructurado:

Este estudio conceptualiza la arquitectura de la inmunidad organizacional no como un reflejo defensivo que se activa tras la aparición de una crisis, sino como una arquitectura cíclica de diagnóstico y aprendizaje capaz de interpretar los indicios tempranos que generan la posibilidad de una crisis, distinguir las fuentes de vulnerabilidad, evaluar los umbrales de riesgo, iniciar intervenciones preventivas y transformar esta experiencia en aprendizaje y memoria organizacionales. La pregunta central del estudio es cómo las

organizaciones reconocen las señales débiles antes de que una crisis se vuelva visible, cómo diagnostican sus puntos vulnerables internos, a partir de qué umbrales generan alertas y cómo traducen este diagnóstico en acciones directivas preventivas. Las organizaciones contemporáneas afrontan no solo presiones competitivas y cambios tecnológicos, sino también interrupciones en las cadenas de suministro, movilidad de la fuerza laboral, riesgos reputacionales, deterioro de los flujos de información y fluctuaciones repentinas del entorno. En estas condiciones, resulta insuficiente explicar el éxito organizacional únicamente en función de la rapidez con la que una organización se recupera después de una crisis. La cuestión verdaderamente decisiva es si se detectan las señales débiles que aparecen antes de que la crisis se vuelva visible, si se diagnostican oportunamente los puntos vulnerables de la organización y si este diagnóstico puede traducirse en acciones directivas preventivas.

Aunque la arquitectura de la inmunidad organizacional comparte un mismo campo de debate con la literatura sobre resiliencia, capacidades dinámicas, gestión de riesgos, señales débiles, aprendizaje organizacional, memoria organizacional y capital intelectual, no constituye una mera suma de estos conceptos. La literatura sobre resiliencia explica la capacidad de las organizaciones para mantener su funcionalidad ante acontecimientos imprevistos, adaptarse bajo presión y establecer un nuevo equilibrio tras una perturbación. Sin embargo, la arquitectura de la inmunidad organizacional aborda las condiciones que hacen posible la resiliencia desde una fase más temprana: ¿mediante qué indicadores se detecta el deterioro interno antes de que se traduzca en una disminución del desempeño, comportamientos de crisis o un colapso visible, y cómo se vincula esta detección con las decisiones preventivas? Mientras que el enfoque de las capacidades dinámicas se centra en la capacidad de las organizaciones para integrar, reconfigurar y transformar sus recursos en entornos cambiantes, la arquitectura de la inmunidad organizacional examina cómo se diagnostica la necesidad de dicha reconfiguración y en qué condiciones adquiere prioridad. La gestión de riesgos ofrece un marco sistemático para identificar, clasificar, supervisar y controlar las incertidumbres; no obstante, dentro de la arquitectura de la inmunidad organizacional, la cuestión no consiste únicamente en identificar o reducir los riesgos. El aspecto más fundamental radica en la capacidad de la organización para reconocer oportunamente las pérdidas de inmunidad que se producen en su interior, interpretarlas desde una perspectiva directiva e incorporar la información obtenida a los procesos de aprendizaje y memoria organizacionales.

Este estudio se fundamenta en un enfoque de desarrollo de un modelo conceptual. Por consiguiente, no se recurrió a una población ni a una muestra en el marco de un diseño cuantitativo o cualitativo, ni se utilizaron datos de campo, instrumentos de recopilación de datos o escalas de medición. Su principal fundamento metodológico consiste en la integración analítica de la literatura que explica la arquitectura de la inmunidad organizacional y en su rearticulación en torno a los procesos de alerta temprana, diagnóstico de eslabones débiles, determinación de umbrales de riesgo, intervención preventiva, aprendizaje organizacional y memoria organizacional. El modelo propuesto se estructura en cuatro paneles principales: liderazgo/estructura, adaptación, integración y capital intelectual. Estos paneles no constituyen categorías de medición independientes, sino ámbitos diagnósticos complementarios que contribuyen a explicar dónde se debilita la organización, por qué canales se propaga esa debilidad y qué tipo de intervención requiere. Si el modelo se somete a contrastación empírica en el futuro, podrán utilizarse conjuntamente encuestas al personal, informes de errores, datos sobre retrasos en los proyectos, tasas de rotación del personal, reclamaciones de clientes, hallazgos de auditoría interna y actas de reuniones.

Como resultado del estudio conceptual, se concluye que la arquitectura de la inmunidad organizacional no constituye una actividad de control realizada a intervalos determinados, sino un ciclo continuo de alerta temprana e intervención preventiva. La organización recopila señales procedentes del entorno y de su propio funcionamiento interno, las interpreta, distingue el origen de la debilidad, interviene cuando resulta necesario e incorpora esta experiencia a sus decisiones posteriores. La calidad diagnóstica del modelo deriva de la evaluación de los indicadores internos de alerta temprana como patrones asociados con las funciones organizacionales, en lugar de tratarlos como síntomas aislados. La prolongación inusual de los procesos de toma de decisiones, la difuminación de los límites de los roles y de la autoridad, la circulación tardía o incompleta de la información entre unidades, las deficiencias de coordinación, la concentración del conocimiento crítico en unas pocas personas, la reiteración de los mismos errores o la incapacidad del personal

para expresar abiertamente los problemas no implican, por sí solos, la existencia de una crisis. Sin embargo, cuando estos indicadores se supervisan de manera conjunta y a lo largo del tiempo, pueden proporcionar indicios importantes sobre el ámbito en el que la organización está experimentando una pérdida de inmunidad. Los ejemplos de Challenger y Columbia muestran por qué la arquitectura de la inmunidad organizacional debe centrarse no solo en los riesgos técnicos, sino también en la interpretación organizacional, la cultura, la comunicación y la estructura de toma de decisiones.

En conclusión, la arquitectura de la inmunidad organizacional fundamenta su pretensión de aumentar la resiliencia de las organizaciones frente a las crisis en la capacidad de percibir con mayor anticipación, interpretar con mayor precisión e intervenir de manera más oportuna. El modelo no promete un sistema de control infalible; recuerda que las vulnerabilidades suelen manifestarse antes de que sus consecuencias sean visibles, en forma de pequeñas desviaciones y señales desatendidas. Por ello, la antelación, la honestidad y la orientación al aprendizaje con las que las organizaciones son capaces de interpretar sus propias debilidades deberían ocupar un lugar central en la investigación sobre administración y organización, tanto como su grado de fortaleza. Para los profesionales, pueden desarrollarse paneles de alerta temprana, análisis de eslabones débiles, indicadores de umbrales de riesgo y mecanismos de gobernanza preventiva. Para los investigadores, se recomienda someter el modelo a contrastación mediante diseños longitudinales, con múltiples fuentes y basados en acontecimientos, así como a través de los paneles de liderazgo/estructura, adaptación, integración y capital intelectual.

Palabras clave: Arquitectura de la inmunidad organizacional; sistemas de alerta temprana; detección de señales débiles; diagnóstico previo a la crisis; intervención preventiva; aprendizaje organizacional; administración y organización; comportamiento organizacional.

结构化摘要:

本研究将组织免疫架构概念化为一种循环运行的诊断与学习架构，而非危机发生后才被激活的防御性反应。该架构能够识读可能引发危机的早期征兆，区分脆弱性的来源，评估风险阈值，启动预防性干预，并将相关经验转化为组织学习与组织记忆。本研究的核心问题是：组织如何在危机显现之前识别弱信号，如何诊断内部脆弱环节，在何种阈值下触发警报，以及如何将诊断结果转化为预防性管理行动。当代组织不仅面临竞争压力与技术变革，还面临供应链中断、劳动力流动、声誉风险、信息流恶化以及外部环境的突发性波动。在此背景下，仅依据组织在危机后的恢复速度来解释其成功，仍显不足。真正关键的问题在于：危机显现之前出现的弱信号能否被察觉，组织内部的脆弱环节能否得到及时诊断，以及这些诊断能否转化为预防性管理行动。

尽管组织免疫架构与组织韧性、动态能力、风险管理、弱信号、组织学习、组织记忆及智力资本等领域的文献处于共同的学术讨论范畴，但它并非这些概念的简单叠加。组织韧性文献阐释了组织在面对突发事件时维持功能、在压力下适应以及在扰动后建立新均衡的能力。组织免疫架构则从更早的阶段探讨韧性何以形成：在组织内部的劣化演变为绩效下降、危机行为或显性崩溃之前，组织通过哪些指标察觉这一过程，又如何将这种察觉与预防性决策相衔接？动态能力视角关注组织在变化的环境中整合、重构与转化资源的能力，而组织免疫架构则讨论如何诊断此类资源重构的必要性，以及这种需求在何种条件下获得优先地位。风险管理为识别、分类、监测和控制不确定性提供了系统性框架；然而，在组织免疫架构中，问题并不仅限于识别或降低风险。更为根本的问题在于，组织能否及时识别自身发生的免疫功能减损，从管理角度加以解释，并将所获取的信息融入组织学习与组织记忆过程。

本研究采用概念模型开发方法。因此，研究未采用定量或定性研究设计中的研究总体、样本、实地数据、数据收集工具或测量量表。其主要方法论基础是对阐释组织免疫架构的相关文献进行分析性整合，并围绕早期预警、薄弱环节诊断、风险阈值、预防性干预、组织学习和组织记忆等过程，重新梳理这些文献之间的关联。所提出的模型由四个主要模块构成：领导力／组织结构、适应

、整合和智力资本。这些模块并非相互独立的测量类别，而是彼此补充的诊断领域，有助于解释组织在哪些方面出现弱化、这种弱化通过何种渠道扩散，以及需要何种类型的干预。若未来对该模型进行实证检验，可综合使用员工问卷调查、错误报告、项目延误情况、员工流动率、客户投诉、内部审计发现及会议记录等资料。

概念研究得出的结论是，组织免疫架构并非按特定间隔开展的控制活动，而是持续运行的早期预警与预防性干预循环。组织从外部环境及自身内部运行体系中收集信号，对其进行解释，辨别薄弱状态的来源，在必要时实施干预，并将相关经验应用于后续决策。该模型的诊断质量源于其将组织内部的早期预警指标视为与组织功能相关联的模式，而非孤立的症状。决策过程异常延长、角色与权限边界模糊、部门间信息流转迟滞或不完整、协调不足、关键知识集中于少数个体、相同错误反复发生，或员工无法公开表达问题，这些现象本身并不意味着危机已经发生。然而，当这些指标得到联合监测与持续追踪时，它们可能为判断组织在哪一领域出现免疫功能减损提供重要线索。“挑战者号”与“哥伦比亚号”的案例说明，组织免疫架构为何不仅应关注技术风险，还应关注组织层面的解释、文化、沟通以及决策结构。

综上，组织免疫架构将增强组织危机韧性的主张建立在更早感知、更准确解释和更及时干预的能力之上。该模型并不承诺构建一个毫无缺陷的控制系统，而是提醒我们：在可见后果出现之前，脆弱性往往已通过微小偏差和被忽视的信号表现出来。因此，组织能够多早、多坦诚地以学习为导向识读自身弱点，应当与组织的强健程度一样，成为管理与组织研究的核心议题。对于实践者而言，可以开发早期预警面板、薄弱环节分析方法、风险阈值指标及预防性治理机制。对于研究者而言，建议采用纵向、多来源及基于事件的研究设计，并围绕领导力／组织结构、适应、整合和智力资本四个模块，对该模型进行检验。

关键词：组织免疫架构；早期预警系统；弱信号检测；危机前诊断；预防性干预；组织学习；管理与组织；组织行为。

Структурированная Аннотация:

В настоящем исследовании архитектура организационного иммунитета концептуализируется не как защитная реакция, активируемая после возникновения кризиса, а как циклическая архитектура диагностики и обучения, способная распознавать ранние признаки, создающие предпосылки возникновения кризиса, разграничивать источники уязвимости, оценивать пороговые значения риска, инициировать превентивное вмешательство и преобразовывать полученный опыт в организационное обучение и организационную память. Основным исследовательский вопрос заключается в том, каким образом организации распознают слабые сигналы до того, как кризис становится явным, как диагностируют внутренние уязвимые звенья, при достижении каких пороговых значений формируют сигналы тревоги и как преобразуют результаты диагностики в превентивные управленческие действия. Современные организации сталкиваются не только с конкурентным давлением и технологическими изменениями, но и с нарушениями цепей поставок, мобильностью рабочей силы, репутационными рисками, ухудшением информационных потоков и резкими колебаниями внешней среды. В этих условиях объяснение организационного успеха исключительно скоростью восстановления после кризиса остаётся недостаточным. Принципиальное значение имеет то, замечаются ли слабые сигналы, возникающие до явного проявления кризиса, своевременно ли диагностируются внутренние уязвимые звенья и могут ли результаты такой диагностики быть преобразованы в превентивные управленческие действия.

Хотя архитектура организационного иммунитета находится в общем дискуссионном поле с исследованиями организационной резильентности, динамических способностей, управления рисками, слабых сигналов, организационного обучения, организационной памяти и интеллектуального капитала, она не представляет собой простую сумму этих концепций. Литература по организационной

резильентности объясняет способность организаций сохранять функциональность при столкновении с непредвиденными событиями, адаптироваться в условиях давления и устанавливать новое равновесие после нарушения функционирования. Архитектура организационного иммунитета, однако, рассматривает условия формирования резильентности на более раннем этапе: посредством каких индикаторов выявляется ухудшение внутреннего состояния организации до того, как оно перерастёт в снижение результативности, кризисное поведение или явный коллапс, и каким образом это выявление связывается с превентивными решениями? В то время как подход динамических способностей сосредоточен на способности организаций интегрировать, реконфигурировать и преобразовывать свои ресурсы в изменяющейся среде, архитектура организационного иммунитета рассматривает, как диагностируется потребность в такой реконфигурации и при каких условиях она приобретает приоритетное значение. Управление рисками предлагает систематическую основу для выявления, классификации, мониторинга и контроля неопределённостей; однако в рамках архитектуры организационного иммунитета задача не сводится лишь к выявлению или снижению рисков. Более фундаментальный вопрос состоит в способности организации своевременно распознавать происходящее внутри неё ослабление иммунитета, интерпретировать его с управленческой точки зрения и включать полученную информацию в процессы организационного обучения и памяти.

Исследование основано на подходе к разработке концептуальной модели. Соответственно, в нём не использовались исследовательская совокупность или выборка в рамках количественного либо качественного дизайна, полевые данные, инструменты сбора данных или измерительные шкалы. Основу методологии составляет аналитическая интеграция научной литературы, объясняющей архитектуру организационного иммунитета, и переосмысление взаимосвязей между соответствующими подходами в контексте процессов раннего предупреждения, диагностики слабых звеньев, определения пороговых значений риска, превентивного вмешательства, организационного обучения и организационной памяти. Предлагаемая модель включает четыре основных диагностических блока: лидерство/структура, адаптация, интеграция и интеллектуальный капитал. Эти блоки представляют собой не независимые категории измерения, а взаимодополняющие диагностические области, позволяющие объяснить, где организация ослабевает, по каким каналам распространяется это ослабление и какого вмешательства оно требует. При последующей эмпирической проверке модели могут совместно использоваться опросы сотрудников, отчёты об ошибках, сведения о задержках реализации проектов, показатели текучести кадров, жалобы клиентов, результаты внутреннего аудита и протоколы совещаний.

По результатам концептуального исследования сделан вывод о том, что архитектура организационного иммунитета представляет собой не контрольную деятельность, осуществляемую через определённые промежутки времени, а непрерывно функционирующий цикл раннего предупреждения и превентивного вмешательства. Организация собирает сигналы из внешней среды и собственной внутренней системы, интерпретирует их, определяет источник ослабления, при необходимости вмешивается и использует полученный опыт при принятии последующих решений. Диагностическое качество модели обусловлено тем, что внутренние индикаторы раннего предупреждения оцениваются не как изолированные симптомы, а как паттерны, связанные с организационными функциями. Необычное увеличение продолжительности процессов принятия решений, размывание границ ролей и полномочий, несвоевременная или неполная циркуляция информации между подразделениями, недостатки координации, концентрация критически важных знаний у небольшого числа сотрудников, повторение одних и тех же ошибок или неспособность сотрудников открыто говорить о проблемах сами по себе не означают наличия кризиса. Однако совместный мониторинг этих индикаторов в динамике может предоставить важные сведения о том, в какой области организация испытывает ослабление иммунитета. Примеры «Челленджера» и «Колумбии» показывают, почему архитектура организационного иммунитета должна учитывать не только технические риски, но и организационную интерпретацию, культуру, коммуникацию и структуру принятия решений.

V заключение отмечается, что архитектура организационного иммунитета связывает возможность повышения резильентности организаций перед лицом кризисов со способностью раньше распознавать сигналы, точнее их интерпретировать и своевременнее вмешиваться. Модель не обещает безупречной системы контроля; она напоминает, что уязвимости нередко проявляются ещё до возникновения видимых последствий — в форме незначительных отклонений и оставленных без внимания сигналов. Поэтому вопрос о том, насколько рано, насколько честно и в какой мере с ориентацией на обучение организации способны распознавать собственные слабости, должен занимать центральное место в исследованиях управления и организаций наряду с вопросом об их силе. Для практиков могут быть разработаны панели раннего предупреждения, методы анализа слабых звеньев, индикаторы пороговых значений риска и механизмы превентивного организационного управления. Исследователям рекомендуется проверять модель посредством лонгитюдных дизайнов, дизайнов с использованием нескольких источников данных и дизайнов, основанных на событиях, рассматривая блоки лидерства/структуры, адаптации, интеграции и интеллектуального капитала.

Ключевые слова: архитектура организационного иммунитета; системы раннего предупреждения; обнаружение слабых сигналов; докризисная диагностика; превентивное вмешательство; организационное обучение; управление и организация; организационное поведение.

Yapılandırılmış Özet:

Bu çalışma, örgütsel bağışıklık mimarisini kriz ortaya çıktıktan sonra harekete geçen savunmacı bir refleks olarak değil; kriz olasılığını doğuran erken işaretleri okuyabilen, kırılmalıkların kaynaklarını ayırt edebilen, risk eşiklerini değerlendirebilen, önleyici müdahaleyi başlatabilen ve bu deneyimi örgütsel öğrenme ve örgütsel hafızaya dönüştürebilen döngüsel bir teşhis ve öğrenme mimarisi olarak kavramsallaştırmaktadır. Çalışmanın temel sorusu, örgütlerin kriz görünür hâle gelmeden önce zayıf sinyalleri nasıl fark ettikleri, örgüt içerisindeki kırılmalı noktaları nasıl teşhis ettikleri, hangi eşiklerde alarm ürettikleri ve bu teşhisi nasıl önleyici yönetsel eyleme dönüştürdükleridir. Günümüz örgütleri yalnızca rekabet baskısı ve teknolojik değişimle değil, aynı zamanda tedarik zinciri aksamaları, iş gücü hareketliliği, itibar riski, bilgi akışındaki bozulma ve ani çevresel dalgalanmalarla da karşı karşıyadır. Bu koşullar altında örgütsel başarıyı yalnızca bir örgütün kriz sonrasında ne kadar hızlı toparlandığı üzerinden açıklamak yetersiz kalmaktadır. Gerçek anlamda kritik mesele, kriz görünür hâle gelmeden önce ortaya çıkan zayıf sinyallerin fark edilip edilmediği, örgüt içerisindeki kırılmalı noktaların zamanında teşhis edilip edilmediği ve bu teşhisin önleyici yönetsel eyleme dönüştürülemediğidir.

Örgütsel bağışıklık mimarisi; dayanıklılık, dinamik yetenekler, risk yönetimi, zayıf sinyaller, örgütsel öğrenme, örgütsel hafıza ve entelektüel sermaye yazınlarıyla aynı tartışma alanını paylaşırsa da bu kavramların basit bir toplamı değildir. Dayanıklılık yazını, örgütlerin beklenmedik olaylar karşısında işlevselliklerini sürdürme, baskı altında uyum sağlama ve bir aksama sonrasında yeni bir denge kurma kapasitesini açıklamaktadır. Buna karşılık örgütsel bağışıklık mimarisi, dayanıklılığın nasıl mümkün hâle geldiğini daha erken bir noktadan ele almaktadır: Örgüt içerisindeki bozulma, performans kaybına, kriz davranışına veya görünür bir çöküşe dönüşmeden önce hangi göstergeler aracılığıyla fark edilmekte ve önleyici kararlarla nasıl ilişkilendirilmektedir? Dinamik yetenekler yaklaşımı örgütlerin değişen çevrelerde kaynaklarını bütünleştirme, yeniden yapılandırma ve dönüştürme yeteneklerine odaklanırken örgütsel bağışıklık mimarisi, böyle bir yeniden yapılandırma ihtiyacının nasıl teşhis edildiğini ve hangi koşullar altında öncelik kazandığını tartışmaktadır. Risk yönetimi, belirsizliklerin belirlenmesi, sınıflandırılması, izlenmesi ve kontrol edilmesi için sistematik bir çerçeve sunmaktadır; ancak örgütsel bağışıklık mimarisi içerisinde mesele yalnızca riskleri belirlemek veya azaltmak değildir. Daha temel mesele, örgütün kendi içerisinde ortaya çıkan bağışıklık kayıplarını zamanında fark etme, bu kayıpları yönetsel açıdan yorumlama ve elde edilen bilgiyi öğrenme ve hafıza süreçlerine aktarma yeteneğidir.

Bu çalışma, kavramsal model geliştirme yaklaşımına dayanmaktadır. Bu nedenle çalışmada nicel veya nitel bir evren, örneklem, saha verisi, veri toplama aracı veya ölçek kullanılmamıştır. Temel yöntemsel

dayanak, örgütsel bağışıklık mimarisini açıklayan yazınların analitik olarak bütünleştirilmesi ve erken uyarı, zayıf halka teşhisi, risk eşiği, önleyici müdahale, örgütsel öğrenme ve örgütsel hafıza süreçleri içerisinde yeniden eklemlenmesidir. Önerilen model dört temel panel üzerine kurulmuştur: liderlik/yapı, adaptasyon, entegrasyon ve entelektüel sermaye. Bu paneller bağımsız ölçüm başlıkları değil, örgütün nerede zayıfladığını, bu zayıflığın hangi kanallar aracılığıyla yayıldığını ve ne tür bir müdahale gerektirdiğini açıklamaya yardımcı olan tamamlayıcı tanısal alanlardır. Model gelecekte ampirik olarak sınırsız çalışan anketleri, hata raporları, proje gecikmeleri, çalışan devir oranları, müşteri şikâyetleri, iç denetim bulguları ve toplantı kayıtları birlikte kullanılabilir.

Kavramsal çalışma sonucunda örgütsel bağışıklık mimarisinin belirli aralıklarla yürütülen bir kontrol faaliyeti değil, sürekli işleyen bir erken uyarı ve önleyici müdahale döngüsü olduğu sonucuna ulaşılmıştır. Örgüt, çevreden ve kendi iç düzeninden gelen sinyalleri toplamakta, bunları yorumlamakta, zayıflığın kaynağını ayırt etmekte, gerektiğinde müdahale etmekte ve bu deneyimi sonraki kararlarına aktarmaktadır. Modelin tanısal niteliği, örgüt içerisindeki erken uyarı göstergelerini birbirinden bağımsız belirtiler olarak değil, örgütsel işlevlerle ilişkili örüntüler olarak değerlendirmesinden kaynaklanmaktadır. Karar alma süreçlerinin olağandışı biçimde uzaması, rol ve yetki sınırlarının belirsizleşmesi, bilginin birimler arasında gecikmeli veya eksik dolaşımı, koordinasyon zayıflıkları, kritik bilginin az sayıda kişide yoğunlaşması, aynı hataların tekrarlanması veya çalışanların sorunları açıkça ifade edememeleri tek başına kriz anlamına gelmemektedir. Bununla birlikte bu tür göstergeler birlikte ve zaman içerisinde izlendiğinde, örgütün hangi alanında bağışıklık kaybı yaşandığına ilişkin önemli ipuçları sağlayabilir. Challenger ve Columbia örnekleri, örgütsel bağışıklık mimarisinin neden yalnızca teknik risklere değil, aynı zamanda örgütsel yorumlama, kültür, iletişim ve karar alma yapısına da odaklanması gerektiğini göstermektedir.

Sonuç olarak örgütsel bağışıklık mimarisi, örgütleri krizler karşısında daha dayanıklı hâle getirme iddiasını daha erken algılama, daha doğru yorumlama ve daha zamanında müdahale etme kapasitesi üzerine kurmaktadır. Model kusursuz bir kontrol sistemi vaat etmemekte; kırılganlıkların çoğu zaman görünür sonuçlardan önce küçük sapmalar ve ihmal edilen sinyaller biçiminde ortaya çıktığını bize hatırlatmaktadır. Bu nedenle örgütlerin ne kadar güçlü oldukları kadar kendi zayıflıklarını ne kadar erken, ne kadar dürüst ve ne ölçüde öğrenme yönelimli biçimde okuyabildikleri de yönetim ve organizasyon araştırmalarının merkezinde yer almalıdır. Uygulayıcılar açısından erken uyarı panelleri, zayıf halka analizleri, risk eşiği göstergeleri ve önleyici yönetim mekanizmaları geliştirilebilir. Araştırmacılar açısından ise modelin boylamsal, çok kaynaklı ve olay temelli tasarımlar yoluyla ve liderlik/yapı, adaptasyon, entegrasyon ve entelektüel sermaye panelleri aracılığıyla sınanması önerilmektedir.

Anahtar Kelimeler: Örgütsel bağışıklık mimarisi; erken uyarı sistemleri, zayıf sinyal tespiti; kriz öncesi teşhis, önleyici müdahale; örgütsel öğrenme, Yönetim ve Organizasyon; Örgütsel Davranış.



www.turkishstudies.net/economy

Turkish Studies - Economics, Finance, Politics

eISSN: 2667-5625



ANKARA SCIENCE
UNIVERSITY

Organizational Immunity Architecture: A Preventive Early Warning Model Proposal

Introduction

Organizations today must contend not only with competitive pressures and technological change but also with supply chain disruptions, workforce mobility, reputational risks, disruptions in information flows, and sudden environmental volatility (Allen et al., 2010; Christopher & Peck, 2004; Galbraith, 1973; Power et al., 2009; Teece et al., 1997; Weick & Sutcliffe, 2007). Under these conditions, explaining organizational success solely in terms of how quickly an organization recovers after a crisis remains insufficient (Duchek, 2020; Lengnick-Hall et al., 2011). The central issue is whether weak signals emerging before a crisis becomes visible are recognized, whether vulnerabilities within the organization are diagnosed in a timely manner, and whether those diagnoses are translated into preventive managerial action (Ansoff, 1975; Reason, 1997; Weick et al., 1999; Weick & Sutcliffe, 2007). Ansoff's (1975) weak signals approach continues to provide a robust point of departure for this discussion because it demonstrates that strategic surprises often become apparent not through clear and definitive indicators but through early signs that are initially ambiguous, dispersed, and open to interpretation.

In response to this need, this article proposes the concept of organizational immunity architecture. Rather than viewing the organization as a passive entity that reacts only after a crisis has occurred, the concept treats it as a cyclical institutional system that identifies perceived threats, weak signals, and systemic vulnerabilities at an early stage; renders risk thresholds visible; links preventive interventions to governance arrangements; and converts this process into organizational learning and memory (Ansoff, 1975; Argyris & Schön, 1978; Reason, 1997; Walsh & Ungson, 1991; Weick et al., 1999). In this sense, organizational immunity architecture operates according to the logic of a diagnostic dashboard (Simons, 1995). Indicators such as delays in decision-making, role ambiguity, information silos, coordination failures, slow organizational learning, the loss of critical capabilities, and the recurrence of the same errors can be regarded as early warning signals that reveal otherwise hidden weaknesses in organizational immunity (Edmondson, 1996; Galbraith, 1973; Lawrence & Lorsch, 1967; Lengnick-Hall et al., 2011; Rizzo et al., 1970; Weick & Sutcliffe, 2007).

The primary aim of this article is to develop a theoretical model that does not confine organizational immunity to post-crisis recovery or general resilience capacity but instead explains early warning, diagnosis, weak-link analysis, risk thresholds, preventive intervention, governance arrangements, and organizational learning within a single cycle (Ansoff, 1975; Duchek, 2020; Reason, 1997; Simons, 1995; Weick & Sutcliffe, 2007). Four panels lie at the core of the model: leadership/structure, adaptation, integration, and intellectual capital. The leadership/structure panel represents decision clarity, the distribution of authority, and governance readiness; the adaptation panel represents environmental responsiveness and renewal capacity; the integration panel represents cross-unit coherence and systemic alignment; and the intellectual capital panel represents knowledge preservation, organizational memory, and organizational immunity intelligence (Cohen & Levinthal,

1990; Galbraith, 1973; Lawrence & Lorsch, 1967; March, 1991; Nahapiet & Ghoshal, 1998; Teece et al., 1997; Walsh & Ungson, 1991). Nahapiet and Ghoshal's (1998) conceptualization of the relationship between social and intellectual capital as a source of organizational advantage provides an important theoretical foundation for the knowledge, relational, and intellectual capital dimensions of the model.

The contribution of this article is threefold. First, organizational immunity is repositioned from a post-crisis defensive or recovery capacity to a cyclical architecture that enables early diagnosis and preventive intervention before a crisis occurs (Ansoff, 1975; Duchek, 2020; Weick & Sutcliffe, 2007). Second, the literatures on organizational resilience, dynamic capabilities, weak-signal detection, organizational learning, organizational memory, and intellectual capital are integrated within a single theoretical model (Argyris & Schön, 1978; Duchek, 2020; Levitt & March, 1988; Nahapiet & Ghoshal, 1998; Teece et al., 1997; Walsh & Ungson, 1991). Third, rather than leaving organizational immunity at the level of an abstract capacity, the model conceptualizes it as a system that can be monitored, diagnosed, and translated into managerial intervention through the leadership/structure, adaptation, integration, and intellectual capital panels (Cohen & Levinthal, 1990; Galbraith, 1973; Lawrence & Lorsch, 1967; Simons, 1995). The study thus offers an original theoretical framework that explains not only how organizations withstand crises but also how they detect the early signals from which crises emerge, diagnose weak links, and transform learning into enduring organizational intelligence (Crossan et al., 1999; March, 1991; Walsh & Ungson, 1991; Weick et al., 1999).¹

Conceptual Research Design and Model Development

This study was designed not as an empirical test or a systematic literature review, but as a conceptual study combining theory synthesis with conceptual model development. Conceptual studies must also be grounded in an explicit research design that explains why particular theories and concepts were selected, what roles they perform in the analysis, and through which stages of reasoning the resulting model was developed (Jaakkola, 2020). Accordingly, the focal phenomenon addressed in this study concerns how organizations recognize and diagnose weaknesses that have not yet developed into full-blown crises, bring them to the threshold of managerial decision-making, and translate their post-intervention experience into organizational learning.

The pool of theoretical sources was purposively delimited according to the functions required to explain this focal phenomenon. The weak-signal and high-reliability literatures were included because they explain the detection of early warning signs; the organizational resilience and dynamic capabilities literatures because they explain the capacities for anticipation, adaptation, and reconfiguration; the organization design and risk management literatures because they explain diagnostic domains, thresholds, and managerial intervention; and the organizational learning, organizational memory, and intellectual capital literatures because they explain the institutionalization of experience. Sources were included in the model if they provided an organization-level explanation, offered a direct theoretical foundation for at least one function of the cycle, and explained the relationships among the relevant concepts. Studies that merely described post-crisis outcomes, were not linked to an organizational mechanism, or did not develop the

¹ For studies addressing these issues across different sectors and institutional contexts—including the relationship among intellectual capital, adaptation, and organizational resilience; conceptual model development methodology; intervention, change, and organizational learning; the generation and sharing of knowledge and its integration into organizational processes; leadership, a supportive organizational climate, and knowledge sharing; and employees' ability to report problems, psychological safety, and the communication of weak signals to management—see also Agostini & Nosella (2023); Jaakkola (2020); Schein (1996); Töre (2020); Mertel, Bozkurt, & Demirhan (2020); Köse, Mohan Bursalı, & Dolma (2023).

biological metaphor into an explanatory framework were not included among the model's foundational sources.

The model-development process was conducted in four analytical stages. First, recurring theoretical functions across the relevant literatures—sensing, diagnosis, threshold assessment, intervention, governance arrangements, and learning—were analytically differentiated. Second, concepts that explained the same function under different labels were consolidated, whereas concepts performing different functions were kept distinct. Third, leadership/structure, adaptation, integration, and intellectual capital were organized as horizontal diagnostic panels indicating where organizational weaknesses are concentrated, while sensing, diagnosis, threshold assessment, intervention, governance arrangements, and learning were structured as a six-stage process showing how diagnosis is translated into action over time. Finally, the directional linkages between the stages and the feedback relationship were specified, and the propositions were derived in a manner that makes explicit what the model explains, how and why it explains it, and under what conditions its explanations apply (Whetten, 1989).

At this point, a clear distinction must be drawn between the conceptual origins of the four panels and the contribution of the present study. Using the Organizational DNA Profile Scale, Kara and Yalçın (2026) empirically examined organizational immunity through the dimensions of leadership/structure, adaptation, integration, and intellectual capital and investigated whether employees' perceptions of these dimensions differed according to their demographic characteristics. The present study does not claim to have rediscovered these four dimensions as independent elements. Instead, it repositions them as diagnostic panels that distinguish the organizational domains in which weak signals are concentrated and connects them to a cycle comprising sensing, diagnosis, risk-threshold assessment, preventive intervention, governance arrangements, and organizational learning. Thus, whereas the previous study focused on the dimensions through which organizational immunity can be measured, the present study explains how these dimensions operate together within a continuous process of early warning and preventive intervention.

In line with this distinction, the article's claim to originality does not rest on proposing the four panels for the first time, but on functionally integrating these panels—previously employed as domains of empirical measurement—within a six-stage process architecture characterized by feedback. The four panels explain where organizational weaknesses are located; the six-stage cycle explains how a weak signal progresses from diagnosis to intervention and institutional learning; and the feedback link explains how each completed cycle alters subsequent sensing and threshold assessment.

Theoretical Framework

Although organizational immunity architecture occupies the same domain of inquiry as several established concepts in the management and organization literature, it is not merely the sum of these concepts (Ansoff, 1975; Ducheck, 2020; Huang, 2013; Teece et al., 1997; Walsh & Ungson, 1991). Accordingly, rather than sequentially summarizing the literature, this study aims to explain the theoretical strands with which the proposed model is associated and where it departs from them (Ansoff, 1975; Ducheck, 2020; Huang, 2013; Teece et al., 1997; Walsh & Ungson, 1991). Such a distinction is necessary because, while the literatures on organizational resilience, dynamic capabilities, organizational learning, organizational memory, and weak signals provide robust accounts of different aspects of organizational vulnerability, organizational immunity architecture proposes a more diagnostically oriented framework that integrates these aspects within a logic of early diagnosis, threshold assessment, and preventive organizational adjustment (Ansoff, 1975; Argyris & Schön, 1978; Ducheck, 2020; Reason, 1997; Simons, 1995; Teece et al., 1997; Walsh & Ungson, 1991).

Table 1 summarizes this division of theoretical roles by comparing the primary focus of each concept with its function within and distinction from organizational immunity architecture. Organizational resilience contributes the capacities for maintaining functionality, recovery, and adaptation (Duchek, 2020); dynamic capabilities provide the logic of resource and competence reconfiguration (Teece et al., 1997); organizational learning and memory explain how experience is transformed into routines and retrievable knowledge (Levitt & March, 1988; Walsh & Ungson, 1991); and the weak signals approach supplies early but uncertain diagnostic inputs (Ansoff, 1975). Table 1 therefore serves as a conceptual boundary map by identifying both the contribution drawn from each literature and the specific explanatory task retained by organizational immunity architecture: connecting pre-crisis sensing and vulnerability diagnosis to risk-threshold assessment, preventive intervention, and institutional learning.

The weak signals approach equips organizational immunity architecture with sensitivity to early detection (Ansoff, 1975). Ansoff's (1975) work remains a key point of reference because it demonstrates that strategic surprises often first become apparent not through clear, strong, and definitive indicators, but through signals that are ambiguous, fragmented, and open to interpretation. This insight indicates that organizations must pay attention not only to confirmed threats but also to signals whose meaning has not yet become fully clear (Ansoff, 1975; Weick et al., 1999; Weick & Sutcliffe, 2007). However, the weak signals approach alone is insufficient to explain the diagnostic categories through which such signals should be assessed within the organization, the thresholds at which they should become managerial priorities, and the forms of intervention through which they should be addressed (Ansoff, 1975; Reason, 1997; Simons, 1995). At this point, organizational immunity architecture treats weak signals not merely as inputs for environmental scanning, but as diagnostic data for interpreting vulnerabilities within the organization's own internal configuration (Ansoff, 1975; Reason, 1997; Simons, 1995; Weick et al., 1999).

The central claim is as follows: organizational immunity architecture is neither an alternative to organizational resilience, another name for dynamic capabilities, nor a new label for organizational learning (Ansoff, 1975; Duchek, 2020; Huang, 2013; Teece et al., 1997; Walsh & Ungson, 1991). More precisely, it is a higher-order theoretical framework that draws on each of these literatures while reorganizing their insights around the axes of early diagnosis, risk thresholds, and preventive intervention (Ansoff, 1975; Duchek, 2020; Huang, 2013; Reason, 1997; Simons, 1995; Teece et al., 1997; Walsh & Ungson, 1991). The theoretical value of the model lies in its claim to explain not only how organizations withstand crises, but also how they make sense of the internal and external signals from which the possibility of a crisis emerges and translate this sensemaking into timely institutional action (Ansoff, 1975; Reason, 1997; Weick et al., 1999; Weick & Sutcliffe, 2007).

Table 1: Conceptual Distinctions between Organizational Immunity Architecture and Related Theoretical Approaches

Concept	Main Focus	Relationship with Organizational Immunity Architecture	Distinguishing Difference
Organizational resilience	Preserving functionality, recovery, and adaptation	It is one of the capacity areas that immunity architecture aims to strengthen.	It is more concerned with remaining standing and adapting under pressure; it does not place the early diagnosis and thresholding mechanism at the center.
Dynamic capabilities	Integrating, reconfiguring, and transforming resources	It supports the intervention and readjustment logic of immunity architecture.	It explains reconfiguration; it does not detail how the need for reconfiguration is diagnosed.
Organizational learning/memory	The transformation of experience into knowledge, routines, and institutional memory	It enables the immunity cycle to become permanent.	It explains the institutionalization of what has been learned; it does not model the early diagnosis–intervention–feedback cycle on its own.
Weak signals	Noticing uncertain early signs	It provides the initial data for immunity architecture.	It shows the importance of early signs; it does not explain on its own how these signs will be linked to the risk threshold and preventive intervention.
Organizational immunity architecture	Early diagnosis, risk threshold, preventive intervention, and learning cycle	It brings other literatures together within a diagnostic cyclical framework.	It integrates pre-crisis signs, vulnerability diagnosis, threshold assessment, and institutional learning within the same model.

Source: Author's own elaboration.

Conceptual Boundaries of Organizational Immunity Architecture

Organizational immunity architecture is closely related to several established concepts in the management and organization literature (Ansoff, 1975; Ducheck, 2020; Huang, 2013; Kaplan & Mikes, 2012; Teece et al., 1997; Walsh & Ungson, 1991). Organizational resilience, risk management, dynamic capabilities, organizational learning, and organizational memory are the foremost among these concepts (Ducheck, 2020; International Organization for Standardization, 2018; Levitt & March, 1988; Teece et al., 1997; Walsh & Ungson, 1991). However, this close relationship should not be interpreted as meaning that organizational immunity architecture is synonymous with these concepts (Ansoff, 1975; Ducheck, 2020; Huang, 2013; Teece et al., 1997). The distinctive feature of the model is that it seeks to explain not only the organization's capacity to withstand crises or adapt to changing conditions, but also how it recognizes hidden vulnerabilities, interprets them, and generates preventive institutional action on the basis of that interpretation (Ansoff, 1975; Reason, 1997; Simons, 1995; Weick et al., 1999; Weick & Sutcliffe, 2007).

The first distinction concerns organizational resilience (Duchek, 2020; Lengnick-Hall et al., 2011). The resilience literature explains organizations' capacity to maintain their functionality in the face of unexpected events, restore a disrupted equilibrium, and adapt to changing conditions (Duchek, 2020; Lengnick-Hall et al., 2011; Weick & Sutcliffe, 2007). Duchek's (2020) treatment of resilience through the processes of anticipation, coping, and adaptation demonstrates that the concept cannot be reduced solely to post-crisis recovery. By contrast, organizational immunity architecture focuses less on resilience itself than on the capacities for early recognition and preventive adjustment that make resilience possible (Ansoff, 1975; Duchek, 2020; Reason, 1997; Simons, 1995). In other words, while resilience explains how an organization survives under pressure, organizational immunity architecture considers how weaknesses that could intensify that pressure can be interpreted before they deepen (Ansoff, 1975; Duchek, 2020; Weick et al., 1999; Weick & Sutcliffe, 2007).

The second distinction must be drawn in relation to risk management (International Organization for Standardization, 2018; Kaplan & Mikes, 2012). Risk management provides organizations with a systematic framework for identifying, classifying, monitoring, and controlling uncertainties (International Organization for Standardization, 2018; Kaplan & Mikes, 2012). Kaplan and Mikes's (2012) classification of risks as preventable, strategic, and external is important because it demonstrates that risks cannot be managed through a single control logic. Organizational immunity architecture draws on this insight but cannot be reduced to the conventional logic of risk management (Huang, 2013; Kaplan & Mikes, 2012; Reason, 1997; Simons, 1995). The issue here is not merely to identify or mitigate risks. The more fundamental issue is whether the organization can recognize, in a timely manner, the losses of immunity arising within itself, interpret these losses in managerial terms, and incorporate the knowledge obtained into its learning and memory processes (Argyris & Schön, 1978; Huang, 2013; Levitt & March, 1988; Walsh & Ungson, 1991; Weick et al., 1999).

The third boundary concerns the dynamic capabilities approach (Teece et al., 1997). The study by Teece et al. (1997) focuses on organizations' ability to integrate, reconfigure, and transform their resources in changing environments. This approach is valuable for understanding the adaptation and readjustment dimension of organizational immunity architecture (Teece et al., 1997). However, the two concepts do not operate at the same level (Ansoff, 1975; Huang, 2013; Teece et al., 1997). Dynamic capabilities primarily explain how organizations reorganize their resources in response to changing conditions (Teece et al., 1997). Organizational immunity architecture, by contrast, asks how the need for such reorganization is recognized (Ansoff, 1975; Reason, 1997; Simons, 1995). In this respect, the model draws attention to the diagnostic foundation that precedes transformation itself: from which signals do an organization conclude that intervention is required? (Ansoff, 1975; Reason, 1997; Weick et al., 1999; Weick & Sutcliffe, 2007).

The fourth boundary concerns the concepts of organizational learning and organizational memory (Levitt & March, 1988; Walsh & Ungson, 1991). Levitt and March (1988) explain organizational learning through the reflection of past experiences in routines and patterns of behavior. Walsh and Ungson (1991), in turn, associate organizational memory with retaining past knowledge within the organization and reusing it in decision-making processes. Organizational immunity architecture builds on this body of knowledge but does not view learning solely as the institutionalization of the past (Argyris & Schön, 1978; Crossan et al., 1999; Huang, 2013; Levitt & March, 1988; Walsh & Ungson, 1991). Within this model, learning is an active feedback capacity that enables the organization to perceive more effectively, interpret more accurately, and intervene earlier in subsequent cycles (Argyris & Schön, 1978; Crossan et al., 1999; Levitt & March, 1988; Walsh & Ungson, 1991). Organizational memory is therefore regarded not merely as a record of the past, but as a living institutional mechanism that helps future vulnerabilities to be interpreted at an earlier stage (Crossan et al., 1999; Huang, 2013; Walsh & Ungson, 1991).

At this point, the limits of the metaphor of biological immunity and preventive medicine must also be made explicit (Cornelissen, 2005; Morgan, 1980). Organizational immunity architecture does not regard organizations as structures identical to biological organisms (Huang, 2013; Morgan, 1980). The metaphor is used not to reduce organizational reality to a medical model, but to explain the idea of recognizing hidden forms of deterioration at an early stage, interpreting critical values, and intervening in a timely manner (Ansoff, 1975; Cornelissen, 2005; Morgan, 1980; Reason, 1997). Morgan's (1980) work on the role of metaphors in organization theory demonstrates that, although metaphors can be powerful tools for theory development, they may also create conceptual blind spots when used without sufficient care. Accordingly, the "biochemistry panel" analogy does not reduce the organization to a living body; rather, it functions as a limited analytical tool that makes organizational indicators more interpretable (Cornelissen, 2005; Morgan, 1980; Simons, 1995).

Within this framework, organizational immunity architecture is not a new designation that replaces the concepts of organizational resilience, risk management, dynamic capabilities, or organizational learning (Duchek, 2020; Huang, 2013; Kaplan & Mikes, 2012; Levitt & March, 1988; Teece et al., 1997). More precisely, it represents a specific theoretical position that brings together the explanatory power of these fields around the axes of early diagnosis, weak-link analysis, preventive adjustment, and institutional learning (Ansoff, 1975; Argyris & Schön, 1978; Huang, 2013; Reason, 1997; Simons, 1995; Walsh & Ungson, 1991). The value of the concept lies precisely here: it seeks to explain not only how an organization withstands crises, but also how it senses the weaknesses that increase the possibility of a crisis, translates them into managerial decisions, and develops stronger institutional attentiveness through this experience (Ansoff, 1975; Crossan et al., 1999; Reason, 1997; Weick et al., 1999; Weick & Sutcliffe, 2007).

Organizational Immunity Architecture as A Diagnostic System

Organizational immunity architecture should not be viewed merely as a framework that explains an organization's response after disruption has occurred (Ansoff, 1975; Huang, 2013; Reason, 1997; Weick & Sutcliffe, 2007). The principal value of the model lies in its ability to interpret signals within the organizational system that have not yet developed into a full-blown crisis, place these signals within meaningful diagnostic domains, and initiate managerial intervention in a timely manner (Ansoff, 1975; Reason, 1997; Simons, 1995; Weick et al., 1999). Accordingly, the model operates in a manner analogous to diagnostic reasoning in preventive medicine, but it does not reduce organizations to biological structures (Biomarkers Definitions Working Group, 2001; Cornelissen, 2005; Morgan, 1980). The analogy employed here is more limited and analytical: just as certain values in the human body may provide insight into risk before symptoms appear, indicators within organizations—such as delays in decision-making, disruptions in information flows, coordination weaknesses, the loss of critical knowledge, recurring errors, or employees' reluctance to voice problems—can be interpreted as early warning signs of more significant breakdowns (Biomarkers Definitions Working Group, 2001; Edmondson, 1996, 1999; Galbraith, 1973; Morrison, 2014; Rizzo et al., 1970; Walsh & Ungson, 1991). Ansoff's (1975) weak signals approach constitutes one of the classical foundations of this diagnostic logic because it demonstrates that strategic surprises often emerge not as clearly identifiable threats, but as signals that are initially incomplete and open to interpretation.

The term "organizational biomarker," as used in this study, should be understood not as an established medical measurement concept, but as an analytical metaphor proposed to make early warning indicators within the organization more interpretable (Biomarkers Definitions Working Group, 2001; Cornelissen, 2005; Morgan, 1980). For example, none of the following indicators constitutes a crisis in isolation: an unusual prolongation of decision-making processes, blurred role and authority boundaries, delayed or incomplete circulation of information between units, recurrence of the same errors, concentration of critical knowledge in a small number of individuals, or an

inability to voice problems openly (Edmondson, 1996, 1999; Galbraith, 1973; Morrison, 2014; Rizzo et al., 1970; Walsh & Ungson, 1991). However, when such indicators are monitored collectively and over time, they may provide important clues as to which area of the organization is experiencing a loss of immunity (Ansoff, 1975; Reason, 1997; Simons, 1995; Weick et al., 1999). Diagnostic value therefore lies less in an isolated symptom than in the pattern and persistence of symptoms and their relationship with organizational functions (Reason, 1997; Simons, 1995; Weick & Sutcliffe, 2007).

At this point, organizational immunity architecture intersects with risk management but cannot be reduced to it (Huang, 2013; International Organization for Standardization, 2018; Kaplan & Mikes, 2012; Miller, 1992). Miller's integrated risk management approach argues that the uncertainties faced by firms should be considered not in isolation from one another, but within a more holistic framework (Miller, 1992). Organizational immunity architecture similarly focuses not on individual risks, but on the relationships among the organizational weaknesses that generate risk (Huang, 2013; Reason, 1997; Simons, 1995). Here, the "risk threshold" is not merely a technical boundary, but a decision point indicating when managerial attention should intensify (International Organization for Standardization, 2018; Kaplan & Mikes, 2012; Simons, 1995). Some signals may remain within the range of normal variation; some require attention; and others indicate critical weaknesses that demand intervention without delay (Ansoff, 1975; Reason, 1997; Weick & Sutcliffe, 2007). The diagnostic nature of the model lies in its claim to distinguish among these levels (Reason, 1997; Simons, 1995).

Establishing Risk Thresholds and Managing False Alarms

In the model, the risk threshold is treated not as a universal numerical value or a fixed score applicable to all organizations, but as a context-specific managerial decision criterion that is subject to recalibration. The approach adopted by ISO 31000:2018, which addresses risk identification, analysis, evaluation, treatment, monitoring, and communication as an integrated process, together with Kaplan and Mikes's (2012) distinction demonstrating that different types of risk cannot be managed through the same control logic, requires thresholds to be established in relation to the organization's objectives, risk appetite, the regulatory structure of its industry, and the magnitude of the potential impact (Aven & Thekdi, 2024; International Organization for Standardization, 2018; Kaplan & Mikes, 2012).

The threshold-setting process is conducted using five criteria: the magnitude of the indicator's deviation from the organization's historical normal range; the persistence and direction of the deviation; confirmation of the same signal across multiple diagnostic panels; the severity and reversibility of the potential impact; and the criticality of the indicator in terms of safety, regulatory compliance, or the continuity of core operations. Indicators are not assumed to be equal in relation to these criteria. The weights are determined by a cross-functional committee comprising representatives from the data-owning units associated with the relevant panel, as well as representatives from risk management, internal audit, and senior management, taking into account the organization's past incidents and scenario analyses. The rationale and data sources used are documented. Weighting is thus transformed into a contextual yet auditable decision-making process rather than being left to the intuition of a single manager.

The normal level refers to a situation in which the indicator remains within its historical range and occurs in isolation; the attention level refers to a situation in which the deviation becomes persistent or signals from different panels converge on the same weakness; and the critical level refers to a situation in which the potential impact exceeds the organization's risk appetite, threatens its core operations, or requires immediate action on safety or regulatory grounds. Unless a single indicator is critical in terms of safety or regulatory compliance, it does not directly trigger permanent intervention; data verification, confirmation by the responsible unit, and cross-panel verification are conducted first.

False alarm management is conducted by monitoring alarm outcomes and recalibrating the system rather than establishing and permanently fixing the thresholds. For each alarm, whether the signal corresponds to an actual weakness, whether intervention is necessary, and whether any signals have been overlooked are recorded. False positives are evaluated in terms of the cost of unnecessary intervention, whereas false negatives are evaluated in terms of the impact of the missed risk. During the organizational learning and memory stage, these records provide input for readjusting indicator weights, alarm levels, and validation rules. Feedback therefore does not merely preserve past experience; it also regulates the balance between the diagnostic system's sensitivity and selectivity.

Real-world events demonstrate why this distinction is important. The board that investigated the Columbia accident emphasized that the accident could not be explained solely by the foam strike as a technical event and that NASA's organizational culture was also a determining factor in its occurrence (Columbia Accident Investigation Board, 2003). The report clearly demonstrated that, in complex technological systems, technical failures must be considered together with organizational decision-making, communication, and interpretation processes (Columbia Accident Investigation Board, 2003; Reason, 1997). This example demonstrates why organizational immunity architecture must focus not only on external threats, but also on internal decision-making habits, communication channels, and the capacity to take weak signals seriously (Ansoff, 1975; Columbia Accident Investigation Board, 2003; Weick et al., 1999). Similarly, the literature on high-reliability organizations emphasizes the importance of taking small deviations seriously, even when the probability of error appears low, and maintaining close attention to operational processes (Roberts, 1990; Weick et al., 1999; Weick & Sutcliffe, 2007). Roberts's study of nuclear-powered aircraft carriers demonstrates that reliability in complex, high-risk systems depend not only on technology, but also on the disciplined execution of organizational processes (Roberts, 1990).

The distinctive link in the diagnostic system is weak-link diagnosis (Galbraith, 1973; Lawrence & Lorsch, 1967; Reason, 1997). Organizational weaknesses do not always originate at the same point (Reason, 1997; Weick & Sutcliffe, 2007). At times, organizational vulnerability is increased by ambiguity in the decision-making structure, a delayed response to environmental change, disconnection between units, or the loss of knowledge and experience (Galbraith, 1973; Lawrence & Lorsch, 1967; Rizzo et al., 1970; Walsh & Ungson, 1991). Organizational immunity architecture therefore does not settle for a generalized language of "organizational weakness"; it seeks to distinguish the domain in which the weakness is concentrated and the form of intervention it requires (Reason, 1997; Simons, 1995). When this distinction is not made, organizations often correct the visible symptom, while the deeper mechanism producing the weakness remains in place (Argyris & Schön, 1978; Reason, 1997).

Preventive intervention is therefore a natural extension of diagnosis (Ansoff, 1975; Reason, 1997; Schein, 1996). When diagnosis is not translated into managerial action, it produces only awareness (Argyris & Schön, 1978; Schein, 1996; Simons, 1995). Schein's interpretation of planned change as "managed learning" is consistent with this discussion because it demonstrates that organizational intervention is not merely a structural correction, but also a learning process (Schein, 1996). From the perspective of organizational immunity architecture, intervention may involve simplifying decision-making processes, restoring information flows, clarifying roles and responsibilities, ensuring the preservation of critical knowledge, or strengthening coordination between units (Galbraith, 1973; Lawrence & Lorsch, 1967; Rizzo et al., 1970; Walsh & Ungson, 1991). However, the enduring value of an intervention depends on what the organization learns from the experience and whether it can transform this learning into a form of memory that enables better diagnosis in subsequent cycles (Argyris & Schön, 1978; Crossan et al., 1999; Walsh & Ungson, 1991).

Organizational immunity architecture should therefore not be regarded as a one-off assessment tool (Crossan et al., 1999; Simons, 1995; Walsh & Ungson, 1991). More precisely, the model is a continuous diagnostic system that explains how an organization monitors weak signals, interprets them within diagnostic domains, transforms risk thresholds into managerial decision points, and links the outcomes of intervention to organizational memory through learning (Ansoff, 1975; Argyris & Schön, 1978; Crossan et al., 1999; Reason, 1997; Simons, 1995; Walsh & Ungson, 1991). The preventive character of the model also emerges here: the aim is not to wait until a crisis becomes inevitable, but to mobilize organizational attention while the weakening remains at a manageable level (Ansoff, 1975; Reason, 1997; Weick & Sutcliffe, 2007).

Core Panels of Organizational Immunity Architecture

Organizational immunity architecture does not reduce an organization's weaknesses to a single symptom or a single managerial domain (Galbraith, 1974; Lawrence & Lorsch, 1967; Teece et al., 1997; Walsh & Ungson, 1991). An organization's immunity is often tested simultaneously through its decision structure, its response to change, its interunit connections, and its way of using knowledge (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Teece et al., 1997). Therefore, the model is built on four core panels: leadership/structure, adaptation, integration, and intellectual capital (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Teece et al., 1997). These panels are not independent measurement headings; rather, they are complementary diagnostic domains that help to understand where the organization is weakening, through which channels this weakness spreads, and what kind of intervention it requires (Galbraith, 1974; Lawrence & Lorsch, 1967; Simons, 1995; Walsh & Ungson, 1991).

The leadership/structure panel monitors how decisions are made in the organization, how information reaches decision points, how clearly authority and responsibilities are defined, and to what extent managerial coordination functions (Galbraith, 1974; Rizzo et al., 1970; Tushman & Nadler, 1978). Galbraith's (1974) approach, which links organizational design with information-processing capacity, provides a strong foundation for this panel, because as uncertainty increases, organizations need to process more information, convey it to the right place, and arrange decision-making processes accordingly. Tushman and Nadler's (1978) information-processing perspective also shows that organizational design is not only about hierarchical order, but also about the collection, sharing, and transformation of information into decisions. Therefore, the leadership/structure panel is not concerned only with the question of "who makes the decision?"; it also questions on the basis of what information, at what speed, and within what clarity of responsibility the decision is made (Galbraith, 1974; Rizzo et al., 1970; Tushman & Nadler, 1978). The continuous delay of decisions, the blurring of areas of authority, the ambiguity of responsibility, or the failure of critical information to reach decision centers can be read as early-warning signs from the perspective of this panel (Columbia Accident Investigation Board, 2003; Galbraith, 1974; Rizzo et al., 1970; Tushman & Nadler, 1978). The official investigation report on the Columbia Space Shuttle accident is instructive at this point. The report evaluated the accident not only through technical damage, but also together with organizational culture, communication, and decision-making processes at NASA (Columbia Accident Investigation Board, 2003). This example shows that weaknesses in leadership and structure may produce consequences in complex systems that are as decisive as technical problems (Columbia Accident Investigation Board, 2003; Galbraith, 1974; Weick et al., 1999).

The adaptation panel shows how early the organization notices change in its environment and to what extent it can transfer this change into its own functioning (Cohen & Levinthal, 1990; Teece et al., 1997). What is important here is not only monitoring the external environment; it is also that information coming from outside gains meaning within the organization, can be discussed, and can be transformed into behavior (Cohen & Levinthal, 1990; Vuori & Huy, 2016). Cohen and Levinthal's (1990) absorptive capacity approach demonstrates that organizations' ability to recognize, assimilate, and use external knowledge is critical for innovation. The dynamic capabilities approach developed by Teece et al. (1997), in turn, emphasizes that resources and competencies need to be rearranged in changing environments. When these two lines are considered together, adaptation means not only seeing change, but also being able to provide an organizational response to the change that is seen (Cohen & Levinthal, 1990; Teece et al., 1997). Excessive attachment to old routines, the inability to carry new knowledge into decision-making processes, late interpretation of environmental change, or the failure of what has been learned to turn into practice are weaknesses to which this panel should attend (Cohen & Levinthal, 1990; Crossan et al., 1999; Teece et al., 1997; Vuori & Huy, 2016). Vuori and Huy's (2016) study on Nokia's decline in smartphone competition shows that adaptation capacity does not depend only on technological choices; attention, emotion, communication, and top-middle management relations within the organization also affect the innovation process. This case reveals that noticing change alone is not sufficient; knowledge must also be openly discussed within the organization and carried into decision-making processes in a sound manner (Cohen & Levinthal, 1990; Vuori & Huy, 2016).

The integration panel is concerned with the extent to which the different parts of the organization can come together around a common direction and meaning (Lawrence & Lorsch, 1967; Tushman & Nadler, 1978). In complex organizations, differentiation is inevitable; units have their own areas of expertise, priorities, and work rhythms (Lawrence & Lorsch, 1967). However, when this differentiation is not supported by effective integration, information silos, disconnected decisions, and recurring processes emerge (Galbraith, 1974; Lawrence & Lorsch, 1967; Tushman & Nadler, 1978). Lawrence and Lorsch's (1967) classic study on differentiation and integration showed that organizational effectiveness depends not only on specialization, but also on how specialized units are brought together. Therefore, the integration panel monitors more than a superficial indicator of cooperation; it examines whether information, meaning, and action gain continuity within the organization (Galbraith, 1974; Lawrence & Lorsch, 1967; Tushman & Nadler, 1978). The failure of a risk noticed by one department to reach another unit, the different interpretation of a common goal in different departments, the retention of critical information in silos, or the disconnected progression of processes weakens the organizational immunity response (Columbia Accident Investigation Board, 2003; Galbraith, 1974; Lawrence & Lorsch, 1967; Tushman & Nadler, 1978). In the Columbia report, the central place of the relationship among the interpretation of technical findings, communication channels, and decision-making processes in understanding the accident shows how a lack of integration may produce severe consequences in high-risk structures (Columbia Accident Investigation Board, 2003).

The intellectual capital panel monitors to what extent the organization can preserve and use the knowledge, experience, expertise, relationships, and institutional memory it possesses (Nahapiet & Ghoshal, 1998; Nonaka, 1994; Walsh & Ungson, 1991). In this panel, knowledge is not viewed only as individual expertise or technical accumulation; it is evaluated together with relationships, trust, shared meanings, and the transfer of experience (Nahapiet & Ghoshal, 1998; Nonaka, 1994). Nahapiet and Ghoshal's (1998) study on the relationship between social capital and intellectual capital shows that knowledge needs relational and structural ties in order to be transformed into organizational value. Nonaka's (1994) knowledge creation approach also emphasizes that knowledge does not remain closed within individuals, but is transformed through social interaction and carried to the organizational level. Therefore, the intellectual capital panel monitors not so much how much

knowledge exists in the organization, but whether this knowledge enters circulation, whether it is carried into decision-making processes, and whether past experiences are transformed into institutional memory (Nahapiet & Ghoshal, 1998; Nonaka, 1994; Walsh & Ungson, 1991). The concentration of critical knowledge in a few individuals, the lack of sharing of expertise among units, the loss of knowledge together with employee departure, or the repetition of the same errors indicates an immunity weakness from the perspective of this panel (Edmondson, 1996; Nahapiet & Ghoshal, 1998; Walsh & Ungson, 1991). The Nokia case is also meaningful in this respect; the findings of Vuori and Huy (2016) show that the mere existence of knowledge in the organization is not sufficient, and that this knowledge must be openly discussed, interpreted, and transformed into strategic decisions.

When these four panels work together, organizational immunity architecture ceases to be a simple checklist and turns into a diagnostic arrangement that reads the organization's weaknesses in a more holistic manner (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Simons, 1995; Teece et al., 1997). The leadership/structure panel makes decision and governance clarity visible; the adaptation panel makes the capacity to respond to change visible; the integration panel makes connection and alignment within the organization visible; and the intellectual capital panel makes the preservation, sharing, and renewal of knowledge visible (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Nonaka, 1994; Walsh & Ungson, 1991). A weakness in any one of these panels may also affect the others (Galbraith, 1974; Lawrence & Lorsch, 1967; Tushman & Nadler, 1978). If the decision structure is ambiguous, information does not reach the right place; if adaptation is weak, what has been learned does not turn into behavior; if integration is weak, signals remain fragmented; if intellectual capital is weak, the organization reproduces the same problems (Cohen & Levinthal, 1990; Crossan et al., 1999; Edmondson, 1996; Galbraith, 1974; Lawrence & Lorsch, 1967; Walsh & Ungson, 1991). Therefore, the main function of the panels is not to produce individual performance indicators, but to show how the structural, cognitive, relational, and adaptive mechanisms that constitute organizational immunity work together (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Teece et al., 1997). Organizational immunity architecture does not reduce an organization's weaknesses to a single symptom or a single area of management (Galbraith, 1974; Lawrence & Lorsch, 1967; Teece et al., 1997; Walsh & Ungson, 1991). An organization's immunity is often tested simultaneously in its decision-making structure, its response to change, its connections between units, and the way it uses knowledge (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Teece et al., 1997). The model is therefore built around four core panels: leadership/structure, adaptation, integration, and intellectual capital (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Teece et al., 1997). These panels are not independent measurement categories; rather, they are complementary diagnostic domains that help identify where the organization is weakening, through which channels that weakness is spreading, and what form of intervention it requires (Galbraith, 1974; Lawrence & Lorsch, 1967; Simons, 1995; Walsh & Ungson, 1991).

Cyclical Model and Theoretical Propositions

Organizational immunity architecture should not be understood as a control activity conducted by the organization at specified intervals (Simons, 1995; Weick & Sutcliffe, 2007). A more continuous mode of operation underlies the model: the organization gathers signals from its environment and internal configuration, makes sense of them, distinguishes the source of the weakness, intervenes when necessary, and carries this experience into subsequent decisions (Ansoff, 1975; Argyris & Schön, 1978; Crossan et al., 1999; Weick et al., 1999). The model therefore differs from the conventional sequence of "problem identification and solution" (Argyris & Schön, 1978; Schein, 1996). Here, each intervention generates new learning, and each instance of learning

contributes to the earlier and more careful interpretation of subsequent signals (Argyris & Schön, 1978; Crossan et al., 1999; Levitt & March, 1988; Walsh & Ungson, 1991). Ansoff's (1975) weak signals approach provides a strong foundation for the first link in this cycle by demonstrating that strategic surprises often emerge initially not as complete and explicit threats, but as fragmented signals that require interpretation.

The signals at the beginning of the model do not originate solely from the market, technology, or the external environment (Ansoff, 1975; Weick et al., 1999; Weick & Sutcliffe, 2007). Small deviations arising within the organization itself are equally important (Reason, 1997; Vaughan, 1996; Weick et al., 1999). Slower decision-making, the failure to escalate problems to senior management, disruptions in the flow of information between units, the recurrence of the same errors, or the concentration of critical knowledge in a limited number of individuals do not generally indicate impending disaster when considered in isolation (Edmondson, 1996, 1999; Galbraith, 1974; Morrison, 2014; Walsh & Ungson, 1991). However, when these signals are observed collectively and over time, they may indicate the direction in which organizational weakness is progressing (Reason, 1997; Simons, 1995; Weick & Sutcliffe, 2007). Vaughan's study of the Challenger disaster is noteworthy in this respect. Vaughan explained the gradual normalization of technical deviations at NASA in relation to its organizational culture and decision-making processes; this phenomenon has become one of the best-known examples in the literature on the "normalization of deviance" (Vaughan, 1996). Vaughan's book, published by the University of Chicago Press, is an established work examining the Challenger decision in the context of risk, culture, and deviance at NASA (Vaughan, 1996).

The value of such signals becomes apparent only when they are placed within the appropriate diagnostic domain (Reason, 1997; Simons, 1995). Within organizational immunity architecture, the leadership/structure, adaptation, integration, and intellectual capital panels perform this function (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Walsh & Ungson, 1991). In one organization, the visible problem may arise from its decision-making arrangements; in another case, the underlying weakness may be a delayed response to change, information becoming trapped between units, or the failure to preserve experience (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Walsh & Ungson, 1991). The report of the board that investigated the Columbia accident illustrates this distinction. The report did not limit its explanation of the accident to a technical cause such as the foam strike; it also stated that NASA's organizational culture, communication, and decision-making processes played a role in the accident (Columbia Accident Investigation Board, 2003). This example demonstrates that, in complex organizations, physical or technical problems often cannot be considered independently of organizational interpretation and decision-making arrangements (Columbia Accident Investigation Board, 2003; Reason, 1997; Weick et al., 1999).

At the next stage of the cycle, the organization does not assign equal weight to every signal (Kaplan & Mikes, 2012; Simons, 1995). Some deviations may remain within the range of normal variation; some require closer monitoring; and others indicate a weakness that requires intervention without delay (International Organization for Standardization, 2018; Kaplan & Mikes, 2012; Reason, 1997). The risk threshold is therefore not merely a measurement boundary within the model, but a decision boundary indicating the point at which managerial attention should intensify (International Organization for Standardization, 2018; Kaplan & Mikes, 2012; Simons, 1995). Once this boundary is crossed, the nature of the intervention also varies according to the diagnosis (Reason, 1997; Schein, 1996; Simons, 1995). If the decision-making structure has become ambiguous, authority and responsibility arrangements can be simplified; if the flow of information has been interrupted, communication channels can be reestablished; if coordination has deteriorated, connections between units can be strengthened; and if critical knowledge has been lost, mechanisms for knowledge preservation and the transfer of experience can be activated (Galbraith, 1974; Lawrence & Lorsch,

1967; Rizzo et al., 1970; Walsh & Ungson, 1991). Duchek's (2020) study, which conceptualizes organizational resilience through the processes of anticipation, coping, and adaptation, is consistent with this logic because it demonstrates that resilience concerns not only post-crisis recovery, but also the development of capacity before a crisis.

The cycle is completed through learning and memory (Argyris & Schön, 1978; Crossan et al., 1999; Levitt & March, 1988; Walsh & Ungson, 1991). Even if an organization recognizes a weakness and intervenes, the same problem may return in different forms if this experience is not incorporated into decision-making processes, routines, and organizational memory (Argyris & Schön, 1978; Froughi et al., 2020; Lee et al., 2020; Levitt & March, 1988; Walsh & Ungson, 1991). Levitt and March (1988) conceptualize organizational learning as a routine-based, history-dependent, and target-oriented process. Walsh and Ungson (1991), in turn, discuss organizational memory in terms of the storage of knowledge within the organization and its reuse when needed. When these two approaches are considered together, it becomes clear that learning does not consist merely of recording the past (Crossan et al., 1999; Levitt & March, 1988; Walsh & Ungson, 1991). Learning is a form of institutional attention that determines what the organization will notice earlier in the next cycle, which signal it will take more seriously, and which intervention it will select more rapidly (Argyris & Schön, 1978; Crossan et al., 1999; Weick et al., 1999; Weick & Sutcliffe, 2007) (Figure 1).

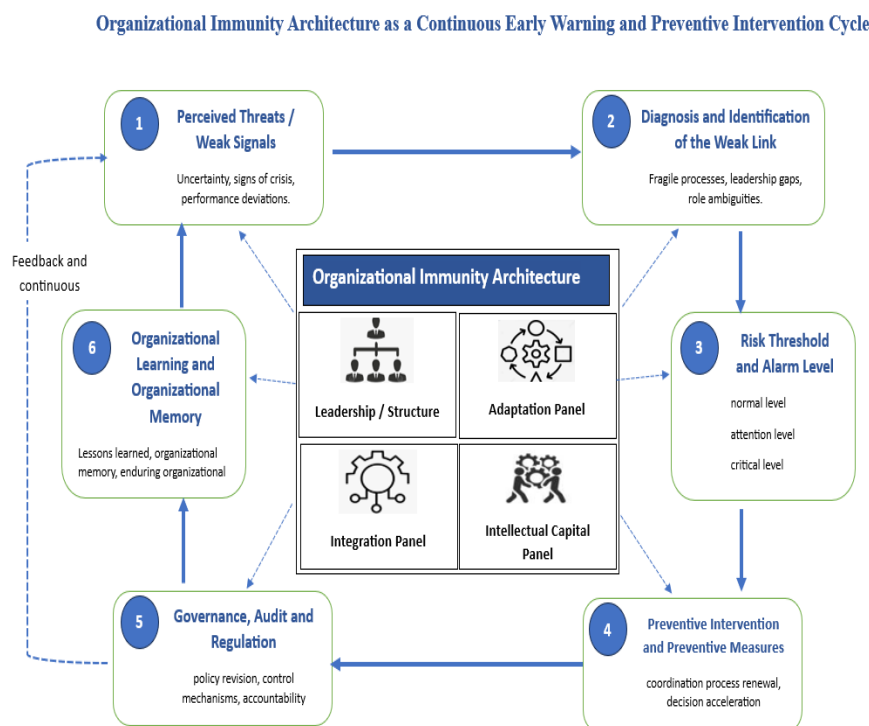


Figure 1. Organizational Immunity Architecture as a Continuous Early Warning and Preventive Intervention Cycle

Source: Author's own elaboration.

Figure 1 depicts two levels simultaneously. The continuous arrows in the outer ring represent the temporal process that begins with perceived threats and weak signals and proceeds through diagnosis, risk threshold, preventive intervention, governance arrangements, and organizational learning; the dashed feedback link indicates that learning and memory influence the sensing of new signals. The four panels at the center are not sequential stages of the cycle; they are horizontal diagnostic domains used at each stage to distinguish the organizational area in which the weakness is concentrated. The dashed links between the panels and the outer ring indicate that panel data provide input into diagnosis, threshold, and intervention decisions and that intervention outcomes are subsequently monitored again through the same panels.

The fifth stage of the cycle—governance, control, and adjustment—is the point at which temporary intervention is transformed into permanent institutional change. At this stage, the outcomes of intervention are incorporated into policies and decision rules, control mechanisms, authority and responsibility structures, and accountability arrangements. When governance adjustment does not occur, the intervention may remain local and temporary; when the adjustment is linked to learning and memory, the organization not only addresses a specific problem but also renews the rules governing its future responses to similar signals (Argyris & Schön, 1978; Simons, 1995; Walsh & Ungson, 1991).

The directional relationships in the model have been translated into the following four theoretical propositions, taking into account researchable outcomes and boundary conditions (Jaakkola, 2020; Whetten, 1989).

The transmission of weak signals to decision-making centers does not depend solely on the existence of information systems. It requires that employees do not perceive voicing concerns as an interpersonal risk, that managers are receptive to critical information, and that open communication channels exist between units (Edmondson & Bransby, 2023; Morrison, 2023). Findings indicating that employee voice can bolster team resilience in the face of environmental change also support the rationale for treating the sharing of signals within the organization as a boundary condition in the model (Li & Tangirala, 2022).

Proposition 1: As the degree to which weak signals obtained from the four diagnostic panels are jointly evaluated increases, the speed with which organizational weaknesses are detected and the accuracy of diagnosis increase; this relationship is stronger under conditions of high environmental uncertainty and when signals are dispersed across organizational units.

Proposition 2: The convergence of signals from different panels on the same weak link increases the accuracy of preventive intervention compared with signals obtained from a single panel; this effect weakens in organizations characterized by fragmented information flows and low psychological safety.

Proposition 3: Calibrating risk thresholds in alignment with the organization's historical normal ranges, risk appetite, and the magnitude of the potential impact strengthens the positive relationship between diagnosis and timely intervention. Overly sensitive thresholds increase the false-positive alarm rate, whereas insufficiently sensitive thresholds increase the false-negative alarm rate.

Proposition 4: As the extent to which intervention outcomes are incorporated into organizational learning and memory through governance arrangements increases, the speed of weak-signal detection and the accuracy of diagnosis increase in subsequent cycles; this relationship is stronger in organizations characterized by clear accountability and a high capacity for organizational knowledge preservation.

In the empirical testing of these propositions, panel integration may be treated as the independent variable; signal detection time, diagnostic accuracy, intervention accuracy, and false alarm rates as outcome variables; and environmental uncertainty, information fragmentation, psychological safety, accountability, and knowledge preservation capacity as boundary conditions. The combined use of event records collected at multiple points in time, alarm logs, intervention decisions, and employee and managerial assessments would enable the propositions to be tested using behavioral indicators as well as perceptual data.

Discussion

The organizational immunity architecture proposed in this study does not merely explain the extent to which organizations remain strong in the face of crises; it focuses on an earlier question: through what configuration of attention, information, and decision-making can an organization interpret its own signs of weakening? In this respect, the theoretical contribution of the model emerges at a level that complements the organizational resilience literature. Duchek (2020) places strong emphasis on crisis preparedness by explaining resilience through the processes of anticipation, coping, and adaptation. Organizational immunity architecture places this idea of preparedness on a more diagnostic foundation, arguing that resilience is related not only to what happens after a crisis, but also to the interpretation of early deterioration that gives rise to the possibility of a crisis (Ansoff, 1975; Weick & Sutcliffe, 2007). The model thus treats resilience not as an outcome-based capacity, but as an organizational attribute that develops through a cycle of organizational attention, diagnosis, threshold assessment, and learning.

The Challenger and Columbia cases clearly demonstrate why the model must consider not only technical risks, but also organizational interpretation and decision-making arrangements. Vaughan's (1996) study of the Challenger accident demonstrated that the normalization of technical deviations over time must be considered in conjunction with organizational culture and decision-making processes. The Columbia Accident Investigation Board (2003) likewise did not explain the Columbia accident solely in terms of physical damage; it also placed NASA's organizational culture, communication patterns, and decision-making processes at the center of its analysis. These two cases substantiate the central claim of organizational immunity architecture: in complex systems, vulnerability often does not emerge suddenly; how small deviations are interpreted, who is able to say what, and which information decision centers take seriously become decisive over time.

The empirical testing of the model should also be designed in accordance with this cyclical logic. Single-wave, single-source surveys may reveal certain dimensions of organizational immunity, but they remain limited in capturing the model's logic of early warning, threshold assessment, and feedback. Future studies would therefore be more robust if they adopted multi-wave, multisource, and, where possible, event-based designs. Employee surveys may provide data on decision clarity, psychological safety, information sharing, or perceptions of adaptation; by contrast, error reports, project delays, employee turnover rates, customer complaints, internal audit findings, and meeting minutes may enable an organization's weak signals to be monitored at a more behavioral level. Such multisource approaches are also important for reducing the risk of common method bias. Podsakoff et al. (2003, 2024) discuss in detail how common method bias can constitute an important alternative explanation for findings in behavioral research.

From a managerial perspective, the model assigns organizations the task of designing institutional attention before a crisis rather than merely controlling damage after it. This attention should not be directed solely toward financial outcomes or final performance indicators. Why decisions are delayed, where information becomes trapped, which problems cannot be voiced, which units become disconnected from one another, and which experiences fail to become embedded in organizational memory must be monitored with equal seriousness. However, an important boundary must be recognized here. Unless continuous monitoring is established as an early warning system

that supports learning, it can easily develop into a culture of control and punishment. The healthy functioning of organizational immunity architecture therefore depends less on the collection of data than on how those data are interpreted and the climate of trust in which employees can share problems. Edmondson's (1999) findings add a strong warning to the managerial dimension of the model: in organizations where speaking up is perceived as risky, early warning mechanisms may exist formally while remaining functionally weak.

The limitations of the model must also be made explicit. First, the analogy to preventive medicine and a biochemistry panel is an explanatory device; it should not be used to equate organizations directly with biological systems. Organizations are political and cultural structures that are open to interpretation; the same indicator may carry different meanings in different contexts. Second, not every weak signal foreshadows an actual crisis. This creates the risk of false alarms. An overly sensitive system may generate unnecessary interventions, whereas an insufficiently sensitive system may detect critical signals too late. Third, the functioning of the model may vary according to industry, organizational size, technological complexity, and the regulatory environment. In fields requiring high reliability, such as aviation, healthcare, energy, or defense, the logic of early warning and thresholds may be more central; in lower-risk industries, the same indicators may carry different weights (Weick & Sutcliffe, 2007). Organizational immunity architecture should therefore be treated not as a universal prescription, but as a theoretical framework that must be tested across different contexts.

Conclusion

This study has conceptualized organizational immunity not as a defensive reflex that becomes operative after a crisis has emerged, but as a cyclical architecture of diagnosis and learning capable of interpreting an organization's vulnerabilities while they are still at a manageable level. The proposed model brings together the classical approach to the strategic importance of weak signals, the anticipation-coping-adaptation logic of organizational resilience, the dynamic capabilities literature's emphasis on reconfiguring competencies in response to environmental change, the logic of risk assessment, and the role of organizational learning and memory in institutionalizing experience (Ansoff, 1975; Ducheck, 2020; International Organization for Standardization, 2018; Levitt & March, 1988; Teece et al., 1997; Walsh & Ungson, 1991; Weick & Sutcliffe, 2007). Organizational immunity architecture is thus positioned not as a new label that replaces the literatures on resilience, dynamic capabilities, or organizational learning, but as a specific theoretical framework that integrates their explanatory power within a cycle of early diagnosis, risk threshold, preventive intervention, and feedback.

The central claim of the model is clear: the long-term health of organizations is determined not only by how they respond during a crisis, but also by what they recognize before a crisis, which signals they take seriously, where they diagnose weakness, and what they transform into organizational memory following intervention. The leadership/structure, adaptation, integration, and intellectual capital panels are therefore not merely conceptual dimensions within the model; they are diagnostic domains that enable the organization to interpret its loss of immunity. As the Challenger and Columbia cases demonstrate, major breakdowns in complex organizations are often driven not by a single technical failure, but by how weak signals are interpreted, where information becomes trapped, and the assumptions that underpin decision-making processes (Columbia Accident Investigation Board, 2003; Vaughan, 1996). Organizational immunity architecture therefore grounds its claim to make organizations "more resilient" in their capacity to detect earlier, interpret more accurately, and intervene more promptly.

In conclusion, this study has sought to transform organizational immunity from an abstract metaphor into a holistic theoretical model linking organizational attention, diagnosis, intervention, and learning. The value of the model lies not in promising organizations a flawless control system,

but in reminding them that vulnerabilities often emerge as small deviations and neglected signals before they produce visible outcomes. Organizational immunity architecture therefore opens a productive line of inquiry for future conceptual and empirical research: management and organization research should focus not only on how strong organizations are, but also on how early and honestly, they can interpret their own weaknesses and how much they can learn through that process.

www.turkishstudies.net/economy**Turkish Studies - Economics, Finance, Politics**

eISSN: 2667-5625

**ANKARA SCIENCE
UNIVERSITY**

Örgütsel Bağışıklık Mimarisi: Önleyici Bir Erken Uyarı Model Önerisi

Giriş

Günümüzde örgütler yalnızca rekabet baskıları ve teknolojik değişimle değil, aynı zamanda tedarik zinciri aksamaları, iş gücü hareketliliği, itibar riskleri, bilgi akışındaki kesintiler ve ani çevresel dalgalanmalarla da mücadele etmek zorundadır (Allen vd., 2010; Christopher & Peck, 2004; Galbraith, 1973; Power vd., 2009; Teece vd., 1997; Weick & Sutcliffe, 2007). Bu koşullar altında örgütsel başarıyı yalnızca bir örgütün kriz sonrasında ne kadar hızlı toparlandığı üzerinden açıklamak yetersiz kalmaktadır (Duchek, 2020; Lengnick-Hall vd., 2011). Temel mesele, kriz görünür hâle gelmeden önce ortaya çıkan zayıf sinyallerin fark edilip edilmediği, örgüt içindeki kırılganlıkların zamanında teşhis edilip edilmediği ve bu teşhislerin önleyici yönetsel eyleme dönüştürülüp dönüştürülmediğidir (Ansoff, 1975; Reason, 1997; Weick vd., 1999; Weick & Sutcliffe, 2007). Ansoff'un (1975) zayıf sinyaller yaklaşımı, stratejik sürprizlerin çoğu zaman açık ve kesin göstergeler aracılığıyla değil, başlangıçta belirsiz, dağınık ve yoruma açık olan erken işaretler aracılığıyla görünür hâle geldiğini göstermesi nedeniyle bu tartışma için sağlam bir hareket noktası sunmaya devam etmektedir.

Bu ihtiyaca yanıt olarak bu makalede örgütsel bağışıklık mimarisi kavramı önerilmektedir. Bu kavram, örgütü yalnızca kriz meydana geldikten sonra tepki veren pasif bir varlık olarak görmek yerine; algılanan tehditleri, zayıf sinyalleri ve sistemik kırılganlıkları erken aşamada belirleyen, risk eşiklerini görünür hâle getiren, önleyici müdahaleleri yönetim düzenlemeleriyle ilişkilendiren ve bu süreci örgütsel öğrenmeye ve hafızaya dönüştüren döngüsel bir kurumsal sistem olarak ele almaktadır (Ansoff, 1975; Argyris & Schön, 1978; Reason, 1997; Walsh & Ungson, 1991; Weick vd., 1999). Bu anlamda örgütsel bağışıklık mimarisi, tanısal bir gösterge panelinin mantığına göre işlemektedir (Simons, 1995). Karar alma süreçlerindeki gecikmeler, rol belirsizliği, bilgi siloları, koordinasyon başarısızlıkları, örgütsel öğrenmenin yavaşlığı, kritik yeteneklerin kaybı ve aynı hataların tekrarlanması gibi göstergeler, örgütsel bağışıklıkta aksi takdirde gizli kalacak zayıflıkları ortaya çıkaran erken uyarı sinyalleri olarak değerlendirilebilir (Edmondson, 1996; Galbraith, 1973; Lawrence & Lorsch, 1967; Lengnick-Hall vd., 2011; Rizzo vd., 1970; Weick & Sutcliffe, 2007).

Bu makalenin temel amacı, örgütsel bağışıklığı kriz sonrası toparlanma veya genel dayanıklılık kapasitesiyle sınırlandırmayan; bunun yerine erken uyarı, teşhis, zayıf halka analizi, risk eşikleri, önleyici müdahale, yönetim düzenlemeleri ve örgütsel öğrenmeyi tek bir döngü içerisinde açıklayan teorik bir model geliştirmektir (Ansoff, 1975; Duchek, 2020; Reason, 1997; Simons, 1995; Weick & Sutcliffe, 2007). Modelin merkezinde dört panel yer almaktadır: liderlik/yapı, adaptasyon, entegrasyon ve entelektüel sermaye. Liderlik/yapı paneli karar netliğini, yetki dağılımını ve yönetim hazırlığını; adaptasyon paneli çevresel duyarlılığı ve yenilenme kapasitesini; entegrasyon paneli birimler arası tutarlılığı ve sistemik uyumu; entelektüel sermaye paneli ise bilginin korunmasını, örgütsel hafızayı ve örgütsel bağışıklık zekâsını temsil etmektedir (Cohen & Levinthal, 1990; Galbraith, 1973; Lawrence & Lorsch, 1967; March, 1991; Nahapiet & Ghoshal, 1998; Teece

vd., 1997; Walsh & Ungson, 1991). Nahapiet ve Ghoshal'ın (1998) sosyal sermaye ile entelektüel sermaye arasındaki ilişkiyi bir örgütsel avantaj kaynağı olarak kavramsallaştırması, modelin bilgi, ilişkisel ve entelektüel sermaye boyutları için önemli bir teorik temel sağlamaktadır.

Bu makalenin katkısı üç yönlüdür. İlk olarak örgütsel bağımsızlık, kriz sonrası savunma veya toparlanma kapasitesi olarak görülmekten çıkarılarak kriz meydana gelmeden önce erken teşhis ve önleyici müdahaleyi mümkün kılan döngüsel bir mimari olarak yeniden konumlandırılmaktadır (Ansoff, 1975; Duchek, 2020; Weick & Sutcliffe, 2007). İkinci olarak örgütsel dayanıklılık, dinamik yetenekler, zayıf sinyal tespiti, örgütsel öğrenme, örgütsel hafıza ve entelektüel sermaye yazınları tek bir teorik model içerisinde bütünleştirilmektedir (Argyris & Schön, 1978; Duchek, 2020; Levitt & March, 1988; Nahapiet & Ghoshal, 1998; Teece vd., 1997; Walsh & Ungson, 1991). Üçüncü olarak model, örgütsel bağımsızlığı soyut bir kapasite düzeyinde bırakmak yerine, liderlik/yapı, adaptasyon, entegrasyon ve entelektüel sermaye panelleri aracılığıyla izlenebilen, teşhis edilebilen ve yönetsel müdahaleye dönüştürülebilen bir sistem olarak kavramsallaştırmaktadır (Cohen & Levinthal, 1990; Galbraith, 1973; Lawrence & Lorsch, 1967; Simons, 1995). Böylece çalışma, yalnızca örgütlerin krizlere nasıl dayandığını değil, aynı zamanda krizlerin ortaya çıkışına işaret eden erken sinyalleri nasıl tespit ettiklerini, zayıf halkaları nasıl teşhis ettiklerini ve öğrenmeyi kalıcı örgütsel zekâyâ nasıl dönüştürdüklerini açıklayan özgün bir teorik çerçeve sunmaktadır (Crossan vd., 1999; March, 1991; Walsh & Ungson, 1991; Weick vd., 1999).²

Kavramsal Araştırma Tasarımı ve Model Geliştirme

Bu çalışma, ampirik bir sına veya sistematik bir literatür taraması olarak değil, kuramsal sentezi kavramsal model geliştirmeyle birleştiren kavramsal bir çalışma olarak tasarlanmıştır. Kavramsal çalışmaların da belirli kuram ve kavramların neden seçildiklerini, analizde hangi rolleri üstlendiklerini ve ortaya çıkan modelin hangi akıl yürütme aşamaları aracılığıyla geliştirildiğini açıklayan açık bir araştırma tasarımına dayanması gerekmektedir (Jaakkola, 2020). Buna göre bu çalışmada ele alınan odak olgu, örgütlerin henüz tam anlamıyla krize dönüşmemiş zayıflıkları nasıl fark ettikleri ve teşhis ettikleri, bunları yönetsel karar alma eşiğine nasıl taşıdıkları ve müdahale sonrası deneyimlerini örgütsel öğrenmeye nasıl dönüştürdükleriyle ilgilidir.

Kuramsal kaynak havuzu, bu odak olguyu açıklamak için gerekli işlevler doğrultusunda amaçlı olarak sınırlandırılmıştır. Zayıf sinyaller ve yüksek güvenilirlik yazınları, erken uyarı işaretlerinin tespit edilmesini açıkladıkları için; örgütsel dayanıklılık ve dinamik yetenekler yazınları, öngörme, adaptasyon ve yeniden yapılandırma kapasitelerini açıkladıkları için; örgüt tasarımı ve risk yönetimi yazınları, tanınan alanları, eşikleri ve yönetsel müdahaleyi açıkladıkları için; örgütsel öğrenme, örgütsel hafıza ve entelektüel sermaye yazınları ise deneyimin kurumsallaştırılmasını açıkladıkları için çalışmaya dâhil edilmiştir. Kaynaklar; örgüt düzeyinde bir açıklama sunmaları, döngünün en az bir işlevi için doğrudan kuramsal temel sağlamaları ve ilgili kavramlar arasındaki ilişkileri açıklamaları durumunda modele dâhil edilmiştir. Yalnızca kriz sonrası sonuçları betimleyen, örgütsel bir mekanizmayla ilişkilendirilmeyen veya biyolojik metaforu açıklayıcı bir çerçeveye dönüştürmeyen çalışmalar, modelin temel kaynakları arasına alınmamıştır.

Model geliştirme süreci dört analitik aşamada yürütülmüştür. İlk olarak ilgili yazınlarda tekrar eden kuramsal işlevler —algılama, teşhis, eşik değerlendirmesi, müdahale, yönetim düzenlemeleri ve öğrenme— analitik olarak birbirinden ayrılmıştır. İkinci olarak farklı adlandırmalar altında aynı işlevi açıklayan kavramlar birleştirilmiş, farklı işlevleri yerine getiren kavramlar ise birbirinden ayrı tutulmuştur. Üçüncü olarak liderlik/yapı, adaptasyon, entegrasyon ve entelektüel

² Entelektüel sermaye, uyum ve örgütsel dayanıklılık arasındaki ilişki; kavramsal model geliştirme yöntemi; müdahale, değişim ve örgütsel öğrenme; bilginin üretilmesi, paylaşılması ve örgütsel süreçlere aktarılması; liderlik, destekleyici iklim ve bilgi paylaşımı; çalışanların sorunları bildirebilmesi, psikolojik güvenlik ve zayıf sinyallerin yönetime ulaşması gibi farklı sektörler ve kurumlar bağlamında ele alan çalışmalar için ayrıca bk. Agostini, & Nosella, 2023; Jaakkola, 2020; Schein, 1996; Töre, 2020; Mertel, Bozkurt, & Demirhan, 2020; Köse, Mohan Bursalı, & Dolma, 2023.

sermaye, örgütsel zayıflıkların nerede yoğunlaştığını gösteren yatay tanısallık paneller olarak düzenlenirken; algılama, teşhis, eşik değerlendirmesi, müdahale, yönetim düzenlemeleri ve öğrenme, teşhisin zaman içerisinde nasıl eyleme dönüştürüldüğünü gösteren altı aşamalı bir süreç olarak yapılandırılmıştır. Son olarak aşamalar arasındaki yönlü bağlantılar ve geri bildirim ilişkisi belirlenmiş; önermeler, modelin neyi açıkladığını, bunu nasıl ve neden açıkladığını ve açıklamalarının hangi koşullar altında geçerli olduğunu açıkça ortaya koyacak biçimde türetilmiştir (Whetten, 1989).

Bu noktada, dört panelin kavramsal kökenleri ile mevcut çalışmanın katkısı arasında açık bir ayrım yapılmalıdır. Kara ve Yalçın (2026), Örgütsel DNA Profili Ölçeği'ni kullanarak örgütsel bağışıklığı liderlik/yapı, adaptasyon, entegrasyon ve entelektüel sermaye boyutları üzerinden ampirik olarak incelemiş ve çalışanların bu boyutlara ilişkin algılarının demografik özelliklerine göre farklılaşıp farklılaşmadığını araştırmıştır. Mevcut çalışma, bu dört boyutu bağımsız unsurlar olarak yeniden keşfettiği iddiasında değildir. Bunun yerine çalışma, bu boyutları zayıf sinyallerin yoğunlaştığı örgütsel alanları birbirinden ayıran tanısallık paneller olarak yeniden konumlandırmakta ve bunları algılama, teşhis, risk eşik değeri değerlendirme, önleyici müdahale, yönetim düzenlemeleri ve örgütsel öğrenmeden oluşan bir döngüyle ilişkilendirmektedir. Dolayısıyla önceki çalışma örgütsel bağışıklığın ölçülebileceği boyutlara odaklanırken mevcut çalışma, bu boyutların sürekli bir erken uyarı ve önleyici müdahale süreci içerisinde nasıl birlikte işlediğini açıklamaktadır.

Bu ayrım doğrultusunda makalenin özgünlük iddiası, dört panelin ilk kez önerilmesine değil, daha önce ampirik ölçüm alanları olarak kullanılan bu panellerin geri bildirim özelliği taşıyan altı aşamalı bir süreç mimarisi içerisinde işlevsel olarak bütünleştirilmesine dayanmaktadır. Dört panel, örgütsel zayıflıkların nerede bulunduğunu; altı aşamalı döngü, zayıf bir sinyalin teşhisten müdahaleye ve kurumsal öğrenmeye nasıl ilerlediğini; geri bildirim bağlantısı ise tamamlanan her döngünün sonraki algılama ve eşik değerlendirmesini nasıl değiştirdiğini açıklamaktadır.

Kuramsal Çerçeve

Örgütsel bağışıklık mimarisi, yönetim ve organizasyon yazınındaki yerleşik bazı kavramlarla aynı inceleme alanında yer alsa da yalnızca bu kavramların toplamından ibaret değildir (Ansoff, 1975; Duchek, 2020; Huang, 2013; Teece vd., 1997; Walsh & Ungson, 1991). Buna göre bu çalışma, yazını sıralı biçimde özetlemek yerine, önerilen modelin ilişkili olduğu kuramsal yaklaşımları ve bu yaklaşımlardan hangi noktalarda ayrıldığını açıklamayı amaçlamaktadır (Ansoff, 1975; Duchek, 2020; Huang, 2013; Teece vd., 1997; Walsh & Ungson, 1991). Böyle bir ayrım gereklidir; çünkü örgütsel dayanıklılık, dinamik yetenekler, örgütsel öğrenme, örgütsel hafıza ve zayıf sinyaller yazınları örgütsel kırılabilirliğin farklı yönlerine ilişkin güçlü açıklamalar sunarken örgütsel bağışıklık mimarisi, bu yönleri erken teşhis, eşik değerlendirme ve önleyici örgütsel uyarılma mantığı içerisinde bütünleştiren, tanısallık yönelimi daha belirgin bir çerçeve önermektedir (Ansoff, 1975; Argyris & Schön, 1978; Duchek, 2020; Reason, 1997; Simons, 1995; Teece vd., 1997; Walsh & Ungson, 1991).

Tablo 1, her kavramın temel odağı ile örgütsel bağışıklık mimarisi içerisindeki işlevini ve bu mimariden ayrıldığı noktaları karşılaştırarak kuramsal rollerin bu dağılımını özetlemektedir. Örgütsel dayanıklılık, işlevselliği sürdürme, toparlanma ve adaptasyon kapasitelerini sağlamakta (Duchek, 2020); dinamik yetenekler, kaynakların ve yetkinliklerin yeniden yapılandırılmasına ilişkin mantığı sunmakta (Teece vd., 1997); örgütsel öğrenme ve örgütsel hafıza, deneyimin rutinlere ve geri çağrılabilir bilgiye nasıl dönüştürüldüğünü açıklamakta (Levitt & March, 1988; Walsh & Ungson, 1991); zayıf sinyaller yaklaşımı ise erken fakat belirsiz tanısallık girdiler sunmaktadır (Ansoff, 1975). Dolayısıyla Tablo 1, hem her bir yazından alınan katkıyı hem de örgütsel bağışıklık mimarisinin üstlendiği özgül açıklama görevini belirleyerek kavramsal bir sınır haritası işlevi görmektedir: kriz öncesi algılama ve kırılabilirlik teşhisini risk eşik değeri değerlendirme, önleyici müdahale ve kurumsal öğrenmeyle ilişkilendirmek.

Zayıf sinyaller yaklaşımı, örgütsel bağıklık mimarisine erken tespit konusunda duyarlılık kazandırmaktadır (Ansoff, 1975). Ansoff'un (1975) çalışması, stratejik sürprizlerin çoğu zaman ilk olarak açık, güçlü ve kesin göstergeler aracılığıyla değil, belirsiz, parçalı ve yoruma açık sinyaller aracılığıyla görünür hâle geldiğini göstermesi nedeniyle temel bir başvuru noktası olmayı sürdürmektedir. Bu görüş, örgütlerin yalnızca doğrulanmış tehditlere değil, anlamı henüz tam olarak netleşmemiş sinyallere de dikkat etmeleri gerektiğini göstermektedir (Ansoff, 1975; Weick vd., 1999; Weick & Sutcliffe, 2007). Bununla birlikte zayıf sinyaller yaklaşımı tek başına, bu tür sinyallerin örgüt içerisinde hangi tanısal kategoriler aracılığıyla değerlendirilmesi gerektiğini, hangi eşiklerde yönetsel önceliklere dönüşmesi gerektiğini ve hangi müdahale biçimleri aracılığıyla ele alınması gerektiğini açıklamakta yetersiz kalmaktadır (Ansoff, 1975; Reason, 1997; Simons, 1995). Bu noktada örgütsel bağıklık mimarisi, zayıf sinyalleri yalnızca çevresel tarama girdileri olarak değil, örgütün kendi iç yapılanmasındaki kırılganlıkları yorumlamaya yönelik tanısal veriler olarak ele almaktadır (Ansoff, 1975; Reason, 1997; Simons, 1995; Weick vd., 1999).

Temel iddia şu şekildedir: Örgütsel bağıklık mimarisi ne örgütsel dayanıklılığın bir alternatifi ne dinamik yeteneklerin başka bir adı ne de örgütsel öğrenmeye verilmiş yeni bir etikettir (Ansoff, 1975; Duchek, 2020; Huang, 2013; Teece vd., 1997; Walsh & Ungson, 1991). Daha kesin bir ifadeyle örgütsel bağıklık mimarisi, bu yazınların her birinden yararlanırken bunların sunduğu içgörülerini erken teşhis, risk eşikleri ve önleyici müdahale eksenleri etrafında yeniden düzenleyen üst düzey bir kuramsal çerçevedir (Ansoff, 1975; Duchek, 2020; Huang, 2013; Reason, 1997; Simons, 1995; Teece vd., 1997; Walsh & Ungson, 1991). Modelin kuramsal değeri, yalnızca örgütlerin krizlere nasıl dayandığını değil, aynı zamanda kriz olasılığının ortaya çıktığı iç ve dış sinyalleri nasıl anlamlandırdıklarını ve bu anlamlandırmayı zamanında kurumsal eyleme nasıl dönüştürdüklerini açıklama iddiasında yatmaktadır (Ansoff, 1975; Reason, 1997; Weick vd., 1999; Weick & Sutcliffe, 2007).

Tablo 1: Örgütsel Bağıklık Mimarisi ile İlişkili Kuramsal Yaklaşımlar Arasındaki Kavramsal Ayrım

Kavram	Temel Odak	Örgütsel Bağıklık Mimarisiyle İlişkisi	Ayrt Edici Fark
Örgütsel dayanıklılık	İşlevselliğin korunması, toparlanma ve adaptasyon	Bağıklık mimarisinin güçlendirmeyi amaçladığı kapasite alanlarından biridir.	Daha çok ayakta kalma ve baskı altında uyum sağlama üzerinde durur; erken teşhis ve eşik belirleme mekanizmasını merkeze almaz.
Dinamik yetenekler	Kaynakların bütünleştirilmesi, yeniden yapılandırılması ve dönüştürülmesi	Bağıklık mimarisinin müdahale ve yeniden uyarlama mantığını destekler.	Yeniden yapılandırmayı açıklar; yeniden yapılandırma ihtiyacının nasıl teşhis edildiğini ayrıntılandırmaz.
Örgütsel öğrenme/örgütsel hafıza	Deneyimin bilgiye, rutinlere ve kurumsal hafızaya dönüştürülmesi	Bağıklık döngüsünün kalıcı hâle gelmesini sağlar.	Öğrenilenlerin kurumsallaştırılmasını açıklar; erken teşhis–müdahale–geri bildirim döngüsünü tek başına modellemez.
Zayıf sinyaller	Belirsiz erken işaretlerin fark edilmesi	Bağıklık mimarisi için başlangıç verilerini sağlar.	Erken işaretlerin önemini gösterir; bu işaretlerin risk eşiği ve önleyici müdahaleyle nasıl ilişkilendirileceğini tek başına açıklamaz.
Örgütsel bağıklık mimarisi	Erken teşhis, risk eşiği, önleyici müdahale ve öğrenme döngüsü	Diğer yazınları tanısal ve döngüsel bir çerçeve içerisinde bir araya getirir.	Kriz öncesi işaretleri, kırılganlık teşhisini, eşik değerlendirmesini ve kurumsal öğrenmeyi aynı model içerisinde bütünleştirir.

Kaynak: Yazarın kendi çalışması.

Örgütsel Bağışıklık Mimarisinin Kavramsal Sınırları

Örgütsel bağışıklık mimarisi, yönetim ve organizasyon yazınındaki yerleşik çeşitli kavramlarla yakından ilişkilidir (Ansoff, 1975; Duchek, 2020; Huang, 2013; Kaplan & Mikes, 2012; Teece vd., 1997; Walsh & Ungson, 1991). Örgütsel dayanıklılık, risk yönetimi, dinamik yetenekler, örgütsel öğrenme ve örgütsel hafıza bu kavramların başında gelmektedir (Duchek, 2020; International Organization for Standardization, 2018; Levitt & March, 1988; Teece vd., 1997; Walsh & Ungson, 1991). Bununla birlikte bu yakın ilişki, örgütsel bağışıklık mimarisinin söz konusu kavramlarla eş anlamlı olduğu şeklinde yorumlanmamalıdır (Ansoff, 1975; Duchek, 2020; Huang, 2013; Teece vd., 1997). Modelin ayırt edici özelliği, yalnızca örgütün krizlere dayanma veya değişen koşullara uyum sağlama kapasitesini değil, aynı zamanda gizli kırılma noktaları nasıl fark ettiğini, bunları nasıl yorumladığını ve bu yorum temelinde nasıl önleyici kurumsal eylem ürettiğini açıklamaya çalışmasıdır (Ansoff, 1975; Reason, 1997; Simons, 1995; Weick vd., 1999; Weick & Sutcliffe, 2007).

İlk ayırım örgütsel dayanıklılıkla ilgilidir (Duchek, 2020; Lengnick-Hall vd., 2011). Dayanıklılık yazını, örgütlerin beklenmedik olaylar karşısında işlevselliklerini sürdürme, bozulmuş dengeyi yeniden kurma ve değişen koşullara uyum sağlama kapasitelerini açıklamaktadır (Duchek, 2020; Lengnick-Hall vd., 2011; Weick & Sutcliffe, 2007). Duchek'in (2020) dayanıklılığı öngörme, başa çıkma ve adaptasyon süreçleri üzerinden ele alması, kavramın yalnızca kriz sonrası toparlanmaya indirgenemeyeceğini göstermektedir. Buna karşılık örgütsel bağışıklık mimarisi, dayanıklılığın kendisinden çok, dayanıklılığı mümkün kılan erken fark etme ve önleyici uyarılma kapasitelerine odaklanmaktadır (Ansoff, 1975; Duchek, 2020; Reason, 1997; Simons, 1995). Başka bir ifadeyle dayanıklılık, bir örgütün baskı altında nasıl ayakta kaldığını açıklarken örgütsel bağışıklık mimarisi, bu baskıyı şiddetlendirebilecek zayıflıkların derinleşmeden önce nasıl yorumlanabileceğini ele almaktadır (Ansoff, 1975; Duchek, 2020; Weick vd., 1999; Weick & Sutcliffe, 2007).

İkinci ayırım risk yönetimiyle ilişkili olarak yapılmalıdır (International Organization for Standardization, 2018; Kaplan & Mikes, 2012). Risk yönetimi, örgütlere belirsizlikleri belirlemek, sınıflandırmak, izlemek ve kontrol etmek için sistematik bir çerçeve sağlamaktadır (International Organization for Standardization, 2018; Kaplan & Mikes, 2012). Kaplan ve Mikes'in (2012) riskleri önlenabilir, stratejik ve dışsal olarak sınıflandırması önemlidir; çünkü bu sınıflandırma, risklerin tek bir kontrol mantığıyla yönetilemeyeceğini göstermektedir. Örgütsel bağışıklık mimarisi bu görüşten yararlanmakla birlikte geleneksel risk yönetimi mantığına indirgenemez (Huang, 2013; Kaplan & Mikes, 2012; Reason, 1997; Simons, 1995). Buradaki mesele yalnızca riskleri belirlemek veya azaltmak değildir. Daha temel mesele, örgütün kendi bünyesinde ortaya çıkan bağışıklık kayıplarını zamanında fark edip edemediği, bu kayıpları yönetsel açıdan yorumlayıp yorumlayamadığı ve elde edilen bilgiyi öğrenme ve hafıza süreçlerine dâhil edip edemediğidir (Argyris & Schön, 1978; Huang, 2013; Levitt & March, 1988; Walsh & Ungson, 1991; Weick vd., 1999).

Üçüncü sınır dinamik yetenekler yaklaşımıyla ilgilidir (Teece vd., 1997). Teece vd.'nin (1997) çalışması, örgütlerin değişen çevrelerde kaynaklarını bütünleştirme, yeniden yapılandırma ve dönüştürme yeteneklerine odaklanmaktadır. Bu yaklaşım, örgütsel bağışıklık mimarisinin adaptasyon ve yeniden uyarılma boyutunun anlaşılması açısından değerlidir (Teece vd., 1997). Bununla birlikte iki kavram aynı düzeyde işlememektedir (Ansoff, 1975; Huang, 2013; Teece vd., 1997). Dinamik yetenekler öncelikle örgütlerin değişen koşullara yanıt olarak kaynaklarını nasıl yeniden düzenlediklerini açıklamaktadır (Teece vd., 1997). Buna karşılık örgütsel bağışıklık mimarisi, böyle bir yeniden düzenleme ihtiyacının nasıl fark edildiğini sorgulamaktadır (Ansoff, 1975; Reason, 1997; Simons, 1995). Bu bakımdan model, dönüşümün kendisinden önce gelen tanısal temele dikkat çekmektedir: Bir örgüt, müdahalenin gerekli olduğu sonucuna hangi sinyallerden hareketle ulaşır? (Ansoff, 1975; Reason, 1997; Weick vd., 1999; Weick & Sutcliffe, 2007).

Dördüncü sınır, örgütsel öğrenme ve örgütsel hafıza kavramlarıyla ilgilidir (Levitt & March, 1988; Walsh & Ungson, 1991). Levitt ve March (1988), örgütsel öğrenmeyi geçmiş deneyimlerin rutinlere ve davranış kalıplarına yansımaları üzerinden açıklamaktadır. Walsh ve Ungson (1991) ise örgütsel hafızayı geçmiş bilginin örgüt içerisinde korunması ve karar alma süreçlerinde yeniden kullanılmasıyla ilişkilendirmektedir. Örgütsel bağışıklık mimarisi bu bilgi birikimine dayanmakla birlikte öğrenmeyi yalnızca geçmişin kurumsallaştırılması olarak görmemektedir (Argyris & Schön, 1978; Crossan vd., 1999; Huang, 2013; Levitt & March, 1988; Walsh & Ungson, 1991). Bu modelde öğrenme, örgütün sonraki döngülerde daha etkili algılamasını, daha doğru yorumlamasını ve daha erken müdahale etmesini sağlayan aktif bir geri bildirim kapasitesidir (Argyris & Schön, 1978; Crossan vd., 1999; Levitt & March, 1988; Walsh & Ungson, 1991). Bu nedenle örgütsel hafıza yalnızca geçmişin bir kaydı olarak değil, gelecekteki kırılmalıkların daha erken bir aşamada yorumlanmasına yardımcı olan canlı bir kurumsal mekanizma olarak değerlendirilmektedir (Crossan vd., 1999; Huang, 2013; Walsh & Ungson, 1991).

Bu noktada biyolojik bağışıklık ve koruyucu hekimlik metaforunun sınırları da açıkça ortaya konulmalıdır (Cornelissen, 2005; Morgan, 1980). Örgütsel bağışıklık mimarisi, örgütleri biyolojik organizmalarla özdeş yapılar olarak değerlendirmemektedir (Huang, 2013; Morgan, 1980). Metafor, örgütsel gerçekliği tıbbi bir modele indirgemek için değil, gizli bozulma biçimlerinin erken aşamada fark edilmesi, kritik değerlerin yorumlanması ve zamanında müdahale edilmesi düşüncesini açıklamak için kullanılmaktadır (Ansoff, 1975; Cornelissen, 2005; Morgan, 1980; Reason, 1997). Morgan'ın (1980) örgüt kuramında metaforların rolüne ilişkin çalışması, metaforların kuram geliştirme açısından güçlü araçlar olabilmelerine karşın yeterli özen gösterilmeden kullanıldıklarında kavramsal kör noktalar da oluşturabileceklerini göstermektedir. Buna göre "biyokimya paneli" benzetmesi örgütü canlı bir bedene indirgememekte; bunun yerine örgütsel göstergeleri daha yorumlanabilir hâle getiren sınırlı bir analitik araç işlevi görmektedir (Cornelissen, 2005; Morgan, 1980; Simons, 1995).

Bu çerçevede örgütsel bağışıklık mimarisi; örgütsel dayanıklılık, risk yönetimi, dinamik yetenekler veya örgütsel öğrenme kavramlarının yerine geçen yeni bir adlandırma değildir (Duchek, 2020; Huang, 2013; Kaplan & Mikes, 2012; Levitt & March, 1988; Teece vd., 1997). Daha kesin bir ifadeyle örgütsel bağışıklık mimarisi, bu alanların açıklama gücünü erken teşhis, zayıf halka analizi, önleyici uyarılma ve kurumsal öğrenme eksenleri etrafında bir araya getiren özgül bir kuramsal konumu temsil etmektedir (Ansoff, 1975; Argyris & Schön, 1978; Huang, 2013; Reason, 1997; Simons, 1995; Walsh & Ungson, 1991). Kavramın değeri tam olarak burada yatmaktadır: Kavram, yalnızca bir örgütün krizlere nasıl dayandığını değil, aynı zamanda kriz olasılığını artıran zayıflıkları nasıl algıladığını, bunları yönetsel kararlara nasıl dönüştürdüğünü ve bu deneyim aracılığıyla nasıl daha güçlü bir kurumsal dikkatlilik geliştirdiğini açıklamaya çalışmaktadır (Ansoff, 1975; Crossan vd., 1999; Reason, 1997; Weick vd., 1999; Weick & Sutcliffe, 2007).

Tanısal Bir Sistem Olarak Örgütsel Bağışıklık Mimarisi

Örgütsel bağışıklık mimarisi, yalnızca bir aksama meydana geldikten sonra örgütün verdiği tepkiyi açıklayan bir çerçeve olarak görülmemelidir (Ansoff, 1975; Huang, 2013; Reason, 1997; Weick & Sutcliffe, 2007). Modelin temel değeri, örgütsel sistem içerisinde henüz tam anlamıyla bir krize dönüşmemiş sinyalleri yorumlama, bu sinyalleri anlamlı tanısal alanlar içerisinde konumlandırma ve yönetsel müdahaleyi zamanında başlatma yeteneğinde yatmaktadır (Ansoff, 1975; Reason, 1997; Simons, 1995; Weick vd., 1999). Buna göre model, koruyucu hekimlikteki tanısal akıl yürütmeye benzer biçimde işlemekte, ancak örgütleri biyolojik yapılara indirgememektedir (Biomarkers Definitions Working Group, 2001; Cornelissen, 2005; Morgan, 1980). Burada kullanılan benzetme daha sınırlı ve analitiktir: İnsan bedenindeki belirli değerler, belirtiler ortaya çıkmadan önce risk hakkında fikir verebileceği gibi; karar alma süreçlerindeki gecikmeler, bilgi akışındaki kesintiler, koordinasyon zayıflıkları, kritik bilginin kaybı, tekrarlanan

hatalar veya çalışanların sorunları dile getirme konusundaki isteksizliği gibi örgüt içindeki göstergeler de daha ciddi bozulmaların erken uyarı işaretleri olarak yorumlanabilir (Biomarkers Definitions Working Group, 2001; Edmondson, 1996, 1999; Galbraith, 1973; Morrison, 2014; Rizzo vd., 1970; Walsh & Ungson, 1991). Ansoff'un (1975) zayıf sinyaller yaklaşımı, stratejik sürprizlerin çoğu zaman açıkça tanımlanabilir tehditler olarak değil, başlangıçta eksik ve yoruma açık sinyaller olarak ortaya çıktığını göstermesi nedeniyle bu tanısal mantığın klasik temellerinden birini oluşturmaktadır.

Bu çalışmada kullanılan "örgütsel biyobelirteç" terimi, yerleşik bir tıbbi ölçüm kavramı olarak değil, örgüt içerisindeki erken uyarı göstergelerini daha yorumlanabilir hâle getirmek amacıyla önerilen analitik bir metafor olarak anlaşılmalıdır (Biomarkers Definitions Working Group, 2001; Cornelissen, 2005; Morgan, 1980). Örneğin karar alma süreçlerinin olağandışı biçimde uzaması, rol ve yetki sınırlarının belirsizleşmesi, bilginin birimler arasındaki dolaşımının gecikmeli veya eksik olması, aynı hataların tekrarlanması, kritik bilginin az sayıda kişide yoğunlaşması veya sorunların açıkça dile getirilememesi gibi göstergelerin hiçbirisi tek başına bir kriz oluşturmamaktadır (Edmondson, 1996, 1999; Galbraith, 1973; Morrison, 2014; Rizzo vd., 1970; Walsh & Ungson, 1991). Bununla birlikte bu tür göstergeler birlikte ve zaman içerisinde izlendiğinde, örgütün hangi alanında bağışıklık kaybı yaşandığına ilişkin önemli ipuçları sağlayabilir (Ansoff, 1975; Reason, 1997; Simons, 1995; Weick vd., 1999). Dolayısıyla tanısal değer, tekil bir belirtiden çok belirtilerin oluşturduğu örüntüde, bu belirtilerin sürekliliğinde ve örgütsel işlevlerle olan ilişkilerinde yatmaktadır (Reason, 1997; Simons, 1995; Weick & Sutcliffe, 2007).

Bu noktada örgütsel bağışıklık mimarisi risk yönetimiyle kesişmekte, ancak risk yönetimine indirgenememektedir (Huang, 2013; International Organization for Standardization, 2018; Kaplan & Mikes, 2012; Miller, 1992). Miller'ın bütünlük risk yönetimi yaklaşımı, işletmelerin karşılaştığı belirsizliklerin birbirinden yalıtılmış biçimde değil, daha bütüncül bir çerçeve içerisinde ele alınması gerektiğini savunmaktadır (Miller, 1992). Benzer şekilde örgütsel bağışıklık mimarisi de tek tek risklere değil, riski ortaya çıkaran örgütsel zayıflıklar arasındaki ilişkilere odaklanmaktadır (Huang, 2013; Reason, 1997; Simons, 1995). Burada "risk eşiği" yalnızca teknik bir sınır değil, yönetsel dikkatin ne zaman yoğunlaştırılması gerektiğini gösteren bir karar noktasıdır (International Organization for Standardization, 2018; Kaplan & Mikes, 2012; Simons, 1995). Bazı sinyaller normal değişim aralığında kalabilir; bazıları dikkat gerektirir; bazıları ise gecikmesiz müdahale edilmesini gerektiren kritik zayıflıklara işaret eder (Ansoff, 1975; Reason, 1997; Weick & Sutcliffe, 2007). Modelin tanısal niteliği, bu düzeyler arasında ayırım yapma iddiasında yatmaktadır (Reason, 1997; Simons, 1995).

Risk Eşiklerinin Belirlenmesi ve Yanlış Alarmların Yönetilmesi

Modelde risk eşiği, evrensel bir sayısal değer veya tüm örgütlere uygulanabilecek sabit bir puan olarak değil, yeniden kalibre edilebilen ve bağlama özgü bir yönetsel karar ölçütü olarak ele alınmaktadır. Riskin belirlenmesi, analizi, değerlendirilmesi, işleme tabi tutulması, izlenmesi ve iletişimi aşamalarını bütünlük bir süreç olarak ele alan ISO 31000:2018 yaklaşımı ile Kaplan ve Mikes'in (2012) farklı risk türlerinin aynı kontrol mantığıyla yönetilemeyeceğini gösteren ayrımı, eşiklerin örgütün amaçları, risk iştahı, faaliyet gösterdiği sektörün düzenleyici yapısı ve olası etkinin büyüklüğüyle ilişkili olarak belirlenmesini gerektirmektedir (Aven & Thekdi, 2024; International Organization for Standardization, 2018; Kaplan & Mikes, 2012).

Eşik belirleme süreci beş ölçüt kullanılarak yürütülmektedir: göstergenin örgütün tarihsel normal aralığından sapma büyüklüğü; sapmanın sürekliliği ve yönü, aynı sinyalin birden fazla tanısal panelde doğrulanması; olası etkinin şiddeti ve tersine çevrilebilirliği, göstergenin güvenlik, mevzuata uyum veya temel faaliyetlerin sürekliliği açısından kritiklik düzeyi. Göstergelerin bu ölçütler bakımından eşit olduğu varsayılmamaktadır. Ağırlıklar; ilgili panellerle bağlantılı ve verilerin sahibi olan birimlerin temsilcilerinin yanı sıra risk yönetimi, iç denetim ve üst yönetim temsilcilerinden

oluşan işlevler arası bir komite tarafından, örgütün geçmişte yaşadığı olaylar ve senaryo analizleri dikkate alınarak belirlenmektedir. Kullanılan gerekçe ve veri kaynakları belgelendirilmektedir. Böylece ağırlıklandırma, tek bir yöneticinin sezgisine bırakılmak yerine bağlamsal fakat denetlenebilir bir karar alma sürecine dönüştürülmektedir.

Normal düzey, göstergenin tarihsel aralığı içerisinde kaldığı ve tek başına ortaya çıktığı bir durumu ifade etmektedir. Dikkat düzeyi, sapmanın süreklilik kazandığı veya farklı panellerden gelen sinyallerin aynı zayıflık üzerinde birleştiği bir durumu ifade etmektedir. Kritik düzey ise olası etkinin örgütün risk iştahını aştığı, temel faaliyetlerini tehdit ettiği veya güvenlik ya da mevzuat gerekçeleriyle derhâl harekete geçilmesini gerektirdiği bir durumu ifade etmektedir. Tek bir gösterge güvenlik veya mevzuata uyum açısından kritik olmadığı sürece doğrudan kalıcı müdahaleyi tetiklememekte; öncelikle verilerin doğrulanması, sorumlu birim tarafından teyit edilmesi ve paneller arası doğrulama gerçekleştirilmektedir.

Yanlış alarm yönetimi, eşiklerin belirlenip kalıcı olarak sabitlenmesi yerine alarm sonuçlarının izlenmesi ve sistemin yeniden kalibre edilmesi yoluyla yürütülmektedir. Her alarm için sinyalin gerçek bir zayıflığa karşılık gelip gelmediği, müdahalenin gerekli olup olmadığı ve herhangi bir sinyalin gözden kaçırılıp kaçırılmadığı kaydedilmektedir. Yanlış pozitifler gereksiz müdahalenin maliyeti açısından, yanlış negatifler ise gözden kaçırılan riskin etkisi açısından değerlendirilmektedir. Örgütsel öğrenme ve hafıza aşamasında bu kayıtlar; gösterge ağırlıklarının, alarm düzeylerinin ve doğrulama kurallarının yeniden ayarlanması için girdi sağlamaktadır. Dolayısıyla geri bildirim yalnızca geçmiş deneyimi muhafaza etmemekte, aynı zamanda tanısıl sistemin duyarlılığı ile seçiciliği arasındaki dengeyi de düzenlemektedir.

Gerçek dünyada yaşanan olaylar, bu ayrımın neden önemli olduğunu göstermektedir. Columbia kazasını araştıran kurul, kazanın yalnızca teknik bir olay olan köpük parçası çarpmasıyla açıklanamayacağını ve NASA'nın örgüt kültürünün de kazanın meydana gelmesinde belirleyici bir etken olduğunu vurgulamıştır (Columbia Accident Investigation Board, 2003). Rapor, karmaşık teknolojik sistemlerde teknik arızaların örgütsel karar alma, iletişim ve yorumlama süreçleriyle birlikte ele alınması gerektiğini açıkça ortaya koymuştur (Columbia Accident Investigation Board, 2003; Reason, 1997). Bu örnek, örgütsel bağışıklık mimarisinin neden yalnızca dış tehditlere değil, aynı zamanda örgüt içindeki karar alma alışkanlıklarına, iletişim kanallarına ve zayıf sinyalleri ciddiye alma kapasitesine de odaklanması gerektiğini göstermektedir (Ansoff, 1975; Columbia Accident Investigation Board, 2003; Weick vd., 1999). Benzer şekilde yüksek güvenilirlikli örgütler yazını, hata olasılığı düşük görünse bile küçük sapmaların ciddiye alınmasının ve operasyonel süreçlere yönelik yakın dikkatin sürdürülmesinin önemini vurgulamaktadır (Roberts, 1990; Weick vd., 1999; Weick & Sutcliffe, 2007). Roberts'ın nükleer güçle çalışan uçak gemileri üzerine yaptığı çalışma, karmaşık ve yüksek riskli sistemlerde güvenilirliğin yalnızca teknolojiye değil, örgütsel süreçlerin disiplinli biçimde yürütülmesine de bağlı olduğunu göstermektedir (Roberts, 1990).

Tanısıl sistemdeki ayırt edici bağlantı, zayıf halka teşhisidir (Galbraith, 1973; Lawrence & Lorsch, 1967; Reason, 1997). Örgütsel zayıflıklar her zaman aynı noktadan kaynaklanmamaktadır (Reason, 1997; Weick & Sutcliffe, 2007). Bazı durumlarda karar alma yapısındaki belirsizlik, çevresel değişime gecikmeli tepki verilmesi, birimler arasındaki kopukluk veya bilgi ve deneyim kaybı örgütsel kırılganlığı artırmaktadır (Galbraith, 1973; Lawrence & Lorsch, 1967; Rizzo vd., 1970; Walsh & Ungson, 1991). Bu nedenle örgütsel bağışıklık mimarisi, genelleştirilmiş bir "örgütsel zayıflık" diliyle yetinmemekte; zayıflığın yoğunlaştığı alanı ve gerektirdiği müdahale biçimini ayırt etmeye çalışmaktadır (Reason, 1997; Simons, 1995). Bu ayrım yapılmadığında örgütler çoğu zaman görünür belirtiyi düzeltirken zayıflığı üreten daha derin mekanizma varlığını sürdürmektedir (Argyris & Schön, 1978; Reason, 1997).

Dolayısıyla önleyici müdahale, teşhisin doğal bir uzantısıdır (Ansoff, 1975; Reason, 1997; Schein, 1996). Teşhis yönetsel eyleme dönüştürülmediğinde yalnızca farkındalık üretmektedir (Argyris & Schön, 1978; Schein, 1996; Simons, 1995). Schein'in planlı değişimi "yönetilen öğrenme" olarak yorumlaması, örgütsel müdahalenin yalnızca yapısal bir düzeltme değil, aynı zamanda bir öğrenme süreci olduğunu göstermesi nedeniyle bu tartışmayla uyumludur (Schein, 1996). Örgütsel bağışıklık mimarisi açısından müdahale; karar alma süreçlerinin basitleştirilmesini, bilgi akışlarının yeniden sağlanmasını, rol ve sorumlulukların netleştirilmesini, kritik bilginin korunmasının güvence altına alınmasını veya birimler arasındaki koordinasyonun güçlendirilmesini içerebilir (Galbraith, 1973; Lawrence & Lorsch, 1967; Rizzo vd., 1970; Walsh & Ungson, 1991). Bununla birlikte bir müdahalenin kalıcı değeri, örgütün bu deneyimden ne öğrendiğine ve bu öğrenmeyi sonraki döngülerde daha iyi teşhis yapılmasını sağlayan bir hafıza biçimine dönüştürüp dönüştüremediğine bağlıdır (Argyris & Schön, 1978; Crossan vd., 1999; Walsh & Ungson, 1991).

Bu nedenle örgütsel bağışıklık mimarisi tek seferlik bir değerlendirme aracı olarak görülmemelidir (Crossan vd., 1999; Simons, 1995; Walsh & Ungson, 1991). Daha kesin bir ifadeyle model, bir örgütün zayıf sinyalleri nasıl izlediğini, bunları tanısal alanlar içerisinde nasıl yorumladığını, risk eşiklerini nasıl yönetsel karar noktalarına dönüştürdüğünü ve müdahale sonuçlarını öğrenme yoluyla örgütsel hafızayla nasıl ilişkilendirdiğini açıklayan sürekli bir tanısal sistemdir (Ansoff, 1975; Argyris & Schön, 1978; Crossan vd., 1999; Reason, 1997; Simons, 1995; Walsh & Ungson, 1991). Modelin önleyici niteliği de burada ortaya çıkmaktadır: Amaç, krizin kaçınılmaz hâle gelmesini beklemek değil, zayıflama yönetilebilir bir düzeydeyken örgütsel dikkati harekete geçirmektir (Ansoff, 1975; Reason, 1997; Weick & Sutcliffe, 2007).

Örgütsel Bağışıklık Mimarisinin Temel Panelleri

Örgütsel bağışıklık mimarisi, bir örgütün zayıflıklarını tek bir belirtiye veya tek bir yönetsel alana indirgememektedir (Galbraith, 1974; Lawrence & Lorsch, 1967; Teece vd., 1997; Walsh & Ungson, 1991). Bir örgütün bağışıklığı çoğu zaman karar yapısı, değişime verdiği tepki, birimler arası bağlantıları ve bilgiyi kullanma biçimi üzerinden eş zamanlı olarak sınanmaktadır (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Teece vd., 1997). Bu nedenle model dört temel panel üzerine kurulmuştur: liderlik/yapı, adaptasyon, entegrasyon ve entelektüel sermaye (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Teece vd., 1997). Bu paneller bağımsız ölçüm başlıkları değildir; aksine, örgütün nerede zayıfladığını, bu zayıflığın hangi kanallar aracılığıyla yayıldığını ve ne tür bir müdahale gerektirdiğini anlamaya yardımcı olan tamamlayıcı tanısal alanlardır (Galbraith, 1974; Lawrence & Lorsch, 1967; Simons, 1995; Walsh & Ungson, 1991).

Liderlik/yapı paneli, örgütte kararların nasıl alındığını, bilginin karar noktalarına nasıl ulaştığını, yetki ve sorumlulukların ne kadar açık biçimde tanımlandığını ve yönetsel koordinasyonun ne ölçüde işlediğini izlemektedir (Galbraith, 1974; Rizzo vd., 1970; Tushman & Nadler, 1978). Galbraith'in (1974) örgüt tasarımı bilgi işleme kapasitesiyle ilişkilendiren yaklaşımı bu panel için güçlü bir temel sağlamaktadır; çünkü belirsizlik arttıkça örgütlerin daha fazla bilgiyi işlemesi, doğru yere iletmesi ve karar alma süreçlerini buna göre düzenlemesi gerekmektedir. Tushman ve Nadler'in (1978) bilgi işleme perspektifi de örgüt tasarımının yalnızca hiyerarşik düzenle değil, aynı zamanda bilginin toplanması, paylaşılması ve kararlara dönüştürülmesiyle ilgili olduğunu göstermektedir. Dolayısıyla liderlik/yapı paneli yalnızca "Kararı kim verir?" sorusuyla ilgilenmemekte; kararın hangi bilgiye dayanılarak, hangi hızda ve sorumlulukların ne ölçüde açık olduğu bir çerçevede alındığını da sorgulamaktadır (Galbraith, 1974; Rizzo vd., 1970; Tushman & Nadler, 1978). Kararların sürekli gecikmesi, yetki alanlarının belirsizleşmesi, sorumluluk belirsizliği veya kritik bilginin karar merkezlerine ulaşmaması, bu panel açısından erken uyarı işaretleri olarak okunabilir (Columbia Accident Investigation Board, 2003; Galbraith, 1974; Rizzo vd., 1970; Tushman & Nadler, 1978). Columbia Uzay Mekiği kazasına ilişkin resmî soruşturma raporu bu

noktada öğreticidir. Raporda kaza yalnızca teknik hasar üzerinden değil, NASA'daki örgüt kültürü, iletişim ve karar alma süreçleriyle birlikte değerlendirilmiştir (Columbia Accident Investigation Board, 2003). Bu örnek, liderlik ve yapıdaki zayıflıkların karmaşık sistemlerde teknik sorunlar kadar belirleyici sonuçlar doğurabileceğini göstermektedir (Columbia Accident Investigation Board, 2003; Galbraith, 1974; Weick vd., 1999).

Adaptasyon paneli, örgütün çevresindeki değişimi ne kadar erken fark ettiğini ve bu değişimi kendi işleyişine ne ölçüde aktarabildiğini göstermektedir (Cohen & Levinthal, 1990; Teece vd., 1997). Burada önemli olan yalnızca dış çevrenin izlenmesi değildir; dışarıdan gelen bilginin örgüt içerisinde anlam kazanması, tartışılabilmesi ve davranışa dönüştürülebilmesi de önemlidir (Cohen & Levinthal, 1990; Vuori & Huy, 2016). Cohen ve Levinthal'ın (1990) özümleme kapasitesi yaklaşımı, örgütlerin dış bilgiyi fark etme, özümleme ve kullanma yeteneklerinin yenilik açısından kritik olduğunu göstermektedir. Teece vd. (1997) tarafından geliştirilen dinamik yetenekler yaklaşımı ise değişen çevrelerde kaynakların ve yetkinliklerin yeniden düzenlenmesi gerektiğini vurgulamaktadır. Bu iki kuramsal çizgi birlikte ele alındığında adaptasyon, yalnızca değişimi görmek değil, görülen değişime örgütsel bir karşılık verebilmek anlamına gelmektedir (Cohen & Levinthal, 1990; Teece vd., 1997). Eski rutinelere aşırı bağlılık, yeni bilginin karar alma süreçlerine taşınamaması, çevresel değişimin geç yorumlanması veya öğrenilenlerin uygulamaya dönüşmemesi, bu panelin dikkate alması gereken zayıflıklardır (Cohen & Levinthal, 1990; Crossan vd., 1999; Teece vd., 1997; Vuori & Huy, 2016). Vuori ve Huy'un (2016) Nokia'nın akıllı telefon rekabetindeki gerilemesi üzerine yaptıkları çalışma, adaptasyon kapasitesinin yalnızca teknolojik tercihlere bağlı olmadığını; örgüt içerisindeki dikkat, duygu, iletişim ve üst yönetim ile orta kademe yönetim arasındaki ilişkilerin de yenilik sürecini etkilediğini göstermektedir. Bu örnek, yalnızca değişimi fark etmenin yeterli olmadığını; bilginin örgüt içerisinde açıkça tartışılması ve sağlıklı biçimde karar alma süreçlerine taşınması gerektiğini ortaya koymaktadır (Cohen & Levinthal, 1990; Vuori & Huy, 2016).

Entegrasyon paneli, örgütün farklı bölümlerinin ortak bir yön ve anlam etrafında ne ölçüde bir araya gelebildiğiyle ilgilidir (Lawrence & Lorsch, 1967; Tushman & Nadler, 1978). Karmaşık örgütlerde farklılaşma kaçınılmazdır; birimlerin kendilerine özgü uzmanlık alanları, öncelikleri ve çalışma ritimleri bulunmaktadır (Lawrence & Lorsch, 1967). Bununla birlikte bu farklılaşma etkili bir entegrasyonla desteklenmediğinde bilgi siloları, birbirinden kopuk kararlar ve yinelenen süreçler ortaya çıkmaktadır (Galbraith, 1974; Lawrence & Lorsch, 1967; Tushman & Nadler, 1978). Lawrence ve Lorsch'un (1967) farklılaşma ve entegrasyon üzerine gerçekleştirdikleri klasik çalışma, örgütsel etkililiğin yalnızca uzmanlaşmaya değil, uzmanlaşmış birimlerin nasıl bir araya getirildiğine de bağlı olduğunu göstermiştir. Dolayısıyla entegrasyon paneli, yüzeysel bir iş birliği göstergesinden daha fazlasını izlemekte; bilgi, anlam ve eylemin örgüt içerisinde süreklilik kazanıp kazanmadığını incelemektedir (Galbraith, 1974; Lawrence & Lorsch, 1967; Tushman & Nadler, 1978). Bir bölümün fark ettiği riskin başka bir birime ulaşmaması, ortak bir amacın farklı bölümlerde farklı biçimlerde yorumlanması, kritik bilginin silolarda tutulması veya süreçlerin birbirinden kopuk biçimde ilerlemesi örgütsel bağışıklık tepkisini zayıflatmaktadır (Columbia Accident Investigation Board, 2003; Galbraith, 1974; Lawrence & Lorsch, 1967; Tushman & Nadler, 1978). Columbia raporunda teknik bulguların yorumlanması, iletişim kanalları ve karar alma süreçleri arasındaki ilişkinin kazanın anlaşılmasında merkezi bir yere sahip olması, entegrasyon eksikliğinin yüksek riskli yapılarda nasıl ciddi sonuçlar doğurabileceğini göstermektedir (Columbia Accident Investigation Board, 2003).

Entelektüel sermaye paneli, örgütün sahip olduğu bilgi, deneyim, uzmanlık, ilişkiler ve kurumsal hafızayı ne ölçüde koruyabildiğini ve kullanabildiğini izlemektedir (Nahapiet & Ghoshal, 1998; Nonaka, 1994; Walsh & Ungson, 1991). Bu panelde bilgi yalnızca bireysel uzmanlık veya teknik birikim olarak görülmemekte; ilişkiler, güven, paylaşılan anlamlar ve deneyim aktarımıyla birlikte değerlendirilmektedir (Nahapiet & Ghoshal, 1998; Nonaka, 1994). Nahapiet ve Ghoshal'ın (1998) sosyal sermaye ile entelektüel sermaye arasındaki ilişki üzerine yaptıkları çalışma, bilginin

örgütsel değere dönüştürülebilmesi için ilişkisel ve yapısal bağlara ihtiyaç duyduğunu göstermektedir. Nonaka'nın (1994) bilgi yaratma yaklaşımı da bilginin bireylerin içinde kapalı kalmadığını, sosyal etkileşim yoluyla dönüştürüldüğünü ve örgütsel düzeye taşındığını vurgulamaktadır. Dolayısıyla entelektüel sermaye paneli, örgütte ne kadar bilgi bulunduğundan çok bu bilginin dolaşıma girip girmediğini, karar alma süreçlerine taşınıp taşınmadığını ve geçmiş deneyimlerin kurumsal hafızaya dönüştürülüp dönüştürülmediğini izlemektedir (Nahapiet & Ghoshal, 1998; Nonaka, 1994; Walsh & Ungson, 1991). Kritik bilginin az sayıda kişide yoğunlaşması, uzmanlığın birimler arasında paylaşılmaması, çalışanların ayrılmasıyla birlikte bilginin kaybedilmesi veya aynı hataların tekrarlanması, bu panel açısından bir bağımsızlık zayıflığına işaret etmektedir (Edmondson, 1996; Nahapiet & Ghoshal, 1998; Walsh & Ungson, 1991). Nokia örneği de bu bakımdan anlamlıdır; Vuori ve Huy'un (2016) bulguları, bilginin örgüt içerisinde yalnızca mevcut olmasının yeterli olmadığını ve bu bilginin açıkça tartışılması, yorumlanması ve stratejik kararlara dönüştürülmesi gerektiğini göstermektedir.

Bu dört panel birlikte işlediğinde örgütsel bağımsızlık mimarisi basit bir kontrol listesi olmaktan çıkmakta ve örgütün zayıflıklarını daha bütüncül biçimde okuyan tanısal bir düzenlemeye dönüşmektedir (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Simons, 1995; Teece vd., 1997). Liderlik/yapı paneli karar ve yönetim netliğini; adaptasyon paneli değişime yanıt verme kapasitesini, entegrasyon paneli örgüt içindeki bağlantı ve uyumu; entelektüel sermaye paneli ise bilginin korunmasını, paylaşılmasını ve yenilenmesini görünür hâle getirmektedir (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Nonaka, 1994; Walsh & Ungson, 1991). Bu panellerden herhangi birindeki zayıflık diğer panelleri de etkileyebilir (Galbraith, 1974; Lawrence & Lorsch, 1967; Tushman & Nadler, 1978). Karar yapısı belirsizse bilgi doğru yere ulaşmamakta; adaptasyon zayıfsa öğrenilenler davranışa dönüşmemekte, entegrasyon zayıfsa sinyaller parçalı kalmakta; entelektüel sermaye zayıfsa örgüt aynı sorunları yeniden üretmektedir (Cohen & Levinthal, 1990; Crossan vd., 1999; Edmondson, 1996; Galbraith, 1974; Lawrence & Lorsch, 1967; Walsh & Ungson, 1991). Dolayısıyla panellerin temel işlevi bireysel performans göstergeleri üretmek değil, örgütsel bağımsızlığı oluşturan yapısal, bilişsel, ilişkisel ve adaptif mekanizmaların birlikte nasıl işlediğini göstermektir (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Teece vd., 1997). Örgütsel bağımsızlık mimarisi, bir örgütün zayıflıklarını tek bir belirtiyeye veya tek bir yönetim alanına indirgememektedir (Galbraith, 1974; Lawrence & Lorsch, 1967; Teece vd., 1997; Walsh & Ungson, 1991). Bir örgütün bağımsızlığı çoğu zaman karar alma yapısı, değişime verdiği tepki, birimler arasındaki bağlantıları ve bilgiyi kullanma biçimi üzerinden eş zamanlı olarak sınanmaktadır (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Teece vd., 1997). Bu nedenle model dört temel panel etrafında yapılandırılmıştır: liderlik/yapı, adaptasyon, entegrasyon ve entelektüel sermaye (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Teece vd., 1997). Bu paneller bağımsız ölçüm kategorileri değildir; aksine, örgütün nerede zayıfladığını, bu zayıflığın hangi kanallar aracılığıyla yayıldığını ve ne tür bir müdahale gerektirdiğini belirlemeye yardımcı olan tamamlayıcı tanısal alanlardır (Galbraith, 1974; Lawrence & Lorsch, 1967; Simons, 1995; Walsh & Ungson, 1991).

Döngüsel Model ve Kuramsal Önermeler

Örgütsel bağımsızlık mimarisi, örgüt tarafından belirli aralıklarla yürütülen bir kontrol faaliyeti olarak anlaşılmamalıdır (Simons, 1995; Weick & Sutcliffe, 2007). Modelin temelinde daha sürekli bir işleyiş biçimi bulunmaktadır: Örgüt, çevresinden ve iç yapılanmasından gelen sinyalleri toplamakta, bunları anlamlandırmakta, zayıflığın kaynağını ayırt etmekte, gerektiğinde müdahale etmekte ve bu deneyimi sonraki kararlarına taşımaktadır (Ansoff, 1975; Argyris & Schön, 1978; Crossan vd., 1999; Weick vd., 1999). Bu nedenle model, geleneksel "sorunun belirlenmesi ve çözümü" sıralamasından farklılaşmaktadır (Argyris & Schön, 1978; Schein, 1996). Burada her

müdahale yeni bir öğrenme üretmekte, her bir öğrenme ise sonraki sinyallerin daha erken ve daha dikkatli yorumlanmasına katkıda bulunmaktadır (Argyris & Schön, 1978; Crossan vd., 1999; Levitt & March, 1988; Walsh & Ungson, 1991). Ansoff'un (1975) zayıf sinyaller yaklaşımı, stratejik sürprizlerin başlangıçta çoğu zaman eksiksiz ve açık tehditler olarak değil, yorumlanması gereken parçalı sinyaller olarak ortaya çıktığını göstermesi nedeniyle bu döngünün ilk bağlantısı için güçlü bir temel sağlamaktadır.

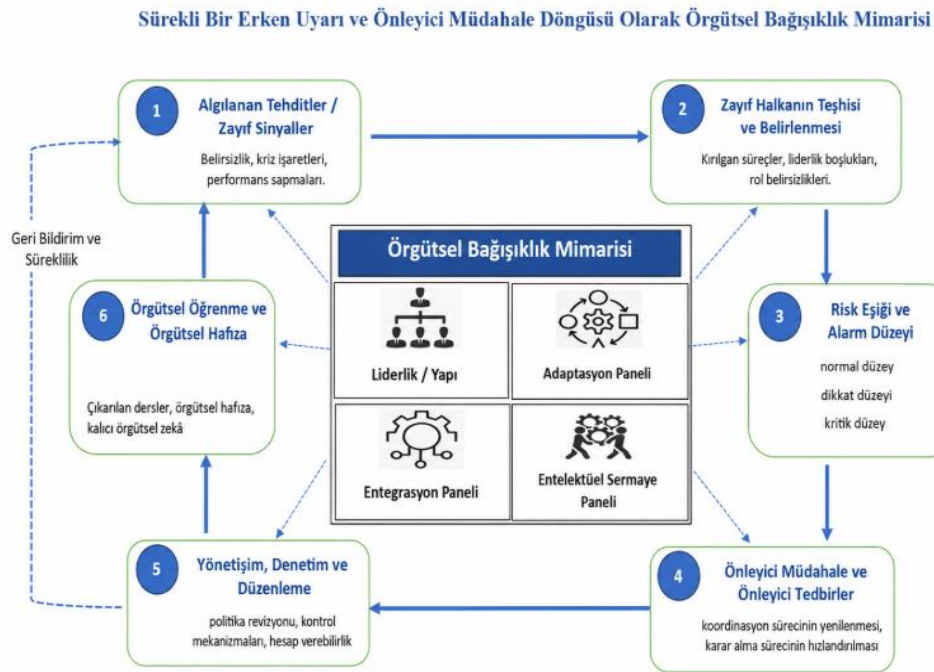
Modelin başlangıcındaki sinyaller yalnızca piyasadan, teknolojiden veya dış çevreden kaynaklanmamaktadır (Ansoff, 1975; Weick vd., 1999; Weick & Sutcliffe, 2007). Örgütün kendi içerisinde ortaya çıkan küçük sapmalar da aynı ölçüde önemlidir (Reason, 1997; Vaughan, 1996; Weick vd., 1999). Karar alma süreçlerinin yavaşlaması, sorunların üst yönetime taşınmaması, birimler arasındaki bilgi akışında kesintiler yaşanması, aynı hataların tekrarlanması veya kritik bilginin sınırlı sayıda kişide yoğunlaşması, tek başına ele alındığında genellikle yaklaşan bir felakete işaret etmemektedir (Edmondson, 1996, 1999; Galbraith, 1974; Morrison, 2014; Walsh & Ungson, 1991). Bununla birlikte bu sinyaller birlikte ve zaman içerisinde gözlemlendiğinde, örgütsel zayıflığın hangi yönde ilerlediğini gösterebilir (Reason, 1997; Simons, 1995; Weick & Sutcliffe, 2007). Vaughan'ın Challenger felaketi üzerine yaptığı çalışma bu bakımdan dikkate değerdir. Vaughan, NASA'daki teknik sapmaların kademeli biçimde normalleşmesini örgüt kültürü ve karar alma süreçleriyle ilişkilendirerek açıklamıştır; bu olgu, "sapmanın normalleştirilmesi" yazınındaki en iyi bilinen örneklerden biri hâline gelmiştir (Vaughan, 1996). Vaughan'ın University of Chicago Press tarafından yayımlanan kitabı, Challenger kararını NASA'daki risk, kültür ve sapma bağlamında inceleyen ve alan yazında yer edinmiş bir eserdir (Vaughan, 1996).

Bu tür sinyallerin değeri, yalnızca uygun tanısıl alan içerisinde konumlandırıldıklarında görünür hâle gelmektedir (Reason, 1997; Simons, 1995). Örgütsel bağımsızlık mimarisi içerisinde liderlik/yapı, adaptasyon, entegrasyon ve entelektüel sermaye panelleri bu işlevi yerine getirmektedir (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Nahapiet & Ghoshal, 1998; Walsh & Ungson, 1991). Bir örgütte görünür sorun karar alma düzenlemelerinden kaynaklanabilirken başka bir durumda temel zayıflık, değişime gecikmeli yanıt verilmesi, bilginin birimler arasında sıkışması veya deneyimin korunamaması olabilir (Cohen & Levinthal, 1990; Galbraith, 1974; Lawrence & Lorsch, 1967; Walsh & Ungson, 1991). Columbia kazasını araştıran kurulun raporu bu ayrımı örneklendirmektedir. Rapor, kazaya ilişkin açıklamasını köpük parçası çarpması gibi teknik bir nedenle sınırlandırmamış; NASA'nın örgüt kültürünün, iletişim ve karar alma süreçlerinin de kazada rol oynadığını belirtmiştir (Columbia Accident Investigation Board, 2003). Bu örnek, karmaşık örgütlerde fiziksel veya teknik sorunların çoğu zaman örgütsel yorumlama ve karar alma düzenlemelerinden bağımsız olarak ele alınamayacağını göstermektedir (Columbia Accident Investigation Board, 2003; Reason, 1997; Weick vd., 1999).

Döngünün bir sonraki aşamasında örgüt, her sinyale eşit ağırlık vermemektedir (Kaplan & Mikes, 2012; Simons, 1995). Bazı sapmalar normal değişim aralığında kalabilir; bazıları daha yakından izlenmeyi gerektirir; bazıları ise gecikmeksizin müdahale gerektiren bir zayıflığa işaret eder (International Organization for Standardization, 2018; Kaplan & Mikes, 2012; Reason, 1997). Dolayısıyla risk eşiği, model içerisinde yalnızca bir ölçüm sınırı değil, yönetsel dikkatin hangi noktada yoğunlaştırılması gerektiğini gösteren bir karar sınırır (International Organization for Standardization, 2018; Kaplan & Mikes, 2012; Simons, 1995). Bu sınır aşıldığında müdahalenin niteliği de teşhise göre değişmektedir (Reason, 1997; Schein, 1996; Simons, 1995). Karar alma yapısı belirsizleşmişse yetki ve sorumluluk düzenlemeleri basitleştirilebilir; bilgi akışı kesintiye uğramışsa iletişim kanalları yeniden kurulabilir; koordinasyon bozulmuşsa birimler arasındaki bağlantılar güçlendirilebilir; kritik bilgi kaybedilmişse bilginin korunmasına ve deneyimin aktarılmasına yönelik mekanizmalar devreye alınabilir (Galbraith, 1974; Lawrence & Lorsch, 1967; Rizzo vd., 1970; Walsh & Ungson, 1991). Duchek'in (2020) örgütsel dayanıklılığı öngörme, başa çıkma ve adaptasyon süreçleri üzerinden kavramsallaştıran çalışması bu mantıkla uyumludur; çünkü

dayanıklılığın yalnızca kriz sonrası toparlanmayla değil, kriz öncesinde kapasite geliştirilmesiyle de ilgili olduğunu göstermektedir.

Döngü, öğrenme ve hafıza yoluyla tamamlanmaktadır (Argyris & Schön, 1978; Crossan vd., 1999; Levitt & March, 1988; Walsh & Ungson, 1991). Bir örgüt zayıflığı fark edip müdahale etse bile bu deneyim karar alma süreçlerine, rutinlere ve örgütsel hafızaya dâhil edilmediğinde aynı sorun farklı biçimlerde yeniden ortaya çıkabilir (Argyris & Schön, 1978; Foroughi vd., 2020; Lee vd., 2020; Levitt & March, 1988; Walsh & Ungson, 1991). Levitt ve March (1988), örgütsel öğrenmeyi rutin temelli, tarihsel bağımlı ve hedef yönelimli bir süreç olarak kavramsallaştırmaktadır. Walsh ve Ungson (1991) ise örgütsel hafızayı bilginin örgüt içerisinde depolanması ve gerektiğinde yeniden kullanılması açısından ele almaktadır. Bu iki yaklaşım birlikte değerlendirildiğinde öğrenmenin yalnızca geçmişin kaydedilmesinden ibaret olmadığı açıkça görülmektedir (Crossan vd., 1999; Levitt & March, 1988; Walsh & Ungson, 1991). Öğrenme, örgütün bir sonraki döngüde neyi daha erken fark edeceğini, hangi sinyali daha fazla ciddiye alacağını ve hangi müdahaleyi daha hızlı seçeceğini belirleyen bir kurumsal dikkat biçimidir (Argyris & Schön, 1978; Crossan vd., 1999; Weick vd., 1999; Weick & Sutcliffe, 2007) (Şekil 1).



Şekil 1. Sürekli Bir Erken Uyarı ve Önleyici Müdahale Döngüsü Olarak Örgütsel Bağışıklık Mimarisi

Kaynak: Yazar tarafından hazırlanmıştır.

Şekil 1 eş zamanlı olarak iki düzeyi göstermektedir. Dış halkadaki kesintisiz oklar, algılanan tehditler ve zayıf sinyallerle başlayan; teşhis, risk eşiği, önleyici müdahale, yönetim düzenlemeleri ve örgütsel öğrenme aşamalarıyla ilerleyen zamansal süreci temsil etmektedir. Kesikli geri bildirim bağlantısı ise öğrenme ve hafızanın yeni sinyallerin algılanmasını etkilediğini göstermektedir. Merkezdeki dört panel, döngünün sıralı aşamaları değildir; bunlar, zayıflığın yoğunlaştığı örgütsel alanı ayırt etmek amacıyla her aşamada kullanılan yatay tanısal alanlardır. Paneller ile dış halka

arasındaki kesikli bağlantılar, panel verilerinin teşhis, eşik ve müdahale kararlarına girdi sağladığını ve müdahale sonuçlarının daha sonra aynı paneller aracılığıyla yeniden izlendiğini göstermektedir.

Döngünün beşinci aşaması olan yönetim, kontrol ve düzenleme, geçici müdahalenin kalıcı kurumsal değişime dönüştürüldüğü noktadır. Bu aşamada müdahale sonuçları; politikalara ve karar kurallarına, kontrol mekanizmalarına, yetki ve sorumluluk yapılarına ve hesap verebilirlik düzenlemelerine dâhil edilmektedir. Yönetim düzenlemesi gerçekleşmediğinde müdahale yerel ve geçici kalabilir; düzenleme öğrenme ve hafızayla ilişkilendirildiğinde ise örgüt yalnızca belirli bir sorunu ele almakla kalmamakta, aynı zamanda gelecekte benzer sinyallere vereceği tepkileri yöneten kuralları da yenilemektedir (Argyris & Schön, 1978; Simons, 1995; Walsh & Ungson, 1991).

Modeldeki yönlü ilişkiler, araştırılabilir sonuçlar ve sınır koşulları dikkate alınarak aşağıdaki dört kuramsal önermeye dönüştürülmüştür (Jaakkola, 2020; Whetten, 1989).

Zayıf sinyallerin karar alma merkezlerine iletilmesi yalnızca bilgi sistemlerinin varlığına bağlı değildir. Bunun için çalışanların kaygılarını dile getirmeyi kişiler arası bir risk olarak algılamamaları, yöneticilerin kritik bilgilere açık olmaları ve birimler arasında açık iletişim kanallarının bulunması gerekmektedir (Edmondson & Bransby, 2023; Morrison, 2023). Çalışan sesliliğinin çevresel değişim karşısında takım dayanıklılığını güçlendirebildiğini gösteren bulgular da örgüt içerisinde sinyallerin paylaşılmasının modelde bir sınır koşulu olarak ele alınmasının gerekçesini desteklemektedir (Li & Tangirala, 2022).

Önerme 1: Dört tanısıl panelden elde edilen zayıf sinyallerin birlikte değerlendirilme derecesi arttıkça örgütsel zayıflıkların tespit edilme hızı ve teşhisin doğruluğu artar; bu ilişki, çevresel belirsizliğin yüksek olduğu ve sinyallerin örgütsel birimler arasında dağılmış olduğu koşullarda daha güçlüdür.

Önerme 2: Farklı panellerden gelen sinyallerin aynı zayıf halka üzerinde birleşmesi, tek bir panelden elde edilen sinyallere kıyasla önleyici müdahalenin doğruluğunu artırır; bu etki, parçalı bilgi akışları ve düşük psikolojik güvenlikle nitelendirilen örgütlerde zayıflar.

Önerme 3: Risk eşiklerinin örgütün tarihsel normal aralıkları, risk iştahı ve olası etkinin büyüklüğüyle uyumlu biçimde kalibre edilmesi, teşhis ile zamanında müdahale arasındaki pozitif ilişkiyi güçlendirir. Aşırı duyarlı eşikler yanlış pozitif alarm oranını artırırken yeterince duyarlı olmayan eşikler yanlış negatif alarm oranını artırır.

Önerme 4: Müdahale sonuçlarının yönetim düzenlemeleri aracılığıyla örgütsel öğrenme ve hafızaya dâhil edilme düzeyi arttıkça sonraki döngülerde zayıf sinyallerin tespit edilme hızı ve teşhisin doğruluğu artar; bu ilişki, hesap verebilirliğin açık olduğu ve örgütsel bilgiyi koruma kapasitesinin yüksek olduğu örgütlerde daha güçlüdür.

Bu önermelerin ampirik olarak sınanmasında panel entegrasyonu bağımsız değişken; sinyal tespit süresi, teşhis doğruluğu, müdahale doğruluğu ve yanlış alarm oranları sonuç değişkenleri; çevresel belirsizlik, bilgi parçalanması, psikolojik güvenlik, hesap verebilirlik ve bilgi koruma kapasitesi ise sınır koşulları olarak ele alınabilir. Farklı zaman noktalarında toplanan olay kayıtlarının, alarm günlüklerinin, müdahale kararlarının ve çalışan ve yönetici değerlendirmelerinin birlikte kullanılması, önermelerin algısal verilerin yanı sıra davranışsal göstergeler kullanılarak da sınanmasına imkân sağlayacaktır.

Tartışma

Bu çalışmada önerilen örgütsel bağışıklık mimarisi, yalnızca örgütlerin krizler karşısında ne ölçüde güçlü kaldıklarını açıklamakla yetinmemekte; daha erken bir soruya odaklanmaktadır: Bir örgüt, dikkat, bilgi ve karar alma unsurlarının nasıl bir yapılanması aracılığıyla kendi zayıflama işaretlerini yorumlayabilir? Bu bakımdan modelin kuramsal katkısı, örgütsel dayanıklılık yazınına tamamlayan bir düzeyde ortaya çıkmaktadır. Duchek (2020), dayanıklılığı öngörme, başa çıkma ve

adaptasyon süreçleri üzerinden açıklayarak krize hazırlıklı olma durumuna güçlü bir vurgu yapmaktadır. Örgütsel bağışıklık mimarisi, bu hazırlık düşüncesini daha tanısal bir temele oturtmakta ve dayanıklılığın yalnızca kriz sonrasında yaşananlarla değil, aynı zamanda kriz olasılığını doğuran erken bozulmanın yorumlanmasıyla da ilişkili olduğunu ileri sürmektedir (Ansoff, 1975; Weick & Sutcliffe, 2007). Böylece model, dayanıklılığı sonuç temelli bir kapasite olarak değil, örgütsel dikkat, teşhis, eşik değerlendirmesi ve öğrenme döngüsü aracılığıyla gelişen örgütsel bir özellik olarak ele almaktadır.

Challenger ve Columbia örnekleri, modelin neden yalnızca teknik riskleri değil, örgütsel yorumlama ve karar alma düzenlemelerini de dikkate alması gerektiğini açıkça göstermektedir. Vaughan'ın (1996) Challenger kazasına ilişkin çalışması, teknik sapmaların zaman içerisinde normalleşmesinin örgüt kültürü ve karar alma süreçleriyle birlikte değerlendirilmesi gerektiğini göstermiştir. Columbia Accident Investigation Board (2003) da Columbia kazasını yalnızca fiziksel hasar üzerinden açıklamamış; NASA'nın örgüt kültürünü, iletişim kalıplarını ve karar alma süreçlerini analizinin merkezine yerleştirmiştir. Bu iki örnek, örgütsel bağışıklık mimarisinin temel iddiasını desteklemektedir: Karmaşık sistemlerde kırılabilirlik çoğu zaman aniden ortaya çıkmamakta; küçük sapmaların nasıl yorumlandığı, kimin neyi dile getirebildiği ve karar merkezlerinin hangi bilgiyi ciddiye aldığı zaman içerisinde belirleyici hâle gelmektedir.

Modelin ampirik olarak sınanması da bu döngüsel mantığa uygun biçimde tasarlanmalıdır. Tek zamanlı ve tek kaynaklı anketler örgütsel bağışıklığın belirli boyutlarını ortaya çıkarabilir; ancak modelin erken uyarı, eşik değerlendirmesi ve geri bildirim mantığını yakalamakta sınırlı kalmaktadır. Bu nedenle gelecekteki çalışmalar, çok zamanlı, çok kaynaklı ve mümkün olduğunda olay temelli tasarımları benimsedikleri takdirde daha sağlam olacaktır. Çalışan anketleri karar netliği, psikolojik güvenlik, bilgi paylaşımı veya adaptasyona ilişkin algılar hakkında veri sağlayabilirken hata raporları, proje gecikmeleri, çalışan devir oranları, müşteri şikâyetleri, iç denetim bulguları ve toplantı tutanakları bir örgütün zayıf sinyallerinin daha davranışsal bir düzeyde izlenmesine imkân sağlayabilir. Bu tür çok kaynaklı yaklaşımlar, ortak yöntem yanlılığı riskinin azaltılması açısından da önemlidir. Podsakoff vd. (2003, 2024), ortak yöntem yanlılığının davranışsal araştırmalardaki bulgular için nasıl önemli bir alternatif açıklama oluşturabileceğini ayrıntılı biçimde ele almaktadır.

Yönetmel açıdan model, örgütlere kriz sonrasında yalnızca hasarı kontrol etme değil, kriz öncesinde kurumsal dikkati tasarlama görevi yüklemektedir. Bu dikkat yalnızca finansal sonuçlara veya nihai performans göstergelerine yöneltilmemelidir. Kararların neden geciktiği, bilginin nerede sıkıştığı, hangi sorunların dile getirilemediği, hangi birimlerin birbirinden koptuğu ve hangi deneyimlerin örgütsel hafızaya yerleşmediği aynı ciddiyetle izlenmelidir. Bununla birlikte burada önemli bir sınırın kabul edilmesi gerekmektedir. Sürekli izleme, öğrenmeyi destekleyen bir erken uyarı sistemi olarak kurulmadığı takdirde kolaylıkla kontrol ve cezalandırma kültürüne dönüşebilir. Dolayısıyla örgütsel bağışıklık mimarisinin sağlıklı işleyişi, verilerin toplanmasından çok bu verilerin nasıl yorumlandığına ve çalışanların sorunları paylaşabildikleri güven iklimine bağlıdır. Edmondson'ın (1999) bulguları, modelin yönetmel boyutuna güçlü bir uyarı eklemektedir: Sorunları açıkça dile getirmenin riskli olarak algılandığı örgütlerde erken uyarı mekanizmaları biçimsel olarak var olabilirken işlevsel açıdan zayıf kalabilir.

Modelin sınırlılıkları da açıkça ortaya konulmalıdır. İlk olarak koruyucu hekimlik ve biyokimya paneli benzetmesi açıklayıcı bir araçtır; örgütleri doğrudan biyolojik sistemlerle eşitlemek için kullanılmamalıdır. Örgütler yoruma açık siyasal ve kültürel yapılardır; aynı gösterge farklı bağlamlarda farklı anlamlar taşıyabilir. İkinci olarak her zayıf sinyal gerçek bir krizin habercisi değildir. Bu durum yanlış alarm riskini ortaya çıkarmaktadır. Aşırı duyarlı bir sistem gereksiz müdahaleler üretebilirken yeterince duyarlı olmayan bir sistem kritik sinyalleri çok geç tespit edebilir. Üçüncü olarak modelin işleyişi sektöre, örgütsel büyüklüğe, teknolojik karmaşıklığa ve düzenleyici çevreye göre farklılık gösterebilir. Havacılık, sağlık hizmetleri, enerji veya savunma gibi

yüksek güvenilirlik gerektiren alanlarda erken uyarı ve eşik mantığı daha merkezi olabilirken daha düşük riskli sektörlerde aynı göstergeler farklı ağırlıklar taşıyabilir (Weick & Sutcliffe, 2007). Bu nedenle örgütsel bağışıklık mimarisi evrensel bir reçete olarak değil, farklı bağlamlarda sınanması gereken kuramsal bir çerçeve olarak ele alınmalıdır.

Sonuç

Bu çalışmada örgütsel bağışıklık, kriz ortaya çıktıktan sonra işlerlik kazanan savunmacı bir refleks olarak değil, örgütün kırılganlıklarını henüz yönetilebilir düzeydeyken yorumlayabilen döngüsel bir teşhis ve öğrenme mimarisi olarak kavramsallaştırılmıştır. Önerilen model; zayıf sinyallerin stratejik önemine ilişkin klasik yaklaşımı, örgütsel dayanıklılığın öngörme-başa çıkma-adaptasyon mantığını, dinamik yetenekler yazınının çevresel değişime yanıt olarak yetkinliklerin yeniden yapılandırılmasına yaptığı vurguyu, risk değerlendirme mantığını ve deneyimin kurumsallaştırılmasında örgütsel öğrenme ve örgütsel hafızanın rolünü bir araya getirmektedir (Ansoff, 1975; Duchek, 2020; International Organization for Standardization, 2018; Levitt & March, 1988; Teece vd., 1997; Walsh & Ungson, 1991; Weick & Sutcliffe, 2007). Böylece örgütsel bağışıklık mimarisi; dayanıklılık, dinamik yetenekler veya örgütsel öğrenme yazınlarının yerine geçen yeni bir etiket olarak değil, bu yazınların açıklama gücünü erken teşhis, risk eşiği, önleyici müdahale ve geri bildirimden oluşan bir döngü içerisinde bütünleştiren özgül bir kuramsal çerçeve olarak konumlandırılmaktadır.

Modelin temel iddiası açıktır: Örgütlerin uzun vadeli sağlığı yalnızca kriz sırasında nasıl tepki verdikleriyle değil, kriz öncesinde neyi fark ettikleri, hangi sinyalleri ciddiye aldıkları, zayıflığı nerede teşhis ettikleri ve müdahale sonrasında neyi örgütsel hafızaya dönüştürdükleriyle de belirlenmektedir. Bu nedenle liderlik/yapı, adaptasyon, entegrasyon ve entelektüel sermaye panelleri model içerisindeki kavramsal boyutlardan ibaret değildir; bunlar, örgütün bağışıklık kaybını yorumlamasını sağlayan tanısal alanlardır. Challenger ve Columbia örneklerinin gösterdiği üzere karmaşık örgütlerdeki büyük çaplı bozulmalar çoğu zaman tek bir teknik arızadan değil, zayıf sinyallerin nasıl yorumlandığından, bilginin nerede sıkıştığından ve karar alma süreçlerinin temelinde yer alan varsayımlardan kaynaklanmaktadır (Columbia Accident Investigation Board, 2003; Vaughan, 1996). Dolayısıyla örgütsel bağışıklık mimarisi, örgütleri “daha dayanıklı” hâle getirme iddiasını örgütlerin daha erken tespit etme, daha doğru yorumlama ve daha hızlı müdahale etme kapasitesine dayandırmaktadır.

Sonuç olarak bu çalışmada örgütsel bağışıklığın soyut bir metafor olmaktan çıkarılarak örgütsel dikkat, teşhis, müdahale ve öğrenmeyi birbirine bağlayan bütüncül bir kuramsal modele dönüştürülmesi amaçlanmıştır. Modelin değeri, örgütlere kusursuz bir kontrol sistemi vaat etmesinde değil, kırılganlıkların görünür sonuçlar üretmeden önce çoğu zaman küçük sapmalar ve ihmal edilen sinyaller biçiminde ortaya çıktığını hatırlatmasında yatmaktadır. Bu nedenle örgütsel bağışıklık mimarisi, gelecekteki kavramsal ve ampirik araştırmalar için verimli bir araştırma hattı açmaktadır: Yönetim ve organizasyon araştırmaları yalnızca örgütlerin ne kadar güçlü olduklarına değil, kendi zayıflıklarını ne kadar erken ve dürüst biçimde yorumlayabildiklerine ve bu süreç aracılığıyla ne ölçüde öğrenebildiklerine de odaklanmalıdır.

References

- Agostini, L., & Nosella, A. (2023). Intellectual capital and resilience: Evidence from two cases of SMEs. *Knowledge Management Research & Practice*, 21(5), 929–942. <https://doi.org/10.1080/14778238.2022.2103047>
- Allen, D. G., Bryant, P. C., & Vardaman, J. M. (2010). Retaining talent: Replacing misconceptions with evidence-based strategies. *Academy of Management Perspectives*, 24(2), 48–64.
- Ansoff, H. I. (1975). Managing strategic surprise by response to weak signals. *California Management Review*, 18(2), 21–33.
- Argyris, C., & Schön, D. A. (1978). *Organizational learning: A theory of action perspective*. Addison-Wesley Publishing Company.
- Aven, T., & Thekdi, S. (2024). *Risk science: An introduction* (2nd ed.). Routledge. <https://doi.org/10.4324/9781003494317>
- Biomarkers Definitions Working Group. (2001). Biomarkers and surrogate endpoints: Preferred definitions and conceptual framework. *Clinical Pharmacology & Therapeutics*, 69(3), 89–95. <https://doi.org/10.1067/mcp.2001.113989>
- Burke, W. W., & Litwin, G. H. (1992). A causal model of organizational performance and change. *Journal of Management*, 18(3), 523–545. <https://doi.org/10.1177/014920639201800306>
- Bükeç, C. M., & Başdemir, M. M. (2021). Türkiye’de ekip kaynak yönetimi eğitimlerinin uçuş emniyetine katkısını artıracak bir model önerisi. *Turkish Studies - Economy*, 16(2), 1051–1073. <https://doi.org/10.47644/TurkishStudies.47963>
- Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *The International Journal of Logistics Management*, 15(2), 1–14.
- Cohen, W. M., & Levinthal, D. A. (1990). Absorptive capacity: A new perspective on learning and innovation. *Administrative Science Quarterly*, 35(1), 128–152.
- Columbia Accident Investigation Board. (2003). *Columbia Accident Investigation Board report: Volume I*.
- Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management: Integrating with strategy and performance*. COSO.
- Cornelissen, J. P. (2005). Beyond compare: Metaphor in organization theory. *Academy of Management Review*, 30(4), 751–764.
- Crossan, M. M., Lane, H. W., & White, R. E. (1999). An organizational learning framework: From intuition to institution. *Academy of Management Review*, 24(3), 522–537.
- Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research*, 13, 215–246.
- Edmondson, A. C. (1996). Learning from mistakes is easier said than done: Group and organizational influences on the detection and correction of human error. *The Journal of Applied Behavioral Science*, 32(1), 5–28.
- Edmondson, A. C. (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly*, 44(2), 350–383.
- Edmondson, A. C., & Bransby, D. P. (2023). Psychological safety comes of age: Observed themes in an established literature. *Annual Review of Organizational Psychology and*

-
- Organizational Behavior*, 10, 55–78. <https://doi.org/10.1146/annurev-orgpsych-120920-055217>
- Fergnani, A. (2022). Corporate foresight: A new frontier for strategy and management. *Academy of Management Perspectives*, 36(2), 820–844. <https://doi.org/10.5465/amp.2018.0178>
- Foroughi, H., Coraiola, D. M., Rintamäki, J., Mena, S., & Foster, W. M. (2020). Organizational memory studies. *Organization Studies*, 41(12), 1725–1748. <https://doi.org/10.1177/0170840620974338>
- Galbraith, J. R. (1973). *Designing complex organizations*. Addison-Wesley Publishing Company.
- Galbraith, J. R. (1974). Organization design: An information processing view. *Interfaces*, 4(3), 28–36.
- Haarhaus, T., & Liening, A. (2020). Building dynamic capabilities to cope with environmental uncertainty: The role of strategic foresight. *Technological Forecasting and Social Change*, 155, Article 120033. <https://doi.org/10.1016/j.techfore.2020.120033>
- Huang, J.-J. (2013). Organizational knowledge, learning and memory – a perspective of an immune system. *Knowledge Management Research & Practice*, 11(3), 230–240.
- International Organization for Standardization. (2018). *Risk management—Guidelines* (ISO Standard No. 31000:2018).
- Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review*, 90(6), 48–60.
- Kara, O., & Yalçın, A. (2026). Examining organizational immunity through organizational DNA dimensions: An application in an industrial enterprise. *Turizm Ekonomi ve İşletme Araştırmaları Dergisi*, 8(1), 1–24. <https://dergipark.org.tr/pub/turek/article/1953325>
- Köse, S., Mohan Bursalı, Y., & Dolma, S. (2023). Örgütsel adalet ve yönetici desteği ile ihbarcılık arasındaki ilişkide psikolojik güvenliğin aracılık rolü. *Turkish Studies - Economy*, 18(1), 305–325. <https://doi.org/10.7827/TurkishStudies.66883>
- Lawrence, P. R., & Lorsch, J. W. (1967). *Organization and environment: Managing differentiation and integration*. Division of Research, Graduate School of Business Administration, Harvard University.
- Lee, G. K., Lampel, J., & Shapira, Z. (2020). After the storm has passed: Translating crisis experience into useful knowledge. *Organization Science*, 31(4), 1037–1051. <https://doi.org/10.1287/orsc.2020.1366>
- Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. *Human Resource Management Review*, 21(3), 243–255.
- Levitt, B., & March, J. G. (1988). Organizational learning. *Annual Review of Sociology*, 14, 319–340.
- Li, A. N., & Tangirala, S. (2022). How employees' voice helps teams remain resilient in the face of exogenous change. *Journal of Applied Psychology*, 107(4), 668–692. <https://doi.org/10.1037/apl0000874>
- March, J. G. (1991). Exploration and exploitation in organizational learning. *Organization Science*, 2(1), 71–87.
-

- Mertel, K., Bozkurt, S., & Demirhan, A. (2020). Dönüşümcü liderlik tarzının bilgi paylaşımına etkisinde destekleyici örgüt ikliminin aracı rolüne yönelik bir araştırma. *Turkish Studies - Social*, 15(6), 3073–3087. <https://doi.org/10.47356/TurkishStudies.44302>
- Miller, K. D. (1992). A framework for integrated risk management in international business. *Journal of International Business Studies*, 23(2), 311–331.
- Moqaddamerad, S., & Ali, M. (2024). Strategic foresight and business model innovation: The sequential mediating role of sensemaking and learning. *Technological Forecasting and Social Change*, 200, Article 123095. <https://doi.org/10.1016/j.techfore.2023.123095>
- Morgan, G. (1980). Paradigms, metaphors, and puzzle solving in organization theory. *Administrative Science Quarterly*, 25(4), 605–622.
- Morrison, E. W. (2014). Employee voice and silence. *Annual Review of Organizational Psychology and Organizational Behavior*, 1, 173–197.
- Morrison, E. W. (2023). Employee voice and silence: Taking stock a decade later. *Annual Review of Organizational Psychology and Organizational Behavior*, 10, 79–107. <https://doi.org/10.1146/annurev-orgpsych-120920-054654>
- Nahapiet, J., & Ghoshal, S. (1998). Social capital, intellectual capital, and the organizational advantage. *Academy of Management Review*, 23(2), 242–266.
- Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science*, 5(1), 14–37.
- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879–903. <https://doi.org/10.1037/0021-9010.88.5.879>
- Podsakoff, P. M., Podsakoff, N. P., Williams, L. J., Huang, C., & Yang, J. (2024). Common method bias: It's bad, it's complex, it's widespread, and it's not easy to fix. *Annual Review of Organizational Psychology and Organizational Behavior*, 11, 17–61. <https://doi.org/10.1146/annurev-orgpsych-110721-040030>
- Power, M., Scheytt, T., Soin, K., & Sahlin, K. (2009). Reputational risk as a logic of organizing in late modernity. *Organization Studies*, 30(2–3), 301–324.
- Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate.
- Rizzo, J. R., House, R. J., & Lirtzman, S. I. (1970). Role conflict and ambiguity in complex organizations. *Administrative Science Quarterly*, 15(2), 150–163.
- Roberts, K. H. (1990). Some characteristics of one type of high reliability organization. *Organization Science*, 1(2), 160–176.
- Schein, E. H. (1996). Kurt Lewin's change theory in the field and in the classroom: Notes toward a model of managed learning. *Systems Practice*, 9(1), 27–47.
- Simons, R. (1995). *Levers of control: How managers use innovative control systems to drive strategic renewal*. Harvard Business School Press.
- Subramaniam, M., & Youndt, M. A. (2005). The influence of intellectual capital on the types of innovative capabilities. *Academy of Management Journal*, 48(3), 450–463. <https://doi.org/10.5465/amj.2005.17407911>

-
- Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533.
- Töre, E. (2020). Örgütsel iklimin bilgi yönetimi süreci üzerindeki etkisinin incelenmesi. *Turkish Studies - Educational Sciences*, 15(3), 2137–2151. <https://doi.org/10.29228/TurkishStudies.40054>
- Tushman, M. L., & Nadler, D. A. (1978). Information processing as an integrating concept in organizational design. *Academy of Management Review*, 3(3), 613–624.
- Vaughan, D. (1996). *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. University of Chicago Press.
- Vuori, T. O., & Huy, Q. N. (2016). Distributed attention and shared emotions in the innovation process: How Nokia lost the smartphone battle. *Administrative Science Quarterly*, 61(1), 9–51.
- Walsh, J. P., & Ungson, G. R. (1991). Organizational memory. *Academy of Management Review*, 16(1), 57–91.
- Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the unexpected: Resilient performance in an age of uncertainty (2nd ed.)*. Jossey-Bass.
- Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfulness. In B. M. Staw & R. I. Sutton (Eds.), *Research in organizational behavior* (Vol. 21, pp. 81–123). JAI Press.

ETHICAL DECLARATIONS**Research and Publication Ethics**

The author(s) declare that this manuscript is an original work prepared in accordance with the principles of scientific research and publication ethics. The manuscript has not been previously published and is not currently under consideration for publication elsewhere. All sources used in the preparation of this study have been properly cited and referenced. The author(s) confirm that the work contains no plagiarism, fabrication, falsification, or manipulation of data. The research findings are presented honestly and transparently in accordance with the principles of academic integrity.

Author Contributions

All authors have significantly contributed to the conception, design, analysis, and preparation of the manuscript. All authors have read and approved the final version of the manuscript and agree to its submission and publication.

Conflict of Interest

The author(s) declare that there is no conflict of interest regarding the publication of this manuscript.

Funding

This research did not receive any specific grant, financial support, or funding from any public, commercial, or non-profit funding agencies.

Artificial Intelligence (AI) Usage Disclosure

During the preparation of this manuscript, artificial intelligence tools may have been used solely for limited purposes such as language editing, translation assistance, and stylistic improvement. Any AI-assisted translations or language corrections were carefully reviewed and verified by the author(s). Artificial intelligence tools were not used to generate the core scientific content, research design, analysis, or scholarly conclusions. All academic responsibility for the content of the manuscript rests entirely with the author(s).

Copyright and Permissions

The author(s) confirm that all necessary permissions for copyrighted materials have been obtained where required and that the manuscript does not violate any intellectual property rights.

Author Approval

All authors confirm that they have read and approved the final version of the manuscript and consent to its submission and publication.

ETİK BEYANLAR**Araştırma ve Yayın Etiği**

Yazar(lar), bu makalenin özgün bir çalışma olduğunu ve bilimsel araştırma ve yayın etiği ilkelerine uygun olarak hazırlandığını beyan eder. Makale daha önce herhangi bir yerde yayımlanmamış olup başka bir dergide değerlendirme sürecinde değildir.

Çalışmada kullanılan tüm kaynaklar akademik kurallara uygun biçimde atıf lanmıştır. Yazar(lar), çalışmanın intihal, veri uydurma, veri tahrifi veya manipölasyon içermediğini; araştırma bulgularının bilimsel dürüstlük ilkelerine uygun şekilde sunulduğunu beyan eder.

Yazar Katkısı

Tüm yazarlar çalışmanın tasarlanması, yürütülmesi, analizi ve makalenin hazırlanmasına önemli ölçüde katkı sağlamıştır. Tüm yazarlar makalenin son hâlini okuyup onaylamış ve yayımlanmasını kabul etmiştir.

Çıkar Çatışması

Yazar(lar), bu makalenin yayımlanmasına ilişkin herhangi bir çıkar çatışması bulunmadığını beyan eder.

Finansal Destek

Bu araştırma herhangi bir kamu kurumu, ticari kuruluş veya kâr amacı gütmeyen kuruluş tarafından finansal olarak desteklenmemiştir.

Yapay Zekâ Kullanım Beyanı

Makalenin hazırlanması sürecinde yapay zekâ araçlarından yalnızca dil düzenleme, çeviri desteği ve anlatım iyileştirmesi amacıyla sınırlı ölçüde yararlanılmış olabilir. Yapay zekâ araçları tarafından yapılan çeviri ve dil düzenlemeleri yazar(lar) tarafından dikkatle kontrol edilmiştir. Yapay zekâ araçları çalışmanın bilimsel içeriğinin, araştırma tasarımının, analizlerinin veya akademik sonuçlarının oluşturulmasında kullanılmamıştır. Makalenin içeriğine ilişkin tüm akademik sorumluluk yazar(lar)a aittir.

Telif Hakları ve İzinler

Yazar(lar), telif hakkı gerektiren materyaller kullanılmışsa gerekli izinlerin alındığını ve çalışmanın herhangi bir fikrî mülkiyet hakkını ihlal etmediğini beyan eder.

Yazar Onayı

Tüm yazarlar makalenin son hâlini okuduklarını, onayladıklarını ve yayımlanmasını kabul ettiklerini beyan eder.