ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΚΑΙ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ

ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ ΓΙΑ ΣΤΕΛΕΧΗ (Ε - MBA)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Η συμμετοχή της QnR στη Νέα Εποχή του CyberSecurity: Στρατηγικές Επιλογές και Επιχειρησιακές Αποφάσεις

Μιχάλης Πιερέττης

Επιβλέπων Καθηγητής: Νικόλαος Β. Γεωργόπουλος

Πειραιάς, 2026

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ ΓΙΑ ΣΤΕΛΕΧΗ (E-MBA)

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ
(περιλαμβάνεται ως ξεχωριστή (δεύτερη) σελίδα στο σώμα της διπλωματικής εργασίας)

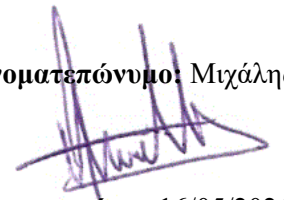
«Δηλώνω υπεύθυνα ότι η διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών, του Πανεπιστημίου Πειραιώς, στη Διοίκηση Επιχειρήσεων για Στελέχη –Ε-ΜΒΑ με τίτλο:

Η συμμετοχή της QnR στη Νέα Εποχή του CyberSecurity: Στρατηγικές Επιλογές και Επιχειρησιακές Αποφάσεις

έχει συγγραφεί από εμένα αποκλειστικά και στο σύνολό της. Δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό, ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

Δηλώνω επίσης υπεύθυνα ότι οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης εργασίας, αναφέρονται στο σύνολό τους, κάνοντας πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ονοματεπώνυμο: Μιχάλης Πιερέττης



Ημερομηνία: 16/05/2026

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Κεφάλαιο 1

Εισαγωγή

1.1 Πλαίσιο και Αφορμή της Έρευνας

Η κυβερνοασφάλεια (cybersecurity) έχει αναδειχθεί σε έναν από τους πλέον κρίσιμους στρατηγικούς τομείς της σύγχρονης ψηφιακής οικονομίας. Η κλιμάκωση των κυβερνοαπειλών, με 4.875 καταγεγραμμένα συμβάντα στην Ευρώπη κατά την περίοδο 2024-2025 σύμφωνα με τον ENISA (2025), σε συνδυασμό με το αυξανόμενο κόστος παραβιάσεων δεδομένων (4,88 εκατομμύρια δολάρια μέσος παγκόσμιος όρος κατά IBM, 2024), καθιστά την κυβερνοασφάλεια κεντρικό ζήτημα τόσο για τους δημόσιους οργανισμούς όσο και για τις επιχειρήσεις. Η Ευρωπαϊκή Ένωση ανταποκρίθηκε στις προκλήσεις αυτές με ένα πολυεπίπεδο ρυθμιστικό πλαίσιο, του οποίου ακρογωνιαίοι λίθοι αποτελούν η Οδηγία NIS2 (EU 2022/2555), ο Κανονισμός DORA (EU 2022/2554), η Πράξη Κυβερνοασφάλειας (EU 2019/881), η Πράξη Κυβερνοανθεκτικότητας (Cyber Resilience Act) και ο Κανονισμός για την Τεχνητή Νοημοσύνη (AI Act, EU 2024/1689).

Στην Ελλάδα, η ενσωμάτωση της NIS2 μέσω του Ν. 5160/2024 (Σεπτέμβριος 2024), η θέσπιση ειδικών απαιτήσεων για το χρηματοπιστωτικό τομέα μέσω του Ν. 5193/2025 και η διαμόρφωση νέας Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026-2030 δημιουργούν ένα δυναμικά μεταβαλλόμενο περιβάλλον που γεννά τόσο υποχρεώσεις όσο και εμπορικές ευκαιρίες. Η ελληνική αγορά κυβερνοασφάλειας, αξίας 185,3 εκατομμυρίων δολαρίων το 2026 με ρυθμό ανάπτυξης 8,36% (Mordor Intelligence, 2025), αναμένεται να αναπτυχθεί σημαντικά τα επόμενα χρόνια, τροφοδοτούμενη από τη ρυθμιστική υποχρέωση συμμόρφωσης εκατοντάδων νέων οργανισμών.

Σε αυτό το πλαίσιο, η εταιρεία Quality & Reliability A.B.E.E. (QnR), ένας εδραιωμένος πάροχος λύσεων πληροφορικής (IT solutions) στην ελληνική αγορά από το 1992, εισηγμένη στο Χρηματιστήριο Αθηνών (ATHEX: QUAL), αποφάσισε το 2025 να εισέλθει στον κλάδο της κυβερνοασφάλειας μέσω της εξαγοράς του 60% της SysteCom S.A., μιας εξειδικευμένης εταιρείας κυβερνοασφάλειας με δωδεκαετή εμπειρία και πάνω από 200 πελάτες. Η κίνηση αυτή

εντάσσεται σε μια ευρύτερη στρατηγική μετασχηματισμού που περιλαμβάνει δύο ακόμη εξαγορές: τη βελγική εταιρεία τεχνητής νοημοσύνης SquareDev BV (51%) και την ελληνική εταιρεία λύσεων SAP Alexander Moore S.A. (76,19%).

Η παρούσα εργασία εξετάζει αυτή τη στρατηγική κίνηση ως μελέτη περίπτωσης (case study), αναλύοντας τις στρατηγικές επιλογές και τις επιχειρησιακές αποφάσεις που οδήγησαν στη μετάβαση από πάροχο πληροφορικής σε διαφοροποιημένο τεχνολογικό όμιλο με ισχυρή παρουσία στην κυβερνοασφάλεια.

Η σημασία του θέματος εδράζεται σε τρεις παράγοντες. Πρώτον, η κυβερνοασφάλεια αποτελεί πλέον τη βασική προτεραιότητα για τα κράτη και τις επιχειρήσεις παγκοσμίως, με τις δαπάνες να αναμένεται να υπερβούν τα 248 δισεκατομμύρια δολάρια το 2026 (Fortune Business Insights, 2025). Δεύτερον, το ελληνικό ρυθμιστικό πλαίσιο μετασχηματίζεται ραγδαία, δημιουργώντας νέες υποχρεώσεις για εκατοντάδες οργανισμούς και αντίστοιχες εμπορικές ευκαιρίες για παρόχους υπηρεσιών κυβερνοασφάλειας. Τρίτον, η στρατηγική εισόδου των ελληνικών εταιρειών τεχνολογίας σε νέους κλάδους μέσω εξαγορών αποτελεί ένα φαινόμενο αυξανόμενης σημασίας που δεν έχει μελετηθεί επαρκώς στην ελληνική ακαδημαϊκή βιβλιογραφία. Η περίπτωση της QnR παρέχει μια σπάνια ευκαιρία εξέτασης αυτού του φαινομένου σε πραγματικό χρόνο, καθώς οι εξαγορές πραγματοποιήθηκαν κατά τη διάρκεια εκπόνησης της εργασίας.

1.2 Σκοπός και Ερευνητικά Ερωτήματα

Σκοπός της παρούσας διπλωματικής εργασίας είναι η στρατηγική ανάλυση και η αξιολόγηση της απόφασης εισόδου του Ομίλου QnR στον κλάδο της κυβερνοασφάλειας μέσω εξαγοράς, αξιοποιώντας θεωρητικά πλαίσια στρατηγικής διοίκησης σε συνδυασμό με τα εμπειρικά δεδομένα της αγοράς και της εταιρείας. Τα κεντρικά ερευνητικά ερωτήματα (research questions) που διερευνώνται είναι τα εξής:

ΕΕ1: Ποια είναι η δομή και η δυναμική του κλάδου της κυβερνοασφάλειας στην Ελλάδα και πώς επηρεάζεται από το ευρωπαϊκό και εθνικό ρυθμιστικό πλαίσιο;

ΕΕ2: Σε ποιο βαθμό η στρατηγική απόφαση εισόδου του Ομίλου QnR στην κυβερνοασφάλεια μέσω εξαγοράς τεκμηριώνεται θεωρητικά από τα πλαίσια στρατηγικής ανάλυσης (Porter, RBV/VRIO, Δυναμικές Ικανότητες, Τεχνολογική Διαφοροποίηση);

ΕΕ3: Ποιες είναι οι κρίσιμες προκλήσεις και οι ευκαιρίες που αντιμετωπίζει ο Όμιλος QnR κατά την ολοκλήρωση των συγχωνεύσεων (Post-Merger Integration) και ποιες στρατηγικές προτάσεις μπορούν να διατυπωθούν;

Τα ερωτήματα αυτά αντιμετωπίζονται μέσω μιας πολυεπίπεδης ανάλυσης (multi-framework analysis) που συνδυάζει εξωτερική ανάλυση του κλάδου (Porter Five Forces), εσωτερική αξιολόγηση των πόρων (VRIO), δυναμική ανάλυση των ικανοτήτων (Teece Dynamic Capabilities), αξιολόγηση της τεχνολογικής διαφοροποίησης (Ceipek et al.), ανάλυση της ολοκλήρωσης των συγχωνεύσεων (M&A/PMI) και σύνθεση SWOT. Η συνδυαστική εφαρμογή πολλαπλών θεωρητικών πλαισίων επιτρέπει τη θεώρηση του ερευνητικού αντικειμένου από διαφορετικές γωνίες, αυξάνοντας την αξιοπιστία των συμπερασμάτων.

1.3 Μεθοδολογία

Η εργασία υιοθετεί μεθοδολογία μελέτης περίπτωσης (case study methodology), η οποία επιτρέπει τη σε βάθος εξέταση ενός σύγχρονου φαινομένου στο πραγματικό του πλαίσιο. Η ανάλυση στηρίζεται σε τρεις πυλώνες δεδομένων.

Ο πρώτος πυλώνας αφορά τη βιβλιογραφική επισκόπηση (literature review) ακαδημαϊκών δημοσιεύσεων σε θέματα στρατηγικού μάνατζμεντ, κυβερνοασφάλειας, ψηφιακού μετασχηματισμού και εξαγορών. Αξιοποιούνται θεωρητικά πλαίσια από τους Porter (1980; 2008), Barney (1991), Teece (2007), Ceipek et al. (2020), Lace και Kirikova (2022), Milde et al. (2024) και Usianeneh (2025), μεταξύ άλλων.

Ο δεύτερος πυλώνας αφορά τα δευτερογενή δεδομένα της αγοράς (secondary market data), συμπεριλαμβανομένων εκθέσεων του ENISA, της IBM, της Gartner, της Fortune Business Insights και της Mordor Intelligence, καθώς και του ευρωπαϊκού και ελληνικού ρυθμιστικού πλαισίου (NIS2, DORA, Ν. 5160/2024, Ν. 5193/2025, ΚΥΑ 1689/2025 και 1645/2025).

Ο τρίτος πυλώνας αφορά τα εταιρικά δεδομένα (corporate data) του Ομίλου QnR και της SysteCom, τα οποία αντλούνται από δημοσίως διαθέσιμες πηγές όπως εταιρικές ιστοσελίδες, ανακοινώσεις στο Χρηματιστήριο Αθηνών, δελτία τύπου και οικονομικά στοιχεία. Τα δεδομένα αυτά περιλαμβάνουν οικονομικά μεγέθη (κύκλος εργασιών, EBITDA, κέρδη προ φόρων), πληροφορίες συναλλαγών (τίμημα, ποσοστά, χρηματοδότηση), στοιχεία πελατειακής βάσης και χαρτοφυλάκιο υπηρεσιών. Πρέπει να σημειωθεί ότι η μη πρόσβαση σε εσωτερικά

εμπιστευτικά δεδομένα αποτελεί περιορισμό της μεθοδολογίας, ο οποίος αναγνωρίζεται και αξιολογείται στο Κεφάλαιο 6.

Η τριγωνοποίηση δεδομένων (data triangulation) μεταξύ ακαδημαϊκής βιβλιογραφίας, δεδομένων αγοράς και εταιρικών στοιχείων ενισχύει την αξιοπιστία (reliability) και την εγκυρότητα (validity) των ευρημάτων, αντισταθμίζοντας τους περιορισμούς κάθε μεμονωμένης πηγής. Η αναλυτική μεθοδολογία (analytical framework) εφαρμόζει πέντε θεωρητικά εργαλεία στα εμπειρικά δεδομένα: ανάλυση Πέντε Δυνάμεων Porter (ανάλυση κλάδου), ανάλυση VRIO (εσωτερικοί πόροι), ανάλυση Δυναμικών Ικανοτήτων Teece (στρατηγικές κινήσεις), ανάλυση Τεχνολογικής Διαφοροποίησης Ceipek et al. (μέθοδος εισόδου) και ανάλυση M&A/PMI (μετασυγχωνευτική ολοκλήρωση). Η σύνθεση πραγματοποιείται μέσω ανάλυσης SWOT.

1.4 Δομή της Εργασίας

Η εργασία αρθρώνεται σε επτά κεφάλαια, τα οποία ακολουθούν μια λογική πορεία από τη θεωρία στην εφαρμογή και την αξιολόγηση.

Το **Κεφάλαιο 1** (παρόν) παρουσιάζει το πλαίσιο, τα ερευνητικά ερωτήματα, τη μεθοδολογία και τη δομή της εργασίας.

Το **Κεφάλαιο 2** αναπτύσσει τη βιβλιογραφική επισκόπηση, παρουσιάζοντας τα θεωρητικά πλαίσια που αποτελούν τη βάση της ανάλυσης όπως μοντέλο Πέντε Δυνάμεων Porter, Θεωρία Πόρων και Ικανοτήτων (RBV/VRIO), Δυναμικές Ικανότητες (Teece), Τεχνολογική Διαφοροποίηση (Ceipek et al.), Εξαγορές και Μετασυγχωνευτική Ολοκλήρωση (M&A/PMI), και Ψηφιακός Μετασχηματισμός.

Το **Κεφάλαιο 3** παρουσιάζει το οικοσύστημα της κυβερνοασφάλειας, το παγκόσμιο τοπίο απειλών, το ευρωπαϊκό ρυθμιστικό πλαίσιο, το ελληνικό θεσμικό πλαίσιο, τις τεχνολογικές τάσεις και τα μεγέθη της ελληνικής αγοράς.

Το **Κεφάλαιο 4** παρουσιάζει την εταιρεία QnR, την ιστορική εξέλιξη, το χαρτοφυλάκιο των υπηρεσιών, την ομιλική δομή, τις τρεις εξαγορές του 2025 και τη στρατηγική λογική εισόδου στην κυβερνοασφάλεια.

Το **Κεφάλαιο 5** εφαρμόζει τα θεωρητικά πλαίσια του Κεφαλαίου 2 στα εμπειρικά δεδομένα των Κεφαλαίων 3 και 4, διενεργώντας αναλύσεις Porter, VRIO, Δυναμικών Ικανοτήτων, Τεχνολογικής Διαφοροποίησης, M&A/PMI και SWOT.

Το **Κεφάλαιο 6** αξιολογεί κριτικά τις στρατηγικές επιλογές, διατυπώνει στρατηγικές προτάσεις, αναγνωρίζει τους περιορισμούς της ανάλυσης και προτείνει κατευθύνσεις μελλοντικής έρευνας.

Κεφάλαιο 2

Βιβλιογραφική Επισκόπηση

2.1 Το Μοντέλο των Πέντε Δυνάμεων του Porter

Η ανάλυση του ανταγωνιστικού περιβάλλοντος ενός κλάδου αποτελεί θεμελιώδες βήμα για τη χάραξη επιχειρηματικής στρατηγικής (business strategy). Το μοντέλο των Πέντε Δυνάμεων (Five Forces), το οποίο εισήγαγε ο Michael E. Porter (1980), παραμένει ένα από τα πλέον διαδεδομένα αναλυτικά εργαλεία στο στρατηγικό μάνατζμεντ. Σκοπός του είναι η αποτίμηση της ελκυστικότητας και της ανταγωνιστικής δομής ενός κλάδου μέσω πέντε διακριτών δυνάμεων, δηλαδή της απειλής νέων εισερχομένων (threat of new entrants), της διαπραγματευτικής ισχύος των προμηθευτών (bargaining power of suppliers), της διαπραγματευτικής ισχύος των αγοραστών (bargaining power of buyers), της απειλής υποκατάστατων προϊόντων ή υπηρεσιών (threat of substitutes) και της έντασης του υφιστάμενου ανταγωνισμού (intensity of competitive rivalry) (Porter, 1980; Dewi et al., 2025).

Κάθε μία από τις πέντε δυνάμεις αντανακλά δομικά χαρακτηριστικά του κλάδου τα οποία διαμορφώνουν τις συνθήκες ανταγωνισμού. Συγκεκριμένα, παράγοντες όπως οι οικονομίες κλίμακας (economies of scale), το κόστος μετακίνησης (switching costs), οι κεφαλαιακές απαιτήσεις (capital requirements), η συγκέντρωση των προμηθευτών (supplier concentration), η διαφοροποίηση των προϊόντων (product differentiation), η ευαισθησία των αγοραστών στην τιμή (buyer sensitivity) και οι ρυθμοί ανάπτυξης της αγοράς (market growth rates) καθορίζουν τη σχετική ισχύ κάθε δύναμης. Η συνδυαστική εξέταση των πέντε δυνάμεων παρέχει στη διοίκηση μια ολιστική εικόνα του ανταγωνιστικού τοπίου, επιτρέποντας τον εντοπισμό τόσο ευκαιριών όσο και απειλών.

Η εφαρμογή του μοντέλου αποκαλύπτει σημαντικές αλληλεξαρτήσεις μεταξύ των πέντε δυνάμεων. Για παράδειγμα, υψηλά εμπόδια εισόδου (entry barriers) μέσω κεφαλαιακών απαιτήσεων και οικονομιών κλίμακας τείνουν να μειώνουν την απειλή νέων εισερχομένων, αλλά ταυτοχρόνως μπορεί να ενισχύουν τη διαπραγματευτική ισχύ των υπαρχόντων προμηθευτών. Αντίστοιχα, η παρουσία υποκατάστατων υπηρεσιών ασκεί πίεση στην τιμολόγηση (pricing), μεταφέροντας ισχύ στους αγοραστές. Στον κλάδο της

κυβερνοασφάλειας, αυτή η δυναμική είναι ιδιαιτέρως εμφανής, αφού η συνεχής εμφάνιση νεοφυών επιχειρήσεων (startups) με καινοτόμες τεχνολογικές λύσεις αυξάνει τον ανταγωνισμό, ενώ η πολυπλοκότητα των λύσεων κυβερνοασφάλειας δημιουργεί σημαντικό κόστος μεταστροφής για τους πελάτες. Η κατανόηση αυτών των αλληλεπιδράσεων είναι απαραίτητη για τη σωστή αξιολόγηση ενός κλάδου.

Παρά την ευρεία εφαρμογή του, το μοντέλο του Porter δέχεται κριτική για τον στατικό και κανονιστικό (normative) χαρακτήρα του. Οι Dewi et al. (2025) επισημαίνουν ότι η εφαρμογή των Πέντε Δυνάμεων στο σύγχρονο κλάδο υπηρεσιών ελέγχου, επιθεώρησης και πιστοποίησης (Testing, Inspection, and Certification - TIC) αμφισβητείται, καθώς το μοντέλο δυσκολεύεται να ενσωματώσει τη ραγδαία τεχνολογική αλλαγή, τη δυναμική της καινοτομίας και τις μεταβολές των ρυθμιστικών πλαισίων. Ειδικότερα, αναφέρεται ότι η πολυπλοκότητα και η ταχύτητα της τεχνολογικής εξέλιξης, ιδίως για τις μικρομεσαίες επιχειρήσεις (ΜΜΕ), καθιστούν το μοντέλο ανεπαρκές ως αυτόνομο εργαλείο ανάλυσης (Dewi et al., 2025). Αυτή η αδυναμία αποκτά ιδιαίτερη σημασία στον κλάδο της κυβερνοασφάλειας (cybersecurity), όπου η τεχνολογική καινοτομία, η ρυθμιστική πίεση και η ψηφιακή μετάβαση (digital transformation) μεταβάλλουν διαρκώς τις ισορροπίες του ανταγωνισμού.

Επιπλέον, ο Porter (2008) στην αναθεωρημένη εκδοχή του μοντέλου αναγνωρίζει ότι η κατανόηση της δομής ενός κλάδου δεν αρκεί από μόνη της για τη χάραξη της στρατηγικής, αλλά αποτελεί αναγκαία προϋπόθεση. Ο ίδιος τονίζει ότι η ανάλυση πρέπει να λαμβάνει υπόψη τους ρυθμούς μεταβολής του κλάδου, τη ρυθμιστική παρέμβαση (regulatory intervention) και τους τεχνολογικούς κύκλους (technology cycles), παράγοντες που είναι κεντρικοί στον κλάδο κυβερνοασφάλειας. Η ταχύτητα εξέλιξης των κυβερνοαπειλών και η συχνή αναθεώρηση των ρυθμιστικών πλαισίων καθιστούν απαραίτητη τη δυναμική επανεξέταση της ανάλυσης του κλάδου σε τακτά χρονικά διαστήματα.

Ωστόσο, η αξία του μοντέλου δεν ακυρώνεται. Αντιθέτως, αποτελεί μια αναγκαία αφετηρία ανάλυσης, η οποία χρήζει συμπλήρωσης από δυναμικότερα θεωρητικά πλαίσια. Όπως υποστηρίζουν οι Dewi et al. (2025), οι επιχειρήσεις μπορούν να αξιοποιήσουν τις Πέντε Δυνάμεις ως βάση για τη χαρτογράφηση της αγοράς, αλλά οφείλουν παράλληλα να ενσωματώσουν πιο ολιστικά και δυναμικά εργαλεία, όπως τις δυναμικές ικανότητες (dynamic capabilities), προκειμένου να αναπτύξουν αποτελεσματικές στρατηγικές σε ταχέως μεταβαλλόμενα περιβάλλοντα. Η σύνθεση εξωτερικής ανάλυσης μέσω του Porter με

εσωτερική αξιολόγηση μέσω θεωριών των πόρων αποτελεί τον πυρήνα του αναλυτικού πλαισίου που υιοθετείται στην παρούσα εργασία.

2.2 Θεωρία Πόρων και Ικανοτήτων (Resource-Based View) και Ανάλυση VRIO

Ενώ το μοντέλο του Porter εστιάζει στο εξωτερικό ανταγωνιστικό περιβάλλον, η Θεωρία των Πόρων και Ικανοτήτων (Resource-Based View - RBV) στρέφει την προσοχή στο εσωτερικό περιβάλλον της επιχείρησης. Ο Barney (1991) θεμελίωσε τη θεωρία υποστηρίζοντας ότι η βιώσιμη ανταγωνιστική θέση (sustained competitive advantage) μιας επιχείρησης δεν πηγάζει αποκλειστικά από τη δομή του κλάδου, αλλά κυρίως από τους εσωτερικούς πόρους (resources) και τις ικανότητές (capabilities) της, εφόσον αυτοί πληρούν ορισμένες προϋποθέσεις. Η RBV αντιπαρατίθεται στην παραδοσιακή προσέγγιση που βασίζεται στην αγορά (Market-Based View - MBV), αναδεικνύοντας τη σημασία της ετερογένειας (heterogeneity) και της ακινησίας (immobility) των πόρων μεταξύ ανταγωνιστικών επιχειρήσεων (Barney, 1991; Dewi et al., 2025).

Κεντρικό αναλυτικό εργαλείο της RBV αποτελεί το πλαίσιο VRIO (Value, Rarity, Imitability, Organization), το οποίο αξιολογεί κατά πόσο ένας πόρος ή μια ικανότητα δημιουργεί αξία (Value), είναι σπάνιος/η (Rarity), δύσκολο να το μιμηθεί ο ανταγωνισμός (Imitability) και αν ο οργανισμός είναι κατάλληλα δομημένος ώστε να τον/την αξιοποιήσει πλήρως (Organization). Ένας πόρος που πληροί και τα τέσσερα κριτήρια παρέχει βιώσιμο ανταγωνιστικό πλεονέκτημα (sustained competitive advantage), ενώ η απουσία έστω ενός κριτηρίου υποβαθμίζει το πλεονέκτημα σε προσωρινό ή ανταγωνιστική ισοτιμία (competitive parity).

Στο πλαίσιο του ψηφιακού μετασχηματισμού (digital transformation), η RBV αποκτά ιδιαίτερη σημασία. Οι Agustian et al. (2023) υποστηρίζουν ότι το ανταγωνιστικό πλεονέκτημα στην ψηφιακή εποχή συνδέεται άρρηκτα με την ικανότητα της επιχείρησης να υιοθετεί ταχέως νέες τεχνολογίες και να τις ενσωματώνει στα επιχειρηματικά της μοντέλα (business models). Το πλεονέκτημα αυτό δεν περιορίζεται στα παρεχόμενα προϊόντα ή υπηρεσίες, αλλά επεκτείνεται στη δημιουργία αποτελεσματικότερων και ευέλικτων εσωτερικών διαδικασιών. Η ψηφιακή τεχνολογία μπορεί, κατά τους ίδιους, να αποτελέσει καταλύτη βαθιών

μετασχηματισμών που επαναπροσδιορίζουν τη φύση της ίδιας της επιχειρηματικής δραστηριότητας.

Αξίζει να σημειωθεί ότι η RBV, ως θεωρητικό πλαίσιο, συμπληρώνει τη Θεωρία της Βιομηχανικής Οργάνωσης (Industrial Organization theory) στην οποία εδράζεται το μοντέλο Porter. Ενώ η τελευταία αναζητά τις πηγές του πλεονεκτήματος στη δομή του κλάδου, η RBV στρέφει το βλέμμα στο εσωτερικό της επιχείρησης. Οι Dewi et al. (2025) ενισχύουν τη συνδυαστική χρήση αυτών των δύο προσεγγίσεων, αναφέροντας ότι η RBV λειτουργεί ως συμπλήρωμα ή εναλλακτική στην προσέγγιση που βασίζεται στην αγορά (Market-Based View - MBV), ανοίγοντας δρόμους για συνδυαστικές προσεγγίσεις που σέβονται τις επιστημολογικές διαφορές μεταξύ των θεωριών. Αυτός ο θεωρητικός πλουραλισμός αντικατοπτρίζεται στη μεθοδολογία της παρούσας εργασίας, η οποία αξιοποιεί τόσο εξωτερικά όσο και εσωτερικά αναλυτικά εργαλεία.

Η σημασία της RBV για τις επιχειρήσεις του κλάδου της κυβερνοασφάλειας είναι ιδιαίτερα κρίσιμη. Πόροι όπως η εξειδικευμένη τεχνογνωσία (technical expertise), οι πιστοποιήσεις ασφαλείας (security certifications), οι ιδιόκτητες τεχνολογικές λύσεις (proprietary technology solutions) και η εδραιωμένη πελατειακή βάση (established customer base) μπορούν να αποτελέσουν πηγές βιώσιμου πλεονεκτήματος, εφόσον πληρούν τα κριτήρια VRIO. Για παράδειγμα, μια ομάδα ειδικών κυβερνοασφάλειας με σπάνια εξειδίκευση σε δοκιμές διείσδυσης (penetration testing) ή ανάλυση κακόβουλου λογισμικού (malware analysis) πληροί τα κριτήρια αξίας και σπανιότητας. Εάν η γνώση αυτή είναι ενσωματωμένη σε οργανωτικές ρουτίνες (organizational routines) και κουλτούρα, γίνεται δύσκολο να τη μιμηθούν, ενώ εάν ο οργανισμός διαθέτει τις κατάλληλες δομές για να την αξιοποιήσει, πληρείται και το τελευταίο κριτήριο. Η ανάλυση VRIO, λοιπόν, δεν αποτελεί αφηρημένη θεωρητική άσκηση, αλλά ένα πρακτικό εργαλείο αξιολόγησης των ανταγωνιστικών πλεονεκτημάτων μιας εταιρείας.

Ωστόσο, η RBV έχει κριθεί ως σχετικά στατική (Dewi et al., 2025), καθώς δεν εξηγεί επαρκώς τον τρόπο με τον οποίο οι επιχειρήσεις δημιουργούν, ανανεώνουν και αναδιαμορφώνουν τους πόρους τους σε απάντηση των μεταβαλλόμενων συνθηκών. Σε έναν κλάδο όπως η κυβερνοασφάλεια, όπου νέες απειλές εμφανίζονται σε καθημερινή βάση και οι τεχνολογικοί κύκλοι (technology cycles) διαρκούν λίγα χρόνια, η στατική αξιολόγηση των πόρων αποδεικνύεται ανεπαρκής. Ένας πόρος που πληρούσε τα κριτήρια VRIO πέντε χρόνια

πριν μπορεί σήμερα να έχει απωλέσει τη σπανιότητα ή τη μη μίμησή του, λόγω της ταχείας εξέλιξης της τεχνολογίας. Αυτό το κενό καλύπτει η θεωρία των δυναμικών ικανοτήτων, η οποία εξετάζεται στην επόμενη ενότητα.

2.3 Δυναμικές Ικανότητες (Dynamic Capabilities)

Η θεωρία των δυναμικών ικανοτήτων (Dynamic Capabilities - DCs) αναπτύχθηκε ως εξέλιξη και συμπλήρωμα της RBV, προκειμένου να εξηγήσει τον τρόπο με τον οποίο οι επιχειρήσεις επιτυγχάνουν και διατηρούν ανταγωνιστικό πλεονέκτημα σε ραγδαία μεταβαλλόμενα περιβάλλοντα. Ο Teece (2007) ορίζει τις δυναμικές ικανότητες ως την ικανότητα μιας επιχείρησης να ενοποιεί, να δομεί και να αναδιαμορφώνει εσωτερικές και εξωτερικές ικανότητες ώστε να ανταποκρίνεται σε ταχέως εξελισσόμενα περιβάλλοντα. Σε αντίθεση με τις παραδοσιακές υποθέσεις της RBV, οι οποίες δίνουν προτεραιότητα στην ομοιογένεια (homogeneity) και την υποκατάσταση (substitutability) των πόρων, οι δυναμικές ικανότητες αντιμετωπίζουν τη δυναμική πολυπλοκότητα του παγκόσμιου ανταγωνισμού (Dewi et al., 2025).

Ο Teece (2007) διαρθρώνει τις δυναμικές ικανότητες σε τρεις θεμελιώδεις διαστάσεις. Την αίσθηση (sensing), δηλαδή τον εντοπισμό και τη διαμόρφωση ευκαιριών και απειλών, τη σύλληψη (seizing), δηλαδή την αξιοποίηση των ευκαιριών μέσω στρατηγικών επενδύσεων και αποφάσεων, και την αναδιαμόρφωση (reconfiguring), δηλαδή τη συνεχή ανανέωση και αναδιάταξη των υλικών και άυλων πόρων της επιχείρησης. Αυτές οι τρεις διαστάσεις επιτρέπουν στην επιχείρηση να μη βασίζεται αποκλειστικά στο υπάρχον απόθεμα των πόρων, αλλά να αναπτύσσει διαρκώς νέες ικανότητες προσαρμοσμένες στις μεταβαλλόμενες συνθήκες.

Η θεωρία του Teece εδράζεται σε μια βαθύτερη παρατήρηση. Σε περιβάλλοντα υψηλής αβεβαιότητας (high uncertainty environments), η κατοχή πόρων δεν αρκεί. Αυτό που διαφοροποιεί τις επιτυχημένες επιχειρήσεις είναι η ταχύτητα και η ευελιξία (agility) με την οποία εντοπίζουν νέες ευκαιρίες, ανακατανέμουν πόρους και αναδιοργανώνουν ικανότητες. Στο πλαίσιο αυτό, η αίσθηση (sensing) περιλαμβάνει δραστηριότητες όπως η παρακολούθηση των τεχνολογικών εξελίξεων (technology scanning), η ανάλυση των ρυθμιστικών αλλαγών και η κατανόηση των αναδυόμενων αναγκών των πελατών. Η σύλληψη αφορά τη σχεδίαση νέων επιχειρηματικών μοντέλων, τις στρατηγικές επενδύσεις σε τεχνολογίες και ταλέντα, και τη

δημιουργία στρατηγικών συμμαχιών. Η αναδιαμόρφωση αφορά την αναδιάρθρωση των οργανωτικών δομών, την ενοποίηση νέων πόρων και τη δημιουργία μηχανισμών συνεχούς μάθησης.

Εμπειρικές μελέτες σε διάφορους κλάδους επιβεβαιώνουν τη σημασία των δυναμικών ικανοτήτων. Οι Dewi et al. (2025) για παράδειγμα μελετώντας τον κλάδο TIC στην Ινδονησία με δείγμα 208 διευθυντικών στελεχών και 4 εμπειρογνωμόνων, αποδεικνύουν ότι η βιώσιμη ανταγωνιστικότητα τροφοδοτείται θεμελιωδώς από δυναμικές ικανότητες όπως η καινοτομία (innovation), η συνεργατικότητα (collaboration), η ψηφιοποίηση (digitalization), η δέσμευση των πελατών (customer bonding) και η ψηφιακή μετάβαση. Τα εμπειρικά τους ευρήματα δείχνουν ότι η ικανότητα συνεργασίας (collaborative capability) σημείωσε τον υψηλότερο μέσο όρο (5,06), ακολουθούμενη από τις λύσεις πελατών (customer solution and bonding, 5,04) και την ψηφιοποίηση (digitalization capability, 4,92). Αντιθέτως, η ικανότητα της καινοτομίας αναδείχθηκε ως η πιο αδύναμη διάσταση μεταξύ εθνικών επιχειρήσεων (μέσος όρος 3,69 σε κλίμακα 7), γεγονός που υπογραμμίζει την επιτακτική ανάγκη ενίσχυσής της για τη βελτίωση της ανταγωνιστικότητας. Αυτά τα ευρήματα υποδηλώνουν ότι οι επιχειρήσεις που εστιάζουν μονομερώς στην εξωτερική ανάλυση αγοράς, αγνοώντας τη δημιουργία εσωτερικών δυναμικών ικανοτήτων, αντιμετωπίζουν αυξημένο κίνδυνο απώλειας ανταγωνιστικής θέσης.

Η ενοποίηση του μοντέλου των Πέντε Δυνάμεων με τις δυναμικές ικανότητες αποτελεί σημαντική θεωρητική συνεισφορά. Προτείνεται ένα ολοκληρωμένο πλαίσιο στο οποίο οι εξωτερικές δυνάμεις του Porter αλληλεπιδρούν με εσωτερικές δυναμικές ικανότητες. Η ικανότητα της καινοτομίας και η ικανότητα της ψηφιοποίησης συνδέονται με την απειλή νέων εισερχομένων, η ικανότητα εξυπηρέτησης πελατών με τη διαπραγματευτική ισχύ των αγοραστών, και η ικανότητα της συνεργασίας με τη συνολική ανταγωνιστική ένταση.

Στον κλάδο της κυβερνοασφάλειας, η θεωρία των δυναμικών ικανοτήτων αποκτά εξαιρετική πρακτική αξία. Η ταχύτητα της εξέλιξης των κυβερνοαπειλών, η συνεχής αλλαγή του ρυθμιστικού πλαισίου και η εμφάνιση νέων τεχνολογικών λύσεων, όπως η τεχνητή νοημοσύνη (artificial intelligence - AI) και η αρχιτεκτονική της μηδενικής εμπιστοσύνης (Zero Trust architecture), απαιτούν από τις επιχειρήσεις μια αδιάλειπτη διεργασία αίσθησης, σύλληψης και αναδιαμόρφωσης. Μια εταιρεία κυβερνοασφάλειας που αδυνατεί να εντοπίσει εγκαίρως νέες τεχνολογικές τάσεις, να επενδύσει στρατηγικά στη νέα τεχνολογία και να

αναδιοργανώσει τις λειτουργίες της ανάλογα, κινδυνεύει να απωλέσει γρήγορα την ανταγωνιστική της θέση.

Η σύνδεση των δυναμικών ικανοτήτων και της κυβερνοασφάλειας γίνεται ακόμη σαφέστερη εάν εξεταστεί μέσω του πρίσματος της επένδυσης σε ασφάλεια των πληροφοριών. Οι Rowe και Gallaher (2006) διαπίστωσαν ότι οι περισσότεροι οργανισμοί δεν αντιμετωπίζουν τις επενδύσεις σε κυβερνοασφάλεια με την ίδια αυστηρότητα που αντιμετωπίζουν άλλες επενδυτικές αποφάσεις. Αντί για ανάλυση κόστους-οφέλους (cost-benefit analysis) ή καθαρής παρούσας αξίας (Net Present Value - NPV), οι επιχειρήσεις βασίζονται κυρίως σε ποιοτικές αξιολογήσεις, στη γνώση του προσωπικού τεχνολογίας πληροφορικής (IT staff knowledge) και σε αντιδραστικές (reactive) αποφάσεις μετά από παραβιάσεις ασφαλείας (security breaches). Σύμφωνα με τα ευρήματά τους, οι κανονισμοί (regulations) αποτελούν τον πρωταρχικό κινητήριο παράγοντα (driver) της στρατηγικής επένδυσης σε κυβερνοασφάλεια, με μέσο ποσοστό 30,1% μεταξύ των οργανισμών, ακολουθούμενοι από τη γνώση του ιστορικού δικτύων/τεχνολογίας πληροφοριών (18,9%) και τις απαιτήσεις των πελατών (16,2%) (Rowe & Gallaher, 2006). Αυτό το εύρημα αναδεικνύει τον κρίσιμο ρόλο του ρυθμιστικού περιβάλλοντος ως εξωτερικού παράγοντα που τροφοδοτεί τη ζήτηση των υπηρεσιών κυβερνοασφάλειας, ένα θέμα που αναλύεται εκτενώς στο Κεφάλαιο 3.

2.4 Στρατηγικές Εισόδου σε Νέες Αγορές: Τεχνολογική Διαφοροποίηση και Εξαγορές

Όταν μια επιχείρηση αποφασίζει να εισέλθει σε νέο κλάδο ή τομέα δραστηριότητας, οι στρατηγικές επιλογές που έχει στη διάθεσή της περιλαμβάνουν, μεταξύ άλλων, την τεχνολογική διαφοροποίηση και τις εξαγορές και συγχωνεύσεις (mergers and acquisitions - M&A). Η κατανόηση των θεωρητικών υποβάθρων αυτών των στρατηγικών είναι απαραίτητη για την αξιολόγηση των επιχειρηματικών αποφάσεων, όπως η είσοδος μιας εταιρείας τεχνολογίας στον κλάδο της κυβερνοασφάλειας.

2.4.1 Τεχνολογική Διαφοροποίηση (Technological Diversification)

Η τεχνολογική διαφοροποίηση αφορά την επιλογή μιας επιχείρησης να διευρύνει την τεχνολογική της βάση σε ευρύτερο φάσμα τεχνολογικών πεδίων (Ceipek et al., 2020). Ορίζει το εύρος του γνωστικού συστήματος (knowledge system) και των τεχνολογικών ικανοτήτων

μιας επιχείρησης και επηρεάζει την ικανότητά της να συνδυάζει, να ανασυνθέτει και να αφομοιώνει νέα γνώση. Η τεχνολογική διαφοροποίηση επιδρά στη δραστηριότητα της καινοτομίας και στην απόδοση της καινοτομίας, καθώς οδηγεί συχνά σε υψηλότερη ένταση έρευνας και ανάπτυξης και σε αυξημένο αριθμό διπλωμάτων ευρεσιτεχνίας (patents).

Ιδιαίτερη θεωρητική αξία έχει η διάκριση μεταξύ συγγενούς και μη συγγενούς τεχνολογικής διαφοροποίησης. Η συγγενής τεχνολογική διαφοροποίηση αφορά την επέκταση σε τεχνολογικά πεδία που βρίσκονται κοντά στον πυρήνα τεχνογνωσίας (core-field) της επιχείρησης, ενώ η μη συγγενής αφορά την επέκταση σε πεδία μακριά από τον υπάρχοντα τεχνολογικό πυρήνα (broad-field). Η έρευνα δείχνει ότι η μη συγγενής τεχνολογική διαφοροποίηση είναι ιδιαίτερα ριψοκίνδυνη, καθώς η τεχνολογική αβεβαιότητα είναι υψηλή, το κόστος συντονισμού, επικοινωνίας και ενοποίησης αυξάνεται σημαντικά και η συνεχής απομάκρυνση από τον πυρήνα αποδυναμώνει τη γνώση που σχετίζεται με τις βασικές τεχνολογίες.

Αντιθέτως, η συγγενής τεχνολογική διαφοροποίηση μπορεί να ενισχύσει τις ικανότητες εξερεύνησης, καθώς η πρόσβαση σε ποικιλία συγγενών τεχνολογικών πεδίων γνώσης επηρεάζει θετικά την κλίση της επιχείρησης να εντοπίζει νέες λύσεις, μειώνοντας το κόστος της εξερεύνησης και επιταχύνοντας τον εντοπισμό νέων ερευνητικών ευκαιριών. Η διάκριση αυτή έχει άμεση πρακτική σημασία για μια εταιρεία τεχνολογίας που εισέρχεται στον κλάδο της κυβερνοασφάλειας. Εάν η εταιρεία διαθέτει ήδη ικανότητες σε πληροφοριακά συστήματα (information systems), δίκτυα (networks) ή ανάπτυξη λογισμικού (software development), η μετάβαση στην κυβερνοασφάλεια αποτελεί συγγενή τεχνολογική διαφοροποίηση, με χαμηλότερο ρίσκο και μεγαλύτερες πιθανότητες επιτυχίας.

Οι Ceipek et al. (2020) εξετάζουν επίσης τη σχέση μεταξύ της τεχνολογικής διαφοροποίησης και της καινοτομίας μέσα από το πρίσμα της εξερεύνησης έναντι της εκμετάλλευσης. Η εξερεύνηση αναφέρεται στη δημιουργία γνώσης που είναι νέα σε σχέση με την υπάρχουσα γνωστική βάση της επιχείρησης, ενώ η εκμετάλλευση αφορά τη συσσώρευση εμπειρίας εντός ενός ήδη γνωστού γνωστικού πεδίου. Στο πλαίσιο της ψηφιακής μετάβασης, οι δύο αυτές κατευθύνσεις δημιουργούν ένα στρατηγικό δίλημμα. Η εξερεύνηση νέων τεχνολογικών πεδίων ενέχει υψηλότερο ρίσκο αλλά δυνητικά μεγαλύτερη ανταμοιβή, ενώ η εκμετάλλευση της υπάρχουσας τεχνογνωσίας προσφέρει μεγαλύτερη ασφάλεια αλλά περιορισμένες δυνατότητες διαφοροποίησης. Για μια εταιρεία που εισέρχεται στον κλάδο της

κυβερνοασφάλειας μέσω εξαγοράς, η ισορροπία μεταξύ της εξερεύνησης και της εκμετάλλευσης αποτελεί κρίσιμη στρατηγική παράμετρο.

Η σημασία αυτής της ισορροπίας ενισχύεται από τη μελέτη της βιβλιογραφίας σχετικά με την τεχνολογία του Διαδικτύου των Πραγμάτων (Internet of Things - IoT), η οποία αναδεικνύεται παράλληλα με τον κλάδο της κυβερνοασφάλειας. Το IoT, ως τεχνολογία ταχείας εξέλιξης με υψηλή πολυπλοκότητα, ποικιλία τεχνολογιών και πρωτοκόλλων, και ανάγκη συμπληρωματικότητας με πολλαπλές ψηφιακές τεχνολογίες γενικού σκοπού, παρουσιάζει χαρακτηριστικά ανάλογα με αυτά της κυβερνοασφάλειας. Τόσο στη μία όσο και στην άλλη περίπτωση η επιτυχής είσοδος απαιτεί τη διαχείριση ενός πολύπλοκου τεχνολογικού οικοσυστήματος και τη σύζευξη πολλαπλών τεχνολογικών τομέων.

2.4.2 Εξαγορές, Συγχωνεύσεις και Ολοκλήρωση μετά τη Συγχώνευση (M&A και PMI)

Η εξαγορά (acquisition) αποτελεί μία εναλλακτική στρατηγική εισόδου σε νέο κλάδο, η οποία επιτρέπει στην εξαγοράζουσα εταιρεία να αποκτήσει ταχέως πρόσβαση σε τεχνολογικούς πόρους, πελατειακή βάση, εξειδικευμένο ανθρώπινο δυναμικό και τεκμηριωμένη τεχνογνωσία. Η επιτυχία μιας εξαγοράς, ωστόσο, εξαρτάται σε μεγάλο βαθμό από την ολοκλήρωση μετά τη συγχώνευση (Post-Merger Integration - PMI), η οποία αποτελεί ίσως το πιο κρίσιμο στάδιο της όλης διαδικασίας.

Οι Lace και Kirikova (2022) μελετούν τις στρατηγικές ολοκλήρωσης πληροφοριακών συστημάτων (IS integration strategies) μετά από εξαγορά και εντοπίζουν τέσσερις κύριες προσεγγίσεις όπως την απορρόφηση (absorption), κατά την οποία τα συστήματα του εξαγοραζόμενου ενσωματώνονται πλήρως στα συστήματα του αποκτώντος, το συνδυασμό βέλτιστων πρακτικών (best-of-breed), κατά τον οποίο επιλέγονται τα καλύτερα στοιχεία από αμφότερους τους οργανισμούς, τη συνύπαρξη (coexistence), κατά την οποία τα συστήματα λειτουργούν παράλληλα και το σχεδιασμό νέας αρχιτεκτονικής (renewal), κατά τον οποίο δημιουργείται εξαρχής ένα νέο ενοποιημένο σύστημα. Η επιλογή στρατηγικής εξαρτάται από παράγοντες όπως ο βαθμός τεχνολογικής συμβατότητας, η κουλτούρα των οργανισμών και οι στρατηγικοί στόχοι της εξαγοράς.

Η σημασία της τεχνολογίας στη διαδικασία PMI αναδεικνύεται εμφατικά από τη μελέτη της Boston Consulting Group (Milde et al., 2024), η οποία προτείνει ένα μοντέλο τριών

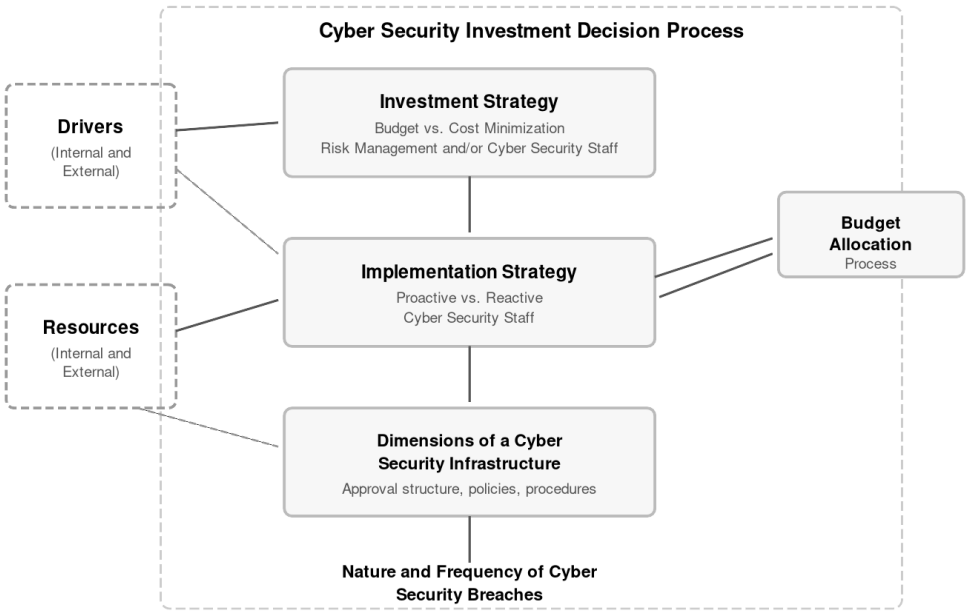
οριζόντων. Ο πρώτος ορίζοντας (Horizon 1, έως 100 ημέρες) εστιάζει στη διασφάλιση της επιχειρησιακής συνέχειας, μέσω της εγκατάστασης κοινών δικτύων, εργαλείων επικοινωνίας και ενιαίων μέτρων κυβερνοασφάλειας. Η μελέτη επισημαίνει ότι οι κυβερνοεπιθέσεις αυξάνονται σημαντικά αμέσως μετά από μια εξαγορά, καθιστώντας την ενοποίηση της ψηφιακής ασφάλειας προτεραιότητα. Ο δεύτερος ορίζοντας (Horizon 2, ημέρα 100 έως έτος 2-3) αφορά την ολοκλήρωση των επιχειρηματικών διαδικασιών και πλατφορμών, ενώ ο τρίτος ορίζοντας (Horizon 3, έτη 2-5) επικεντρώνεται στη στρατηγική φιλοδοξία, δηλαδή στον πλήρη μετασχηματισμό διαδικασιών και ικανοτήτων μέσω τεχνολογίας, τεχνητής νοημοσύνης και ανάλυσης δεδομένων.

Σύμφωνα με τα ευρήματα της BCG, η τεχνολογία και τα δεδομένα (data) οδηγούν άμεσα περίπου το 10% των συνεργειών (synergies) κόστους μιας εξαγοράς, αλλά υποστηρίζουν την υλοποίηση έως και 85% των επιχειρηματικών συνεργειών σε διάφορες κατηγορίες κόστους. Αυτό το εύρημα αναδεικνύει τον κεντρικό ρόλο της τεχνολογικής ολοκλήρωσης στην επιτυχία μιας εξαγοράς και υποστηρίζει τη θέση ότι η PMI δεν αποτελεί απλώς τεχνική διαδικασία αλλά στρατηγική επιταγή.

Ο Usianeneh (2025) εμπλουτίζει τη συζήτηση μελετώντας τους κινδύνους της ολοκλήρωσης μετά τη συγχώνευση σε εξαγορές που σχετίζονται με τεχνολογία. Η μελέτη αναδεικνύει κρίσιμους παράγοντες κινδύνου, όπως τη σύγκρουση εταιρικών κουλτουρών, την ασυμβατότητα τεχνολογικών πλατφορμών, την απώλεια βασικού ανθρώπινου δυναμικού και την υποεκτίμηση της πολυπλοκότητας ολοκλήρωσης. Η αντιμετώπιση αυτών των κινδύνων απαιτεί μεθοδική σχεδίαση, ξεκάθαρη διακυβέρνηση και ευέλικτο χρονοδιάγραμμα ολοκλήρωσης.

Είναι σημαντικό να τονιστεί ότι η επιτυχία μιας εξαγοράς δε μετράται μόνο στο χρηματοοικονομικό πεδίο, αλλά και στο βαθμό στον οποίο η εξαγοράζουσα εταιρεία καταφέρνει να αξιοποιήσει τους πόρους και τις ικανότητες που απέκτησε. Η BCG εκτιμά ότι η επιτυχημένη ολοκλήρωση της τεχνολογίας μπορεί να αποτελέσει στρατηγικό εργαλείο ενεργοποίησης της ανάπτυξης, μέσω διεπαφών προγραμματισμού των εφαρμογών (Application Programming Interfaces - APIs) που επιτρέπουν την απρόσκοπτη ενσωμάτωση με εξωτερικούς παρόχους λογισμικού ως υπηρεσίας (Software-as-a-Service - SaaS) και μέσω κλιμακούμενων εργαλείων που επιτρέπουν τη γρήγορη επώαση νέων τεχνολογιών (Milde et al., 2024). Η οπτική αυτή είναι ιδιαιτέρως συναφής με εξαγορές στον κλάδο της

κυβερνοασφάλειας, όπου η τεχνολογική ολοκλήρωση αποτελεί προϋπόθεση για τη δημιουργία ολοκληρωμένων λύσεων ασφαλείας (integrated security solutions) που προσφέρουν ανταγωνιστικό πλεονέκτημα.



Σχήμα 2.1: Εννοιολογικό μοντέλο αποφάσεων επένδυσης σε κυβερνοασφάλεια
Πηγή: Rowe & Gallaher (2006, Figure 1)

Σχήμα 2.1: Εννοιολογικό μοντέλο αποφάσεων επένδυσης σε κυβερνοασφάλεια (Πηγή: Rowe & Gallaher, 2006, Figure 1)

2.5 Ψηφιακός Μετασχηματισμός και Ανταγωνιστικό Πλεονέκτημα

Ο ψηφιακός μετασχηματισμός αναφέρεται στις θεμελιώδεις αλλαγές που επιφέρει η υιοθέτηση ψηφιακών τεχνολογιών στον τρόπο λειτουργίας, αλληλεπίδρασης με τους πελάτες και ανταγωνιστικής τοποθέτησης των επιχειρήσεων (Agustian et al., 2023). Δεν πρόκειται απλώς για υιοθέτηση νέων εργαλείων, αλλά για ολιστική αναδιάρθρωση (holistic restructuring) των επιχειρηματικών μοντέλων, της εταιρικής κουλτούρας και της στρατηγικής κατεύθυνσης. Η βιβλιογραφία συγκλίνει στη διαπίστωση ότι ο ψηφιακός μετασχηματισμός δεν αποτελεί πλέον επιλογή, αλλά αναγκαιότητα για τη διατήρηση της ανταγωνιστικότητας στη σύγχρονη αγορά.

Η σχέση μεταξύ του ψηφιακού μετασχηματισμού και του ανταγωνιστικού πλεονεκτήματος είναι πολύπλευρη. Οι Agustian et al. (2023) εντοπίζουν πολλαπλούς μηχανισμούς μέσω των οποίων η ψηφιακή τεχνολογία δημιουργεί πλεονέκτημα τη βελτίωση της λειτουργικής αποδοτικότητας μέσω αυτοματισμών και ανάλυσης δεδομένων, τη διαφοροποίηση προϊόντων και υπηρεσιών μέσω εξατομίκευσης και καινοτομίας, την ταχεία ανταπόκριση σε μεταβολές της αγοράς μέσω ανάλυσης δεδομένων σε πραγματικό χρόνο και τη μείωση του λειτουργικού κόστους μέσω ψηφιακής βελτιστοποίησης των διαδικασιών.

Ιδιαίτερο ενδιαφέρον παρουσιάζει η μελέτη των Sihite et al. (2025), οι οποίοι εφαρμόζουν ανάλυση SWOT (Strengths, Weaknesses, Opportunities, Threats) στον ψηφιακό μετασχηματισμό των μικρομεσαίων επιχειρήσεων. Τα ευρήματά τους αναδεικνύουν ότι, ενώ οι ΜΜΕ διαθέτουν εγγενή πλεονεκτήματα όπως η ευελιξία, η ισχυρή σχέση με τους πελάτες και η επιχειρηματική νοοτροπία, αντιμετωπίζουν σημαντικές αδυναμίες σε επίπεδο χρηματοδοτικών πόρων, ψηφιακής υποδομής και ψηφιακών δεξιοτήτων. Στο εξωτερικό περιβάλλον, οι ευκαιρίες περιλαμβάνουν την αυξανόμενη ψηφιακή ζήτηση και τα κυβερνητικά προγράμματα στήριξης, ενώ οι απειλές συμπεριλαμβάνουν τους κινδύνους κυβερνοασφάλειας και τον εντεινόμενο ψηφιακό ανταγωνισμό. Η ανάλυση αυτή είναι ιδιαιτέρως συναφής, καθώς πολλές εταιρείες του ελληνικού κλάδου τεχνολογίας παρουσιάζουν χαρακτηριστικά ΜΜΕ.

Η ανάλυση SWOT, ως εργαλείο στρατηγικής αξιολόγησης, προσφέρει μια δομημένη μεθοδολογία για τη σύνδεση εσωτερικών ικανοτήτων με εξωτερικές συνθήκες. Ο Gurel και Tat (2017) σημειώνουν ότι η SWOT παραμένει αξιόπιστο εργαλείο λόγω της απλότητας, της προσαρμοστικότητας και της ολιστικής προσέγγισής της. Ιδιαίτερα στο πλαίσιο του ψηφιακού μετασχηματισμού, η SWOT βοηθά τους οργανισμούς να αντιληφθούν πώς οι τεχνολογικές εξελίξεις αλληλεπιδρούν με τις εσωτερικές επιχειρηματικές διαδικασίες και το εξωτερικό ανταγωνιστικό τοπίο. Παράλληλα, όταν η SWOT συνδυάζεται με ποσοτικές ή αναλυτικές μεθόδους, αποκτά μεγαλύτερη εγκυρότητα και αξιοπιστία, υπερβαίνοντας τους περιορισμούς της αμιγώς ποιοτικής φύσης της. Στην παρούσα εργασία, η SWOT αξιοποιείται σε συνδυασμό με τις Πέντε Δυνάμεις του Porter, τη VRIO ανάλυση και την ανάλυση μακροπεριβάλλοντος (macro-environment analysis), δημιουργώντας ένα τριγωνοποιημένο (triangulated) αναλυτικό πλαίσιο που παρέχει πολυδιάστατη εικόνα της στρατηγικής θέσης της υπό μελέτη εταιρείας.

Η σχέση μεταξύ του ψηφιακού μετασχηματισμού και των δυναμικών ικανοτήτων αποτελεί ένα ιδιαίτερα γόνιμο πεδίο θεωρητικής σύνθεσης. Οι Sihite et al. (2025) σημειώνουν

ότι, από στρατηγική σκοπιά, ο ψηφιακός μετασχηματισμός ενισχύει τις δυναμικές ικανότητες της επιχείρησης, επιτρέποντάς της να αισθάνεται, να συλλαμβάνει και να μετασχηματίζει ευκαιρίες σε ταχέως εξελισσόμενες αγορές. Οι ΜΜΕ που υιοθετούν ψηφιακά εργαλεία εμφανίζουν συχνά βελτιωμένη αποδοτικότητα, ενισχυμένη ικανοποίηση των πελατών και ισχυρότερη ανταγωνιστική τοποθέτηση. Αυτές οι ευκαιρίες καταδεικνύουν τη σημασία των εργαλείων στρατηγικής αξιολόγησης, ιδίως της SWOT, για τον εντοπισμό των τομέων στους οποίους οι επιχειρήσεις μπορούν να αξιοποιήσουν τα δυνατά τους σημεία ώστε να μεγιστοποιήσουν τα ψηφιακά οφέλη.

Στο ευρύτερο πλαίσιο του ψηφιακού μετασχηματισμού, η εξέλιξη των επιχειρηματικών μοντέλων αποτελεί μια κρίσιμη διάσταση. Οι Agustian et al. (2023) αναδεικνύουν τη μετάβαση από παραδοσιακά μοντέλα εφάπαξ πωλήσεων (one-time sales) σε μοντέλα βασισμένα στη συνδρομή (subscription-based models), η οποία ενισχύει την προβλεψιμότητα των εσόδων (revenue predictability) και τη μακροχρόνια δέσμευση των πελατών (long-term customer retention). Παράλληλα, η ψηφιακή τεχνολογία ανοίγει δρόμους για την επέκταση σε παγκόσμιες αγορές μέσω του ηλεκτρονικού εμπορίου (e-commerce), της ψηφιακής διαφήμισης και των διασυνοριακών συνεργασιών.

Πέρα από τις ευκαιρίες, ο ψηφιακός μετασχηματισμός απαιτεί σημαντικές αρχικές επενδύσεις σε τεχνολογική υποδομή, εκπαίδευση προσωπικού και αλλαγή της εταιρικής κουλτούρας. Οι Agustian et al. (2023) τονίζουν ότι οι επενδύσεις αυτές δεν πρέπει να αντιμετωπίζονται ως κόστος, αλλά ως μακροπρόθεσμη επένδυση σε ανταγωνιστικότητα. Η ψηφιακή τεχνολογία μεταβάλλει θεμελιωδώς τον τρόπο λειτουργίας και αλληλεπίδρασης με τους πελάτες, επηρεάζοντας δυνητικά ολόκληρο το επιχειρηματικό μοντέλο. Για αυτόν τον λόγο, οι επιχειρήσεις οφείλουν να διαθέτουν σαφές όραμα για τους μακροπρόθεσμους στόχους του ψηφιακού μετασχηματισμού και να αναπτύξουν ολοκληρωμένη στρατηγική για την επίτευξή τους.

Η σημασία του ανθρώπινου κεφαλαίου στον ψηφιακό μετασχηματισμό αναδεικνύεται ως κρίσιμος παράγοντας επιτυχίας. Οι εργαζόμενοι χρειάζονται δεξιότητες ψηφιακού εγγραμματισμού, αναλυτικής ικανότητας και προσαρμοστικότητας ώστε να αξιοποιήσουν αποτελεσματικά τις νέες τεχνολογίες. Αυτή η απαίτηση συνδέεται άμεσα με τον κλάδο της κυβερνοασφάλειας, ο οποίος αντιμετωπίζει παγκοσμίως σημαντικό έλλειμμα εξειδικευμένου προσωπικού (skills gap).

Ωστόσο, ο ψηφιακός μετασχηματισμός δε στερείται προκλήσεων. Η κυβερνοασφάλεια αναδεικνύεται ως μια από τις σημαντικότερες απειλές, καθώς η αυξανόμενη ψηφιοποίηση δημιουργεί νέες ευπάθειες και εκθέτει τις επιχειρήσεις σε κυβερνοεπιθέσεις. Παράλληλα, η αβεβαιότητα σχετικά με τη ρυθμιστική συμμόρφωση, ιδίως σε τομείς όπως η προστασία των δεδομένων και η ψηφιακή φορολόγηση, αποτελεί πρόσθετη πρόκληση. Αυτή η σχέση μεταξύ του ψηφιακού μετασχηματισμού και της κυβερνοασφάλειας δημιουργεί μια αυτοτροφοδοτούμενη δυναμική. Όσο περισσότερο ψηφιοποιούνται οι οργανισμοί, τόσο μεγαλύτερη γίνεται η ανάγκη για υπηρεσίες κυβερνοασφάλειας, γεγονός που επεκτείνει συνεχώς την αγορά για τους παρόχους τέτοιων υπηρεσιών. Τα στοιχεία δείχνουν ότι η αυξανόμενη πολυπλοκότητα των ψηφιακών συστημάτων, σε συνδυασμό με την κλιμακούμενη εξέλιξη (sophistication) των κυβερνοαπειλών, δημιουργεί μια αγορά με δομικά υψηλή ζήτηση και σημαντικές προοπτικές ανάπτυξης.

Σε αυτό το πλαίσιο, η βέλτιστη κατανομή των επενδύσεων σε κυβερνοασφάλεια αποτελεί κρίσιμη στρατηγική απόφαση. Οι Mazzoccoli και Naldi (2022) αναπτύσσουν μοντέλα βελτιστοποίησης των επενδύσεων σε κυβερνοασφάλεια σε βάθος χρόνου, υποστηρίζοντας ότι η δυναμική φύση των κυβερνοαπειλών απαιτεί αντίστοιχα δυναμικές στρατηγικές επένδυσης. Σε αντίθεση με τα στατικά μοντέλα, τα οποία αντιμετωπίζουν την επένδυση σε ασφάλεια ως εφάπαξ απόφαση, τα δυναμικά μοντέλα λαμβάνουν υπόψη την εξέλιξη των απειλών, τη φθορά των υφιστάμενων μέτρων ασφαλείας και τη χρονική αξία του χρήματος. Η θεωρητική αυτή προσέγγιση ενισχύει τη σημασία των δυναμικών ικανοτήτων στον κλάδο κυβερνοασφάλειας. Η ικανότητα μιας επιχείρησης να αναπροσαρμόζει συνεχώς την επενδυτική της στρατηγική σε ασφάλεια αποτελεί αυτή καθαυτή δυναμική ικανότητα, που αντανακλά τον κύκλο αίσθησης-σύλληψης-αναδιαμόρφωσης του Teece (2007).

Η βιβλιογραφία αναδεικνύει επίσης τη σημασία της οργανωτικής ευελιξίας ως ανταγωνιστικού πλεονεκτήματος στο πλαίσιο του ψηφιακού μετασχηματισμού. Οι Agustian et al. (2023) τονίζουν ότι οι εταιρείες που έχουν υλοποιήσει επιτυχώς τον ψηφιακό μετασχηματισμό διαθέτουν σημαντικά μεγαλύτερη ικανότητα προσαρμογής στις αλλαγές του περιβάλλοντος. Η προσαρμοστική υποδομή πληροφορικής (adaptive IT infrastructure), η ευέλικτη εταιρική κουλτούρα και η ικανότητα αξιοποίησης δεδομένων για λήψη αποφάσεων σε πραγματικό χρόνο (real-time data-driven decision making) αποτελούν βασικά χαρακτηριστικά αυτής της ευελιξίας. Για τις εταιρείες που δραστηριοποιούνται ή εισέρχονται στον κλάδο της κυβερνοασφάλειας, αυτή η ευελιξία αποκτά διττή σημασία. Αφενός ως

εσωτερική ικανότητα που ενισχύει τη δική τους ανταγωνιστικότητα, αφετέρου ως υπηρεσία που μπορούν να προσφέρουν στους πελάτες τους, βοηθώντας τους να αντιμετωπίσουν τις προκλήσεις του ψηφιακού μετασχηματισμού τους.

2.6 Σύνδεση Θεωρητικού Πλαισίου με την Παρούσα Έρευνα

Η βιβλιογραφική επισκόπηση αναδεικνύει ένα σύνολο αλληλοσυμπληρούμενων θεωρητικών εργαλείων τα οποία, σε συνδυασμό, παρέχουν ένα ολοκληρωμένο αναλυτικό πλαίσιο για τη μελέτη στρατηγικών αποφάσεων στον κλάδο της κυβερνοασφάλειας.

Το μοντέλο των Πέντε Δυνάμεων του Porter αποτελεί τη βάση για την κατανόηση της εξωτερικής δομής του κλάδου, εντοπίζοντας τις πηγές ανταγωνιστικής πίεσης και τους παράγοντες ελκυστικότητας. Η RBV και η ανάλυση VRIO παρέχουν τα εργαλεία για την αξιολόγηση των εσωτερικών πόρων μιας εταιρείας και τον προσδιορισμό των πηγών βιώσιμου ανταγωνιστικού πλεονεκτήματος. Η θεωρία των δυναμικών ικανοτήτων εξηγεί τον τρόπο με τον οποίο οι επιχειρήσεις μπορούν να προσαρμόσουν και να ανανεώσουν τους πόρους τους σε ένα ραγδαία εξελισσόμενο περιβάλλον. Η θεωρία της τεχνολογικής διαφοροποίησης και η βιβλιογραφία των εξαγορών και PMI προσφέρουν το αναλυτικό υπόβαθρο για την κατανόηση των στρατηγικών εισόδου σε νέες αγορές. Τέλος, η σχέση μεταξύ ψηφιακού μετασχηματισμού και ανταγωνιστικού πλεονεκτήματος αναδεικνύει τη δυναμική του κλάδου κυβερνοασφάλειας ως πεδίου ανάπτυξης.

Η αλληλοσυμπληρωματικότητα αυτών των θεωρητικών πλαισίων μπορεί να απεικονιστεί ως εξής: το μοντέλο Porter λειτουργεί ως φακός για το εξωτερικό περιβάλλον, η RBV/VRIO ως φακός για τους εσωτερικούς πόρους, οι δυναμικές ικανότητες ως μηχανισμός σύνδεσης εσωτερικών και εξωτερικών παραγόντων σε συνθήκες αβεβαιότητας, η θεωρία τεχνολογικής διαφοροποίησης ως πλαίσιο αξιολόγησης κινδύνου εισόδου σε νέα τεχνολογικά πεδία, και η βιβλιογραφία PMI ως πρακτικός οδηγός για τη μετασυγχωνευτική ολοκλήρωση. Η σύνθεση αυτή ανταποκρίνεται στην πρόταση των Dewi et al. (2025) για ένα ολοκληρωμένο πλαίσιο ανταγωνιστικότητας που συνδυάζει την ανάλυση εξωτερικών δυνάμεων με εσωτερικές δυναμικές ικανότητες.

Παράλληλα, η βιβλιογραφία αναδεικνύει ορισμένα κοινά νήματα που διατρέχουν τα επιμέρους θεωρητικά πλαίσια. Πρώτον, η σημασία της στρατηγικής ευθυγράμμισης μεταξύ εσωτερικών ικανοτήτων και εξωτερικών απαιτήσεων αναγνωρίζεται σε όλα τα πλαίσια.

Δεύτερον, ο ρόλος της τεχνολογίας ως πηγή τόσο ευκαιριών όσο και απειλών αποτελεί κεντρικό θέμα, ιδίως στο πλαίσιο του ψηφιακού μετασχηματισμού. Τρίτον, η ανάγκη για δυναμική προσαρμογή αναγνωρίζεται ευρέως ως κρίσιμος παράγοντας επιτυχίας σε κλάδους υψηλής τεχνολογίας. Τα κοινά αυτά νήματα ενισχύουν τη συνοχή του αναλυτικού πλαισίου και τη δυνατότητα εφαρμογής του σε μια πραγματική μελέτη περίπτωσης.

Βιβλιογραφία Κεφαλαίου

1. Agustian, K., Mubarok, E. S., Zen, A., Wiwin, & Malik, A. J. (2023). The impact of digital transformation on business models and competitive advantage. *Technology and Society Perspectives (TACIT), 1*(2), 79–93. https://doi.org/10.61100/tacit.v1i2.55

2. Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99–120. https://doi.org/10.1177/014920639101700108

3. Ceipek, R., Hautz, J., De Massis, A., Matzler, K., & Ardito, L. (2020). Digital transformation through exploratory and exploitative Internet of Things innovations: The impact of family management and technological diversification. *Journal of Product Innovation Management, 38*(1), 142–165. https://doi.org/10.1111/jpim.12551

4. Dewi, H., Huseini, M., & Atmoko, A. W. (2025). Strategic competitiveness framework for Indonesian TIC companies: Integrating Porter's Five Forces and dynamic capabilities in the global market. *Qubahan Academic Journal, 5*(3). https://doi.org/10.48161/qaj.v5n3a1982

5. Gurel, E., & Tat, M. (2017). SWOT analysis: A theoretical review. *The Journal of International Social Research, 10*(51), 994–1006.

6. Lace, K., & Kirikova, M. (2022). Pre-evaluation of post-merger information system integration strategies. *Procedia Computer Science, 200*, 298–308.

7. Mazzoccoli, A., & Naldi, M. (2022). Optimizing cybersecurity investments over time. *Algorithms, 15*(7), 211. https://doi.org/10.3390/algorithms15070211

8. Milde, J., Govers, J., Barrett, C., & Di Vittorio, C. (2024). *Technology's central role in post-merger integration*. Boston Consulting Group.

9. Porter, M. E. (1980). *Competitive strategy: Techniques for analyzing industries and competitors*. Free Press.

10. Porter, M. E. (2008). The five competitive forces that shape strategy. *Harvard Business Review, 86*(1), 78–93.

11. Rowe, B. R., & Gallaher, M. P. (2006). *Private sector cyber security investment strategies: An empirical analysis* (NIST GCR 06-885). RTI International.

12. Sihite, M., Suparwata, D. O., Arafah, M. N., & Uhai, S. (2025). SWOT analysis of the strategy of digital transformation of SMEs. *International Journal of Business and Life Economics, 6*(2).

13. Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal, 28*(13), 1319–1350. https://doi.org/10.1002/smj.640

14. Usianeneh, K. E. (2025). *Increase successful outcomes with technology-driven mergers and acquisitions: Prioritize post-merger integration risk mitigation* [Doctoral dissertation, University of Alabama in Huntsville].

Κεφάλαιο 3

Το Οικοσύστημα της Κυβερνοασφάλειας

3.1 Το Παγκόσμιο Τοπίο των Κυβερνοαπειλών

Η κυβερνοασφάλεια (cybersecurity) έχει μετατραπεί από ένα τεχνικό ζήτημα πληροφορικής σε κεντρικό στρατηγικό πυλώνα για κράτη, οργανισμούς και επιχειρήσεις παγκοσμίως. Η επιτάχυνση του ψηφιακού μετασχηματισμού, η εκτεταμένη υιοθέτηση του υπολογιστικού νέφους, η ενσωμάτωση του Διαδικτύου των Πραγμάτων, καθώς και η εξάπλωση της τηλεργασίας μετά την πανδημία COVID-19 έχουν διευρύνει δραματικά τις επιθέσεις των σύγχρονων ψηφιακών υποδομών. Σύμφωνα με την έκθεση IBM Cost of a Data Breach Report 2024, το μέσο παγκόσμιο κόστος μίας παραβίασης δεδομένων (data breach) ανήλθε σε 4,88 εκατομμύρια δολάρια, σημειώνοντας τη μεγαλύτερη ετήσια αύξηση μετά την πανδημία (IBM, 2024). Αντίστοιχα, η έκθεση του 2025 κατέγραψε κόστος 10,22 εκατομμυρίων δολαρίων για εταιρείες στις Ηνωμένες Πολιτείες, ενώ ο μέσος παγκόσμιος όρος διαμορφώθηκε στα 4,44 εκατομμύρια δολάρια (IBM, 2025). Τα στοιχεία αυτά καταδεικνύουν ότι οι κυβερνοεπιθέσεις δε συνιστούν απλώς τεχνολογικά συμβάντα, αλλά γεγονότα με ουσιαστικές οικονομικές, λειτουργικές και νομικές συνέπειες.

Η Έκθεση του «Threat Landscape» του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (European Union Agency for Cybersecurity, ENISA) για το 2025 ανέλυσε 4.875 συμβάντα κατά την περίοδο Ιουλίου 2024 έως Ιουνίου 2025 (ENISA, 2025). Από αυτά, οι επιθέσεις κατανεμημένης άρνησης υπηρεσιών (Distributed Denial-of-Service, DDoS) αντιπροσώπευαν το 76,7% των συμβάντων, κυρίως από ομάδες χακτιβισμού (hacktivism). Το ηλεκτρονικό ψάρεμα (phishing) παρέμεινε η κύρια μέθοδος αρχικής εισβολής (initial intrusion), ευθυνόμενο για το 60% των περιπτώσεων, ενώ η εκμετάλλευση ευπαθειών αντιστοιχούσε στο 21,3%. Ιδιαίτερα ανησυχητικό είναι ότι, σύμφωνα με την ίδια έκθεση, πάνω από το 80% των μηνυμάτων του ηλεκτρονικού ψαρέματος μεταξύ Σεπτεμβρίου 2024 και Φεβρουαρίου 2025 χρησιμοποιούσαν τεχνητή νοημοσύνη, γεγονός που καταδεικνύει τη ραγδαία εξέλιξη των τεχνικών των κυβερνοεγκληματιών.

Η συστηματική επισκόπηση της βιβλιογραφίας των Haque et al. (2025), η οποία ανέλυσε 87 δημοσιεύσεις μεταξύ 2014 και 2024, αναδεικνύει ότι η διαχείριση των κινδύνων κυβερνοασφάλειας στην εποχή του ψηφιακού μετασχηματισμού αντιμετωπίζει πολυεπίπεδες προκλήσεις. Οι τεχνικοί κίνδυνοι που αφορούν αδυναμίες λογισμικού, υλικού και διαμόρφωσης των δικτύων, συνυπάρχουν με τους ανθρωποκεντρικούς κινδύνους. Σύμφωνα με την αναφορά Verizon Data Breach Investigations Report 2023, το 74% των παραβιάσεων οφείλεται σε ανθρώπινους παράγοντες, όπως κοινωνική μηχανική, αδύναμοι κωδικοί πρόσβασης και ακούσια διαρροή των δεδομένων. Επιπλέον, οι κίνδυνοι της αλυσίδας εφοδιασμού και τρίτων μερών αποτελούν ταχύτατα αναπτυσσόμενη κατηγορία, όπως κατέδειξαν τα περιστατικά SolarWinds (2020) και MOVEit (2023), τα οποία αποκάλυψαν ότι ακόμη και οργανισμοί με υψηλό επίπεδο ασφάλειας μπορούν να πληγούν μέσω ευπαθειών στους προμηθευτές τους.

Η παγκόσμια αγορά της κυβερνοασφάλειας αντικατοπτρίζει αυτή τη δυναμική. Σύμφωνα με εκτιμήσεις της Fortune Business Insights, το μέγεθος της αγοράς ανέρχεται σε περίπου 219 δισεκατομμύρια δολάρια για το 2025, με προβολή στα 248 δισεκατομμύρια δολάρια για το 2026 (Fortune Business Insights, 2025). Η Gartner εκτιμά ότι οι παγκόσμιες δαπάνες των τελικών χρηστών σε ασφάλεια πληροφοριών θα φτάσουν τα 213 δισεκατομμύρια δολάρια το 2025, με αύξηση 12,5% το 2026 στα 240 δισεκατομμύρια (Gartner, 2025). Η διαρκής αυτή ανοδική τάση δεν αντανακλά μόνο την κλιμάκωση των απειλών, αλλά και τη σταδιακή αναγνώριση από τις διοικήσεις ότι η κυβερνοασφάλεια αποτελεί στρατηγική επένδυση και όχι απλώς λειτουργικό κόστος.

Η τομεακή διάσταση των κυβερνοαπειλών αποτελεί ιδιαίτερα σημαντική παράμετρο. Ο κλάδος της υγειονομικής περίθαλψης (healthcare) παραμένει ο πλέον επιβαρυμένος για δεκατέσσερα συναπτά έτη, με μέσο κόστος παραβίασης 7,42 εκατομμύρια δολάρια, παρά τη μείωση 24% σε ετήσια βάση. Ο βιομηχανικός τομέας κατέγραψε μέσο κόστος 5,56 εκατομμυρίων δολαρίων, αύξηση 18% σε σχέση με το 2023. Οι κρίσιμες υποδομές αποτελούν ιδιαίτερα ελκυστικό στόχο, καθώς η εταιρεία ασφάλειας των βιομηχανικών συστημάτων Dragos κατέγραψε αύξηση 300% στις επιθέσεις λογισμικού εκβιασμού (ransomware) εναντίον βιομηχανικών συστημάτων ελέγχου (Industrial Control Systems, ICS), ενώ η ENISA προειδοποιεί ότι τα δίκτυα 5G εισάγουν νέες και ελάχιστα κατανοητές επιφάνειες επίθεσης μέσω αρχιτεκτονικών τεμαχισμού του δικτύου (Haque et al., 2025). Αξίζει να σημειωθεί ότι ο μέσος χρόνος εντοπισμού και περιορισμού μίας παραβίασης μειώθηκε σε 241 ημέρες το 2025,

φτάνοντας σε χαμηλό εννέα ετών, γεγονός που αποδίδεται εν μέρει στη χρήση εργαλείων τεχνητής νοημοσύνης για ανίχνευση (IBM, 2025).

3.2 Το Ευρωπαϊκό Ρυθμιστικό Πλαίσιο

Η Ευρωπαϊκή Ένωση έχει αναπτύξει ένα πολυεπίπεδο ρυθμιστικό πλαίσιο που αποτελεί παγκοσμίως ένα από τα πιο ολοκληρωμένα νομοθετικά οικοδομήματα στον τομέα της κυβερνοασφάλειας. Το πλαίσιο αυτό εξελίσσεται συνεχώς, αντανακλώντας τη δυναμική φύση των κυβερνοαπειλών και τις γεωπολιτικές ανακατατάξεις. Όπως επισημαίνει ο Gauthier-Maxence (2024), η αρχιτεκτονική αυτή στηρίζεται σε τρεις θεμελιώδεις πυλώνες, την ασφάλεια των δικτύων και των πληροφοριών, την πιστοποίηση της κυβερνοασφάλειας και τη ρύθμιση συγκεκριμένων τομέων υψηλού κινδύνου, όπως ο χρηματοπιστωτικός τομέας.

Η κατανόηση αυτού του πλαισίου είναι ζωτικής σημασίας για κάθε εταιρεία που δραστηριοποιείται ή σκοπεύει να δραστηριοποιηθεί στην κυβερνοασφάλεια εντός της ΕΕ, καθώς ο κανονιστικός χάρτης (regulatory map) καθορίζει τόσο τις υποχρεώσεις όσο και τις εμπορικές ευκαιρίες. Οι ρυθμίσεις δε λειτουργούν μεμονωμένα, αλλά αλληλοσυμπληρώνονται, δημιουργώντας ένα πολυεπίπεδο σύστημα απαιτήσεων που αφορά ταυτόχρονα τη γενική ασφάλεια των δικτύων, τις τομεακές απαιτήσεις, την πιστοποίηση των προϊόντων και την προστασία των δεδομένων.

3.2.1 Οδηγία NIS2 (EU 2022/2555)

Η Οδηγία NIS2 (Network and Information Security Directive 2) αποτελεί τον ακρογωνιαίο λίθο της ευρωπαϊκής στρατηγικής κυβερνοασφάλειας. Εγκρίθηκε τον Δεκέμβριο 2022 και αντικατέστησε την αρχική Οδηγία NIS (2016/1148), επεκτείνοντας σημαντικά τόσο το πεδίο εφαρμογής (scope) όσο και τις υποχρεώσεις των οντοτήτων. Σύμφωνα με τους Castiglione et al. (2025), η NIS2 καλύπτει πλέον 18 τομείς της οικονομίας, διακρίνοντας μεταξύ ουσιωδών οντοτήτων (essential entities) και σημαντικών οντοτήτων (important entities). Οι ερευνητές ανέπτυξαν μάλιστα ένα σημασιολογικό μοντέλο οντολογίας, το NIS2Onto, για την αυτοματοποίηση και διευκόλυνση της αξιολόγησης συμμόρφωσης, αναγνωρίζοντας ότι η πολυπλοκότητα της Οδηγίας καθιστά αναγκαία τη χρήση τεχνολογικών εργαλείων για τη συστηματική εφαρμογή της.

Η NIS2 εισάγει αυστηρότερες υποχρεώσεις για τη διαχείριση των κινδύνων, τη γνωστοποίηση των συμβάντων εντός 24 ωρών και 72 ωρών, και την ασφάλεια της αλυσίδας εφοδιασμού. Σημαντική καινοτομία αποτελεί η προσωπική ευθύνη των μελών της ανώτατης διοίκησης για τη μη συμμόρφωση, καθώς και η δυνατότητα επιβολής προστίμων που μπορούν να φτάσουν τα 10 εκατομμύρια ευρώ ή το 2% του παγκόσμιου κύκλου εργασιών για τις ουσιώδεις οντότητες (Gauthier-Maxence, 2024). Η Οδηγία εισάγει επίσης το πλαίσιο EU-CyCLONe (European Cyber Crisis Liaison Organisation Network) για τη συντονισμένη διαχείριση μεγάλης κλίμακας κυβερνοπεριστατικών σε επίπεδο ένωσης, ενισχύοντας τη διακρατική συνεργασία (Virag, 2025).

3.2.2 Κανονισμός DORA (EU 2022/2554)

Ο Κανονισμός DORA (Digital Operational Resilience Act) στοχεύει ειδικά στο χρηματοπιστωτικό τομέα (financial sector), ο οποίος σύμφωνα με την IBM (2024) παρουσιάζει μέσο κόστος παραβίασης 6,08 εκατομμυρίων δολαρίων, 22% υψηλότερο από τον παγκόσμιο μέσο όρο. Ο DORA θεσπίζει ενιαίες απαιτήσεις λειτουργικής ψηφιακής ανθεκτικότητας για χρηματοπιστωτικά ιδρύματα, ασφαλιστικές εταιρείες και παρόχους υπηρεσιών πληροφορικής. Όπως αναλύει ο Gauthier-Maxence (2024), ο DORA απαιτεί τη διενέργεια τακτικών δοκιμών ανθεκτικότητας, τη διαχείριση κινδύνων τρίτων μερών και τη δημιουργία μηχανισμών ανταλλαγής πληροφοριών απειλών μεταξύ χρηματοπιστωτικών οντοτήτων. Ο Κανονισμός τέθηκε σε πλήρη εφαρμογή τον Ιανουάριο 2025 και αναμένεται να αναβαθμίσει σημαντικά την κυβερνοανθεκτικότητα ενός τομέα που αποτελεί πρωταρχικό στόχο κυβερνοεπιθέσεων παγκοσμίως. Για τις εταιρείες πληροφορικής που παρέχουν υπηρεσίες σε χρηματοπιστωτικά ιδρύματα, ο DORA δημιουργεί πρόσθετες υποχρεώσεις ως πάροχοι κρίσιμων υπηρεσιών τρίτων (critical third-party providers), καθώς ο Κανονισμός θεσπίζει ενιαίο ευρωπαϊκό πλαίσιο εποπτείας (oversight framework) για τους σημαντικούς παρόχους υπηρεσιών τεχνολογιών πληροφοριών και επικοινωνιών (ICT service providers).

3.2.3 Κανονισμός Κυβερνοασφάλειας (Cybersecurity Act, EU 2019/881) και Πράξη Κυβερνοανθεκτικότητας (Cyber Resilience Act)

Ο Κανονισμός Κυβερνοασφάλειας (Cybersecurity Act) του 2019 θεσμοθέτησε το μόνιμο ρόλο του ENISA και δημιούργησε το ευρωπαϊκό πλαίσιο πιστοποίησης κυβερνοασφάλειας (European Cybersecurity Certification Framework), μέσω του οποίου

προϊόντα, υπηρεσίες και διαδικασίες τεχνολογιών πληροφορικής μπορούν να πιστοποιηθούν σε τρία επίπεδα εμπιστοσύνης: βασικό (basic), ουσιαστικό (substantial) και υψηλό (high) (Gauthier-Maxence, 2024). Η Πράξη Κυβερνοανθεκτικότητας (Cyber Resilience Act, CRA), η οποία εγκρίθηκε το 2024, συμπληρώνει αυτό το πλαίσιο θεσπίζοντας υποχρεωτικές απαιτήσεις ασφάλειας για προϊόντα με ψηφιακά στοιχεία (products with digital elements) καθ' όλη τη διάρκεια του κύκλου ζωής τους. Ο Virag (2025) εντοπίζει ότι η CRA αντιμετωπίζει ένα κρίσιμο κενό, καθώς το 90% των κυβερνοεπιθέσεων εκμεταλλεύεται ευπάθειες λογισμικού που θα μπορούσαν να είχαν αποτραπεί μέσω ασφαλούς σχεδίασης (secure by design).

3.2.4 Γενικός Κανονισμός Προστασίας των Δεδομένων (GDPR) και Κανονισμός Τεχνητής Νοημοσύνης (AI Act)

Ο Γενικός Κανονισμός Προστασίας των Δεδομένων (General Data Protection Regulation, GDPR), αν και πρωτίστως κανονισμός προστασίας προσωπικών δεδομένων (data protection), συνιστά αναπόσπαστο μέρος του οικοσυστήματος της κυβερνοασφάλειας. Το Άρθρο 32 του GDPR απαιτεί κατάλληλα τεχνικά και οργανωτικά μέτρα, ενώ η μη συμμόρφωση μπορεί να οδηγήσει σε πρόστιμα έως 20 εκατομμύρια ευρώ ή 4% του παγκόσμιου κύκλου εργασιών. Οι Haque et al. (2025) επισημαίνουν ότι η ρυθμιστική πίεση αποτελεί βασικό κινητήριο μοχλό για τη βελτίωση των πρακτικών κυβερνοασφάλειας, αν και η διασυνοριακή εφαρμογή παραμένει ασυνεπής.

Ο Κανονισμός Τεχνητής Νοημοσύνης (AI Act, EU 2024/1689), ο πρώτος ολοκληρωμένος κανονισμός για την τεχνητή νοημοσύνη παγκοσμίως, εισάγει μία ταξινόμηση βάσει κινδύνου (risk-based classification) για τα συστήματα τεχνητής νοημοσύνης. Όπως αναλύει ο Gauthier-Maxence (2024), ο Κανονισμός αυτός διασταυρώνεται με την κυβερνοασφάλεια σε πολλαπλά επίπεδα. Αφενός τα συστήματα τεχνητής νοημοσύνης υψηλού κινδύνου πρέπει να πληρούν αυστηρές απαιτήσεις ασφάλειας και ανθεκτικότητας, αφετέρου η ίδια η τεχνητή νοημοσύνη χρησιμοποιείται ολοένα και περισσότερο τόσο για επιθετικούς σκοπούς (π.χ. δημιουργία πολυμορφικού κακόβουλου λογισμικού) όσο και για αμυντικούς σκοπούς (π.χ. ανίχνευση ανωμαλιών). Η αλληλοεπικάλυψη αυτή καθιστά αναγκαία μία ολιστική προσέγγιση της ρύθμισης, κάτι που αναγνωρίζεται ρητά στον AI Act μέσω των παραπομπών στην Οδηγία NIS2 και στον Κανονισμό DORA. Για τις εταιρείες κυβερνοασφάλειας, η αλληλοσύνδεση αυτών των κανονισμών δημιουργεί ζήτηση για

ολοκληρωμένες υπηρεσίες συμμόρφωσης που καλύπτουν ταυτόχρονα πολλαπλές ρυθμιστικές απαιτήσεις, αντί αποσπασματικών λύσεων για κάθε κανονισμό χωριστά.

3.2.5 Ο Ρόλος του ENISA και η Ευρωπαϊκή Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας

Ο ENISA διαδραματίζει κεντρικό ρόλο στο ευρωπαϊκό οικοσύστημα κυβερνοασφάλειας, λειτουργώντας ως κέντρο τεχνογνωσίας (expertise hub) και συντονισμού μεταξύ κρατών-μελών. Πέρα από την ετήσια Έκθεση του Τοπίου Απειλών, ο ENISA ανέπτυξε το Ευρωπαϊκό Πλαίσιο Δεξιοτήτων Κυβερνοασφάλειας (European Cybersecurity Skills Framework, ECSF), το οποίο σύμφωνα με τους Almeida (2025) αποτελεί ένα από τα δέκα κύρια πλαίσια δεξιοτήτων κυβερνοασφάλειας στην Ευρώπη. Η ανάλυσή τους αποκαλύπτει ότι, ενώ υπάρχει πληθώρα πλαισίων δεξιοτήτων, τα περισσότερα παρουσιάζουν σημαντικά κενά στη σύνδεση μεταξύ στρατηγικών στόχων και πρακτικής εφαρμογής. Αυτό επιβεβαιώνεται από τον Virag (2025), ο οποίος εντοπίζει 14 συστημικά κενά (systematic gaps) στην ικανότητα κυβερνοχωρητικότητας (cyber capacity-building) της ΕΕ, μεταξύ των οποίων η ανεπαρκής στρατηγική νοημοσύνη του εργατικού δυναμικού, η απουσία τυποποιημένων δεικτών αποτελεσματικότητας και η αδύναμη ενσωμάτωση μη τεχνικών κυβερνοδεξιοτήτων στα εκπαιδευτικά προγράμματα.

Το έλλειμμα δεξιοτήτων αποτελεί κρίσιμη παράμετρο του ευρωπαϊκού οικοσυστήματος. Σύμφωνα με στοιχεία του (ISC)², το παγκόσμιο χάσμα του εργατικού δυναμικού στην κυβερνοασφάλεια ανήλθε σε 4,8 εκατομμύρια επαγγελματίες το 2024, παρά το γεγονός ότι το συνολικό εργατικό δυναμικό της κυβερνοασφάλειας αυξήθηκε στα 5,5 εκατομμύρια (Virag, 2025). Η ΕΕ ανταποκρίθηκε στο πρόβλημα αυτό με τη δημιουργία της Ευρωπαϊκής Ακαδημίας Δεξιοτήτων Κυβερνοασφάλειας (European Cybersecurity Skills Academy) και το πρόγραμμα Ψηφιακή Ευρώπη (Digital Europe Programme), αν και ο Virag (2025) αξιολογεί ότι τα μέτρα αυτά παραμένουν αποσπασματικά και χωρίς ενιαίο μηχανισμό παρακολούθησης αποτελεσματικότητας.

Οι Almeida (2025) εντοπίζουν ότι τα δέκα κύρια πλαίσια δεξιοτήτων κυβερνοασφάλειας στην Ευρώπη, μεταξύ των οποίων το ECSF, το CyBOK (Cyber Security Body of Knowledge), το e-CF (e-Competence Framework) και το πλαίσιο του ECSO (European Cyber Security Organisation), παρουσιάζουν σημαντική αλληλοεπικάλυψη σε ορισμένους τομείς αλλά και κρίσιμα κενά σε άλλους, ιδίως στις μη τεχνικές δεξιότητες όπως η

ηγεσία της κυβερνοασφάλειας, η επικοινωνία των κινδύνων και η οργανωσιακή ανθεκτικότητα. Η κατακερματισμένη αυτή κατάσταση δυσχεραίνει τόσο την εκπαίδευση νέων επαγγελματιών όσο και τη σύνδεση μεταξύ ακαδημαϊκών προγραμμάτων και αναγκών της αγοράς εργασίας.

3.3 Το Ελληνικό Θεσμικό Πλαίσιο Κυβερνοασφάλειας

Η Ελλάδα ακολούθησε μία διαδρομή ψηφιακού μετασχηματισμού που, σύμφωνα με την Pattergiannaki (2023), χαρακτηρίστηκε από χρόνιες καθυστερήσεις στην εφαρμογή ευρωπαϊκών στρατηγικών ηλεκτρονικής διακυβέρνησης (e-Government). Ωστόσο, τα τελευταία έτη παρατηρείται εντυπωσιακή επιτάχυνση, ιδίως μετά τη σύσταση του Υπουργείου Ψηφιακής Διακυβέρνησης (Ministry of Digital Governance) το 2019 και τη θεσμοθέτηση ενός ολοκληρωμένου νομοθετικού πλαισίου κυβερνοασφάλειας.

Η σημασία αυτής της θεσμικής εξέλιξης υπογραμμίζεται από το γεγονός ότι η Ελλάδα ήταν μεταξύ των πρώτων κρατών-μελών που ολοκλήρωσαν την ενσωμάτωση της Οδηγίας NIS2 στο εθνικό δίκαιο, δείχνοντας πολιτική βούληση για την αναβάθμιση του κυβερνοχώρου. Η ταχεία αυτή ενσωμάτωση αντικατοπτρίζει την αναγνώριση ότι η κυβερνοασφάλεια αποτελεί πλέον ζήτημα εθνικής ασφάλειας και οικονομικής ανταγωνιστικότητας, και όχι απλώς τεχνική απαίτηση.

3.3.1 Νόμος 5160/2024: Η Ενσωμάτωση της Οδηγίας NIS2

Ο Νόμος 5160/2024, ο οποίος δημοσιεύθηκε στην Εφημερίδα της Κυβερνήσεως στις 27 Νοεμβρίου 2024, αποτελεί την ελληνική ενσωμάτωση της Οδηγίας NIS2. Πρόκειται για μία ολοκληρωτική αναδιοργάνωση του εθνικού πλαισίου κυβερνοασφάλειας, η οποία διευρύνει σημαντικά τον αριθμό των ρυθμιζόμενων φορέων, εισάγει αυστηρότερες εποπτικές υποχρεώσεις και θεσπίζει τις υποχρεώσεις της διακυβέρνησης, ευθυγραμμισμένες με την αρχιτεκτονική της NIS2. Ο Νόμος εφαρμόζεται τόσο σε δημόσιους όσο και σε ιδιωτικούς φορείς που λειτουργούν στην Ελλάδα και παρέχουν υπηρεσίες σε κρίσιμους και εξαιρετικά κρίσιμους τομείς, με πεδίο εφαρμογής που εξαρτάται από το μέγεθος, τον τύπο της υπηρεσίας ή την κρισιμότητα της δραστηριότητας.

Η Εθνική Αρχή της Κυβερνοασφάλειας (National Cybersecurity Authority, NCA), η οποία λειτουργεί εντός του Υπουργείου Ψηφιακής Διακυβέρνησης, ορίζεται ως αρμόδιος

εποπτικός φορέας και μοναδικό σημείο επαφής για θέματα κυβερνοασφάλειας. Η NCA είναι υπεύθυνη για την παραλαβή δηλώσεων εγγραφής και αναφορών συμβάντων, τη διαχείριση μεγάλης κλίμακας κυβερνοκρίσεων και τη συνεργασία με άλλα κράτη-μέλη και τα θεσμικά όργανα της ΕΕ.

3.3.2 Νόμος 5193/2025 και Κοινή Υπουργική Απόφαση 1689/2025

Ο Νόμος 5193/2025 εξειδικεύει τις υποχρεώσεις κυβερνοασφάλειας στο χρηματοπιστωτικό τομέα, καθιστώντας τις υποχρεώσεις διακυβέρνησης, διαχείρισης των κινδύνων, διαχείρισης συμβάντων και αναφοράς συμβάντων εφαρμοστές από την Τράπεζα της Ελλάδος (Bank of Greece) ή την Επιτροπή Κεφαλαιαγοράς (Hellenic Capital Market Commission). Η ρύθμιση αυτή αντανακλά το υψηλό κόστος των κυβερνοεπιθέσεων στο χρηματοπιστωτικό τομέα, το οποίο σύμφωνα με την IBM (2024) ανέρχεται σε 6,08 εκατομμύρια δολάρια κατά μέσο όρο ανά παραβίαση.

Η Κοινή Υπουργική Απόφαση (Joint Ministerial Decision, JMD) 1689/2025 θεσπίζει το Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας (National Cybersecurity Requirements Framework) για ουσιώδεις και σημαντικές οντότητες. Μεταξύ των βασικών απαιτήσεων περιλαμβάνεται η κατάρτιση σχεδίου διακυβέρνησης της κυβερνοασφάλειας, η εποπτεία κινδύνων σε επίπεδο ανώτατης διοίκησης, ο ορισμός Υπεύθυνου Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων, ο οποίος αντιστοιχεί στο ρόλο του Επικεφαλή Ασφάλειας των Πληροφοριών (Chief Information Security Officer, CISO), και η υποχρέωση αναφοράς αυτού στην Εθνική Αρχή Κυβερνοασφάλειας. Παράλληλα, η Υπουργική Απόφαση 1645/2025 θεσπίζει τη διαδικασία εγγραφής (registration process) για τις ρυθμιζόμενες οντότητες.

3.3.3 Εθνική Στρατηγική Κυβερνοασφάλειας 2026-2030

Η Ελλάδα εξέδωσε τη νέα Εθνική Στρατηγική Κυβερνοασφάλειας (National Cybersecurity Strategy) για την περίοδο 2026-2030, η οποία ευθυγραμμίζεται με τις ευρωπαϊκές κατευθύνσεις και τις απαιτήσεις της NIS2. Η στρατηγική αυτή εντάσσεται στο πλαίσιο ευρύτερων ψηφιακών πρωτοβουλιών, συμπεριλαμβανομένης της αξιοποίησης πόρων από το Ταμείο Ανάκαμψης και Ανθεκτικότητας (Recovery and Resilience Facility, RRF) για τη χρηματοδότηση των ψηφιακών υποδομών. Αξιοσημείωτο γεγονός αποτελεί η ανακοίνωση της Microsoft τον Ιούνιο 2025 για επένδυση ενός δισεκατομμυρίου δολαρίων στη δημιουργία

υποδομής υπερκλίμακας κέντρου δεδομένων (hyperscale datacenter) στην Ελλάδα, γεγονός που αναμένεται να ενισχύσει τη ζήτηση για υπηρεσίες κυβερνοασφάλειας.

Αξιοσημείωτο είναι ότι η ελληνική νομοθεσία κυβερνοασφάλειας αντιμετωπίζεται πλέον ως συνεκτικό σύστημα. Ο Ν. 5160/2024 αποτελεί το γενικό πλαίσιο, ο Ν. 5193/2025 εξειδικεύει τις απαιτήσεις στο χρηματοπιστωτικό τομέα, ενώ η ΚΥΑ 1689/2025 θεσπίζει τις τεχνικές, οργανωτικές και λειτουργικές απαιτήσεις για όλες τις ρυθμιζόμενες οντότητες. Το πλαίσιο αυτό, σε συνδυασμό με την Εθνική Στρατηγική Κυβερνοασφάλειας 2026-2030, τοποθετεί τη χώρα σε τροχιά πλήρους ευθυγράμμισης με τις ευρωπαϊκές απαιτήσεις, αν και η πρακτική εφαρμογή εξαρτάται σε μεγάλο βαθμό από τη διαθεσιμότητα εξειδικευμένου προσωπικού και κατάλληλων τεχνολογικών λύσεων.

Η ψηφιακή ετοιμότητα της Ελλάδας παραμένει ωστόσο κάτω από τον ευρωπαϊκό μέσο όρο. Η Patergiannaki (2023) τεκμηριώνει ότι η χώρα ακολούθησε ένα διαφορετικό πλαίσιο ψηφιακού μετασχηματισμού από αυτό που πρότεινε η Ευρωπαϊκή Επιτροπή, με αποτέλεσμα να παρουσιάζει αντικρουόμενες επιδόσεις στις εκθέσεις αξιολόγησης ψηφιακής ετοιμότητας. Η έρευνά της στους ελληνικούς δήμους αποκαλύπτει μεσαίο επίπεδο ποιότητας ηλεκτρονικής διακυβέρνησης, με κύριο πρόβλημα τη χαμηλή χρησιμότητα των παρεχόμενων υπηρεσιών. Το δομικό αυτό έλλειμμα στον ψηφιακό μετασχηματισμό του δημόσιου τομέα έχει άμεσες επιπτώσεις στην κυβερνοασφάλεια, καθώς η δημόσια διοίκηση αποτελεί τον πλέον στοχοποιημένο τομέα στην ΕΕ, με 38,2% όλων των καταγεγραμμένων κυβερνοσυμβάντων σύμφωνα με τον ENISA (2025).

3.4 Τεχνολογικές Τάσεις στην Κυβερνοασφάλεια

3.4.1 Τεχνητή Νοημοσύνη και Μηχανική Μάθηση στην Κυβερνοάμυνα

Η τεχνητή νοημοσύνη και η μηχανική μάθηση αναδεικνύονται ως οι πλέον μετασχηματιστικές τεχνολογίες στον τομέα της κυβερνοασφάλειας. Οι Das et al. (2025) εξέτασαν τέσσερα βασικά πεδία εφαρμογής, την ανίχνευση των εισβολών, την ταξινόμηση του κακόβουλου λογισμικού, τον εντοπισμό του ηλεκτρονικού ψαρέματος και ανάλυση των εσωτερικών απειλών. Τα ευρήματά τους καταδεικνύουν ότι τα μοντέλα βαθιάς μάθησης, ιδίως οι αυτοκωδικοποιητές και τα δίκτυα μακράς βραχυπρόθεσμης μνήμης, υπερτερούν στην ανίχνευση πρωτόγνωρων απειλών (zero-day threats) και ανωμαλιών συμπεριφοράς των χρηστών (user behavior anomalies), ενώ τα μοντέλα συνόλων (ensemble models), όπως τα

«Random Forest» και το «XGBoost», αποδίδουν καλύτερα στην ταξινόμηση δομημένων δεδομένων κακόβουλου λογισμικού (Das et al., 2025).

Ωστόσο, οι ίδιοι ερευνητές επισημαίνουν σημαντικές προκλήσεις. Η ανισορροπία των κλάσεων (class imbalance) αποτελεί χρόνιο πρόβλημα, καθώς τα πραγματικά κυβερνοσυμβάντα αντιπροσωπεύουν ένα μικρό ποσοστό της συνολικής κίνησης των δεδομένων. Επιπλέον, οι αντιπαραθετικές επιθέσεις (adversarial attacks) μπορούν να παρακάμψουν ακόμη και τα πλέον εξελιγμένα μοντέλα τεχνητής νοημοσύνης, όπως τεκμηριώνουν οι Haque et al. (2025), αναφέροντας πειράματα όπου ειδικά σχεδιασμένες είσοδοι παραπλάνησαν μοντέλα μηχανικής μάθησης. Η επεξηγησιμότητα (explainability) αποτελεί επίσης κρίσιμο ζήτημα. Τα εργαλεία SHAP (SHapley Additive exPlanations) και LIME (Local Interpretable Model-agnostic Explanations) βοηθούν στην ερμηνεία των αποφάσεων, αλλά η πλήρης διαφάνεια (transparency) σε πραγματικό χρόνο παραμένει τεχνική πρόκληση.

Η τεχνητή νοημοσύνη χρησιμοποιείται παράλληλα και από τους επιτιθέμενους. Η Microsoft ανέφερε αύξηση 35% στις επιθέσεις που χρησιμοποιούν τεχνητή νοημοσύνη, παρακάμπτοντας τις τυπικές προστασίες (Haque et al., 2025), ενώ η δημιουργία πολυμορφικού κακόβουλου λογισμικού μέσω τεχνητής νοημοσύνης αποτελεί πλέον πραγματικότητα. Αυτός ο χαρακτήρας διπλής χρήσης (dual-use character) της τεχνητής νοημοσύνης καθιστά αναγκαία τη συνεχή προσαρμογή τόσο των αμυντικών μηχανισμών όσο και του ρυθμιστικού πλαισίου, κάτι που αναγνωρίζεται στον Κανονισμό AI Act (Gauthier-Maxence, 2024).

Σε λειτουργικό επίπεδο, η ενσωμάτωση της τεχνητής νοημοσύνης στα σύγχρονα Κέντρα Επιχειρήσεων Ασφάλειας (Security Operations Centers, SOC) αλλάζει ριζικά τον τρόπο ανίχνευσης και αντιμετώπισης των κυβερνοαπειλών. Τα συστήματα Διαχείρισης Πληροφοριών και Συμβάντων Ασφάλειας, όπως τα Splunk, IBM QRadar και Microsoft Sentinel, ενσωματώνουν πλέον αλγορίθμους μηχανικής μάθησης για τη βαθμολόγηση του κινδύνου βάσει συμπεριφοράς και τον κυνηγό απειλών (threat hunting) (Haque et al., 2025). Η έρευνα δείχνει ότι οργανισμοί που ανέπτυξαν συστήματα παρακολούθησης βασισμένα σε μηχανική μάθηση μείωσαν κατά 25% τον χρόνο ανίχνευσης συμβάντων και κατά 30% το κόστος αποκατάστασης, σε σύγκριση με οργανισμούς που βασίζονται αποκλειστικά σε χειροκίνητη ανάλυση. Η εξέλιξη αυτή δημιουργεί νέες ευκαιρίες για παρόχους υπηρεσιών διαχειριζόμενης ασφάλειας (Managed Security Service Providers, MSSP) που μπορούν να

προσφέρουν υπηρεσίες ανίχνευσης και αντιμετώπισης (Managed Detection and Response, MDR) βασισμένες σε τεχνητή νοημοσύνη.

3.4.2 Αρχιτεκτονική Μηδενικής Εμπιστοσύνης (Zero Trust)

Η αρχιτεκτονική μηδενικής εμπιστοσύνης (Zero Trust Architecture, ZTA) αποτελεί μία θεμελιώδη αλλαγή παραδείγματος στην προσέγγιση της κυβερνοασφάλειας, βασιζόμενη στην αρχή «ποτέ μην εμπιστεύεσαι, πάντα επαλήθευε» (never trust, always verify). Σε αντίθεση με τα παραδοσιακά μοντέλα ασφάλειας περιμέτρου (perimeter-based security), τα οποία σύμφωνα με τους Haque et al. (2025) δεν επαρκούν πλέον στο σύγχρονο υβριδικό περιβάλλον εργασίας, η αρχιτεκτονική μηδενικής εμπιστοσύνης αντιμετωπίζει κάθε πρόσβαση ως δυνητικά μη ασφαλή, ανεξάρτητα από τη θέση του χρήστη. Το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology, NIST) έχει εκδώσει κατευθυντήριες οδηγίες για αρχιτεκτονικές μηδενικής εμπιστοσύνης, ενώ η Microsoft υιοθετεί τη νοοτροπία «assume breach» (υπόθεση παραβίασης) ως βασική αρχή αμυντικής στρατηγικής.

Η υιοθέτηση αρχιτεκτονικής μηδενικής εμπιστοσύνης αποτελεί πρόκληση ιδιαίτερα για μεσαίου μεγέθους οργανισμούς, καθώς απαιτεί θεμελιώδη αναδιοργάνωση της υποδομής ασφάλειας. Η εφαρμογή μηδενικής εμπιστοσύνης περιλαμβάνει συνεχή επαλήθευση ταυτότητας (continuous authentication), τμηματοποίηση του δικτύου (micro-segmentation), αρχή ελάχιστου δικαιώματος (least privilege access) και αξιολόγηση του κινδύνου σε πραγματικό χρόνο (real-time risk assessment). Η σύγκλιση μηδενικής εμπιστοσύνης και τεχνητής νοημοσύνης ενισχύει σημαντικά τη δυνατότητα ανίχνευσης ανώμαλης συμπεριφοράς, καθώς τα συστήματα ανάλυσης συμπεριφοράς χρηστών και οντοτήτων (User and Entity Behavior Analytics, UEBA) μπορούν να εντοπίσουν απόκλιση από τα κανονικά μοτίβα πρόσβασης.

Για εταιρείες κυβερνοασφάλειας που δραστηριοποιούνται στην ελληνική αγορά, η αρχιτεκτονική μηδενικής εμπιστοσύνης αποτελεί πεδίο υψηλής ζήτησης, καθώς η εφαρμογή της απαιτεί εξειδικευμένες υπηρεσίες σχεδιασμού, εγκατάστασης και συνεχούς παρακολούθησης. Η αρχιτεκτονική μηδενικής εμπιστοσύνης δεν αποτελεί ένα μεμονωμένο προϊόν, αλλά ένα ολοκληρωμένο στρατηγικό πλαίσιο που ενσωματώνει πολλαπλές τεχνολογίες και διαδικασίες, γεγονός που ευνοεί παρόχους ικανούς να προσφέρουν ολιστικές λύσεις αντί αποσπασματικών τεχνολογικών εργαλείων.

3.4.3 Ασφάλεια Νέφους και Κρίσιμων Υποδομών

Η μετάβαση σε υποδομές υπολογιστικού νέφους αποτελεί τη μεγαλύτερη τεχνολογική μετατόπιση στην εταιρική πληροφορική. Σύμφωνα με εκτιμήσεις της Gartner που αναφέρουν οι Haque et al. (2025), μέχρι το 2025 το 99% των αστοχιών ασφαλείας νέφους θα οφείλεται σε λανθασμένη διαμόρφωση από τους πελάτες και όχι σε αδυναμίες των παρόχων. Αυτό αναδεικνύει ότι η ασφάλεια νέφους δεν είναι αποκλειστική ευθύνη του παρόχου, αλλά απαιτεί μοντέλο κοινής ευθύνης (shared responsibility model) και εξειδικευμένη τεχνογνωσία εκ μέρους των οργανισμών.

Ειδικότερα, οι κίνδυνοι ασφάλειας νέφους περιλαμβάνουν τη μη εξουσιοδοτημένη πρόσβαση μέσω εκτεθειμένων διεπαφών προγραμματισμού εφαρμογών (Application Programming Interface, API), τη μη κρυπτογράφηση των δεδομένων σε αποθήκευση και μεταφορά, και τις πολυμισθωτικές αρχιτεκτονικές (multi-tenant architectures) που μπορούν να εκθέσουν πολλούς πελάτες ταυτόχρονα. Η ασφάλεια των κρίσιμων υποδομών αποτελεί ιδιαίτερα ευαίσθητο πεδίο, καθώς η σύγκλιση τεχνολογιών πληροφορικής και τεχνολογιών λειτουργίας δημιουργεί νέους υβριδικούς κινδύνους. Η επίθεση στον Colonial Pipeline το 2021 κατέδειξε πώς μία κυβερνοεπίθεση μπορεί να διαταράξει τον εφοδιασμό καυσίμων μίας ολόκληρης περιφέρειας, αναδεικνύοντας τους κινδύνους που ενέχει η ψηφιοποίηση λειτουργικών δικτύων (Haque et al., 2025). Στον τομέα της υγείας, οι Zhang et al. (2018), διαπίστωσαν ότι πάνω από το 60% των διασυνδεδεμένων ιατρικών συσκευών λειτουργούν με παρωχημένο υλικολογισμικό (outdated firmware), καθιστώντας τες ευάλωτες σε στοχευμένες επιθέσεις λογισμικού εκβιασμού (ransomware). Η κβαντική υπολογιστική (quantum computing) αποτελεί μία ακόμη αναδυόμενη απειλή, καθώς η ικανότητά της να σπάσει τους υφιστάμενους κρυπτογραφικούς αλγορίθμους οδήγησε το NIST στην ανάπτυξη μετα-κβαντικών κρυπτογραφικών προτύπων (post-quantum cryptography standards), η μετάβαση στα οποία αναμένεται να απαιτήσει χρόνια συντονισμού και σημαντικές επενδύσεις.

3.5 Η Αγορά Κυβερνοασφάλειας στην Ελλάδα

Η ελληνική αγορά κυβερνοασφάλειας βρίσκεται σε φάση δυναμικής ανάπτυξης, αντανακλώντας τόσο τις παγκόσμιες τάσεις όσο και τις ιδιαίτερες συνθήκες του εγχώριου περιβάλλοντος. Σύμφωνα με στοιχεία της Mordor Intelligence, η αγορά αποτιμάται σε 185,3 εκατομμύρια δολάρια για το 2026, παρουσιάζοντας σύνθετο ετήσιο ρυθμό ανάπτυξης

(Compound Annual Growth Rate, CAGR) 8,36% με πρόβλεψη να φτάσει τα 276,83 εκατομμύρια δολάρια μέχρι το 2031 (Mordor Intelligence, 2026). Η ανάπτυξη αυτή υποστηρίζεται από τρεις βασικούς μοχλούς, τη ρυθμιστική πίεση μέσω της υποχρεωτικής εφαρμογής της NIS2 βάσει του Ν. 5160/2024, τις επενδύσεις μέσω του Ταμείου Ανάκαμψης και Ανθεκτικότητας (RRF), και την αυξημένη ζήτηση λόγω της εγκατάστασης υποδομών υπερκλίμακας από διεθνείς παρόχους τεχνολογίας.

Η δομή της ελληνικής αγοράς κυβερνοασφάλειας παρουσιάζει ιδιαίτερα χαρακτηριστικά. Ο τομέας κυριαρχείται από μικρομεσαίες επιχειρήσεις και λίγους εγχώριους παρόχους με ισχυρή τεχνογνωσία, ενώ οι πολυεθνικές εταιρείες κατέχουν σημαντικό μερίδιο μέσω τοπικών αντιπροσωπειών. Η είσοδος στην αγορά κυβερνοασφάλειας αποτελεί στρατηγική απόφαση ιδιαίτερου ενδιαφέροντος για εγχώριες εταιρείες πληροφορικής, οι οποίες μπορούν να αξιοποιήσουν τις σχέσεις τους με υπάρχοντες πελάτες, τη γνώση του ρυθμιστικού περιβάλλοντος και τη γεωγραφική εγγύτητα ως ανταγωνιστικά πλεονεκτήματα.

Η αυξημένη ρυθμιστική πολυπλοκότητα λειτουργεί ταυτόχρονα ως απειλή και ως ευκαιρία. Αφενός, οι μικρομεσαίες επιχειρήσεις αντιμετωπίζουν δυσκολίες στη συμμόρφωση λόγω περιορισμένων πόρων και τεχνογνωσίας, γεγονός που αυξάνει τη ζήτηση για εξωτερικές υπηρεσίες κυβερνοασφάλειας. Αφετέρου, η πολυπλοκότητα του πλαισίου απαιτεί εξειδικευμένη γνώση που δεν είναι εύκολα προσβάσιμη, δημιουργώντας φραγμούς εισόδου για ανεπαρκώς προετοιμασμένους ανταγωνιστές. Οι Haque et al. (2025) επισημαίνουν ότι λιγότερο από 30% των επιχειρήσεων εφαρμόζει πλήρως τα πρότυπα κυβερνοασφάλειας, πρωτίστως λόγω αδράνειας (inertia), απαγορευτικού κόστους και έλλειψης εσωτερικής τεχνογνωσίας, τάση που είναι ιδιαίτερα έντονη στην ελληνική αγορά.

Σε επίπεδο αγοραστικής δομής, οι κύριοι τομείς ζήτησης υπηρεσιών κυβερνοασφάλειας στην Ελλάδα περιλαμβάνουν τον χρηματοπιστωτικό τομέα (τράπεζες, ασφαλιστικές εταιρείες), τη δημόσια διοίκηση (κεντρική και τοπική αυτοδιοίκηση), τις τηλεπικοινωνίες, την ενέργεια και τον τουρισμό. Η υποχρεωτική συμμόρφωση με τον Ν. 5160/2024 αναμένεται να δημιουργήσει ένα κύμα ζήτησης, ιδίως από οργανισμούς που δεν είχαν προηγουμένως εντάξει στην επιχειρησιακή τους στρατηγική τη συστηματική διαχείριση κυβερνοκινδύνων. Οι υπηρεσίες με τη μεγαλύτερη ζήτηση αφορούν αξιολόγηση ευπαθειών, δοκιμές διείσδυσης (penetration testing), υπηρεσίες διαχειριζόμενης ασφάλειας (Managed Security Services, MSS) και σχεδιασμό πολιτικών κυβερνοασφάλειας (cybersecurity policy design).

Ιδιαίτερα κρίσιμο είναι το ελληνικό έλλειμμα δεξιοτήτων κυβερνοασφάλειας. Η χώρα αντιμετωπίζει τις ίδιες διαρθρωτικές προκλήσεις με την υπόλοιπη Ευρώπη, αλλά σε εντονότερο βαθμό λόγω της διαρροής εγκεφάλων (brain drain) κατά τα χρόνια της οικονομικής κρίσης. Σύμφωνα με τον Virag (2025), η Ευρώπη στο σύνολό της αντιμετωπίζει δομικό πρόβλημα στη σύνδεση εκπαιδευτικών προγραμμάτων με τις πραγματικές ανάγκες της αγοράς εργασίας, ενώ η υιοθέτηση του Ευρωπαϊκού Πλαισίου Δεξιοτήτων Κυβερνοασφάλειας (ECSF) παραμένει χαμηλή στα περισσότερα κράτη-μέλη. Η κατάσταση αυτή δημιουργεί τόσο προκλήσεις όσο και ευκαιρίες για εταιρείες που μπορούν να προσελκύσουν, να εκπαιδεύσουν και να διατηρήσουν ταλαντούχο προσωπικό σε έναν τομέα υψηλής ζήτησης. Η στρατηγική σημασία του ανθρώπινου κεφαλαίου στην κυβερνοασφάλεια δεν πρέπει να υποτιμάται. Σύμφωνα με τους Haque et al. (2025), η εκπαίδευση της ευαισθητοποίησης σε θέματα ασφάλειας (security awareness training) μπορεί να μειώσει τα περιστατικά παραβίασης έως και 45%, ενώ ο (ISC)² εκτιμά ότι απαιτούνται 3,4 εκατομμύρια επιπλέον επαγγελματίες παγκοσμίως για την επαρκή προστασία των ψηφιακών υποδομών.

3.6 Σύνδεση με την Παρούσα Έρευνα

Η ανάλυση του οικοσυστήματος κυβερνοασφάλειας σε παγκόσμιο, ευρωπαϊκό και ελληνικό επίπεδο αναδεικνύει ένα περιβάλλον ταυτόχρονα γεμάτο προκλήσεις και ευκαιρίες. Ο Πίνακας 3.1 συνοψίζει τους βασικούς κανονισμούς που διαμορφώνουν το τοπίο, αναδεικνύοντας τη σύγκλιση μεταξύ ευρωπαϊκού και ελληνικού πλαισίου.

Πίνακας 3.1: Βασικοί Κανονισμοί Κυβερνοασφάλειας και Πεδίο Εφαρμογής

Κανονισμός	Πεδίο Εφαρμογής	Κύριες Υποχρεώσεις	Ελληνική Ενσωμάτωση
NIS2 (EU 2022/2555)	18 τομείς, ουσιώδεις και σημαντικές οντότητες	Διαχείριση κινδύνων, αναφορά συμβάντων, ασφάλεια αλυσίδας εφοδιασμού	Ν. 5160/2024, ΚΥΑ 1689/2025
DORA (EU 2022/2554)	Χρηματοπιστωτικός τομέας	Ψηφιακή ανθεκτικότητα, δοκιμές, διαχείριση τρίτων	Ν. 5193/2025
GDPR (EU 2016/679)	Επεξεργασία προσωπικών δεδομένων	Τεχνικά και οργανωτικά μέτρα ασφάλειας	Ν. 4624/2019

Κανονισμός	Πεδίο Εφαρμογής	Κύριες Υποχρεώσεις	Ελληνική Ενσωμάτωση
Cybersecurity Act (EU 2019/881)	Πιστοποίηση προϊόντων και υπηρεσιών	Πλαίσιο πιστοποίησης τριών επιπέδων	Άμεση εφαρμογή
AI Act (EU 2024/1689)	Συστήματα τεχνητής νοημοσύνης	Ταξινόμηση κινδύνου, απαιτήσεις ασφάλειας	Σε εξέλιξη

Η εκθετική αύξηση των κυβερνοαπειλών, η κλιμάκωση του ρυθμιστικού πλαισίου, οι ραγδαίες τεχνολογικές εξελίξεις και το χρόνιο έλλειμμα δεξιοτήτων διαμορφώνουν μία αγορά με σημαντικό αναπτυξιακό δυναμικό. Συνολικά, τέσσερις βασικοί μοχλοί ζήτησης αναδεικνύονται ως καθοριστικοί για την ελληνική αγορά κυβερνοασφάλειας κατά την περίοδο 2025-2030. Πρώτον, η υποχρεωτική συμμόρφωση με τη NIS2 και τον DORA, που αφορά εκατοντάδες νέους ρυθμιζόμενους οργανισμούς. Δεύτερον, η ψηφιοποίηση του δημόσιου τομέα μέσω πόρων RRF, που δημιουργεί ανάγκες ασφάλειας νέων ψηφιακών υπηρεσιών. Τρίτον, η εγκατάσταση υποδομών νέφους υπερκλίμακας (Microsoft, AWS) στην ελληνική επικράτεια. Τέταρτον, η αυξημένη ευαισθητοποίηση του ιδιωτικού τομέα μετά τη σειρά κυβερνοεπιθέσεων σε ελληνικούς οργανισμούς κατά τα τελευταία έτη.

Τα δεδομένα αυτά αποτελούν τη βάση για την ανάλυση που ακολουθεί στα επόμενα κεφάλαια. Στο Κεφάλαιο 4 θα παρουσιαστεί η εταιρεία QnR (Quality & Reliability S.A.) και η πρόσφατη στρατηγική της κίνηση εισόδου στον τομέα κυβερνοασφάλειας μέσω της εξαγοράς πλειοψηφικού πακέτου της SysteCom-Cybersecurity. Στο Κεφάλαιο 5 θα εφαρμοστούν τα θεωρητικά πλαίσια του Κεφαλαίου 2 στα εμπειρικά δεδομένα της αγοράς που τεκμηριώθηκαν εδώ, προκειμένου να αξιολογηθούν οι στρατηγικές επιλογές της εταιρείας. Η σύγκλιση ρυθμιστικών απαιτήσεων (ιδίως NIS2 και DORA), τεχνολογικών τάσεων (τεχνητή νοημοσύνη, μηδενική εμπιστοσύνη, ασφάλεια νέφους) και αυξανόμενης ζήτησης στην ελληνική αγορά ($185 εκατ. το 2026, CAGR 8,36%) δημιουργεί ένα παράθυρο ευκαιρίας που μία ενσωματωμένη εταιρεία πληροφορικής με εγχώρια παρουσία και πελατειακή βάση μπορεί δυνητικά να εκμεταλλευτεί. Ταυτόχρονα, οι προκλήσεις που τεκμηριώθηκαν στο παρόν κεφάλαιο, από την κλιμακούμενη πολυπλοκότητα των απειλών και τη ρυθμιστική πίεση μέχρι το έλλειμμα δεξιοτήτων και τις ταχέως εξελισσόμενες τεχνολογίες, καθιστούν σαφές ότι η είσοδος στην αγορά κυβερνοασφάλειας απαιτεί προσεκτικό στρατηγικό σχεδιασμό, κατάλληλους πόρους και ικανότητα ταχείας προσαρμογής. Η εκτίμηση αυτών των παραγόντων

θα αποτελέσει αντικείμενο ανάλυσης στα επόμενα κεφάλαια, όπου τα εμπειρικά δεδομένα της αγοράς θα συνδυαστούν με τα θεωρητικά πλαίσια του Κεφαλαίου 2 για τη στρατηγική αξιολόγηση μίας συγκεκριμένης επιχειρησιακής απόφασης.

Βιβλιογραφία Κεφαλαίου

1. Almeida, F. (2025). Comparative analysis of EU-based cybersecurity skills frameworks. *Computers & Security, 151*, 104329. https://doi.org/10.1016/j.cose.2024.104329

2. Castiglione, G., Santamaria, D. F., Bella, G., Brisinda, L., & Puccia, G. (2025). Guiding cybersecurity compliance: An ontology for the NIS2 directive. *Computers & Security, 157*, 104617. https://doi.org/10.1016/j.cose.2024.104617

3. Das, B. C., Sartaz, M. S., Reza, S. A., Hossain, A., Nasiruddin, M. D., Bishnu, K. K., & Sultana, K. S. (2025). AI-driven cybersecurity threat detection: Building resilient defense systems using predictive analytics. *International Journal of Basic and Applied Sciences, 14*(4), 33–45. https://doi.org/10.14419/hysdg957

4. ENISA. (2025). *ENISA Threat Landscape 2024–2025*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

5. Fortune Business Insights. (2025). *Cybersecurity market size, share & COVID-19 impact analysis, 2025–2032*. https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

6. Gartner. (2025). *Forecast: Information security, worldwide, 2022–2028*. Gartner, Inc.

7. Gauthier-Maxence, C. (2024). European cybersecurity and AI framework: Towards proactive regulation for a secure digital future. *EU Law Live, 212*, 1–8.

8. Haque, G. M. M., Akula, D. K., Mohammed, Y. S., Syed, A., & Arafat, Y. (2025). Cybersecurity risk management in the age of digital transformation: A systematic literature review. *The American Journal of Engineering and Technology, 7*(8), 126–150. https://doi.org/10.37547/tajet/Volume07Issue08-14

9. IBM. (2024). *Cost of a data breach report 2024*. IBM Security. https://www.ibm.com/reports/data-breach

10. IBM. (2025). *Cost of a data breach report 2025*. IBM Security. https://www.ibm.com/reports/data-breach

11. Mordor Intelligence. (2026). *Greece cybersecurity market size & share analysis – Growth trends & forecasts (2026–2031)*. https://www.mordorintelligence.com/industry-reports/greece-cybersecurity-market

12. Virág, C. (2025). *Building competitive cyber capacity for Europe: A strategic framework for digital readiness* [Master's thesis, Tallinn University of Technology].

13. Πατεργιαννάκη, Ζ. (2023). *Ο ψηφιακός μετασχηματισμός στον δημόσιο τομέα: Η περίπτωση της ελληνικής τοπικής αυτοδιοίκησης* [Διδακτορική διατριβή, Πανεπιστήμιο Πειραιώς]. Ιδρυματικό Αποθετήριο Πανεπιστημίου Πειραιώς.

Κεφάλαιο 4

Η Εταιρεία Quality & Reliability (QnR)

4.1 Ιστορική Εξέλιξη και Εταιρικό Προφίλ

Η εταιρεία Quality & Reliability A.B.E.E. (QnR) ιδρύθηκε το 1992 στη Μεταμόρφωση Αττικής, με αντικείμενο την ανάπτυξη λογισμικού και την ολοκλήρωση πληροφοριακών συστημάτων για μεγάλους και μεσαίους οργανισμούς τόσο του δημόσιου όσο και του ιδιωτικού τομέα. Κατά τη διάρκεια τριών και πλέον δεκαετιών λειτουργίας, η εταιρεία εδραιώθηκε ως αξιόπιστος πάροχος λύσεων πληροφορικής στην ελληνική αγορά, αναπτύσσοντας μία σταθερή πελατειακή βάση που υπερβαίνει τους 250 μεγάλους οργανισμούς και επιχειρήσεις (QnR, 2025).

Η εισαγωγή της μετοχής της QnR στο Χρηματιστήριο Αθηνών (Athens Exchange, ATHEX) το 2000, με σύμβολο διαπραγμάτευσης QUAL, αποτέλεσε σημαντικό σταθμό στην ιστορία της εταιρείας, παρέχοντάς της πρόσβαση στις κεφαλαιαγορές και ενισχύοντας τη θεσμική της αναγνώριση. Η εταιρική πορεία χαρακτηρίστηκε από σταδιακή διεύρυνση του χαρτοφυλακίου υπηρεσιών, ξεκινώντας από λύσεις βάσεων δεδομένων σε συνεργασία με την Oracle (στρατηγικός συνεργάτης από το 1993) και εξελισσόμενη σε ολοκληρωμένες λύσεις ψηφιακού μετασχηματισμού. Η προσθήκη της IBM ως στρατηγικού συνεργάτη (strategic partner) το 2022 ενίσχυσε περαιτέρω τις δυνατότητες σε τομείς όπως η ρομποτική αυτοματοποίηση διαδικασιών (Robotic Process Automation, RPA), οι εικονικοί βοηθοί (Watson Assistant) και η αυτοματοποίηση επιχειρηματικών ροών εργασίας (Business Automation Workflow). Η QnR τιμήθηκε με το IBM Automation Award το 2024, αναγνωρίζοντας τη συνεισφορά της στην υιοθέτηση λύσεων αυτοματοποίησης.

Σημαντικοί σταθμοί στην ιστορία του Ομίλου περιλαμβάνουν την ίδρυση της θυγατρικής Greenovative (2018) στον τομέα των ανανεώσιμων πηγών ενέργειας και τη δημιουργία της QnR Financial Services (2021) με εξειδίκευση στο χρηματοπιστωτικό τομέα. Η Greenovative αξιοποιεί τεχνολογίες μηχανικής μάθησης για την πρόβλεψη παραγωγής

ενέργειας, ενώ η QnR Financial Services εστιάζει σε λύσεις ψηφιακής τραπεζικής, ρυθμιστικής συμμόρφωσης και αναφορών για χρηματοπιστωτικά ιδρύματα. Αυτές οι κινήσεις αντικατοπτρίζουν μία σταδιακή στρατηγική διαφοροποίησης που προετοίμασε το έδαφος για την πλέον φιλόδοξη αναπτυξιακή φάση της εταιρείας, η οποία πραγματοποιήθηκε το 2025. Αξίζει να σημειωθεί ότι η εμπειρία στο χρηματοπιστωτικό τομέα μέσω της QnR Financial Services αποδείχθηκε στρατηγικά σημαντική, καθώς η κατανόηση των ρυθμιστικών απαιτήσεων του κλάδου (DORA, NIS2, PSD2) διευκόλυνε την ενσωμάτωση της SysteCom, η οποία εξυπηρετεί τις τέσσερις μεγαλύτερες ελληνικές τράπεζες.

4.2 Βασικές Δραστηριότητες και Χαρτοφυλάκιο Υπηρεσιών

Οι βασικές δραστηριότητες της QnR εκτείνονται σε τέσσερις κύριους πυλώνες. Ο πρώτος πυλώνας αφορά την ανάπτυξη λογισμικού, η οποία αποτελεί τον ιστορικό πυρήνα της εταιρείας. Η QnR έχει αναπτύξει ιδιόκτητα (proprietary) λογισμικά προϊόντα, μεταξύ των οποίων ξεχωρίζουν το Orama ERP, ένα ολοκληρωμένο σύστημα διαχείρισης επιχειρησιακών πόρων βασισμένο σε τεχνολογία Oracle, το σύστημα διαχείρισης ακίνητης περιουσίας για τον κλάδο φιλοξενίας και ακίνητης περιουσίας, λύσεις ηλεκτρονικής τιμολόγησης, ηλεκτρονικών εγγυήσεων και διαχείρισης αδειών (myLeave), το Enerforecast4all, μία λύση πρόβλεψης παραγωγής ανανεώσιμης ενέργειας βασισμένη σε μηχανική μάθηση και βαθιά μάθηση και ένα σύστημα ψηφιοποίησης λιμενικών λειτουργιών.

Ο δεύτερος πυλώνας αφορά την ολοκλήρωση συστημάτων, προσφέροντας υπηρεσίες σύνδεσης ετερογενών πληροφοριακών περιβαλλόντων, αυτοματοποίησης επιχειρηματικών λειτουργιών και ανάπτυξης ενοποιημένων αρχιτεκτονικών δεδομένων. Η τεχνογνωσία σε Oracle middleware, IBM Integration Bus και σύγχρονα πρότυπα διαλειτουργικότητας επιτρέπει στην QnR να αναλαμβάνει σύνθετα έργα ψηφιακού μετασχηματισμού σε δημόσιους οργανισμούς και μεγάλες επιχειρήσεις. Ο τρίτος πυλώνας περιλαμβάνει τις επιχειρηματικές λύσεις για σύνθετες οργανωτικές ανάγκες, με εξειδίκευση στη σχεδίαση και υλοποίηση συστημάτων διαχείρισης επιχειρησιακών πόρων (ERP), διαχείρισης σχέσεων με πελάτες (CRM) και επιχειρηματικής ευφυΐας (Business Intelligence). Ο τέταρτος πυλώνας αφορά τις εφαρμογές νέφους, παρέχοντας κλιμακούμενες λύσεις που επιτρέπουν στους πελάτες τη μετάβαση σε υβριδικά ή πλήρως νεφο-κεντρικά (cloud-native) περιβάλλοντα λειτουργίας. Οι τομείς εξειδίκευσης της εταιρείας καλύπτουν ένα ευρύ φάσμα όπως ηλεκτρονική διακυβέρνηση, ηλεκτρονικό εμπόριο, τεχνητή νοημοσύνη και μηχανική μάθηση, ανάπτυξη

κινητών εφαρμογών, συστήματα ERP/CRM, χρηματοοικονομική τεχνολογία, υπολογιστικό νέφος, ανάλυση δεδομένων και πρακτικές DevOps/CI-CD.

Η πελατειακή βάση της QnR αντικατοπτρίζει τη γεωγραφική και τομεακή διάχυση των δραστηριοτήτων της. Η εταιρεία εξυπηρετεί σημαντικό αριθμό φορέων του δημόσιου τομέα, συμπεριλαμβανομένων υπουργείων, φορέων κοινωνικής ασφάλισης και εκπαιδευτικών ιδρυμάτων. Στον ιδιωτικό τομέα, οι πελάτες εκτείνονται σε κλάδους όπως η τραπεζική και οι χρηματοπιστωτικές υπηρεσίες, η βιομηχανική παραγωγή, η αγροδιατροφή, το λιανεμπόριο και ο τουρισμός. Το ανεκτέλεστο υπόλοιπο των συμβάσεων υπερβαίνει τα 40 εκατομμύρια ευρώ για την περίοδο 2024-2026, παρέχοντας σημαντική ορατότητα εσόδων.

4.3 Ομιλική Δομή και Στρατηγικές Εξαγορές

4.3.1 Η Στρατηγική Στροφή του 2025

Το 2025 αποτέλεσε ένα έτος-ορόσημο (landmark year) για τον Όμιλο QnR, καθώς σηματοδότησε τη μετάβαση από έναν μονοδιάστατο πάροχο υπηρεσιών πληροφορικής σε ένα διαφοροποιημένο τεχνολογικό όμιλο. Μέσω τριών διαδοχικών εξαγορών, η QnR επέκτεινε τις δραστηριότητές της σε τρεις νέους στρατηγικούς τομείς στην κυβερνοασφάλεια, στην τεχνητή νοημοσύνη και σε λύσεις επιχειρηματικού λογισμικού SAP. Οι εξαγορές χρηματοδοτήθηκαν μέσω κοινοπρακτικού ομολογιακού δανείου ύψους 19,1 εκατομμυρίων ευρώ, το οποίο εγκρίθηκε τον Ιούλιο 2024. Η ισχυρή θεσμική στήριξη αντικατοπτρίζεται στη συμμετοχή θεσμικών επενδυτών που κατέχουν περίπου το 13% του μετοχικού κεφαλαίου. Η συγκέντρωση ενός τμήματος του μετοχικού κεφαλαίου στον ιδρυτή παρέχει σταθερότητα στρατηγικής κατεύθυνσης, ιδιαίτερα κρίσιμη κατά την περίοδο μετασχηματισμού μέσω πολλαπλών εξαγορών.

Η τρέχουσα δομή του Ομίλου QnR περιλαμβάνει τις εξής θυγατρικές εταιρείες:

- **QnR Cyprus Ltd** (100%): Θυγατρική εδρεύουσα στην Κύπρο, με δραστηριότητες ανάπτυξης λογισμικού (software development) και παροχής συμβουλών πληροφορικής (IT consulting).
- **SysteCom S.A.** (60%): Ελληνική εταιρεία ψηφιακών υποδομών πληροφορικής και κυβερνοασφάλειας, ιδρυθείσα το 2013.

- **SquareDev BV** (51%): Βελγική εταιρεία λογισμικού τεχνητής νοημοσύνης (AI software), ιδρυθείσα το 2018.
- **Alexander Moore S.A.** (76,19%): Ελληνική εταιρεία παροχής λύσεων SAP Business One, με εξειδίκευση σε κλάδους τουρισμού, ασφαλίσεων, εμπορίου και βιομηχανίας.
- **MTIS S.A.** (στρατηγική συμμετοχή): Εταιρεία ναυτιλιακής τεχνολογίας (maritime technology), η οποία αναπτύσσει πλατφόρμες IoT, συστήματα ψηφιακών διδύμων (digital twin systems) και λύσεις αυτοματοποίησης βασισμένες σε τεχνητή νοημοσύνη για εμπορικές και αμυντικές ναυτιλιακές εφαρμογές. Η συμμετοχή στη MTIS ανοίγει προοπτικές στον τομέα της ναυτιλιακής κυβερνοασφάλειας (maritime cybersecurity), ένα αναδυόμενο πεδίο με αυξανόμενες ρυθμιστικές απαιτήσεις από τον Διεθνή Ναυτιλιακό Οργανισμό (International Maritime Organization, IMO) και τις ευρωπαϊκές αρχές.

Ο πίνακας 4.1 συνοψίζει τις τρεις εξαγορές του 2025 και τα βασικά τους χαρακτηριστικά.

Πίνακας 4.1: Συνοπτική Παρουσίαση Εξαγορών Ομίλου QnR (2025)

Εταιρεία	Τομέας	Ποσοστό	Τίμημα (€)	Ημερομηνία	Κύκλος Εργασιών
SysteCom S.A.	Κυβερνοασφάλεια	60%	1.500.000	Ιανουάριος 2025	2,7 εκ. (2023)
SquareDev BV	Τεχνητή Νοημοσύνη	51%	1.100.000	Μάρτιος 2025	898.000 (2023)
Alexander Moore S.A.	SAP / Επιχειρηματικό Λογισμικό	76,19%	N/A	Οκτώβριος 2025	N/A

4.3.2 Η Εξαγορά της SysteCom: Είσοδος στην Κυβερνοασφάλεια

Η πρώτη και πλέον καθοριστική εξαγορά αφορούσε την απόκτηση του 60% της SysteCom S.A. έναντι 1,5 εκατομμυρίων ευρώ, με πρόβλεψη για απόκτηση του υπολοίπου 40% εντός τριετίας. Η δομή της συναλλαγής ως σταδιακή απόκτηση επιτρέπει τη διατήρηση

κινήτρων για τον ιδρυτή μέτοχο κατά τη μεταβατική περίοδο, ελαχιστοποιώντας τον κίνδυνο απώλειας κρίσιμης τεχνογνωσίας. Η συμφωνία ανακοινώθηκε τον Ιανουάριο 2025 και αποτελεί την κεντρική επιχειρησιακή απόφαση που εξετάζεται στην παρούσα εργασία.

Η SysteCom S.A. ιδρύθηκε τον Ιανουάριο 2013 από τη μοναδική μέτοχο κα Ευτυχία Φιλιπάκη, με αντικείμενο την παροχή ψηφιακών υποδομών πληροφορικής (digital IT infrastructure) και λύσεων κυβερνοασφάλειας (cybersecurity solutions). Κατά τη δωδεκαετή λειτουργία της, η SysteCom ανέπτυξε ισχυρή παρουσία στην ελληνική αγορά κυβερνοασφάλειας, εξυπηρετώντας πάνω από 200 πελάτες σε ολόκληρη την Ευρώπη. Η πελατειακή της βάση περιλαμβάνει κορυφαίους ελληνικούς οργανισμούς, μεταξύ των οποίων η Τράπεζα Πειραιώς (Piraeus Bank), η Εθνική Τράπεζα (NBG), η Eurobank, η Alpha Bank, ο ΟΤΕ (OTE), η Vodafone, η Nova, η ΔΕΗ (PPC), ο ΑΔΜΗΕ (ADMIE), καθώς και κυβερνητικοί οργανισμοί.

Το χαρτοφυλάκιο υπηρεσιών κυβερνοασφάλειας της SysteCom καλύπτει ένα ευρύ φάσμα κρίσιμων υπηρεσιών όπως αξιολόγηση και διαχείριση κινδύνων κυβερνοασφάλειας (Cybersecurity Rating & Risk Management), διαχείριση κινδύνων προμηθευτών (Vendor Risk Management), αυτοματοποιημένη επικύρωση ασφάλειας και δοκιμές διείσδυσης (Automatic Security Validation / Pentesting), διαχείριση περιουσιακών στοιχείων ασφάλειας σε λειτουργικά και πληροφοριακά δίκτυα (Security Asset Management OT/IT), πρόληψη απώλειας δεδομένων (Data Loss Prevention), ταξινόμηση δεδομένων (Data Classification), ασφάλεια δικτύων και νέφους (Networking/Cloud Security), περιορισμός λογισμικού εκβιασμού (Ransomware Containment), εκπαίδευση ευαισθητοποίησης ασφάλειας (Security Awareness Training), προσομοίωση ηλεκτρονικού ψαρέματος (Phishing Simulation), διαχείριση ευπαθειών (Vulnerability Management), διαχείριση δικαιωμάτων πληροφοριών (Information Rights Management), κέντρο επιχειρήσεων ασφάλειας (Security Operations Center, SOC) και ανάλυση ασφάλειας για πλοία (Security Monitoring & Analytics for Vessels) (SysteCom, 2025).

Η οικονομική απόδοση της SysteCom κατά την περίοδο πριν από την εξαγορά ήταν ανοδική. Ο κύκλος εργασιών (turnover) ανήλθε σε 2,7 εκατομμύρια ευρώ το 2023, ενώ για το 2024 αναμενόταν να υπερβεί τα 3 εκατομμύρια ευρώ, με EBITDA 330.000 ευρώ και κέρδη προ φόρων (pre-tax profits) 310.000 ευρώ. Η SysteCom διαθέτει πιστοποιημένες συνεργασίες με κορυφαίους διεθνείς κατασκευαστές λύσεων κυβερνοασφάλειας, μεταξύ των οποίων οι Palo

Alto Networks, Fortinet, CrowdStrike, Proofpoint, Bitsight και SecurityScorecard, γεγονός που ενισχύει τη δυνατότητά της να παρέχει λύσεις βασισμένες σε ηγετικές τεχνολογίες. Η εταιρεία έχει λάβει σημαντικές βραβεύσεις, μεταξύ των οποίων χρυσά βραβεία (Gold Awards) στα Cybersecurity Awards 2023 και 2024 στις κατηγορίες υπηρεσιών χρηματοπιστωτικού τομέα (Financial Services) και κυβερνητικών υποδομών (Government and Infrastructure). Το 2026 απέσπασε τρεις διακρίσεις στα Cyber Security Awards, επιβεβαιώνοντας τη συνεχή αναγνώριση της αγοράς.

4.3.3 Η Εξαγορά της SquareDev: Επέκταση στην Τεχνητή Νοημοσύνη

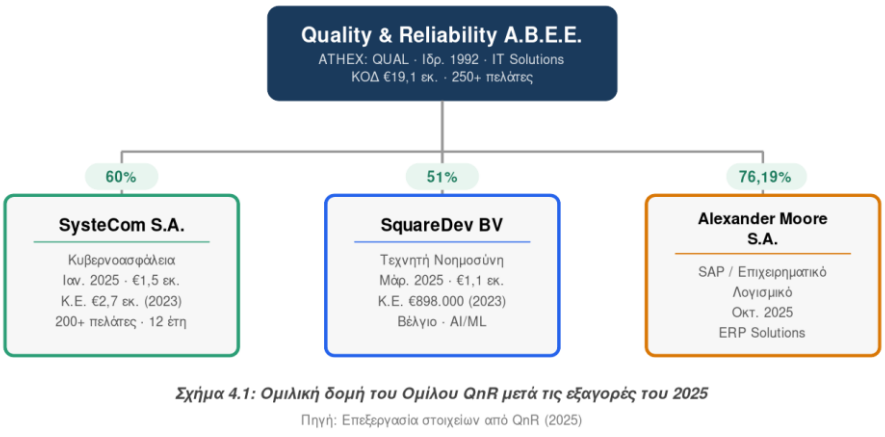
Η δεύτερη εξαγορά, η οποία ανακοινώθηκε τον Μάρτιο 2025, αφορούσε την απόκτηση του 51% της βελγικής εταιρείας SquareDev BV έναντι 1,1 εκατομμυρίων ευρώ (1 εκατομμύριο ευρώ για αύξηση μετοχικού κεφαλαίου και 100.000 ευρώ για υφιστάμενες μετοχές). Η SquareDev, ιδρυθείσα το 2018, εξειδικεύεται στην ανάπτυξη λύσεων τεχνητής νοημοσύνης (AI solutions), προσφέροντας εσωτερικούς επιχειρηματικούς βοηθούς (Internal Business Assistants) για αναζήτηση εγγράφων, δημιουργία περιεχομένου και αυτοματοποίηση εργασιών, βοηθούς εξυπηρέτησης πελατών (Customer Support Assistants), αυτοματοποίηση εισαγωγής δεδομένων (Data Entry Automation), ασφάλεια συστημάτων τεχνητής νοημοσύνης (AI System Security) και λύσεις μηχανικής μάθησης (Machine Learning Solutions) για ανίχνευση αντικειμένων, πρόβλεψη, ομαδοποίηση, ανίχνευση ανωμαλιών και πρόληψη κινδύνων.

Η εταιρεία εδρεύει στις Βρυξέλλες του Βελγίου, ένα σημαντικό ευρωπαϊκό κέντρο τεχνολογικής καινοτομίας (technology innovation hub), και διατηρεί πελατειακή βάση κυρίως σε Βέλγιο και Ελλάδα. Ο κύκλος εργασιών της SquareDev ανήλθε σε 898.000 ευρώ το 2023, με πρόβλεψη υπέρβασης του 1.287.000 ευρώ το 2024, σημειώνοντας ετήσια αύξηση περίπου 43%. Η στρατηγική σημασία αυτής της εξαγοράς είναι διττή. Αφενός εμπλουτίζει τις ικανότητες του Ομίλου σε τεχνολογίες τεχνητής νοημοσύνης που αποτελούν αναπόσπαστο μέρος της σύγχρονης κυβερνοασφάλειας (όπως αναλύθηκε στην ενότητα 3.4.1), αφετέρου δημιουργεί δυνατότητα ανάπτυξης καινοτόμων λύσεων κυβερνοασφάλειας βασισμένων σε τεχνητή νοημοσύνη, συνδυάζοντας την τεχνογνωσία της SquareDev σε μηχανική μάθηση και ανίχνευση ανωμαλιών (anomaly detection) με τις υπηρεσίες κέντρου επιχειρήσεων ασφάλειας (SOC) και αξιολόγησης κινδύνου της SysteCom. Η δυνητική ανάπτυξη προϊόντων κυβερνοασφάλειας ενισχυμένων με τεχνητή νοημοσύνη (AI-enhanced cybersecurity products)

αποτελεί μία στρατηγική δυνατότητα που μπορεί να διαφοροποιήσει τον Όμιλο QnR από τους παραδοσιακούς παρόχους κυβερνοασφάλειας στην ελληνική αγορά.

4.3.4 Η Εξαγορά της Alexander Moore: Εισαγωγή ενός μεγάλου ERP

Η τρίτη εξαγορά αφορούσε την απόκτηση του 76,19% της Alexander Moore S.A., ενός εκ των πλέον εδραιωμένων παρόχων λύσεων SAP Business One στην Ελλάδα. Η ενσωμάτωση (integration) ολοκληρώθηκε τον Οκτώβριο 2025 και καλύπτει πλήρως τους στρατηγικούς στόχους επέκτασης του Ομίλου στην αγορά επιχειρηματικού λογισμικού (enterprise software) και SAP. Η Alexander Moore εξειδικεύεται σε κάθετες εφαρμογές (vertical applications) για τους κλάδους τουρισμού, ασφαλίσεων, εμπορίου και βιομηχανίας, ενσωματώνοντας τεχνολογίες προγνωστικής ανάλυσης (predictive analytics). Η εξαγορά αυτή ενισχύει τη δυνατότητα του Ομίλου να προσφέρει ολοκληρωμένα οικοσυστήματα SAP σε μεσαίες και μεγάλες επιχειρήσεις, ενώ παράλληλα δημιουργεί ευκαιρίες διασταυρούμενων πωλήσεων (cross-selling) υπηρεσιών κυβερνοασφάλειας και τεχνητής νοημοσύνης σε υφιστάμενους πελάτες SAP, οι οποίοι εκ φύσεως διαχειρίζονται ευαίσθητα εταιρικά δεδομένα (sensitive corporate data) και αντιμετωπίζουν αυξημένες απαιτήσεις ψηφιακής ασφάλειας.



Σχήμα 4.1: Ομιλική δομή του Ομίλου QnR μετά τις εξαγορές του 2025

Πηγή: Επεξεργασία στοιχείων από QnR (2025)

Σχήμα 4.1: Δομή του Ομίλου QnR μετά τις εξαγορές του 2025

(Πηγή: Επεξεργασία στοιχείων από QnR, 2025)

4.4 Χαρακτηριστικά και Προφίλ του Ομίλου

Μετά την ολοκλήρωση των εξαγορών του 2025, ο Όμιλος QnR απαρτίζεται από πέντε βασικές δραστηριότητες: κυβερνοασφάλεια (SysteCom), τεχνητή νοημοσύνη (SquareDev),

επιχειρηματικό λογισμικό (Alexander Moore), ναυτιλιακή τεχνολογία (MTIS) και τον ιστορικό πυρήνα λύσεων πληροφορικής.

Τα βασικά χαρακτηριστικά του Ομίλου QnR περιλαμβάνουν, πρώτον, τη μακρόχρονη παρουσία στην ελληνική αγορά (30+ έτη), η οποία παρέχει αναγνωρισιμότητα επωνυμίας και εμπιστοσύνη πελατών. Δεύτερον, την εισηγμένη μετοχή στο Χρηματιστήριο Αθηνών (ATHEX: QUAL), που παρέχει θεσμική αξιοπιστία και δυνατότητα πρόσβασης σε κεφάλαια. Τρίτον, τη σημαντική πελατειακή βάση στον δημόσιο τομέα, που αριθμεί πάνω από 250 οργανισμούς. Τέταρτον, τις συμμαχίες με κορυφαίους διεθνείς προμηθευτές τεχνολογίας (Oracle, IBM, SAP). Πέμπτον, το ανεκτέλεστο υπόλοιπο συμβάσεων ύψους 40+ εκατομμυρίων ευρώ.

Παράλληλα, ο Όμιλος παρουσιάζει ορισμένα χαρακτηριστικά που αποτελούν αντικείμενο παρακολούθησης. Η μετοχή εντάσσεται στη μικρή κεφαλαιοποίηση του Χρηματιστηρίου Αθηνών, με περιορισμένη ρευστότητα. Η παράλληλη ενσωμάτωση τριών εταιρειών με διαφορετικές εταιρικές κουλτούρες, λειτουργικές διαδικασίες και τεχνολογικά υποσυστήματα αποτελεί σύνθετη επιχειρησιακή διαδικασία. Κάθε θυγατρική φέρει διακριτές εσωτερικές μεθοδολογίες παράδοσης έργων και αυτόνομα συμβατικά πλαίσια με τους πελάτες της. Η χρηματοδότηση μέσω ομολογιακού δανείου ύψους 19,1 εκατομμυρίων ευρώ αποτελεί σημαντική δανειακή υποχρέωση.

4.5 Δηλωμένη Λογική Εισόδου στην Κυβερνοασφάλεια

Η απόφαση εισόδου στην αγορά κυβερνοασφάλειας μέσω της εξαγοράς της SysteCom αποτελεί την κεντρική κίνηση που εξετάζεται στην παρούσα εργασία. Σύμφωνα με τον Διευθύνοντα Σύμβουλο (CEO) κ. Παναγιώτη Πασχαλάκη, η εξαγορά αντιπροσωπεύει «μία εξαιρετική ευκαιρία για την QnR να επεκταθεί στον τομέα της κυβερνοασφάλειας», τοποθετώντας τον Όμιλο σε θέση ισχυρότερης ικανότητας προστασίας δεδομένων σε ένα περιβάλλον κλιμακούμενων κυβερνοαπειλών.

Η εταιρεία επέλεξε τη μέθοδο εισόδου μέσω εξαγοράς, αντί της εσωτερικής ανάπτυξης. Σύμφωνα με τις εταιρικές ανακοινώσεις, η επιλογή αυτή βασίστηκε στην ανάγκη ταχείας πρόσβασης σε εξειδικευμένο ανθρώπινο δυναμικό, πιστοποιημένες υπηρεσίες και εδραιωμένες πελατειακές σχέσεις. Επιπλέον, η QnR δήλωσε ότι η κίνηση αυτή αποσκοπεί στην αξιοποίηση της υφιστάμενης πελατειακής βάσης 250+ οργανισμών ως αγοράς για υπηρεσίες

κυβερνοασφάλειας, καθώς και στη δημιουργία δυνατοτήτων ολοκληρωμένης παροχής υπηρεσιών που συνδυάζουν πληροφορική και κυβερνοασφάλεια.

Η πελατειακή βάση της SysteCom (βλ. ενότητα 4.3.1) περιλαμβάνει οργανισμούς τόσο από το χρηματοπιστωτικό τομέα όσο και από τις τηλεπικοινωνίες, ενώ η εσωτερική τεχνογνωσία (in-house expertise) της QnR σε ανάπτυξη εφαρμογών, ολοκλήρωση συστημάτων και αυτοματοποίηση διαδικασιών παρουσιάζεται ως συμπληρωματική προς τις υπηρεσίες κυβερνοασφάλειας. Η συνδυασμένη πελατειακή βάση QnR και SysteCom υπερβαίνει αθροιστικά τους 450 μοναδικούς οργανισμούς.

4.6 Σύνδεση με την Παρούσα Έρευνα

Το παρόν κεφάλαιο παρουσίασε τα εμπειρικά δεδομένα σχετικά με την εταιρεία QnR, τη θυγατρική SysteCom και τη στρατηγική κίνηση εισόδου στην κυβερνοασφάλεια. Συνοπτικά, ο Όμιλος QnR μετασχηματίστηκε εντός του 2025 από πάροχο λύσεων πληροφορικής σε διαφοροποιημένο τεχνολογικό όμιλο, με σαφή στόχευση στην κυβερνοασφάλεια, την τεχνητή νοημοσύνη και το επιχειρηματικό λογισμικό. Η εξαγορά της SysteCom αποτελεί τον ακρογωνιαίο λίθο αυτής της στρατηγικής, παρέχοντας τεχνογνωσία, πελατειακή βάση και αναγνωρισιμότητα στην αγορά κυβερνοασφάλειας, ενώ οι εξαγορές της SquareDev και της Alexander Moore ενισχύουν τις δυνατότητες τεχνητής νοημοσύνης και επιχειρηματικού λογισμικού αντίστοιχα.

Τα δεδομένα αυτά, σε συνδυασμό με τα θεωρητικά πλαίσια του Κεφαλαίου 2 (ανάλυση πέντε δυνάμεων Porter, Θεωρία Πόρων RBV/VRIO, Δυναμικές Ικανότητες Teece, τεχνολογική διαφοροποίηση Ceipek, εξαγορές και μετασυγχωνευτική ολοκλήρωση) και τα δεδομένα αγοράς του Κεφαλαίου 3 (ρυθμιστικό πλαίσιο, τεχνολογικές τάσεις, ελληνική αγορά), θα αποτελέσουν τη βάση για τη στρατηγική ανάλυση (strategic analysis) που θα αναπτυχθεί στο Κεφάλαιο 5. Εκεί, τα θεωρητικά εργαλεία θα εφαρμοστούν στα πραγματικά δεδομένα, αξιολογώντας τη θέση της QnR στο ανταγωνιστικό τοπίο, τη βιωσιμότητα του ανταγωνιστικού πλεονεκτήματος και τις στρατηγικές επιλογές για τη μετασυγχωνευτική περίοδο. Η ανάλυση θα ολοκληρωθεί στο Κεφάλαιο 6 με τη συνολική αξιολόγηση (evaluation) και τις προτάσεις για τη βέλτιστη στρατηγική πορεία του Ομίλου.

Βιβλιογραφία Κεφαλαίου

1. QnR. (2025). *Ετήσια έκθεση και εταιρικές ανακοινώσεις 2024–2025*. Quality & Reliability A.B.E.E. https://www.qnr.com.gr

2. SysteCom. (2025). *Εταιρικό προφίλ και υπηρεσίες κυβερνοασφάλειας 2025*. SysteCom S.A. https://www.syscom.gr

Κεφάλαιο 5

Στρατηγική Ανάλυση

5.1 Ανάλυση Πέντε Δυνάμεων Porter στον Ελληνικό Κλάδο Κυβερνοασφάλειας

Το παρόν κεφάλαιο εφαρμόζει τα θεωρητικά πλαίσια που αναλύθηκαν στο Κεφάλαιο 2 στα εμπειρικά δεδομένα των Κεφαλαίων 3 (οικοσύστημα κυβερνοασφάλειας) και 4 (εταιρεία QnR). Η ανάλυση ακολουθεί μια δομή πολλαπλών πλαισίων (multi-framework analysis), ξεκινώντας από την εξωτερική ανάλυση κλάδου (Porter), συνεχίζοντας με την εσωτερική αξιολόγηση πόρων (VRIO), τη δυναμική ανάλυση ικανοτήτων (Teece), την αξιολόγηση τεχνολογικής διαφοροποίησης (Ceipek et al.) και M&A/PMI, και ολοκληρώνοντας με τη σύνθεση SWOT. Η πολυεπίπεδη αυτή προσέγγιση ανταποκρίνεται στην υπόδειξη των Dewi et al. (2025) ότι η βιώσιμη ανταγωνιστικότητα απαιτεί συνδυαστική αξιολόγηση εξωτερικών και εσωτερικών παραγόντων.

Η εφαρμογή του μοντέλου των Πέντε Δυνάμεων (Five Forces) στον ελληνικό κλάδο κυβερνοασφάλειας αποκαλύπτει ένα περιβάλλον μέτριας ελκυστικότητας αλλά σημαντικών ευκαιριών για κατάλληλα τοποθετημένες εταιρείες.

Η *απειλή νέων εισερχομένων* αξιολογείται ως μέτρια προς υψηλή. Αφενός, τα εμπόδια εισόδου είναι σημαντικά. Η ανάγκη εξειδικευμένου ανθρώπινου δυναμικού σε ένα περιβάλλον παγκόσμιου ελλείμματος 4,8 εκατομμυρίων επαγγελματιών κυβερνοασφάλειας, οι πιστοποιήσεις συνεργασίας με διεθνείς κατασκευαστές και η εμπιστοσύνη πελατών σε κρίσιμες υπηρεσίες δημιουργούν σημαντικό κόστος εισόδου. Αφετέρου, η ραγδαία αύξηση της ζήτησης λόγω NIS2 και DORA, σε συνδυασμό με τη δυνατότητα εξ' αποστάσεως παροχής υπηρεσιών, μειώνει τα γεωγραφικά εμπόδια και επιτρέπει σε διεθνείς παρόχους να εισέλθουν στην ελληνική αγορά. Η ψηφιακή φύση του κλάδου σημαίνει ότι νεοφυείς επιχειρήσεις (startups) με καινοτόμες λύσεις μπορούν να αμφισβητήσουν τους εδραιωμένους παρόχους, επιβεβαιώνοντας τις παρατηρήσεις των Dewi et al. (2025) ότι η τεχνολογική αλλαγή μεταβάλλει τα παραδοσιακά εμπόδια εισόδου.

Η *διαπραγματευτική δύναμη των προμηθευτών* είναι υψηλή. Στον κλάδο κυβερνοασφάλειας, οι κύριοι προμηθευτές είναι αφενός οι διεθνείς κατασκευαστές τεχνολογικών λύσεων (Palo Alto Networks, Fortinet, CrowdStrike κ.λπ.) και αφετέρου το εξειδικευμένο ανθρώπινο δυναμικό. Οι κατασκευαστές τεχνολογίας κατέχουν σημαντική ισχύ λόγω υψηλής συγκέντρωσης και μεγάλου κόστους μεταστροφής για τους παρόχους υπηρεσιών. Η εξάρτηση από συγκεκριμένες πλατφόρμες ασφάλειας δημιουργεί κλείδωμα σε προμηθευτή (vendor lock-in). Ταυτόχρονα, η ελλιπής προσφορά εξειδικευμένων επαγγελματιών κυβερνοασφάλειας δίνει σημαντική διαπραγματευτική ισχύ στο ανθρώπινο δυναμικό, αυξάνοντας το μισθολογικό κόστος και τον κίνδυνο αποχώρησης κρίσιμου προσωπικού (key talent attrition).

Η *διαπραγματευτική δύναμη των αγοραστών* αξιολογείται ως μέτρια. Αφενός, η υποχρεωτική συμμόρφωση με τη NIS2 μέσω του Ν. 5160/2024 και τον DORA μειώνει τη δυνατότητα των αγοραστών να αποφύγουν τις επενδύσεις σε κυβερνοασφάλεια, ενισχύοντας τη θέση των παρόχων. Όπως τεκμηρίωσαν οι Rowe και Gallaher (2006), οι κανονισμοί αποτελούν τον κύριο κινητήριο παράγοντα επένδυσης σε κυβερνοασφάλεια (30,1% των οργανισμών), γεγονός ιδιαίτερα σημαντικό στο σημερινό ρυθμιστικό περιβάλλον. Αφετέρου, οι μεγάλοι οργανισμοί (τράπεζες, τηλεπικοινωνίες, δημόσιος τομέας) διαθέτουν σημαντική αγοραστική ισχύ λόγω του μεγέθους των συμβάσεων, ενώ η αυξανόμενη τεχνογνωσία τους σε θέματα κυβερνοασφάλειας ενισχύει την ικανότητα αξιολόγησης και σύγκρισης προσφορών.

Η *απειλή υποκατάστατων* είναι χαμηλή προς μέτρια. Οι υπηρεσίες κυβερνοασφάλειας δεν μπορούν να αντικατασταθούν πλήρως, καθώς η ρυθμιστική υποχρέωση είναι δεσμευτική. Ωστόσο, υπάρχει κίνδυνος αντικατάστασης εξωτερικών παρόχων από εσωτερικές ομάδες κυβερνοασφάλειας σε μεγάλους οργανισμούς, καθώς και κίνδυνος από αυτοματοποιημένες λύσεις βασισμένες σε τεχνητή νοημοσύνη που μειώνουν την ανάγκη για ανθρώπινη παρέμβαση. Παρά ταύτα, η πολυπλοκότητα των σύγχρονων κυβερνοαπειλών και η ανάγκη για συνεχή ανθρώπινη εποπτεία (human oversight) περιορίζουν αυτή την απειλή.

Η *ένταση του υφιστάμενου ανταγωνισμού* είναι μέτρια στην ελληνική αγορά. Ενώ υπάρχουν αρκετοί εδραιωμένοι πάροχοι κυβερνοασφάλειας, η ελληνική αγορά αξίας 185,3 εκατομμυρίων δολαρίων είναι σχετικά μικρή σε σύγκριση με άλλες ευρωπαϊκές αγορές, αλλά αναπτύσσεται με ρυθμό 8,36% ετησίως. Ο ρυθμός ανάπτυξης μετριάζει τον ανταγωνισμό, καθώς η αγορά μεγαλώνει αρκετά ώστε να απορροφήσει νέους παίκτες χωρίς απαραίτητα να

μειωθούν τα μερίδια των υπαρχόντων (Porter, 2008). Η διαφοροποίηση μεταξύ παρόχων βασίζεται κυρίως στην εξειδίκευση τομέα, τις πιστοποιήσεις και την ικανότητα ολοκληρωμένης κάλυψης αναγκών. Αξίζει να σημειωθεί ότι οι Mazzoccoli και Naldi (2022) τεκμηριώνουν πώς η βελτιστοποίηση των επενδύσεων κυβερνοασφάλειας παραμένει πολύπλοκη για τους οργανισμούς, γεγονός που ενισχύει τη θέση εξειδικευμένων παρόχων που μπορούν να προσφέρουν καθοδήγηση στην κατανομή πόρων ασφάλειας. Ο Πίνακας 5.1 συνοψίζει τα αποτελέσματα της ανάλυσης Πέντε Δυνάμεων.

Πίνακας 5.1: Ανάλυση Πέντε Δυνάμεων Porter στον Ελληνικό Κλάδο Κυβερνοασφάλειας

Δύναμη	Ένταση	Κύριοι Παράγοντες
Απειλή Νέων Εισερχομένων	Μέτρια-Υψηλή	Υψηλά εμπόδια εξειδίκευσης, αλλά χαμηλά γεωγραφικά εμπόδια
Διαπραγματευτική Δύναμη Προμηθευτών	Υψηλή	Συγκέντρωση κατασκευαστών, έλλειμμα ταλέντων
Διαπραγματευτική Δύναμη Αγοραστών	Μέτρια	Υποχρεωτική συμμόρφωση, αλλά μεγάλο μέγεθος συμβάσεων
Απειλή Υποκατάστατων	Χαμηλή-Μέτρια	Ρυθμιστική υποχρέωση, πολυπλοκότητα απειλών
Ένταση Ανταγωνισμού	Μέτρια	Αναπτυσσόμενη αγορά (CAGR 8,36%), διαφοροποίηση

Συνολικά, η ανάλυση Porter αναδεικνύει ότι ο κλάδος της κυβερνοασφάλειας στην Ελλάδα παρουσιάζει ευνοϊκό περιβάλλον για εταιρείες που διαθέτουν εδραιωμένη πελατειακή βάση, εξειδικευμένο ανθρώπινο δυναμικό και ικανότητα ολοκληρωμένης παροχής υπηρεσιών. Η ρυθμιστικά καθοδηγούμενη ζήτηση αποτελεί δομικό χαρακτηριστικό του κλάδου που ευνοεί τοποθετημένους παρόχους. Ειδικά η τοποθέτηση του Ομίλου QnR αξιολογείται θετικά σε αυτό το πλαίσιο. Η εξαγορά της SysteCom παρέχει εξειδίκευση και πιστοποιήσεις που αποτελούν εμπόδιο εισόδου για ανταγωνιστές, ενώ η υφιστάμενη πελατειακή βάση στον δημόσιο τομέα και το χρηματοπιστωτικό κλάδο, τους δύο πλέον ρυθμιστικά πιεσμένους τομείς, εξασφαλίζει πρόσβαση σε πελάτες με υποχρεωτική ζήτηση υπηρεσιών κυβερνοασφάλειας. Η ανάλυση επιβεβαιώνει ωστόσο και την προειδοποίηση των Dewi et al. (2025) ότι το μοντέλο Porter

χρήζει συμπλήρωσης από δυναμικά εργαλεία, καθώς η ταχεία τεχνολογική εξέλιξη στην κυβερνοασφάλεια μπορεί να αλλάξει τις ισορροπίες δυνάμεων σε σύντομο χρονικό διάστημα.

5.2 Ανάλυση VRIO του Ομίλου QnR

Η εφαρμογή του πλαισίου VRIO (Barney, 1991) στους πόρους και τις ικανότητες του Ομίλου QnR μετά τις εξαγορές του 2025 αποκαλύπτει τις πηγές ανταγωνιστικού πλεονεκτήματος και τα σημεία που χρήζουν ενίσχυσης.

Ο πρώτος πόρος που εξετάζεται είναι η *πελατειακή βάση του Ομίλου*. Η συνδυασμένη βάση QnR και SysteCom, που υπερβαίνει τους 450 μοναδικούς οργανισμούς, πληροί σαφώς το κριτήριο της αξίας (Value), καθώς παρέχει άμεσα προσβάσιμη αγορά για υπηρεσίες κυβερνοασφάλειας. Η σπανιότητα είναι μέτρια, καθώς λίγοι ανταγωνιστές στην ελληνική αγορά διαθέτουν ταυτόχρονα πελάτες τόσο στο δημόσιο τομέα (πυρήνας QnR) όσο και στο χρηματοπιστωτικό τομέα (πυρήνας SysteCom). Η μη ικανότητα μίμησης από άλλες εταιρείες (Imitability) είναι σημαντική, καθώς οι μακροχρόνιες σχέσεις εμπιστοσύνης με πελάτες δε μπορούν να αναπαραχθούν εύκολα. Ωστόσο, η οργανωτική αξιοποίηση δεν είναι πλήρης, καθώς οι δύο πελατειακές βάσεις δεν έχουν ακόμη ενοποιηθεί πλήρως. Υπάρχει γενικότερα ένα προσωρινό ανταγωνιστικό πλεονέκτημα, με δυνατότητα εξέλιξης σε βιώσιμο μετά την ολοκλήρωση της ενσωμάτωσης.

Ο δεύτερος πόρος είναι η *εξειδικευμένη τεχνογνωσία κυβερνοασφάλειας* της SysteCom. Η αξία είναι προφανής, δεδομένης της αυξανόμενης ζήτησης. Η σπανιότητα είναι υψηλή, καθώς η δωδεκαετής εμπειρία της SysteCom σε κρίσιμες υπηρεσίες (SOC, penetration testing, ransomware containment) και οι πιστοποιημένες συνεργασίες με κορυφαίους κατασκευαστές δεν είναι εύκολο να αντιγραφούν. Η απομίμηση ενισχύεται από την εναπόθεση γνώσης σε οργανωτικές ρουτίνες, όπως τονίζει ο Barney (1991). Η οργανωτική αξιοποίηση αποτελεί σημείο κρίσιμης σημασίας. Η διατήρηση της αυτονομίας της SysteCom κατά τη μεταβατική περίοδο, μέσω της σταδιακής απόκτησης ποσοστού (60% αρχικά, υπόλοιπο 40% εντός τριετίας), διασφαλίζει τη διατήρηση κρίσιμης τεχνογνωσίας.

Ο τρίτος πόρος είναι η *ικανότητα ολοκληρωμένης παροχής υπηρεσιών*. Ο συνδυασμός πληροφορικής (QnR), κυβερνοασφάλειας (SysteCom), τεχνητής νοημοσύνης (SquareDev) και επιχειρηματικού λογισμικού (Alexander Moore) δημιουργεί μια μοναδική πρόταση αξίας στην ελληνική αγορά. Η αξία είναι σημαντική, καθώς οι πελάτες αναζητούν ολιστικές λύσεις (end-

to-end solutions) που μειώνουν τον αριθμό των προμηθευτών και απλοποιούν τη διαχείριση των ψηφιακών υποδομών. Οι Agustian et al. (2023) υπογραμμίζουν ότι η δημιουργία αποτελεσματικότερων εσωτερικών διαδικασιών μέσω ψηφιακής τεχνολογίας αποτελεί κρίσιμο μηχανισμό ανταγωνιστικού πλεονεκτήματος, και η ικανότητα παροχής ολοκληρωμένων λύσεων ψηφιακού μετασχηματισμού συνοδευόμενων από κυβερνοασφάλεια αντικατοπτρίζει ακριβώς αυτή τη λογική. Η σπανιότητα είναι εξαιρετικά υψηλή, καθώς κανένας ελληνικός πάροχος δεν προσφέρει ταυτόχρονα αυτόν τον συνδυασμό ικανοτήτων. Η απομίμηση είναι σημαντική, καθώς η αναπαραγωγή θα απαιτούσε αντίστοιχες πολλαπλές εξαγορές. Η οργανωτική αξιοποίηση παραμένει πρόκληση, καθώς η πραγματική ενοποίηση τεσσάρων εταιρειών βρίσκεται σε αρχικό στάδιο. Υπάρχει λοιπόν ένα δυνητικά βιώσιμο ανταγωνιστικό πλεονέκτημα, υπό την προϋπόθεση επιτυχούς ολοκλήρωσης των συγχωνεύσεων.

Ο τέταρτος πόρος είναι η *θεσμική αξιοπιστία ως εισηγμένη εταιρεία στο Χρηματιστήριο Αθηνών*. Η αξία είναι σημαντική για τη συμμετοχή σε μεγάλους δημόσιους διαγωνισμούς και για την πρόσβαση σε κεφαλαιαγορές. Η σπανιότητα είναι μέτρια, καθώς υπάρχουν και άλλες εισηγμένες εταιρείες τεχνολογίας. Η απομίμηση είναι σχετικά χαμηλή. Εδώ, υπάρχει μια ανταγωνιστική ισοτιμία σε γενικό επίπεδο, αλλά πλεονέκτημα σε συγκεκριμένα τμήματα αγοράς (δημόσιοι διαγωνισμοί, θεσμικοί πελάτες).

Ο πέμπτος πόρος είναι οι *στρατηγικές συμμαχίες με διεθνείς κατασκευαστές τεχνολογίας*. Η πιστοποιημένη συνεργασία της QnR με Oracle (από 1993) και IBM (από 2022), σε συνδυασμό με τις πιστοποιημένες συνεργασίες της SysteCom με Palo Alto Networks, Fortinet και CrowdStrike, δημιουργεί ένα δίκτυο σχέσεων που παρέχει αξία μέσω πρόσβασης σε προηγμένες τεχνολογίες και εκπαίδευση. Η σπανιότητα είναι μέτρια, καθώς και άλλοι πάροχοι μπορούν να αποκτήσουν αντίστοιχες πιστοποιήσεις. Ωστόσο, η απομίμηση ενισχύεται από τη μακροχρόνια φύση ορισμένων συνεργασιών και τη σωρευτική εμπιστοσύνη. Επομένως εδώ, υπάρχει ένα προσωρινό ανταγωνιστικό πλεονέκτημα. Ο Πίνακας 5.2 συνοψίζει τα αποτελέσματα της ανάλυσης VRIO.

Πίνακας 5.2: Ανάλυση VRIO Βασικών Πόρων Ομίλου QnR

Πόρος / Ικανότητα	V	R	I	O	Αξιολόγηση
Συνδυασμένη πελατειακή βάση (450+)	Ναι	Μέτρια	Ναι	Μερικώς	Προσωρινό πλεονέκτημα
Τεχνογνωσία κυβερνοασφάλειας SysteCom	Ναι	Υψηλή	Ναι	Ναι	Βιώσιμο πλεονέκτημα
Ολοκληρωμένη παροχή υπηρεσιών (IT+Cyber+AI)	Ναι	Υψηλή	Ναι	Μερικώς	Δυνητικό βιώσιμο πλεονέκτημα
Θεσμική αξιοπιστία (ATHEX)	Ναι	Μέτρια	Χαμηλή	Ναι	Ανταγωνιστική ισοτιμία
Στρατηγικές συμμαχίες (Oracle, IBM, Palo Alto)	Ναι	Μέτρια	Μέτρια	Ναι	Προσωρινό πλεονέκτημα

Η ανάλυση VRIO αναδεικνύει ότι οι σημαντικότεροι πόροι του Ομίλου, δηλαδή η εξειδικευμένη τεχνογνωσία και η ικανότητα ολοκληρωμένης παροχής υπηρεσιών, πληρούν τα κριτήρια αξίας, σπανιότητας και απομίμησης, αλλά η πλήρης οργανωτική αξιοποίηση εξαρτάται κρίσιμα από την επιτυχία της ολοκλήρωσης των συγχωνεύσεων. Αυτό επιβεβαιώνει τη θεωρητική θέση ότι η RBV, ενώ αποτελεί ισχυρό αναλυτικό εργαλείο, χρήζει συμπλήρωσης από τη θεωρία δυναμικών ικανοτήτων για να ερμηνεύσει τη μεταβατική δυναμική (Dewi et al., 2025).

5.3 Δυναμικές Ικανότητες και Στρατηγικές Κινήσεις της QnR

Η εφαρμογή του πλαισίου δυναμικών ικανοτήτων του Teece (2007) στις στρατηγικές κινήσεις της QnR κατά την περίοδο 2024-2025 αναδεικνύει τον τρόπο με τον οποίο η εταιρεία αξιοποίησε τις τρεις θεμελιώδεις διαστάσεις, αίσθηση (sensing), σύλληψη (seizing) και αναδιαμόρφωση (reconfiguring).

Στη διάσταση της αίσθησης (sensing), η QnR κατέδειξε ικανότητα εντοπισμού στρατηγικών ευκαιριών στο μεταβαλλόμενο περιβάλλον. Η αναγνώριση ότι η ενσωμάτωση της

Οδηγίας NIS2 στο ελληνικό δίκαιο μέσω του Ν. 5160/2024 θα δημιουργούσε κύμα ζήτησης υπηρεσιών κυβερνοασφάλειας, σε συνδυασμό με την παρατήρηση ότι η τεχνητή νοημοσύνη μετασχηματίζει τόσο τις κυβερνοαπειλές όσο και τις λύσεις αντιμετώπισής τους, αντικατοπτρίζει μια συστηματική διαδικασία περιβαλλοντικής σάρωσης. Η απόφαση χρηματοδότησης μέσω κοινοπρακτικού ομολογιακού δανείου τον Ιούλιο 2024, δηλαδή πριν από τη ψήφιση του Ν. 5160/2024 τον Σεπτέμβριο 2024, υποδηλώνει ότι η QnR είχε ήδη αισθανθεί την ευκαιρία και είχε ξεκινήσει τη χρηματοοικονομική προετοιμασία.

Στη διάσταση της σύλληψης (seizing), η QnR μετέτρεψε τις αναγνωρισμένες ευκαιρίες σε συγκεκριμένες στρατηγικές επενδύσεις. Η ταχεία εκτέλεση τριών εξαγορών σε διάστημα δέκα μηνών (Ιανουάριος, Μάρτιος, Οκτώβριος 2025) αντικατοπτρίζει αποφασιστικότητα στη σύλληψη ευκαιριών. Η επιλογή της SysteCom ως κεντρικού στόχου εξαγοράς ήταν στρατηγικά εύστοχη. Η εταιρεία διέθετε τεκμηριωμένη τεχνογνωσία, βραβευμένες υπηρεσίες, πελατειακή βάση στους πλέον ρυθμιστικά πιεσμένους τομείς (τραπεζικός, ενεργειακός, τηλεπικοινωνιακός) και θετική οικονομική πορεία. Η σύλληψη ενισχύθηκε περαιτέρω με την εξαγορά της SquareDev, η οποία πρόσθεσε δυνατότητες τεχνητής νοημοσύνης και μια βάση στην κεντρική Ευρώπη, αναγνωρίζοντας ότι η σύγκλιση AI και κυβερνοασφάλειας αποτελεί βασική τάση του κλάδου.

Στη διάσταση της αναδιαμόρφωσης (reconfiguring), ο Όμιλος βρίσκεται στο πλέον κρίσιμο στάδιο. Η αναδιαμόρφωση περιλαμβάνει την ενοποίηση τεσσάρων διακριτών εταιρικών οντοτήτων σε έναν συνεκτικό τεχνολογικό όμιλο, τη δημιουργία μηχανισμών διασταυρούμενων πωλήσεων (cross-selling mechanisms) και την ανάπτυξη ολοκληρωμένων λύσεων που συνδυάζουν πληροφορική, κυβερνοασφάλεια και τεχνητή νοημοσύνη. Κατά τον Teece (2007), η ικανότητα αναδιαμόρφωσης είναι η πλέον δύσκολη και κρίσιμη διάσταση, καθώς απαιτεί τόσο οργανωτικές αλλαγές όσο και αλλαγή νοοτροπίας. Η επιτυχία αυτής της διάστασης θα καθορίσει τελικώς εάν οι εξαγορές θα μετατραπούν σε βιώσιμο ανταγωνιστικό πλεονέκτημα ή θα παραμείνουν απλώς μια διεύρυνση χαρτοφυλακίου. Συγκεκριμένα, η αναδιαμόρφωση πρέπει να αντιμετωπίσει τρεις κρίσιμες προκλήσεις. Την ενοποίηση των εμπορικών διαδικασιών ώστε οι πωλητές της QnR να μπορούν να προωθούν υπηρεσίες κυβερνοασφάλειας SysteCom και αντιστρόφως, τη δημιουργία κοινών μεθοδολογιών παράδοσης έργων και την ανάπτυξη μηχανισμών μεταφοράς γνώσης μεταξύ των εταιρειών.

Τα εμπειρικά ευρήματα των Dewi et al. (2025) ενισχύουν αυτή την ανάλυση. Η ικανότητα συνεργασίας, η οποία αναδείχθηκε ως η ισχυρότερη διάσταση των δυναμικών ικανοτήτων στην έρευνά τους (μέσος όρος 5,06/7), είναι κρίσιμη για τον Όμιλο QnR. Η αποτελεσματική συνεργασία μεταξύ QnR, SysteCom, SquareDev και Alexander Moore αποτελεί προϋπόθεση για τη δημιουργία αξίας. Αντίστοιχα, η ικανότητα καινοτομίας, η πιο αδύναμη διάσταση στα ευρήματα Dewi et al. (μέσος όρος 3,69/7), αποτελεί σημείο που χρήζει ιδιαίτερης προσοχής για τον Όμιλο.

5.4 Τεχνολογική Διαφοροποίηση: Αξιολόγηση Εισόδου στην Κυβερνοασφάλεια

Η εφαρμογή του θεωρητικού πλαισίου τεχνολογικής διαφοροποίησης (technological diversification) των Ceipek et al. (2020) στην περίπτωση της QnR αναδεικνύει ότι η είσοδος στην κυβερνοασφάλεια αποτελεί κατά κύριο λόγο συγγενή τεχνολογική διαφοροποίηση.

Η QnR διαθέτει ιστορική τεχνογνωσία σε πληροφοριακά συστήματα, ανάπτυξη λογισμικού, ολοκλήρωση συστημάτων και υπολογιστικό νέφος. Αυτές οι ικανότητες βρίσκονται κοντά στον τεχνολογικό πυρήνα (core-field) της κυβερνοασφάλειας, η οποία απαιτεί βαθιά κατανόηση των δικτύων, των λειτουργικών συστημάτων, των αρχιτεκτονικών λογισμικού και των πρωτοκόλλων επικοινωνίας. Σύμφωνα με τους Ceipek et al. (2020), η συγγενής τεχνολογική διαφοροποίηση μειώνει το κόστος εξερεύνησης και επιταχύνει τον εντοπισμό νέων ερευνητικών ευκαιριών, καθώς η πρόσβαση σε ποικιλία συγγενών τεχνολογικών πεδίων γνώσης επηρεάζει θετικά την κλίση της επιχείρησης να εντοπίζει νέες λύσεις.

Ωστόσο, η διαφοροποίηση δεν είναι αποκλειστικά συγγενής. Η κυβερνοασφάλεια ως υπηρεσία (cybersecurity-as-a-service) απαιτεί εξειδικευμένες ικανότητες που υπερβαίνουν την παραδοσιακή πληροφορική, δηλαδή περιέχει ανάλυση κυβερνοαπειλών (threat analysis), ψηφιακή εγκληματολογία (digital forensics), αντιμετώπιση περιστατικών (incident response) και λειτουργία κέντρου επιχειρήσεων ασφάλειας (SOC). Αυτές οι ικανότητες δεν υπήρχαν στην QnR πριν από την εξαγορά της SysteCom, γεγονός που δικαιολογεί την επιλογή εξαγοράς αντί εσωτερικής ανάπτυξης. Η εξαγορά λειτούργησε ως μηχανισμός ταχείας πρόσβασης σε μη συγγενείς ικανότητες, μετριάζοντας τους κινδύνους που τονίζουν οι Ceipek et al. (2020) για τη μη συγγενή διαφοροποίηση.

Η αξιολόγηση μέσω του πρίσματος εξερεύνησης και εκμετάλλευσης αναδεικνύει ένα ισορροπημένο μείγμα. Η εκμετάλλευση αφορά την αξιοποίηση υπαρχουσών ικανοτήτων ολοκλήρωσης συστημάτων και πελατειακών σχέσεων για την πώληση υπηρεσιών κυβερνοασφάλειας σε υφιστάμενους πελάτες. Η εξερεύνηση αφορά τη δημιουργία νέων λύσεων κυβερνοασφάλειας ενισχυμένων με τεχνητή νοημοσύνη (AI-enhanced cybersecurity), συνδυάζοντας την τεχνογνωσία SquareDev και SysteCom. Η ισορροπία αυτή, κατά τους Ceipek et al. (2020), είναι κρίσιμη για τη μακροπρόθεσμη βιωσιμότητα της στρατηγικής.

Η ανάλυση αυτή ενισχύεται από τα ευρήματα των Agustian et al. (2023), οι οποίοι υποστηρίζουν ότι το ανταγωνιστικό πλεονέκτημα στην ψηφιακή εποχή συνδέεται με την ικανότητα ταχείας υιοθέτησης νέων τεχνολογιών και ενσωμάτωσής τους στα επιχειρηματικά μοντέλα. Η QnR, μέσω της εξαγοράς τεχνολογικών εταιρειών αντί της εσωτερικής ανάπτυξης, επέλεξε μια στρατηγική ταχείας πρόσβασης σε νέες ικανότητες, αντισταθμίζοντας το χρόνο που θα απαιτούσε η οργανική ανάπτυξη εξειδίκευσης κυβερνοασφάλειας. Η επιλογή αυτή συνάδει με τη θέση ότι ο ψηφιακός μετασχηματισμός δεν αποτελεί πλέον επιλογή αλλά αναγκαιότητα για τη διατήρηση της ανταγωνιστικότητας. Παράλληλα, η εξαγορά τριών εταιρειών σε διαφορετικούς αλλά συμπληρωματικούς τομείς (κυβερνοασφάλεια, AI, SAP) δημιουργεί συνθήκες τεχνολογικής συμπληρωματικότητας που ενισχύει τόσο την εξερευνητική όσο και την εκμεταλλευτική καινοτομία.

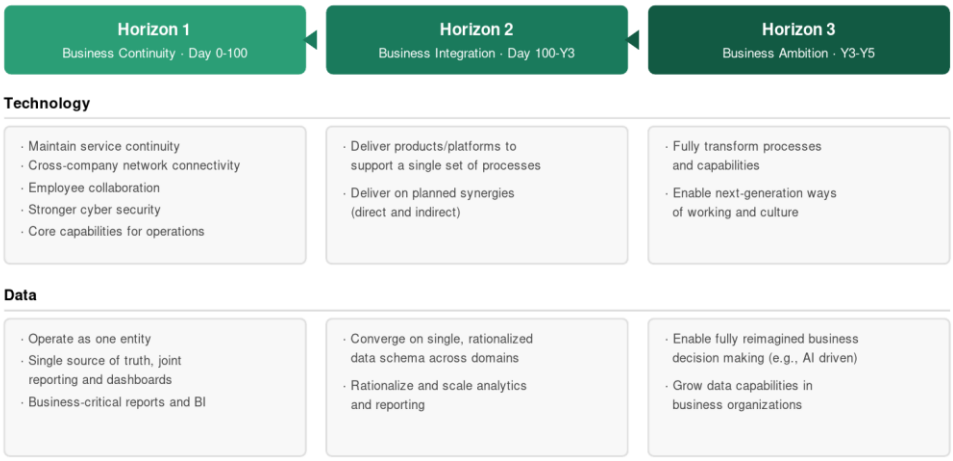
5.5 Ανάλυση Εξαγοράς και Μετασυγχωνευτικής Ολοκλήρωσης (M&A/PMI)

Η εξαγορά της SysteCom αξιολογείται μέσω του θεωρητικού πλαισίου των εξαγορών και της ολοκλήρωσης των συγχωνεύσεων (PMI), αξιοποιώντας τις στρατηγικές ολοκλήρωσης πληροφοριακών συστημάτων των Lace και Kirikova (2022), το μοντέλο τριών οριζόντων της BCG (Milde et al., 2024) και την ανάλυση κινδύνων του Usianeneh (2025).

Αναφορικά με τη στρατηγική ολοκλήρωσης, η περίπτωση QnR-SysteCom φαίνεται να κινείται μεταξύ του μοντέλου συνύπαρξης (coexistence) και του μοντέλου συνδυασμού βέλτιστων πρακτικών (best-of-breed) (Lace & Kirikova, 2022). Η δομή σταδιακής απόκτησης (60% αρχικά) και η διατήρηση αυτόνομης λειτουργίας της SysteCom κατά τη μεταβατική περίοδο υποδηλώνουν μια προσέγγιση συνύπαρξης που σταδιακά θα εξελιχθεί σε βέλτιστη σύνθεση. Η επιλογή αυτή είναι στρατηγικά ορθή, δεδομένου ότι η SysteCom εξυπηρετεί

κρίσιμες υπηρεσίες ασφαλείας για τράπεζες και τηλεπικοινωνιακούς παρόχους, όπου η αδιάλειπτη λειτουργία είναι απόλυτη προτεραιότητα.

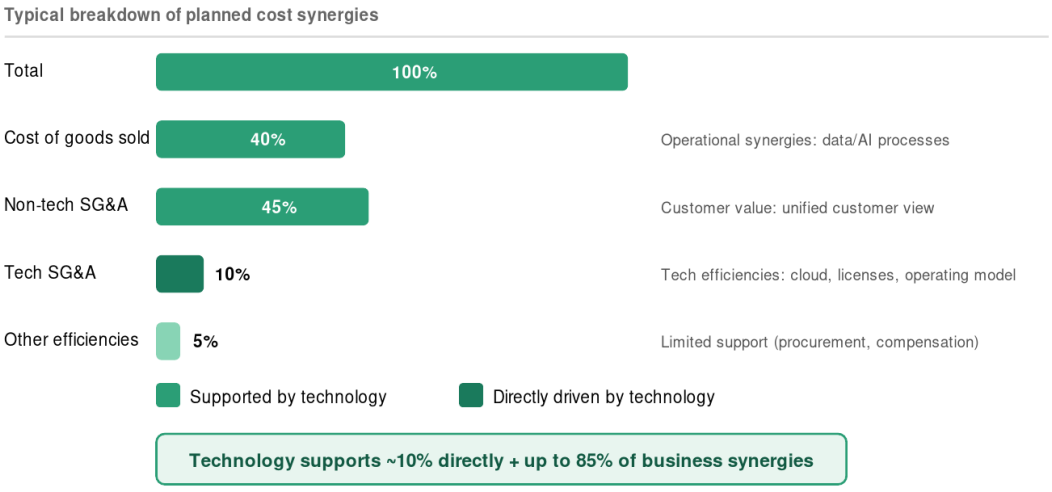
Εφαρμόζοντας το μοντέλο τριών οριζόντων (three horizons model) της BCG (Milde et al., 2024), η πορεία ολοκλήρωσης QnR-SysteCom μπορεί να δομηθεί ως εξής. Στον πρώτο ορίζοντα (Horizon 1, πρώτες 100 ημέρες), η προτεραιότητα ήταν η διασφάλιση της επιχειρησιακής συνέχειας: ενοποίηση μέτρων κυβερνοασφάλειας μεταξύ των δύο εταιρειών, εγκατάσταση κοινών δικτύων επικοινωνίας και χαρτογράφηση πελατειακών αλληλεπικαλύψεων. Η σημασία αυτού του βήματος ενισχύεται από την παρατήρηση της BCG ότι οι κυβερνοεπιθέσεις αυξάνονται σημαντικά αμέσως μετά από εξαγορά (Milde et al., 2024), γεγονός ιδιαίτερα κρίσιμο και παράδοξο όταν η εξαγοραζόμενη εταιρεία δραστηριοποιείται στην κυβερνοασφάλεια: μια αποτυχία ασφάλειας κατά τη μεταβατική περίοδο θα υπονόμευε την αξιοπιστία ολόκληρου του Ομίλου. Στον δεύτερο ορίζοντα (Horizon 2, μήνες 4 έως 30), η εστίαση μετατοπίζεται στην ανάπτυξη διασταυρούμενων πωλήσεων (cross-selling), την ενοποίηση εμπορικών διαδικασιών και τη δημιουργία κοινών πλατφορμών εξυπηρέτησης πελατών. Στον τρίτο ορίζοντα (Horizon 3, έτη 2-5), ο στόχος είναι η δημιουργία ολοκληρωμένων λύσεων που συνδυάζουν πληροφορική, κυβερνοασφάλεια και τεχνητή νοημοσύνη, αξιοποιώντας πλήρως τις συνέργειες μεταξύ QnR, SysteCom και SquareDev. Η BCG εκτιμά ότι η τεχνολογία υποστηρίζει έως και 85% των επιχειρηματικών συνεργειών σε διάφορες κατηγορίες κόστους (Milde et al., 2024), αναδεικνύοντας τη σημασία της τεχνολογικής ολοκλήρωσης.



Σχήμα 5.2: Μοντέλο τριών οριζόντων μετασυγχωνευτικής ολοκλήρωσης: ο ρόλος της τεχνολογίας και των δεδομένων

Πηγή: Milde et al. (2024, Exhibit 1), Boston Consulting Group

Σχήμα 5.2: Μοντέλο τριών οριζόντων μετασυγχωνευτικής ολοκλήρωσης: ο ρόλος της τεχνολογίας και των δεδομένων (Πηγή: Milde et al., 2024, Exhibit 1)



Σχήμα 5.3: Συνεισφορά τεχνολογίας στις συνέργειες κόστους κατά τη PMI

Πηγή: Milde et al. (2024, Exhibit 2), Boston Consulting Group

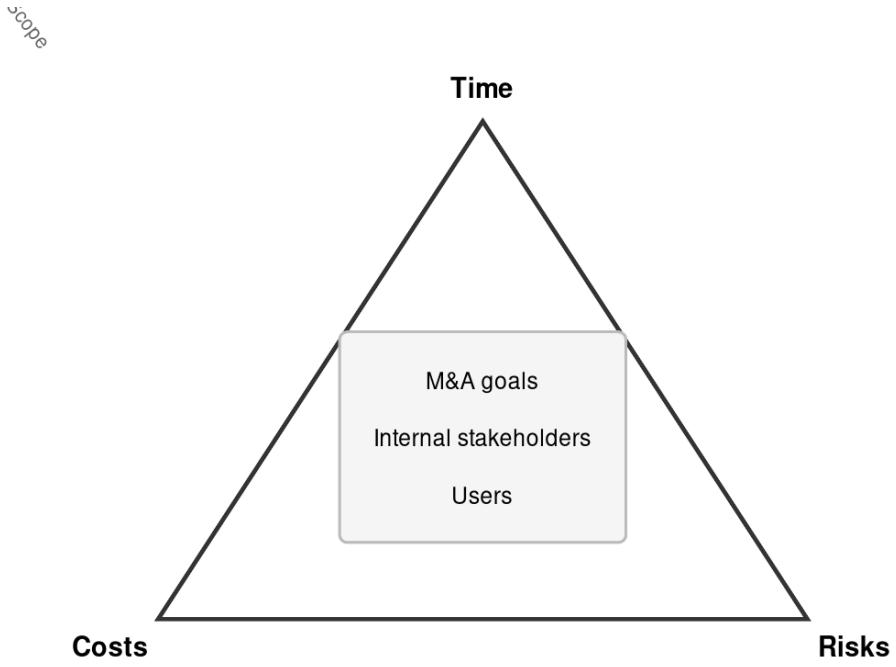
Σχήμα 5.3: Συνεισφορά τεχνολογίας στις συνέργειες κόστους κατά τη μετασυγχωνευτική ολοκλήρωση (Πηγή: Milde et al., 2024, Exhibit 2)

Αναφορικά με τους κινδύνους PMI, η ανάλυση του Usianeneh (2025) αναδεικνύει τέσσερις κρίσιμους παράγοντες που αφορούν άμεσα τον Όμιλο QnR. Πρώτον, *η σύγκρουση εταιρικής κουλτούρας ανάμεσα στις επιχειρήσεις*. Η QnR ως εισηγμένη εταιρεία με τριακονταετή ιστορία και η SysteCom ως ευέλικτη, ιδρυτοκεντρική εταιρεία κυβερνοασφάλειας αντιπροσωπεύουν διαφορετικά οργανωτικά πρότυπα. Δεύτερον, η *απώλεια*

βασικού ανθρώπινου δυναμικού (key talent attrition): σε έναν κλάδο με παγκόσμιο έλλειμμα 4,8 εκατομμυρίων επαγγελματιών, η αποχώρηση κρίσιμου προσωπικού μετά από εξαγορά αποτελεί σημαντικό κίνδυνο. Τρίτον, *η ασυμβατότητα τεχνολογικών πλατφορμών* (platform incompatibility) μεταξύ των τεσσάρων εταιρειών. Τέταρτον, η υποεκτίμηση της πολυπλοκότητας ολοκλήρωσης (integration complexity underestimation), ιδίως όταν η QnR ενσωματώνει παράλληλα τρεις εταιρείες.

Η αντιμετώπιση αυτών των κινδύνων απαιτεί μεθοδική σχεδίαση, ξεκάθαρη διακυβέρνηση (governance) και ευέλικτο χρονοδιάγραμμα ολοκλήρωσης (Usianeneh, 2025). Στην περίπτωση της QnR, η επιλογή σταδιακής απόκτησης ποσοστού (60% αρχικά) αποτελεί μηχανισμό μετριασμού του κινδύνου, καθώς διατηρεί τα κίνητρα της ιδρύτριας μετόχου να παραμείνει ενεργή κατά τη μεταβατική περίοδο. Ταυτόχρονα, η σύμπραξη QnR (τεχνολογίες πληροφορικής) και SysteCom (κυβερνοασφάλεια) παρουσιάζει χαρακτηριστικά τεχνολογικής συμβατότητας που διευκολύνουν την ενοποίηση. Η κοινή τεχνολογική γλώσσα, η παρόμοια πελατειακή βάση (μεγάλοι οργανισμοί δημόσιου και ιδιωτικού τομέα) και η συμπληρωματικότητα υπηρεσιών μειώνουν τον κίνδυνο αποτυχίας ολοκλήρωσης σε σύγκριση με εξαγορές μεταξύ τεχνολογικά ασύνδετων κλάδων.

Ένα επιπρόσθετο σημείο αφορά τον *χρηματοοικονομικό σχεδιασμό* (financial planning) της εξαγοράς. Το τίμημα 1,5 εκατομμυρίων ευρώ για το 60% της SysteCom αντιστοιχεί σε αποτίμηση περίπου 2,5 εκατομμυρίων ευρώ, ενώ ο κύκλος εργασιών της εταιρείας ανέρχεται σε 2,7 εκατομμύρια ευρώ (2023) με αναμενόμενη υπέρβαση των 3 εκατομμυρίων ευρώ το 2024. Ο λόγος τιμήματος προς κύκλο εργασιών (price-to-revenue ratio) κάτω του 1x υποδηλώνει μια εξαγορά σε εύλογη αποτίμηση, ιδιαίτερα για εταιρεία κυβερνοασφάλειας με βραβευμένες υπηρεσίες και πελατειακή βάση που περιλαμβάνει τις τέσσερις συστημικές τράπεζες.



Σχήμα 5.1: Τρίγωνο διαχείρισης ολοκλήρωσης ΠΣ κατά τη μετασυγχωνευτική ολοκλήρωση
Πηγή: Lace & Kirikova (2022, Figure 1)

Σχήμα 5.1: Τρίγωνο διαχείρισης ολοκλήρωσης πληροφοριακών συστημάτων κατά τη μετασυγχωνευτική ολοκλήρωση (Πηγή: Lace & Kirikova, 2022, Figure 1)

5.6 Ανάλυση SWOT

Η σύνθεση των αναλύσεων Porter, VRIO, δυναμικών ικανοτήτων και M&A/PMI αποκρυσταλλώνεται σε μια ολοκληρωμένη ανάλυση SWOT (Strengths, Weaknesses, Opportunities, Threats), αξιοποιώντας τη μεθοδολογία που προτείνουν οι Sihite et al. (2025) για τον ψηφιακό μετασχηματισμό επιχειρήσεων.

Τα δυνατά σημεία (Strengths) του Ομίλου QnR περιλαμβάνουν τη μακρόχρονη παρουσία στην ελληνική αγορά πληροφορικής (30+ έτη) με αναγνωρισιμότητα επωνυμίας και εμπιστοσύνη πελατών, τη συνδυασμένη πελατειακή βάση 450+ οργανισμών που παρέχει άμεσα προσβάσιμη αγορά, την εξειδικευμένη τεχνογνωσία κυβερνοασφάλειας μέσω SysteCom (δωδεκαετής εμπειρία, βραβεύσεις, πιστοποιημένες συνεργασίες), τις ικανότητες τεχνητής νοημοσύνης μέσω SquareDev, τις στρατηγικές συμμαχίες με Oracle, IBM και SAP, την εισαγωγή στο Χρηματιστήριο Αθηνών που προσδίδει θεσμική αξιοπιστία, και το ανεκτέλεστο υπόλοιπο συμβάσεων 40+ εκατομμυρίων ευρώ.

Οι αδυναμίες (Weaknesses) περιλαμβάνουν τη μόχλευση (leverage) λόγω ομολογιακού δανείου 19,1 εκατομμυρίων ευρώ, τους κινδύνους ταυτόχρονης ενσωμάτωσης τριών εταιρειών με διαφορετικές κουλτούρες και τεχνολογικά υποσυστήματα, την περιορισμένη ρευστότητα μετοχής, τον κίνδυνο διάσπασης διοικητικής εστίασης (management bandwidth constraints) λόγω παράλληλης διαχείρισης πολλαπλών ενσωματώσεων, και τη σχετικά μικρή κλίμακα σε σύγκριση με διεθνείς ανταγωνιστές.

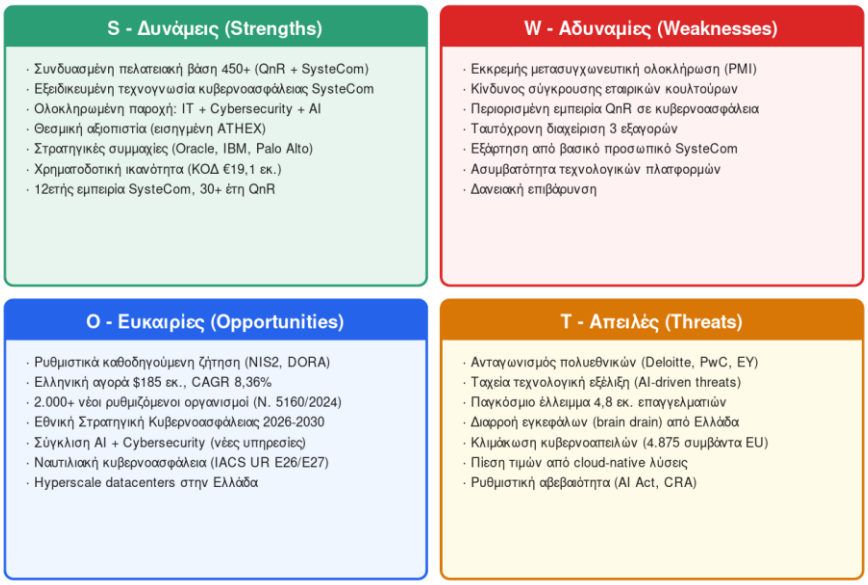
Οι ευκαιρίες (Opportunities) περιλαμβάνουν τη ρυθμιστικά καθοδηγούμενη ζήτηση λόγω NIS2/DORA/Ν. 5160/2024, την ταχέως αναπτυσσόμενη ελληνική αγορά κυβερνοασφάλειας (CAGR 8,36%), τη δυνατότητα ανάπτυξης καινοτόμων λύσεων AI-cybersecurity, τις ανάγκες ψηφιακής ασφάλειας στον ναυτιλιακό τομέα μέσω MTIS, τα ευρωπαϊκά χρηματοδοτικά προγράμματα για κυβερνοασφάλεια (Εθνική Στρατηγική 2026-2030), και τη δυνατότητα διασταυρούμενων πωλήσεων σε υφιστάμενη πελατειακή βάση.

Οι απειλές (Threats) περιλαμβάνουν την κλιμάκωση και εξέλιξη κυβερνοαπειλών (ιδίως AI-driven attacks), τον εντεινόμενο ανταγωνισμό από διεθνείς παρόχους, το παγκόσμιο έλλειμμα ταλέντων κυβερνοασφάλειας που αυξάνει τα μισθολογικά κόστη, τον κίνδυνο τεχνολογικής απαξίωσης (technological obsolescence) λόγω ραγδαίας εξέλιξης, τις πιθανές αλλαγές στο ρυθμιστικό πλαίσιο, και τον μακροοικονομικό κίνδυνο που μπορεί να επιβραδύνει τις επενδύσεις πελατών.

Σύμφωνα με τους Sihite et al. (2025), η αποτελεσματική ανάλυση SWOT δεν περιορίζεται στην απαρίθμηση παραγόντων, αλλά στοχεύει στη σύζευξη εσωτερικών δυνάμεων με εξωτερικές ευκαιρίες (SO strategies) και στην αντιστάθμιση αδυναμιών μέσω εκμετάλλευσης ευκαιριών (WO strategies). Η κύρια στρατηγική SO για τον Όμιλο QnR είναι η αξιοποίηση της συνδυασμένης τεχνογνωσίας (πληροφορική, κυβερνοασφάλεια, AI) για την παροχή ολοκληρωμένων λύσεων συμμόρφωσης (compliance solutions) στη ρυθμιστικά πιεσμένη αγορά. Η κύρια στρατηγική WO είναι η αξιοποίηση των εσόδων από την αυξανόμενη ζήτηση κυβερνοασφάλειας για την ταχεία αποπληρωμή του ομολογιακού δανείου και τη μείωση της μόχλευσης. Η κύρια στρατηγική ST (αντιμετώπιση απειλών μέσω δυνάμεων) είναι η χρήση της τεχνογνωσίας AI μέσω SquareDev για τη δημιουργία προηγμένων λύσεων. Τέλος, η κύρια στρατηγική WT (ελαχιστοποίηση αδυναμιών σε περιβάλλον απειλών) είναι η επένδυση στη διατήρηση ταλέντων μέσω ανταγωνιστικών πακέτων αμοιβών και ευκαιριών

επαγγελματικής εξέλιξης εντός του Ομίλου, μετριάζοντας τον κίνδυνο αποχώρησης κρίσιμου προσωπικού σε ένα περιβάλλον παγκόσμιου ελλείμματος ταλέντων.

Η σύγκριση με τα ευρήματα των Sihite et al. (2025) αναδεικνύει ότι ο Όμιλος QnR μοιράζεται αρκετές αδυναμίες με τις ΜΜΕ του ψηφιακού μετασχηματισμού, ιδίως σε επίπεδο χρηματοδοτικών πόρων και ψηφιακής υποδομής. Ωστόσο, η QnR υπερτερεί σημαντικά σε εξειδίκευση τεχνολογίας, πελατειακή βάση και θεσμική αξιοπιστία. Αυτή η διαπίστωση ενισχύει τη θέση ότι η στρατηγική εισόδου στην κυβερνοασφάλεια μέσω εξαγοράς ήταν μεθοδολογικά ορθή, καθώς αντιστάθμισε τις αδυναμίες της εταιρείας σε εξειδικευμένη τεχνογνωσία κυβερνοασφάλειας με την απόκτηση έτοιμων ικανοτήτων.



Σχήμα 5.4: Ανάλυση SWOT του Ομίλου QnR στον κλάδο κυβερνοασφάλειας

Πηγή: Ιδία επεξεργασία βάσει ανάλυσης Κεφαλαίων 3, 4 και 5

Σχήμα 5.4: Ανάλυση SWOT του Ομίλου QnR στον κλάδο κυβερνοασφάλειας (Πηγή: Ιδία επεξεργασία)

5.7 Σύνθεση Ευρημάτων

Το παρόν κεφάλαιο εφάρμοσε τα θεωρητικά πλαίσια του Κεφαλαίου 2 στα εμπειρικά δεδομένα των Κεφαλαίων 3 και 4, αναδεικνύοντας τόσο τα ανταγωνιστικά πλεονεκτήματα όσο και τις προκλήσεις του Ομίλου QnR. Η προσέγγιση πολλαπλών πλαισίων (multi-framework approach), σύμφωνα με τους Dewi et al. (2025), ενισχύει την αξιοπιστία των ευρημάτων μέσω τριγωνοποίησης (triangulation) θεωρητικών φακών. Η ανάλυση Porter αποκάλυψε ένα ευνοϊκό

κλαδικό περιβάλλον με ρυθμιστικά καθοδηγούμενη ζήτηση. Η ανάλυση VRIO ανέδειξε τους πόρους με δυνατότητα βιώσιμου πλεονεκτήματος, υπογραμμίζοντας τη σημασία της οργανωτικής αξιοποίησης. Η ανάλυση δυναμικών ικανοτήτων κατέδειξε αποτελεσματική αίσθηση και σύλληψη, αλλά εκκρεμή αναδιαμόρφωση που αποτελεί τον πλέον κρίσιμο παράγοντα επιτυχίας. Η ανάλυση τεχνολογικής διαφοροποίησης επιβεβαίωσε τη συγγενή φύση της κίνησης, μειώνοντας τον κίνδυνο αποτυχίας σε σύγκριση με μη συγγενή διαφοροποίηση. Η ανάλυση M&A/PMI ανέδειξε τόσο τις ευκαιρίες (85% των συνεργειών υποστηρίζονται από τεχνολογία) όσο και τους κινδύνους ολοκλήρωσης (πολιτισμική σύγκρουση, απώλεια ταλέντων, πολυπλοκότητα ενοποίησης). Η ανάλυση SWOT συνέθεσε τα ευρήματα σε ένα ολοκληρωμένο πλαίσιο, αναδεικνύοντας ως κύρια στρατηγική κατεύθυνση την αξιοποίηση της ρυθμιστικά καθοδηγούμενης ζήτησης μέσω ολοκληρωμένων λύσεων συμμόρφωσης. Το κεντρικό εύρημα που αναδύεται από τη σύνθεση αυτών των αναλύσεων είναι ότι η στρατηγική απόφαση εισόδου στην κυβερνοασφάλεια τεκμηριώνεται θεωρητικά από πολλαπλά αναλυτικά πλαίσια, ενώ παράλληλα αναδεικνύεται ότι η ποιότητα εκτέλεσης της μετασυγχωνευτικής ολοκλήρωσης αποτελεί καθοριστικό παράγοντα για την τελική έκβαση. Η αξιολόγηση αυτών των ευρημάτων αναπτύσσεται στο επόμενο κεφάλαιο. Ο Πίνακας 5.3 παρουσιάζει τη σύνδεση μεταξύ θεωρητικών πλαισίων και βασικών ευρημάτων.

Πίνακας 5.3: Σύνοψη Θεωρητικών Πλαισίων και Βασικών Ευρημάτων

Θεωρητικό Πλαίσιο	Βασικό Εύρημα	Σημασία για QnR
Porter Five Forces	Ρυθμιστικά καθοδηγούμενη ζήτηση, μέτρια ένταση ανταγωνισμού	Ευνοϊκό κλαδικό περιβάλλον
RBV/VRIO (Barney, 1991)	Τεχνογνωσία SysteCom = βιώσιμο πλεονέκτημα	Κρίσιμη η διατήρηση τεχνογνωσίας
Dynamic Capabilities (Teece, 2007)	Αποτελεσματική αίσθηση/σύλληψη, εκκρεμής αναδιαμόρφωση	Η PMI ως κρίσιμη πρόκληση
Τεχνολογική Διαφοροποίηση (Ceipek et al., 2020)	Κυρίως συγγενής διαφοροποίηση	Χαμηλότερος κίνδυνος εισόδου
M&A/PMI (Milde et al., 2024)	Τεχνολογία υποστηρίζει 85% συνεργειών	Τεχνολογική ολοκλήρωση ως προτεραιότητα
SWOT (Sihite et al., 2025)	SO: Ολοκληρωμένες λύσεις συμμόρφωσης	Στρατηγική αξιοποίησης δυνάμεων

Στο Κεφάλαιο 6, τα ευρήματα αυτά θα αξιολογηθούν κριτικά, διατυπώνοντας αξιολογικές κρίσεις (judgments) σχετικά με τη βιωσιμότητα της στρατηγικής, τις προτεραιότητες δράσης και τις προτάσεις για τη βέλτιστη στρατηγική πορεία του Ομίλου QnR στον κλάδο κυβερνοασφάλειας.

Βιβλιογραφία Κεφαλαίου

1. Agustian, K., Mubarok, E. S., Zen, A., Wiwin, & Malik, A. J. (2023). The impact of digital transformation on business models and competitive advantage. *Technology and Society Perspectives (TACIT), 1*(2), 79–93. https://doi.org/10.61100/tacit.v1i2.55

2. Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99–120. https://doi.org/10.1177/014920639101700108

3. Ceipek, R., Hautz, J., De Massis, A., Matzler, K., & Ardito, L. (2020). Digital transformation through exploratory and exploitative Internet of Things innovations: The impact of family management and technological diversification. *Journal of Product Innovation Management, 38*(1), 142–165. https://doi.org/10.1111/jpim.12551

4. Dewi, H., Huseini, M., & Atmoko, A. W. (2025). Strategic competitiveness framework for Indonesian TIC companies: Integrating Porter's Five Forces and dynamic capabilities in the global market. *Qubahan Academic Journal, 5*(3). https://doi.org/10.48161/qaj.v5n3a1982

5. Lace, K., & Kirikova, M. (2022). Pre-evaluation of post-merger information system integration strategies. *Procedia Computer Science, 200*, 298–308.

6. Mazzoccoli, A., & Naldi, M. (2022). Optimizing cybersecurity investments over time. *Algorithms, 15*(7), 211. https://doi.org/10.3390/algorithms15070211

7. Milde, J., Govers, J., Barrett, C., & Di Vittorio, C. (2024). *Technology's central role in post-merger integration*. Boston Consulting Group.

8. Porter, M. E. (2008). The five competitive forces that shape strategy. *Harvard Business Review, 86*(1), 78–93.

9. Rowe, B. R., & Gallaher, M. P. (2006). *Private sector cyber security investment strategies: An empirical analysis* (NIST GCR 06-885). RTI International.

10. Sihite, M., Suparwata, D. O., Arafah, M. N., & Uhai, S. (2025). SWOT analysis of the strategy of digital transformation of SMEs. *International Journal of Business and Life Economics, 6*(2).

11. Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal, 28*(13), 1319–1350. https://doi.org/10.1002/smj.640

12. Usianeneh, K. E. (2025). *Increase successful outcomes with technology-driven mergers and acquisitions: Prioritize post-merger integration risk mitigation* [Doctoral dissertation, University of Alabama in Huntsville].

Κεφάλαιο 6

Αξιολόγηση Στρατηγικών Επιλογών

6.1 Κριτική Αξιολόγηση της Στρατηγικής Εισόδου στην Κυβερνοασφάλεια

Η στρατηγική απόφαση του Ομίλου QnR να εισέλθει στην αγορά κυβερνοασφάλειας μέσω της εξαγοράς της SysteCom, βάσει της πολυεπίπεδης ανάλυσης του Κεφαλαίου 5, φαίνεται να τεκμηριώνεται τόσο ως προς τη στρατηγική κατεύθυνση όσο και ως προς το χρονισμό της εκτέλεσης. Ωστόσο, η αξιολόγηση αυτή υπόκειται σε σημαντικές επιφυλάξεις που σχετίζονται με τον πρώιμο χαρακτήρα του εγχειρήματος και την απουσία μακροπρόθεσμων δεδομένων επίδοσης. Η κρίση αυτή στηρίζεται σε τρεις ενδείξεις, οι οποίες παρουσιάζονται ακολούθως μαζί με τους αντίστοιχους κινδύνους.

Πρώτον, *η ανάλυση Porter* (ενότητα 5.1) κατέδειξε ότι ο ελληνικός κλάδος κυβερνοασφάλειας παρουσιάζει δομικά ευνοϊκά χαρακτηριστικά, όπως ρυθμιστικά καθοδηγούμενη ζήτηση μέσω NIS2/DORA, αναπτυσσόμενη αγορά (CAGR 8,36%), και μέτρια ένταση ανταγωνισμού. Η ρυθμιστική πίεση αποτελεί ιδιαίτερα σημαντικό παράγοντα, καθώς δημιουργεί υποχρεωτική ζήτηση. Οι οργανισμοί υποχρεούνται να επενδύσουν σε κυβερνοασφάλεια ανεξαρτήτως των μακροοικονομικών συνθηκών, παρέχοντας σχετική σταθερότητα εσόδων στους παρόχους. Αυτό επιβεβαιώνει εμπειρικά τα ευρήματα των Rowe και Gallaher (2006), σύμφωνα με τους οποίους οι κανονισμοί αποτελούν τον πρωταρχικό κινητήριο παράγοντα επένδυσης σε κυβερνοασφάλεια.

Δεύτερον, *η ανάλυση της τεχνολογικής διαφοροποίησης* (ενότητα 5.4) επιβεβαίωσε ότι η κίνηση αυτή αποτελεί κυρίως συγγενή τεχνολογική διαφοροποίηση κατά τους Ceipek et al. (2020), γεγονός που μειώνει σημαντικά τον κίνδυνο αποτυχίας σε σύγκριση με μη συγγενή διαφοροποίηση. Η εμπειρία της QnR σε πληροφοριακά συστήματα, ολοκλήρωση δικτύων και υπολογιστικό νέφος παρέχει γνωστική εγγύτητα με τον τομέα κυβερνοασφάλειας, ειδικά με το συνδιασμό της τεχνητής νοημοσύνης από την εταιρεία Squaredev.

Τρίτον, *η ανάλυση των δυναμικών ικανοτήτων* (ενότητα 5.3) κατέδειξε ότι η QnR επέδειξε αποτελεσματικές ικανότητες αίσθησης και σύλληψης κατά τον Teece (2007), αφού εντόπισε εγκαίρως τη ρυθμιστική ευκαιρία (πριν ακόμη ψηφιστεί ο Ν. 5160/2024), εξασφάλισε χρηματοδότηση μέσω ομολογιακού δανείου και εκτέλεσε τρεις εξαγορές σε δέκα μήνες. Η ταχύτητα εκτέλεσης υποδηλώνει στρατηγική αποφασιστικότητα, η οποία αποτελεί κρίσιμο χαρακτηριστικό σε αναπτυσσόμενους κλάδους.

Πέραν των ανωτέρω, *η ανάλυση SWOT* (ενότητα 5.6) ανέδειξε ότι τα δυνατά σημεία του Ομίλου (μακρόχρονη παρουσία, εξειδικευμένη τεχνογνωσία, πελατειακή βάση) αντιστοιχούν στις ευκαιρίες της αγοράς (ρυθμιστική ζήτηση, ανάπτυξη αγοράς, σύγκλιση AI-κυβερνοασφάλειας), δημιουργώντας ισχυρή στρατηγική σύζευξη. Η σύζευξη αυτή ενισχύεται από τα ευρήματα των Agustian et al. (2023), σύμφωνα με τους οποίους το ανταγωνιστικό πλεονέκτημα στην ψηφιακή εποχή εξαρτάται από την ικανότητα ενσωμάτωσης νέων τεχνολογιών στα επιχειρηματικά μοντέλα. Η QnR, μέσω των εξαγορών, δεν προσθέτει απλώς νέες υπηρεσίες στο χαρτοφυλάκιό της, αλλά μετασχηματίζει θεμελιωδώς το επιχειρηματικό της μοντέλο από πάροχο πληροφορικής σε ολοκληρωμένο πάροχο ψηφιακής ασφάλειας και μετασχηματισμού.

Η επιλογή της μεθόδου εισόδου μέσω εξαγοράς, αντί της εσωτερικής ανάπτυξης, αξιολογείται επίσης ως στρατηγικά εύστοχη. Σε έναν κλάδο με παγκόσμιο έλλειμμα 4,8 εκατομμυρίων επαγγελματιών κυβερνοασφάλειας, η εσωτερική ανάπτυξη εξειδίκευσης θα απαιτούσε πολυετή χρόνο, σημαντικές επενδύσεις σε προσέλκυση ταλέντων και αδυναμία εξασφάλισης αξιοπιστίας στην αγορά χωρίς τεκμηριωμένο ιστορικό. Η εξαγορά της SysteCom, με τη δωδεκαετή εμπειρία, τις βραβευμένες υπηρεσίες και την πελατειακή βάση που περιλαμβάνει τις τέσσερις συστημικές τράπεζες, παρείχε ταχεία πρόσβαση σε όλα αυτά τα στοιχεία. Η αποτίμηση της εξαγοράς σε λόγο τιμήματος ως προς τον κύκλο εργασιών κάτω του 1x ενισχύει περαιτέρω τη θετική αξιολόγηση της συναλλαγής.

6.2 Αξιολόγηση Βιωσιμότητας του Ανταγωνιστικού Πλεονεκτήματος

Η ανάλυση VRIO (ενότητα 5.2) ανέδειξε ότι ο σημαντικότερος πόρος του Ομίλου, η εξειδικευμένη τεχνογνωσία κυβερνοασφάλειας της SysteCom και η μεγάλη τεχνογνωσία της Squaredev σε καινοτόμες τεχνολογίες τεχνητής νοημοσύνης, πληροί τα κριτήρια βιώσιμου

ανταγωνιστικού πλεονεκτήματος κατά Barney (1991). Ωστόσο, η βιωσιμότητα αυτού του πλεονεκτήματος δεν είναι αυτονόητη και εξαρτάται από τρεις κρίσιμους παράγοντες.

Ο πρώτος παράγοντας είναι η διατήρηση του ανθρώπινου κεφαλαίου. Η τεχνογνωσία της κυβερνοασφάλειας ενσωματώνεται κυρίως στο ανθρώπινο δυναμικό και στις οργανωτικές ρουτίνες της SysteCom, και όχι σε υλική υποδομή ή κατοχυρωμένες τεχνολογίες. Αυτό σημαίνει ότι η αποχώρηση κρίσιμου προσωπικού μετά την εξαγορά, κίνδυνος που τονίζεται εμφατικά από τον Usianeneh (2025), μπορεί να υπονομεύσει ριζικά το ανταγωνιστικό πλεονέκτημα. Η δομή σταδιακής απόκτησης (60% αρχικά, 40% εντός τριετίας) αποτελεί μηχανισμό μετριασμού, αλλά δεν εξαλείφει πλήρως τον κίνδυνο. Το ίδιο συμβαίνει και με την τεχνογνωσία τον υπολοίπων εταιρειών του ομίλου.

Ο δεύτερος παράγοντας είναι η δυνατότητα πραγματικής ολοκλήρωσης. Η ανάλυση VRIO ανέδειξε ότι η ικανότητα ολοκληρωμένης παροχής υπηρεσιών (IT + Cybersecurity + AI) αποτελεί δυνητικά τον ισχυρότερο πόρο του Ομίλου, αλλά η πλήρης αξιοποίησή του εξαρτάται από την επιτυχή ολοκλήρωση. Η BCG (Milde et al., 2024) εκτιμά ότι η τεχνολογία υποστηρίζει έως και 85% των επιχειρηματικών συνεργειών, αλλά η πραγματοποίηση αυτών των συνεργειών απαιτεί μεθοδική εκτέλεση σε ορίζοντα 2-5 ετών. Η αξιολόγηση στο παρόν στάδιο δε μπορεί να κρίνει οριστικά εάν οι συνέργειες θα πραγματοποιηθούν, αλλά μπορεί να διαπιστώσει ότι οι δομικές προϋποθέσεις υπάρχουν, όπως η τεχνολογική συμβατότητα, συμπληρωματικότητα των υπηρεσιών και η κοινή πελατειακή βάση. Ένα κρίσιμο ζήτημα αφορά το βαθμό στον οποίο ο Όμιλος θα κατορθώσει να μετατρέψει τη θεωρητική δυνατότητα των διασταυρούμενων πωλήσεων (cross-selling potential) σε πραγματικά έσοδα. Η πελατειακή βάση 250+ οργανισμών της QnR αποτελεί θεωρητικά μια τεράστια αγορά για υπηρεσίες κυβερνοασφάλειας, αλλά η μετατροπή των υφιστάμενων πελατών πληροφορικής σε πελάτες κυβερνοασφάλειας απαιτεί εμπορικές δεξιότητες που πρέπει να αναπτυχθούν ή να μεταφερθούν από τη SysteCom. Η επιτυχία αυτής της διαδικασίας αποτελεί ίσως τον πλέον κρίσιμο δείκτη αξιολόγησης της εξαγοράς μεσοπρόθεσμα.

Ο τρίτος παράγοντας είναι η τεχνολογική εξέλιξη. Ο κλάδος της κυβερνοασφάλειας χαρακτηρίζεται από ταχύτατους τεχνολογικούς κύκλους. Η ανάλυση του Κεφαλαίου 3 κατέδειξε ότι η τεχνητή νοημοσύνη μετασχηματίζει τόσο τις κυβερνοαπειλές (80%+ του phishing χρησιμοποιεί AI) όσο και τις λύσεις αντιμετώπισής τους (Das et al., 2025). Σε αυτό το περιβάλλον, η βιωσιμότητα του πλεονεκτήματος απαιτεί συνεχή επένδυση σε νέες

τεχνολογίες και δεξιότητες, επιβεβαιώνοντας τη θέση του Teece (2007) ότι οι δυναμικές ικανότητες (και όχι μόνο η κατοχή πόρων) αποτελούν τη βάση ενός μακροπρόθεσμου πλεονεκτήματος. Η εξαγορά της SquareDev παρέχει ένα σημαντικό εφαλτήριο σε αυτόν τον τομέα, αλλά η διαρκής ενημέρωση παραμένει αναγκαία.

6.3 Στρατηγικές Προτάσεις για τον Όμιλο QnR

Βάσει της σύνθεσης των αναλυτικών ευρημάτων, διατυπώνονται οι ακόλουθες στρατηγικές προτάσεις για τη βέλτιστη αξιοποίηση της εισόδου στην κυβερνοασφάλεια.

Πρόταση 1: Προτεραιοποίηση της ολοκλήρωσης QnR-SysteCom

Η ανάλυση ανέδειξε ότι η αναδιαμόρφωση αποτελεί τη μεγαλύτερη πρόκληση στο πλαίσιο των δυναμικών ικανοτήτων (ενότητα 5.3). Προτείνεται η υιοθέτηση του μοντέλου τριών οριζόντων της BCG (Milde et al., 2024) με σαφές χρονοδιάγραμμα και μετρήσιμους στόχους για κάθε ορίζοντα. Η ενοποίηση πρέπει να ξεκινήσει από τις εμπορικές διαδικασίες (cross-selling enablement), καθώς αυτές παρέχουν τις πλέον άμεσες αποδόσεις, πριν προχωρήσει στην τεχνολογική ενοποίηση των πλατφορμών. Η στρατηγική ολοκλήρωσης τύπου συνδυασμού βέλτιστων πρακτικών (best-of-breed) κατά Lace και Kirikova (2022) αξιολογείται ως η πλέον κατάλληλη, καθώς επιτρέπει τη διατήρηση των ισχυρότερων στοιχείων κάθε εταιρείας.

Πρόταση 2: Ανάπτυξη ολοκληρωμένων λύσεων συμμόρφωσης (compliance solutions)

Η ανάλυση SWOT (ενότητα 5.6) ανέδειξε ως κύρια στρατηγική SO την αξιοποίηση της συνδυασμένης τεχνογνωσίας για την παροχή ολοκληρωμένων λύσεων ρυθμιστικής συμμόρφωσης. Ο Όμιλος QnR βρίσκεται σε μοναδική θέση να προσφέρει στους πελάτες του μια ενιαία πρόταση αξίας (value proposition), ψηφιακό μετασχηματισμό (QnR), κυβερνοασφάλεια και συμμόρφωση NIS2/DORA (SysteCom), αυτοματοποίηση μέσω τεχνητής νοημοσύνης (SquareDev) και ολοκλήρωση ERP (Alexander Moore). Η δημιουργία δεσμευμένων πακέτων λύσεων για συγκεκριμένους τομείς (χρηματοπιστωτικός, ενεργειακός, δημόσιος) μπορεί να ενισχύσει τη διαφοροποίηση και να δημιουργήσει υψηλότερα εμπόδια εισόδου για τους ανταγωνιστές.

Πρόταση 3: Επένδυση σε λύσεις κυβερνοασφάλειας ενισχυμένες με τεχνητή νοημοσύνη (AI-enhanced cybersecurity)

Η σύγκλιση τεχνητής νοημοσύνης και κυβερνοασφάλειας, τεκμηριωμένη εκτενώς στην ενότητα 3.4.1 μέσω των ευρημάτων Das et al. (2025), αποτελεί τη σημαντικότερη τεχνολογική τάση του κλάδου. Ο Όμιλος QnR, μέσω της SquareDev, διαθέτει ικανότητες μηχανικής μάθησης και ανίχνευσης ανωμαλιών (anomaly detection) που μπορούν να ενσωματωθούν στις υπηρεσίες SOC και αξιολόγησης του κινδύνου της SysteCom. Η δημιουργία ιδιόκτητων λύσεων AI-cybersecurity θα ενισχύσει τη δυσκολία στη μίμηση (imitability) του ανταγωνιστικού πλεονεκτήματος κατά την ανάλυση VRIO (ενότητα 5.2).

Πρόταση 4: Στοχευμένη στρατηγική διατήρησης ταλέντων (talent retention strategy)

Η ανάλυση M&A/PMI (ενότητα 5.5) ανέδειξε τον κίνδυνο απώλειας βασικού ανθρώπινου δυναμικού (key talent attrition) ως κρίσιμο παράγοντα αποτυχίας (Usianeneh, 2025). Προτείνεται η δημιουργία προγραμμάτων δέσμευσης (retention programs) που περιλαμβάνουν ανταγωνιστικά πακέτα αμοιβών, ευκαιρίες επαγγελματικής εξέλιξης εντός του ευρύτερου Ομίλου και συμμετοχή σε καινοτόμα έργα AI-cybersecurity. Η δημιουργία ενός εσωτερικού κέντρου αριστείας κυβερνοασφάλειας (Cybersecurity Center of Excellence) ή πάνω σε καινοτόμες τεχνολογίες τεχνητής νοημοσύνης θα ενισχύσει τόσο τη δέσμευση του προσωπικού όσο και τη μεταφορά γνώσης μεταξύ των εταιρειών του Ομίλου. Η ανάλυση των Dewi et al. (2025) κατέδειξε ότι η ικανότητα καινοτομίας αποτελεί τη πιο αδύναμη διάσταση των δυναμικών ικανοτήτων σε εθνικές επιχειρήσεις τεχνολογίας. Η δημιουργία ενός τέτοιου κέντρου θα αντιμετώπιζε αυτή την αδυναμία, ενθαρρύνοντας την ερευνητική δραστηριότητα (R&D activity) και τη δημιουργία καινοτόμων λύσεων εντός του Ομίλου.

Πρόταση 5: Αξιοποίηση της ναυτιλιακής κυβερνοασφάλειας (maritime cybersecurity) ως στρατηγικού τομέα ανάπτυξης

Η συμμετοχή στη MTIS S.A. (βλ. ενότητα 4.3.1) σε συνδυασμό με τις υπηρεσίες ασφάλειας για πλοία (Security Monitoring & Analytics for Vessels) της SysteCom δημιουργεί μια μοναδική ευκαιρία στον αναδυόμενο τομέα ναυτιλιακής κυβερνοασφάλειας. Η Ελλάδα ως παγκόσμια ναυτιλιακή δύναμη παρέχει φυσική αγορά για τέτοιες υπηρεσίες, ιδίως υπό τις αυξανόμενες ρυθμιστικές απαιτήσεις του IMO και της ΕΕ.

Πρόταση 6: Αξιοποίηση της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026-2030

Η νέα Εθνική Στρατηγική Κυβερνοασφάλειας αναμένεται να κινητοποιήσει σημαντικούς πόρους για την ενίσχυση της κυβερνοανθεκτικότητας του ελληνικού κράτους και των κρίσιμων υποδομών. Ο Όμιλος QnR, με τη μακρόχρονη παρουσία του στον δημόσιο τομέα και τη νέα εξειδίκευση σε κυβερνοασφάλεια, βρίσκεται σε πλεονεκτική θέση για τη συμμετοχή σε έργα της Εθνικής Στρατηγικής. Η στρατηγική προσέγγιση στα σχετικά χρηματοδοτικά προγράμματα μπορεί να αποτελέσει σημαντική πηγή εσόδων και αναγνωρισιμότητας. Ο Πίνακας 6.1 συνοψίζει τις στρατηγικές προτάσεις, τη θεωρητική τεκμηρίωσή τους και την αναμενόμενη προτεραιότητα εφαρμογής.

Πίνακας 6.1: Σύνοψη Στρατηγικών Προτάσεων

Πρόταση	Θεωρητική βάση	Χρονικός ορίζοντας	Προτεραιότητα
Μετασυγχωνευτική ολοκλήρωση	Milde et al. (2024), Lace & Kirikova (2022)	0 έως 36 μήνες	Κρίσιμη
Λύσεις συμμόρφωσης NIS2 / DORA	Porter (2008), Rowe & Gallaher (2006)	6 έως 18 μήνες	Υψηλή
AI cybersecurity λύσεις	Das et al. (2025), Ceipek et al. (2020)	12 έως 36 μήνες	Υψηλή
Διατήρηση ταλέντων	Usianeneh (2025), Barney (1991)	0 έως 12 μήνες	Κρίσιμη
Ναυτιλιακή κυβερνοασφάλεια	SWOT (Sihite et al., 2025)	18 έως 48 μήνες	Μέτρια
Εθνική στρατηγική 2026 έως 2030	Virag (2025), Almeida (2025)	12 έως 60 μήνες	Μέτρια έως Υψηλή

6.4 Περιορισμοί της Ανάλυσης

Η παρούσα αξιολόγηση υπόκειται σε ορισμένους περιορισμούς που πρέπει να ληφθούν υπόψη κατά την ερμηνεία των ευρημάτων. Πρώτον, η ανάλυση βασίζεται σε δημοσίως διαθέσιμα δεδομένα (publicly available data) σχετικά με τον Όμιλο QnR και τις υπόλοιπες εταιρείες του ομίλου, χωρίς πρόσβαση σε εσωτερικά οικονομικά στοιχεία, στρατηγικά σχέδια ή μετρήσεις απόδοσης. Η αξιολόγηση θα εμπλουτιζόταν σημαντικά από πρωτογενή δεδομένα,

όπως συνεντεύξεις με στελέχη, ανάλυση εσωτερικών χρηματοοικονομικών δεικτών και αξιολόγηση της πραγματικής προόδου ενοποίησης.

Δεύτερον, η εξαγορά των εταιρειών όπως SysteCom, Squaredev κλπ. πραγματοποιήθηκε πρόσφατα σχετικά (2025), γεγονός που σημαίνει ότι η ολοκλήρωση των συγχωνεύσεων βρίσκεται σε αρχικό στάδιο. Κατά συνέπεια, η αξιολόγηση της επιτυχίας της ολοκλήρωσης είναι εκ φύσεως προκαταρκτική και βασίζεται σε θεωρητικές προβλέψεις παρά σε εμπειρικά αποτελέσματα. Η πλήρης αξιολόγηση θα απαιτούσε μελέτη σε βάθος 3-5 ετών, καλύπτοντας και τους τρεις ορίζοντες ολοκλήρωσης.

Τρίτον, η ανάλυση Porter αποτυπώνει μια στιγμιαία εικόνα της κλαδικής δομής, η οποία μπορεί να μεταβληθεί λόγω τεχνολογικών εξελίξεων, ρυθμιστικών αλλαγών ή γεωπολιτικών ανακατατάξεων. Η ίδια κριτική απευθύνεται και από τους Dewi et al. (2025), οι οποίοι τονίζουν τον στατικό χαρακτήρα του μοντέλου. Η σύζευξη με δυναμικά πλαίσια (Teece, 2007; Ceipek et al., 2020) μετριάζει αυτόν τον περιορισμό, αλλά δεν τον εξαλείφει.

Τέταρτον, η μελέτη εστιάζει σε μία μεμονωμένη περίπτωση (single case study), γεγονός που περιορίζει τη δυνατότητα γενίκευσης των ευρημάτων. Μελλοντική έρευνα θα μπορούσε να διεξαχθεί σε μεγαλύτερο δείγμα ελληνικών εταιρειών τεχνολογίας που εισέρχονται σε νέους κλάδους μέσω εξαγορών, ώστε να εξαχθούν πιο γενικεύσιμα συμπεράσματα. Παρά τους ανωτέρω περιορισμούς, η μεθοδολογική προσέγγιση πολλαπλών θεωρητικών πλαισίων ενισχύει την αξιοπιστία των ευρημάτων μέσω τριγωνοποίησης, καθώς τα συμπεράσματα προκύπτουν από τη σύγκλιση πολλαπλών αναλυτικών εργαλείων.

6.5 Σύνθεση Αξιολόγησης

Η σύγκριση της περίπτωσης QnR με τα θεωρητικά πλαίσια αναδεικνύει ορισμένα κρίσιμα μαθήματα που μπορούν να αξιοποιηθούν τόσο από τον ίδιο τον Όμιλο όσο και από άλλες ελληνικές εταιρείες τεχνολογίας που εξετάζουν στρατηγικές εισόδου σε νέους κλάδους. Πρώτον, η εξαγορά αποτελεί αποτελεσματική μέθοδο εισόδου σε τομείς που απαιτούν εξειδικευμένη τεχνογνωσία, εφόσον υπάρχει τεχνολογική συγγένεια μεταξύ αποκτώντος και εξαγοραζόμενου (Ceipek et al., 2020). Δεύτερον, ο χρονισμός εισόδου (timing of entry) είναι εξίσου σημαντικός με τη μέθοδο, αφού η είσοδος πριν από την πλήρη εφαρμογή ρυθμιστικών απαιτήσεων (NIS2, DORA) παρέχει πρόωρο πλεονέκτημα (first-mover advantage). Τρίτον, η ταυτόχρονη εξαγορά πολλαπλών εταιρειών, ενώ δημιουργεί δυνατότητες ευρείας

διαφοροποίησης, πολλαπλασιάζει τους κινδύνους ολοκλήρωσης και απαιτεί αυστηρή ιεράρχηση προτεραιοτήτων.

6.6 Προτάσεις για Μελλοντική Έρευνα

Η παρούσα εργασία ανοίγει αρκετές ερευνητικές κατευθύνσεις. Πρώτον, μια διαχρονική μελέτη της ολοκλήρωσης της QnR με τις υπόλοιπες εταιρείες σε βάθος 3-5 ετών θα παρείχε πολύτιμα εμπειρικά δεδομένα σχετικά με την πραγματοποίηση συνεργειών και την εφαρμογή του μοντέλου τριών οριζόντων. Δεύτερον, η συγκριτική μελέτη εξαγορών κυβερνοασφάλειας σε ευρωπαϊκό επίπεδο θα μπορούσε να αναδείξει βέλτιστες πρακτικές ενοποίησης και παράγοντες επιτυχίας. Τρίτον, η εμπειρική εξέταση του αντίκτυπου της NIS2 στην ελληνική αγορά της κυβερνοασφάλειας μετά την πλήρη εφαρμογή του Ν. 5160/2024 θα παρείχε πολύτιμα στοιχεία σχετικά με τη ρυθμιστικά καθοδηγούμενη ζήτηση και τη διαμόρφωση νέων ανταγωνιστικών δυναμικών στον κλάδο. Τέταρτον, η διερεύνηση της σύγκλισης της τεχνητής νοημοσύνης και της κυβερνοασφάλειας ως πηγής ανταγωνιστικού πλεονεκτήματος, μέσω του πλαισίου VRIO, αποτελεί ένα εξαιρετικά επίκαιρο ερευνητικό θέμα. Πέμπτον, η εξέταση του ρόλου που διαδραματίζουν τα ευρωπαϊκά προγράμματα κατάρτισης δεξιοτήτων κυβερνοασφάλειας, όπως η Ευρωπαϊκή Ακαδημία Δεξιοτήτων Κυβερνοασφάλειας (European Cybersecurity Skills Academy) και το πλαίσιο ECSF, στην αντιμετώπιση του ελλείμματος ταλέντων θα εμπλούτιζε την κατανόηση ενός εκ των πλέον κρίσιμων προβλημάτων του κλάδου.

Συνοψίζοντας, η εργασία αυτή τεκμηρίωσε ότι η στρατηγική απόφαση εισόδου του Ομίλου QnR στην κυβερνοασφάλεια μέσω εξαγοράς ήταν θεωρητικά τεκμηριωμένη, χρονικά εύστοχη και στρατηγικά ορθή. Η τελική επιτυχία, ωστόσο, εξαρτάται κρίσιμα από την ποιότητα εκτέλεσης της ολοκλήρωσης, τη διατήρηση του κρίσιμου ανθρώπινου δυναμικού και τη συνεχή επένδυση σε τεχνολογική καινοτομία. Η εμπειρία δείχνει ότι η πλειονότητα των εξαγορών αποτυγχάνει να δημιουργήσει αξία για τους μετόχους, κυρίως λόγω αδυναμιών στη ολοκλήρωση (Usianeneh, 2025). Ο Όμιλος QnR οφείλει να αξιοποιήσει αυτή τη γνώση, επενδύοντας αφοσιωμένους πόρους στη διαδικασία ολοκλήρωσης και αντιμετωπίζοντάς την ως στρατηγική προτεραιότητα και όχι ως τεχνική λεπτομέρεια. Η ικανότητα αναδιαμόρφωσης θα αποτελέσει τον ακρογωνιαίο λίθο μεταξύ μιας επιτυχημένης στρατηγικής μετάβασης και μιας αποτυχημένης διεύρυνσης χαρτοφυλακίου.

Βιβλιογραφία Κεφαλαίου

1. Agustian, K., Mubarok, E. S., Zen, A., Wiwin, & Malik, A. J. (2023). The impact of digital transformation on business models and competitive advantage. *Technology and Society Perspectives (TACIT), 1*(2), 79–93. https://doi.org/10.61100/tacit.v1i2.55

2. Almeida, F. (2025). Comparative analysis of EU-based cybersecurity skills frameworks. *Computers & Security, 151*, 104329. https://doi.org/10.1016/j.cose.2024.104329

3. Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99–120. https://doi.org/10.1177/014920639101700108

4. Ceipek, R., Hautz, J., De Massis, A., Matzler, K., & Ardito, L. (2020). Digital transformation through exploratory and exploitative Internet of Things innovations: The impact of family management and technological diversification. *Journal of Product Innovation Management, 38*(1), 142–165. https://doi.org/10.1111/jpim.12551

5. Das, B. C., Sartaz, M. S., Reza, S. A., Hossain, A., Nasiruddin, M. D., Bishnu, K. K., & Sultana, K. S. (2025). AI-driven cybersecurity threat detection: Building resilient defense systems using predictive analytics. *International Journal of Basic and Applied Sciences, 14*(4), 33–45. https://doi.org/10.14419/hysdg957

6. Dewi, H., Huseini, M., & Atmoko, A. W. (2025). Strategic competitiveness framework for Indonesian TIC companies: Integrating Porter's Five Forces and dynamic capabilities in the global market. *Qubahan Academic Journal, 5*(3). https://doi.org/10.48161/qaj.v5n3a1982

7. Lace, K., & Kirikova, M. (2022). Pre-evaluation of post-merger information system integration strategies. *Procedia Computer Science, 200*, 298–308.

8. Milde, J., Govers, J., Barrett, C., & Di Vittorio, C. (2024). *Technology's central role in post-merger integration*. Boston Consulting Group.

9. Porter, M. E. (2008). The five competitive forces that shape strategy. *Harvard Business Review, 86*(1), 78–93.

10. Rowe, B. R., & Gallaher, M. P. (2006). *Private sector cyber security investment strategies: An empirical analysis* (NIST GCR 06-885). RTI International.

11. Sihite, M., Suparwata, D. O., Arafah, M. N., & Uhai, S. (2025). SWOT analysis of the strategy of digital transformation of SMEs. *International Journal of Business and Life Economics, 6*(2).

12. Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal, 28*(13), 1319–1350. https://doi.org/10.1002/smj.640

13. Usianeneh, K. E. (2025). *Increase successful outcomes with technology-driven mergers and acquisitions: Prioritize post-merger integration risk mitigation* [Doctoral dissertation, University of Alabama in Huntsville].

14. Virág, C. (2025). *Building competitive cyber capacity for Europe: A strategic framework for digital readiness* [Master's thesis, Tallinn University of Technology].

ΚΕΦΑΛΑΙΟ 7

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η παρούσα εργασία εξέτασε τη στρατηγική απόφαση εισόδου του Ομίλου Quality & Reliability (QnR) στον κλάδο κυβερνοασφάλειας μέσω της εξαγοράς της SysteCom S.A., της Squaredev και των άλλων εταιρειών με έμφαση την κυβερνοασφάλεια, αξιοποιώντας πολλαπλά θεωρητικά πλαίσια στρατηγικής ανάλυσης σε συνδυασμό με εμπειρικά δεδομένα αγοράς και εταιρείας. Τα βασικά ευρήματα, σε αντιστοιχία με τα τρία ερευνητικά ερωτήματα, συνοψίζονται ως εξής.

Αναφορικά με το πρώτο ερευνητικό ερώτημα (δομή και δυναμική του κλάδου κυβερνοασφάλειας στην Ελλάδα), η ανάλυση τεκμηρίωσε ότι ο ελληνικός κλάδος κυβερνοασφάλειας βρίσκεται σε φάση δυναμικής ανάπτυξης, τροφοδοτούμενος από τρεις αλληλοενισχυόμενους παράγοντες. Ο πρώτος είναι η κλιμάκωση των κυβερνοαπειλών, με ιδιαίτερη έμφαση στη χρήση τεχνητής νοημοσύνης από κυβερνοεγκληματίες (80%+ των μηνυμάτων ηλεκτρονικού ψαρέματος χρησιμοποιούν AI κατά ENISA, 2025). Ο δεύτερος είναι η ενσωμάτωση πολυεπίπεδου ευρωπαϊκού ρυθμιστικού πλαισίου (NIS2, DORA, Cybersecurity Act, CRA, AI Act) στο ελληνικό δίκαιο, με τον Ν. 5160/2024 να εντάσσει εκατοντάδες νέους οργανισμούς στο ρυθμιστικό πεδίο. Ο τρίτος είναι η αυξανόμενη ζήτηση υπηρεσιών κυβερνοασφάλειας, με την ελληνική αγορά να αναμένεται να αναπτυχθεί από 185,3 εκατομμύρια δολάρια (2026) σε 276,83 εκατομμύρια δολάρια (2031), με CAGR 8,36%. Η ανάλυση Πέντε Δυνάμεων Porter κατέδειξε ένα ευνοϊκό κλαδικό περιβάλλον, με ρυθμιστικά καθοδηγούμενη ζήτηση που μετριάζει τη διαπραγματευτική ισχύ αγοραστών και μέτρια ένταση ανταγωνισμού λόγω ρυθμού ανάπτυξης αγοράς.

Αναφορικά με το δεύτερο ερευνητικό ερώτημα (θεωρητική τεκμηρίωση της στρατηγικής απόφασης), η πολυεπίπεδη ανάλυση κατέληξε σε θετική αξιολόγηση. Η ανάλυση VRIO ανέδειξε ότι η εξειδικευμένη τεχνογνωσία κυβερνοασφάλειας της SysteCom πληροί τα κριτήρια βιώσιμου ανταγωνιστικού πλεονεκτήματος, ενώ η ικανότητα ολοκληρωμένης παροχής υπηρεσιών (IT + Cybersecurity + AI) αποτελεί δυνητικά τον ισχυρότερο πόρο του Ομίλου. Η ανάλυση Δυναμικών Ικανοτήτων κατέδειξε αποτελεσματικές ικανότητες αίσθησης (εντοπισμός ρυθμιστικής ευκαιρίας) και σύλληψης (ταχεία εκτέλεση τριών εξαγορών), με εκκρεμή αλλά κρίσιμη αναδιαμόρφωση. Η ανάλυση Τεχνολογικής Διαφοροποίησης

επιβεβαίωσε τη συγγενή φύση της κίνησης, η οποία μειώνει τον κίνδυνο αποτυχίας. Η ανάλυση SWOT σύνθεσε τα ευρήματα, αναδεικνύοντας ως κύρια στρατηγική κατεύθυνση την αξιοποίηση της ρυθμιστικά καθοδηγούμενης ζήτησης μέσω ολοκληρωμένων λύσεων συμμόρφωσης.

Αναφορικά με το τρίτο ερευνητικό ερώτημα (προκλήσεις PMI και στρατηγικές προτάσεις), η ανάλυση ανέδειξε τέσσερις κρίσιμους κινδύνους, τη σύγκρουση εταιρικών κουλτούρων, απώλεια βασικού ανθρώπινου δυναμικού, ασυμβατότητα τεχνολογικών πλατφορμών και υποεκτίμηση πολυπλοκότητας της ολοκλήρωσης. Διατυπώθηκαν έξι στρατηγικές προτάσεις, ιεραρχημένες κατά προτεραιότητα και χρονικό ορίζοντα με προτεραιοποίηση της ολοκλήρωσης κατά το μοντέλο τριών οριζόντων, ανάπτυξη ολοκληρωμένων λύσεων συμμόρφωσης NIS2/DORA, επένδυση σε AI-cybersecurity, στρατηγική διατήρησης ταλέντων, αξιοποίηση ναυτιλιακής κυβερνοασφάλειας και αξιοποίηση Εθνικής Στρατηγικής Κυβερνοασφάλειας 2026-2030. Οι δύο πρώτες προτάσεις (ολοκλήρωση και διατήρηση ταλέντων) αξιολογήθηκαν ως κρίσιμης προτεραιότητας για τους πρώτους 12 μήνες, καθώς αποτελούν τις απαραίτητες προϋποθέσεις για τη δημιουργία αξίας από τις εξαγορές.

Το κεντρικό συμπέρασμα της εργασίας είναι ότι η στρατηγική απόφαση εισόδου του Ομίλου QnR στον κλάδο κυβερνοασφάλειας μέσω εξαγοράς ήταν θεωρητικά τεκμηριωμένη, χρονικά εύστοχη και στρατηγικά ορθή. Η εξαγορά της SysteCom παρέχει τεχνογνωσία, πελατειακή βάση και αναγνωρισιμότητα σε έναν κλάδο με ισχυρές αναπτυξιακές προοπτικές. Η συγγενής τεχνολογική διαφοροποίηση μειώνει τον κίνδυνο αποτυχίας, ενώ η ρυθμιστικά καθοδηγούμενη ζήτηση παρέχει δομική υποστήριξη στα έσοδα.

Ωστόσο, η ανάλυση ανέδειξε επίσης ότι η τελική επιτυχία της στρατηγικής δεν είναι αυτονόητη και εξαρτάται κρίσιμα από τρεις παράγοντες. Πρώτον, την ποιότητα εκτέλεσης της ολοκλήρωσης, η οποία αποτελεί τη μεγαλύτερη πρόκληση κατά τη θεωρία Δυναμικών Ικανοτήτων (αναδιαμόρφωση). Δεύτερον, τη διατήρηση του κρίσιμου ανθρώπινου δυναμικού κυβερνοασφάλειας, σε ένα περιβάλλον παγκόσμιου ελλείμματος 4,8 εκατομμυρίων επαγγελματιών. Τρίτον, τη συνεχής επένδυση σε τεχνολογική καινοτομία, ιδιαίτερα στη σύγκλιση τεχνητής νοημοσύνης και κυβερνοασφάλειας.

Η παρούσα εργασία συνεισφέρει στη βιβλιογραφία σε δύο επίπεδα. Σε θεωρητικό επίπεδο, η εργασία επιδεικνύει την αξία της συνδυαστικής εφαρμογής πολλαπλών θεωρητικών

πλαισίων στρατηγικής ανάλυσης (Porter, RBV/VRIO, Dynamic Capabilities, Technological Diversification, M&A/PMI, SWOT) σε μία ενιαία μελέτη περίπτωσης. Η πολυεπίπεδη αυτή προσέγγιση αποκαλύπτει πτυχές που δεν θα ήταν ορατές μέσω μεμονωμένων αναλυτικών εργαλείων. Ειδικότερα, η σύζευξη εξωτερικής ανάλυσης (Porter) με εσωτερική αξιολόγηση (VRIO) και δυναμική ανάλυση (Teece) παρέχει μια ολοκληρωμένη εικόνα που υπερβαίνει τους περιορισμούς κάθε μεμονωμένου πλαισίου, επιβεβαιώνοντας τη θέση των Dewi et al. (2025) για τη σημασία του θεωρητικού πλουραλισμού στη στρατηγική ανάλυση.

Σε πρακτικό επίπεδο, η εργασία παρέχει χρήσιμα ευρήματα τόσο για τον Όμιλο QnR όσο και για ελληνικές εταιρείες τεχνολογίας που εξετάζουν στρατηγικές εισόδου σε νέους κλάδους. Τα βασικά πρακτικά μαθήματα περιλαμβάνουν τη σημασία του χρονισμού εισόδου σε σχέση με ρυθμιστικές αλλαγές (η είσοδος πριν την πλήρη εφαρμογή ρυθμίσεων παρέχει πρόωρο πλεονέκτημα), τα πλεονεκτήματα της συγγενούς τεχνολογικής διαφοροποίησης έναντι της μη συγγενούς (χαμηλότερος κίνδυνος αποτυχίας κατά Ceipek et al., 2020), τον κρίσιμο ρόλο της ολοκλήρωσης στη δημιουργία αξίας (η τεχνολογία υποστηρίζει έως 85% των συνεργειών κατά Milde et al., 2024), τη σημασία της διατήρησης ανθρώπινου κεφαλαίου σε κλάδους υψηλής εξειδίκευσης (Usianeneh, 2025), και την αξία της σταδιακής απόκτησης ποσοστού ως μηχανισμού μετριασμού κινδύνου κατά τη μεταβατική περίοδο.

Επιπρόσθετα, η εργασία αναδεικνύει τη σημασία της κυβερνοασφάλειας ως στρατηγικού τομέα ανάπτυξης για τις ελληνικές εταιρείες τεχνολογίας. Η σύγκλιση ρυθμιστικής πίεσης (NIS2, DORA), τεχνολογικής εξέλιξης (AI, Zero Trust, cloud security) και αυξανόμενων απειλών δημιουργεί ένα μοναδικό παράθυρο ευκαιρίας για εταιρείες που διαθέτουν τη βούληση και τους πόρους να επενδύσουν στον κλάδο. Η εμπειρία του Ομίλου QnR, ανεξαρτήτως τελικής έκβασης, παρέχει πολύτιμα διδάγματα για τον ελληνικό κλάδο τεχνολογίας.

Βιβλιογραφία

Agustian, K., Mubarok, E. S., Zen, A., Wiwin, & Malik, A. J. (2023). The impact of digital transformation on business models and competitive advantage. *Technology and Society Perspectives (TACIT)*, *1*(2), 79-93. https://doi.org/10.61100/tacit.v1i2.55

Almeida, F. (2025). Comparative analysis of EU-based cybersecurity skills frameworks. *Computers & Security*, *151*, 104329. https://doi.org/10.1016/j.cose.2024.104329

Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99-120. https://doi.org/10.1177/014920639101700108

Castiglione, G., Santamaria, D. F., Bella, G., Brisinda, L., & Puccia, G. (2025). Guiding cybersecurity compliance: An ontology for the NIS2 directive. *Computers & Security*, *157*, 104617. https://doi.org/10.1016/j.cose.2024.104617

Ceipek, R., Hautz, J., De Massis, A., Matzler, K., & Ardito, L. (2020). Digital transformation through exploratory and exploitative Internet of Things innovations: The impact of family management and technological diversification. *Journal of Product Innovation Management*, *38*(1), 142-165. https://doi.org/10.1111/jpim.12551

Das, B. C., Sartaz, M. S., Reza, S. A., Hossain, A., Nasiruddin, M. D., Bishnu, K. K., & Sultana, K. S. (2025). AI-driven cybersecurity threat detection: Building resilient defense systems using predictive analytics. *International Journal of Basic and Applied Sciences*, *14*(4), 33-45. https://doi.org/10.14419/hysdg957

Dewi, H., Huseini, M., & Atmoko, A. W. (2025). Strategic competitiveness framework for Indonesian TIC companies: Integrating Porter's Five Forces and dynamic capabilities in the global market. *Qubahan Academic Journal*, *5*(3). https://doi.org/10.48161/qaj.v5n3a1982

ENISA. (2025). *ENISA Threat Landscape 2024-2025*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

Fortune Business Insights. (2025). *Cybersecurity market size, share & COVID-19 impact analysis, 2025-2032*. https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

Gartner. (2025). *Forecast: Information security, worldwide, 2022-2028*. Gartner, Inc.

Gauthier-Maxence, C. (2024). European cybersecurity and AI framework: Towards proactive regulation for a secure digital future. *EU Law Live*, *212*, 1-8.

Gurel, E., & Tat, M. (2017). SWOT analysis: A theoretical review. *The Journal of International Social Research*, *10*(51), 994-1006.

Haque, G. M. M., Akula, D. K., Mohammed, Y. S., Syed, A., & Arafat, Y. (2025). Cybersecurity risk management in the age of digital transformation: A systematic literature review. *The American Journal of Engineering and Technology*, *7*(8), 126-150. https://doi.org/10.37547/tajet/Volume07Issue08-14

IBM. (2024). *Cost of a data breach report 2024*. IBM Security. https://www.ibm.com/reports/data-breach

IBM. (2025). *Cost of a data breach report 2025*. IBM Security. https://www.ibm.com/reports/data-breach

Lace, K., & Kirikova, M. (2022). Pre-evaluation of post-merger information system integration strategies. *Procedia Computer Science*, *200*, 298-308.

Mazzoccoli, A., & Naldi, M. (2022). Optimizing cybersecurity investments over time. *Algorithms*, *15*(7), 211. https://doi.org/10.3390/algorithms15070211

Milde, J., Govers, J., Barrett, C., & Di Vittorio, C. (2024). *Technology's central role in post-merger integration*. Boston Consulting Group.

Mordor Intelligence. (2025). *Greece cybersecurity market size & share analysis - Growth trends & forecasts (2025-2030)*. https://www.mordorintelligence.com/industry-reports/greece-cybersecurity-market

Mordor Intelligence. (2026). *Greece cybersecurity market size & share analysis - Growth trends & forecasts (2026-2031)*. https://www.mordorintelligence.com/industry-reports/greece-cybersecurity-market

Πατεργιαννάκη, Ζ. (2023). *Ο ψηφιακός μετασχηματισμός στον δημόσιο τομέα: Η περίπτωση της ελληνικής τοπικής αυτοδιοίκησης* [Διδακτορική διατριβή, Πανεπιστήμιο Πειραιώς]. Ιδρυματικό Αποθετήριο Πανεπιστημίου Πειραιώς.

Porter, M. E. (1980). *Competitive strategy: Techniques for analyzing industries and competitors*. Free Press.

Porter, M. E. (2008). The five competitive forces that shape strategy. *Harvard Business Review*, *86*(1), 78-93.

QnR. (2025). *Ετήσια έκθεση και εταιρικές ανακοινώσεις 2024-2025*. Quality & Reliability A.B.E.E. https://www.qnr.com.gr

Rowe, B. R., & Gallaher, M. P. (2006). *Private sector cyber security investment strategies: An empirical analysis* (NIST GCR 06-885). RTI International.

Sihite, M., Suparwata, D. O., Arafah, M. N., & Uhai, S. (2025). SWOT analysis of the strategy of digital transformation of SMEs. *International Journal of Business and Life Economics*, *6*(2).

SysteCom. (2025). *Εταιρικό προφίλ και υπηρεσίες κυβερνοασφάλειας 2025*. SysteCom S.A. https://www.syscom.gr

SysteCom. (2026). *Ενημέρωση εταιρικών δραστηριοτήτων 2026*. SysteCom S.A. https://www.syscom.gr

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, *28*(13), 1319-1350. https://doi.org/10.1002/smj.640

Usianeneh, K. E. (2025). *Increase successful outcomes with technology-driven mergers and acquisitions: Prioritize post-merger integration risk mitigation* [Doctoral dissertation, University of Alabama in Huntsville].

Virág, C. (2025). *Building competitive cyber capacity for Europe: A strategic framework for digital readiness* [Master's thesis, Tallinn University of Technology].