1. ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΕ ΠΕΡΙΒΑΛΛΟΝ « ΤΕΛΕΙΑΣ ΚΑΤΑΙΓΙΔΑΣ »

Μέσο: . . . . . .ΟΙΚΟΝΟΜΙΚΗ ΕΠΙΘΕΩΡΗΣΗ
Ημ. Έκδοσης: . . .01/04/2026 Ημ. Αποδελτίωσης: . . .04/06/2026
Σελίδα: 102

— ΥΒΡΙΔΙΚΕΣ ΑΠΕΙΛΕΣ —

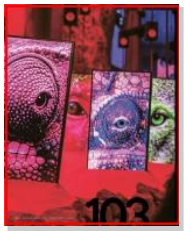
ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΕ ΠΕΡΙΒΑΛΛΟΝ «ΤΕΛΕΙΑΣ ΚΑΤΑΙΓΙΔΑΣ»

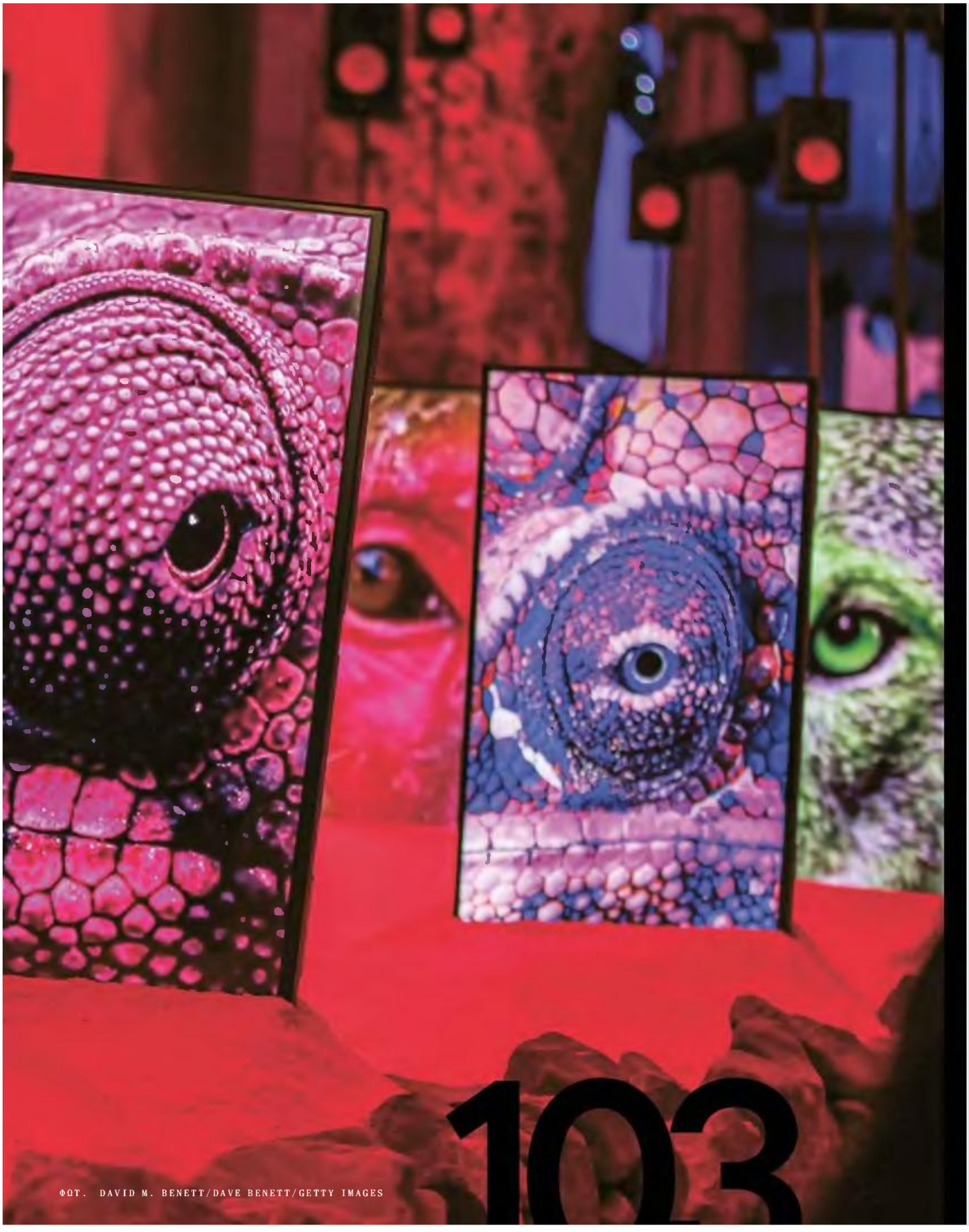
Καθώς ο κυβερνοχώρος εξελίσσεται σε βασικό πεδίο σύγκρουσης, ένεκα της τεχνολογικής προόδου και των αυξανόμενων γεωπολιτικών εντάσεων, η κυβερνοανθεκτικότητα αναδεικνύεται πλέον σε έναν από τους πλέον κρίσιμους παράγοντες παγκόσμιας σταθερότητας. Στο πλαίσιο αυτό, η κυβερνοασφάλεια παύει να είναι αποκλειστικά τεχνικό ζήτημα και μετατρέπεται σε στρατηγικό, οικονομικό και κοινωνικό θέμα. Απαιτεί τη συνεργασία κυβερνήσεων, επιχειρήσεων και διεθνών οργανισμών, καθώς και την ανάπτυξη κουλτούρας ανθεκτικότητας.

ΤΟΥ ΤΡΙΑΝΤΑΦΥΛΛΟΥ ΚΑΡΑΤΡΑΝΤΟΥ

1. ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΕ ΠΕΡΙΒΑΛΛΟΝ « ΤΕΛΕΙΑΣ ΚΑΤΑΙΓΙΔΑΣ »

Μέσο: . . . . . .ΟΙΚΟΝΟΜΙΚΗ ΕΠΙΘΕΩΡΗΣΗ
Ημ. Έκδοσης: . . .01/04/2026 Ημ. Αποδελτίωσης: . . .04/06/2026
Σελίδα: 103





1. ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΕ ΠΕΡΙΒΑΛΛΟΝ « ΤΕΛΕΙΑΣ ΚΑΤΑΙΓΙΔΑΣ »

Μέσο: . . . . . .ΟΙΚΟΝΟΜΙΚΗ ΕΠΙΘΕΩΡΗΣΗ

Ημ. Έκδοσης: . . .01/04/2026 Ημ. Αποδελτίωσης: . . .04/06/2026

Σελίδα: 104

Το 2022 ο σημαντικός αναλυτής Μαρκ Γκαλεότι κυκλοφορεί το εμβληματικό του βιβλίο *The Weaponisation of Everything: A Field Guide to the New Way of War*. Το επιχείρημά του είναι απλό, αλλά και εξαιρετικά έξυπνο. Τα πάντα μπορούν να γίνουν «όπλα». Ο Γκαλεότι υποστηρίζει ότι στη σύγχρονη εποχή σχεδόν οτιδήποτε μπορεί να χρησιμοποιηθεί ως εργαλείο σύγκρουσης. Η οικονομία (κυρώσεις, ενεργειακή εξάρτηση), η πληροφορία (fake news, προπαγάνδα), η μετανάστευση (ως μέσο πίεσης) και ο κυβερνοχώρος (hacking, επιθέσεις σε υποδομές). Δεν χρειάζονται πλέον τανκς για να ασκήσεις ισχύ.

ΓΕΩΠΟΛΙΤΙΚΗ, ΥΒΡΙΔΙΚΟΣ ΠΟΛΕΜΟΣ, ΑΝΑΔΥΟΜΕΝΕΣ ΤΕΧΝΟΛΟΓΙΕΣ

Ο συγγραφέας περιγράφει με εύληπτο τρόπο αυτό που βιώνουμε τα τελευταία χρόνια σε τρεις βασικούς άξονες: α) ευρύς γεωπολιτικός ανταγωνισμός, β) υβριδικός πόλεμος και επιχειρήσεις και γ) έκρηξη των αναδυόμενων τεχνολογιών.

Ο παραδοσιακός γεωπολιτικός ανταγωνισμός έχει διευρυνθεί και βαθύνει, καλύπτοντας πλέον πεδία όπως οι αναδυόμενες τεχνολογίες, με πλέον χαρακτηριστική περίπτωση την αντιπαράθεση ΗΠΑ και Κίνας για την Τεχνητή Νοημοσύνη. Μπορούμε να διακρίνουμε τέσσερις βασικούς δρώντες σε αυτό το πεδίο ανταγωνισμού: τις ΗΠΑ, την ΕΕ, την Κίνα και τη Ρωσία. Κατά την περίοδο της εισβολής της Ρωσίας στην Ουκρανία και της συντονισμένης αντίδρασης της Δύσης, πολλοί αναλυτές μιλούσαν για τον Ψυχρό Πόλεμο 2.0. Η εκ νέου όμως ανάληψη της Προεδρίας των ΗΠΑ από τον Ντόναλντ Τραμπ μας έδειξε πως η κατάσταση είναι περισσότερο περίπλοκη και δεν υπάρχουν γραμμικές αναγνώσεις. Από την Ουκρανία μέχρι την κλιματική αλλαγή και τις αναδυόμενες τεχνολογίες, οι ΗΠΑ και η ΕΕ έχουν διαφορετικές προσεγγίσεις και πρωτοβουλίες, και σε περιπτώσεις όπως η Γροιλανδία, η διατλαντική σχέση πέρασε σε κατάσταση κρίσης. Ο ανταγωνισμός λοιπόν καλύπτει πολλά πεδία: την οικονομία, το εμπόριο, την ενέργεια, τις εφοδιαστικές αλυσίδες και τα στρατηγικά αποθέματα, τις σπάνιες γαίες, τον κυβερνοχώρο, τις αναδυόμενες τεχνολογίες, τις κρίσιμες υποδομές, το Διάστημα, την Αρκτική κ.ά.

Η δεύτερη σημαντική συνθήκη σε αυτό το πλαίσιο είναι ο υβριδικός πόλεμος και οι υβριδικές επιχειρήσεις. Τα θολά όρια μεταξύ πολέμου και ειρήνης. Δεν ξέρεις πότε «ξεκινά» ένας πόλεμος και οι υβριδικές επιχειρήσεις συνήθως είναι συνεχείς, αλλά χαμηλής έντασης. Ο υβριδικός πόλεμος είναι οικονομικότερος και ασύμμετρος, γι' αυτό μικρότεροι ή πιο αδύναμοι δρώντες μπορούν να πλήξουν ισχυρότερους με χαμηλό κόστος και χωρίς άμεση στρατιωτική σύγκρουση. Χαρακτηριστικό παράδειγμα οι κυβερνοεπιθέσεις αντί για τον συμβατικό πόλεμο. Κρίσιμο στον υβριδικό πόλεμο είναι και η δυσκολία απόδοσης ευθύνης (plausible deniability). Αυτό επιτρέπει σε κράτη, αλλά και άλλους δρώντες, να λειτουργούν κακόβουλα χωρίς να προκαλούν ανοιχτή σύγκρουση.

Η ραγδαία ανάπτυξη της τεχνολογίας, στην εποχή της 4ης Βιομηχανικής Επανάστασης, της Τεχνητής Νοημοσύνης και του Διαδικτύου των Πραγμάτων (Internet of Things) έχει μεταβάλει εκ βάθρων τη λειτουργία των κρατών, τις υποδομές και, κυρίως, την καθημερινότητα των πολιτών. Πράγματι, η ανάπτυξη μιας τεχνολογίας μπορεί να βελτιώνει την ποιότητα της ζωής μας αλλά, παράλληλα, διευρύνει και την τρωτότητά μας. Αυτός είναι και ο βασικός λόγος που οι νέες τεχνολογίες είναι πλέον στενά συνδεδεμένες με τις πολιτικές ασφάλειας. Η αλματώδης εξέλιξη της τεχνολογίας είναι αυτή που έχει επηρεάσει τόσο την έννοια της ασφάλειας, όσο και τη φύση των απειλών. Από τις κυβερνοαπειλές μέχρι την τρομοκρατία και τις

Η ΑΝΑΠΤΥΞΗ ΜΙΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΒΕΛΤΙΩΝΕΙ ΤΗΝ ΠΟΙΟΤΗΤΑ ΤΗΣ ΖΩΗΣ ΜΑΣ ΑΛΛΑ, ΠΑΡΑΛΛΗΛΑ, ΔΙΕΥΡΥΝΕΙ ΚΑΙ ΤΗΝ ΤΡΩΤΟΤΗΤΑ ΜΑΣ. ΑΥΤΟΣ ΕΙΝΑΙ ΚΑΙ Ο ΒΑΣΙΚΟΣ ΛΟΓΟΣ ΠΟΥ ΟΙ ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΕΙΝΑΙ ΠΛΕΟΝ ΣΤΕΝΑ ΣΥΝΔΕΔΕΜΕΝΕΣ ΜΕ ΤΙΣ ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ. ΑΠΟ ΤΙΣ ΚΥΒΕΡΝΟΑΠΕΙΛΕΣ ΜΕΧΡΙ ΤΗΝ ΤΡΟΜΟΚΡΑΤΙΑ ΚΑΙ ΤΙΣ ΔΙΑΦΟΡΕΣ ΜΟΡΦΕΣ ΒΙΑΣ, Η ΚΑΚΟΒΟΥΛΗ ΧΡΗΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΕΧΕΙ ΚΑΤΑΣΤΕΙ ΕΡΓΑΛΕΙΟ ΤΩΝ ΕΓΚΛΗΜΑΤΙΩΝ. Η ΤΕΧΝΟΛΟΓΙΑ ΕΙΝΑΙ, ΟΜΩΣ, ΚΑΙ ΤΟ ΜΕΓΑΛΥΤΕΡΟ ΟΠΛΟ ΓΙΑ ΤΟΥΣ ΦΟΡΕΙΣ ΕΠΙΒΟΛΗΣ ΤΟΥ ΝΟΜΟΥ ΚΑΙ ΤΑ ΚΡΑΤΗ.

1. ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΕ ΠΕΡΙΒΑΛΛΟΝ « ΤΕΛΕΙΑΣ ΚΑΤΑΙΓΙΔΑΣ »

Μέσο: . . . . . .ΟΙΚΟΝΟΜΙΚΗ ΕΠΙΘΕΩΡΗΣΗ

Ημ. Έκδοσης: . . .01/04/2026 Ημ. Αποδελτίωσης: . . .04/06/2026

Σελίδα: 105

διάφορες μορφές βίας, η κακόβουλη χρήση της τεχνολογίας έχει καταστεί εργαλείο των εγκληματιών, η τεχνολογία είναι, όμως, και το μεγαλύτερο όπλο για τους φορείς επιβολής του νόμου και τα κράτη. Αντίστοιχα τεχνολογικά εξελιγμένες, ωστόσο, είναι και οι απειλές τόσο από κρατικούς, όσο και μη κρατικούς δρώντες: μετα-δεδομένα, αλγόριθμοι, Τεχνητή Νοημοσύνη, Διαδίκτυο των Πάντων είναι συστατικά αυτής της φάσης.

Η ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΩΣ ΣΤΡΑΤΗΓΙΚΟΣ ΠΑΡΑΓΟΝΤΑΣ

Η κυβερνοασφάλεια αποτελεί πλέον έναν από τους πιο κρίσιμους παράγοντες παγκόσμιας σταθερότητας. Η πρόσφατη αναφλεξη στη Μέση Ανατολή είναι μια ακόμη παράμετρος που εξηγεί γιατί το 2026 οι κυβερνοαπειλές αυξάνονται τόσο σε ένταση όσο και σε πολυπλοκότητα, ενώ η τεχνολογική πρόοδος και οι γεωπολιτικές εντάσεις μετατρέπουν τον κυβερνοχώρο σε βασικό πεδίο σύγκρουσης. Ένας από τους σημαντικότερους παράγοντες αλλαγής είναι η Τεχνητή Νοημοσύνη, η οποία λειτουργεί διττά: από τη μία πλευρά ενισχύει σημαντικά την άμυνα μέσω αυτοματοποίησης και ταχύτερης ανίχνευσης απειλών, από την άλλη όμως καθιστά τις επιθέσεις πιο εξελιγμένες, πιο γρήγορες και πιο δύσκολα ανιχνεύσιμες. Έτσι, δημιουργείται μια δυναμική «κούρσας εξοπλισμών» στον κυβερνοχώρο, όπου επιτιθέμενοι και αμυνόμενοι εξελίσσονται παράλληλα.

Παράλληλα, η γεωπολιτική αστάθεια επηρεάζει άμεσα την κυβερνοασφάλεια. Οι εντάσεις μεταξύ κρατών οδηγούν σε αύξηση κυβερνοεπιθέσεων, ιδιαίτερα σε κρίσιμες υποδομές όπως η ενέργεια, οι μεταφορές και οι τηλεπικοινωνίες. Ο κυβερνοχώρος δεν είναι πλέον ένα απομονωμένο τεχνολογικό πεδίο, αλλά έχει ενσωματωθεί πλήρως στη διεθνή πολιτική και στρατηγική.

Κρίσιμο είναι το γεγονός πως οι απειλές αυξάνονται ταχύτερα από την ικανότητα αντιμετώπισής τους. Υπάρχουν σημαντικά κενά σε δεξιότητες, πόρους και τεχνολογική ετοιμότητα, γεγονός που δημιουργεί ανισότητες μεταξύ χωρών και οργανισμών. Οι μικρότερες ή λιγότερο ανεπτυγμένες δομές είναι ιδιαίτερα ευάλωτες, ενώ ακόμη και μεγάλες επιχειρήσεις δυσκολεύονται να παρακολουθήσουν τον ρυθμό εξέλιξης των επιθέσεων.

Ταυτόχρονα, το κυβερνοέγκλημα βρίσκεται σε ραγδαία άνοδο. Επιθέσεις όπως phishing, ransomware και κλοπή δεδομένων αποτελούν πλέον βασικές απειλές για επιχειρήσεις και οργανισμούς, με σημαντικές οικονομικές επιπτώσεις. Ο κυβερνοχώρος έχει εξελιχθεί σε ένα πλήρες πεδίο οικονομικής δραστηριότητας για εγκληματικά δίκτυα.

Ένα ακόμη κρίσιμο σημείο είναι η ευαλωτότητα των αλυσίδων εφοδιασμού. Πολλές επιθέσεις δεν στοχεύουν άμεσα τον τελικό οργανισμό, αλλά εκμεταλλεύονται τρίτους συνεργάτες ή παρόχους υπηρεσιών, όπως cloud platforms. Αυτό σημαίνει ότι η ασφάλεια ενός οργανισμού εξαρτάται πλέον από ένα ευρύτερο οικοσύστημα.

Ας δούμε όμως πώς εντάσσονται και στο πλαίσιο του υβριδικού πολέμου. Οι υβριδικές απειλές εκδηλώνονται μέσα από έναν συνδυασμό συμπληρωματικών εργαλείων και πρακτικών, τα οποία ενισχύουν αμοιβαία τον αντίκτυπό τους. Κεντρικό ρόλο διαδραματίζουν οι κυβερνοεπιθέσεις, που στοχεύουν τόσο τα πληροφοριακά συστήματα όσο και τα συστήματα επιχειρησιακής τεχνολογίας σε κρίσιμους τομείς, όπως τα δίκτυα ηλεκτρικής ενέργειας, οι εγκαταστάσεις επεξεργασίας νερού και οι χρηματοπιστωτικές υπηρεσίες. Παράλληλα, η οικονομική εξαναγκαστική πίεση αξιοποιεί διαταραχές στις εφοδιαστικές αλυσίδες ή χρηματοοικονομικά εργαλεία με στόχο την αποδυνάμωση της ανθεκτικότητας των υποδομών. Ιδιαίτερη σημασία έχει και ο πληροφοριακός πόλεμος μέσω της συστηματικής διασποράς παραπληροφόρησης που διαβρώνει την εμπιστοσύνη

105

Ο ΚΥΒΕΡΝΟΧΩΡΟΣ ΔΕΝ ΕΙΝΑΙ ΠΛΕΟΝ ΕΝΑ ΑΠΟΜΟΝΩΜΕΝΟ ΤΕΧΝΟΛΟΓΙΚΟ ΠΕΔΙΟ, ΑΛΛΑ ΕΧΕΙ ΕΝΣΩΜΑΤΩΘΕΙ ΠΛΗΡΩΣ ΣΤΗ ΔΙΕΘΝΗ ΠΟΛΙΤΙΚΗ ΚΑΙ ΣΤΡΑΤΗΓΙΚΗ. ΚΡΙΣΙΜΟ ΕΙΝΑΙ ΤΟ ΓΕΓΟΝΟΣ ΠΩΣ ΟΙ ΑΠΕΙΛΕΣ ΑΥΞΑΝΟΝΤΑΙ ΤΑΧΥΤΕΡΑ ΑΠΟ ΤΗΝ ΙΚΑΝΟΤΗΤΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΤΟΥΣ. ΥΠΑΡΧΟΥΝ ΣΗΜΑΝΤΙΚΑ ΚΕΝΑ ΣΕ ΔΕΞΙΟΤΗΤΕΣ, ΠΟΡΟΥΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΗ ΕΤΟΙΜΟΤΗΤΑ, ΓΕΓΟΝΟΣ ΠΟΥ ΔΗΜΙΟΥΡΓΕΙ ΑΝΙΣΟΤΗΤΕΣ ΜΕΤΑΞΥ ΧΩΡΩΝ ΚΑΙ ΟΡΓΑΝΙΣΜΩΝ. ΟΙ ΜΙΚΡΟΤΕΡΕΣ Ή ΛΙΓΟΤΕΡΟ ΑΝΕΠΤΥΓΜΕΝΕΣ ΔΟΜΕΣ ΕΙΝΑΙ ΙΔΙΑΙΤΕΡΑ ΕΥΑΛΩΤΕΣ, ΕΝΩ ΑΚΟΜΗ ΚΑΙ ΜΕΓΑΛΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΔΥΣΚΟΛΕΥΟΝΤΑΙ ΝΑ ΠΑΡΑΚΟΛΟΥΘΗΣΟΥΝ ΤΟΝ ΡΥΘΜΟ ΕΞΕΛΙΞΗΣ ΤΩΝ ΕΠΙΘΕΣΕΩΝ.

1. ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΕ ΠΕΡΙΒΑΛΛΟΝ « ΤΕΛΕΙΑΣ ΚΑΤΑΙΓΙΔΑΣ »

Μέσο: . . . . . .ΟΙΚΟΝΟΜΙΚΗ ΕΠΙΘΕΩΡΗΣΗ

Ημ. Έκδοσης: . . .01/04/2026 Ημ. Αποδελτίωσης: . . .04/06/2026

Σελίδα: 106

των πολιτών και επηρεάζει τη διαδικασία λήψης αποφάσεων. Τέλος, η φυσική δολιοφθορά, όπως άμεσες επιθέσεις σε κρίσιμες εγκαταστάσεις ή παρεμβάσεις σε θαλάσσιες υποδομές, συχνά συνδυάζεται με κυβερνοτακτικές, πολλαπλασιάζοντας τον αποσταθεροποιητικό της αντίκτυπο.

Στο στόχαστρο των υβριδικών απειλών βρίσκονται καίριοι τομείς που στηρίζουν την ομαλή λειτουργία της κοινωνίας και της οικονομίας. Ιδιαίτερη σημασία έχει ο ενεργειακός τομέας, με τα δίκτυα ηλεκτρικής ενέργειας και τους αγωγούς να αποτελούν κρίσιμα σημεία υψηλής ευπάθειας. Αντίστοιχα, οι υποδομές ύδρευσης και αποχέτευσης, όπως οι μονάδες επεξεργασίας και τα δίκτυα διανομής, αποτελούν δυνητικούς στόχους με άμεσες επιπτώσεις στη δημόσια υγεία. Ο τομέας της υγείας, και ειδικότερα τα νοσοκομεία και τα ψηφιακά αρχεία υγείας, έχει αναδειχθεί σε προνομιακό πεδίο επιθέσεων, λόγω της ζωτικής σημασίας και της αυξημένης ψηφιακής εξάρτησής του. Παράλληλα, ο χρηματοπιστωτικός τομέας, συμπεριλαμβανομένων των συστημάτων πληρωμών, βρίσκεται στο επίκεντρο απειλών που μπορούν να κλονίσουν την οικονομική σταθερότητα. Σημαντικούς κινδύνους αντιμετωπίζουν επίσης οι μεταφορές, τόσο στον αέρα όσο και στη θάλασσα και στην ξηρά, καθώς και οι ψηφιακές υποδομές, όπως τα δίκτυα επικοινωνιών και οι υπηρεσίες υπολογιστικού νέφους, οι οποίες αποτελούν τη ραχοκοκαλιά της σύγχρονης διασυνδεδεμένης οικονομίας.

ΟΙ ΚΙΝΔΥΝΟΙ ΚΑΙ ΟΙ ΑΠΕΙΛΕΣ ΓΙΑ ΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

Ένα χαρακτηριστικό παράδειγμα αποτελεί η κυβερνοεπίθεση που έγινε το 2025 εναντίον της βρετανικής αυτοκινητοβιομηχανίας Jaguar Land Rover, που θεωρείται από τις μεγαλύτερες στην ιστορία του Ηνωμένου Βασιλείου και η πιο καταστροφική, με τις συνολικές ζημιές για την οικονομία να εκτιμώνται περίπου στο £1,9 δισ. Η επίθεση προκάλεσε παράλυση στην παραγωγή των εργοστασίων της εταιρείας, καθώς οι hackers εκμεταλλεύτηκαν ευπάθειες στα δίκτυα IT. Επηρεάστηκαν κρίσιμες λειτουργίες, όπως η παραγωγή, τα logistics και οι διοικητικές διαδικασίες, με αποτέλεσμα να σταματήσει η παραγωγή ορισμένων μοντέλων και να υπάρξουν σημαντικές καθυστερήσεις στις παραδόσεις.

Αυτό το περιστατικό είναι ιδιαίτερα σημαντικό, γιατί δείχνει πώς μια κυβερνοεπίθεση μπορεί να προκαλέσει τεράστιες οικονομικές ζημιές, όχι μόνο για τον ίδιο τον οργανισμό, αλλά και για ολόκληρη την εφοδιαστική αλυσίδα. Επιπλέον, η επίθεση υπογραμμίζει ότι οι σύγχρονες βιομηχανικές υποδομές αποτελούν πλέον κρίσιμα ψηφιακά πεδία που μπορούν να γίνουν στόχος χωρίς να απαιτείται κακόβουλη ενέργεια στο πλαίσιο της φυσικής ασφάλειας.

Η περίπτωση της Jaguar Land Rover αποτελεί επίσης χαρακτηριστικό παράδειγμα της θεωρίας του Μαρκ Γκαλεότι για την «οπλοποίηση των πάντων». Η ψηφιακή υποδομή της εταιρείας έγινε στόχος –με αποτέλεσμα να δημιουργηθεί σημαντική ζημιά στην οικονομία και την παραγωγή– χωρίς καν να υπάρξει στρατιωτική σύγκρουση. Δείχνει με τον πιο ξεκάθαρο τρόπο πώς η σύγχρονη εποχή μετατρέπει κάθε τεχνολογικό ή επιχειρησιακό σύστημα σε πιθανό «όπλο» ή στόχο, ενώ υπογραμμίζει την ανάγκη για ανθεκτικότητα και προστασία κρίσιμων υποδομών απέναντι σε τέτοιες ψηφιακές απειλές.

Σήμερα, οι επιχειρήσεις και ο ιδιωτικός τομέας αντιμετωπίζουν πολυδιάστατους και συνεχώς εξελισσόμενους κινδύνους στον κυβερνοχώρο, οι οποίοι επηρεάζουν τόσο την οικονομική τους σταθερότητα όσο και την επιχειρησιακή τους λειτουργία. Οι κυβερνοεπιθέσεις μπορούν να προκαλέσουν διακοπή λειτουργίας ή παραγωγής. Τέτοιες επιθέσεις επηρεάζουν όχι μόνο την ίδια την εταιρεία, αλλά και ολόκληρη την εφοδιαστική αλυσίδα, συμπεριλαμβανομένων προμηθευτών και πελατών. Παράλληλα, η κλοπή δεδομένων και οι διαρροές πληροφοριών αποτελούν σημαντικό κίνδυνο. Οι παραβιάσεις μπορούν να εκθέσουν ευαίσθητα επιχειρησιακά δεδομένα, πελατολόγια ή σχέδια προϊόντων, προκαλώντας οικονομικές ζημιές, απώλεια ανταγωνιστικού πλεονεκτήματος και δικαστικές συνέπειες. Επιπλέον, η παραπληροφόρηση και οι επιθέσεις τύπου deepfake μπορούν να επηρεάσουν

106

ΣΗΜΕΡΑ, ΟΙ ΕΠΙΧΕΙΡΗΣΕΙΣ ΚΑΙ Ο ΙΔΙΩΤΙΚΟΣ ΤΟΜΕΑΣ ΑΝΤΙΜΕΤΩΠΙΖΟΥΝ ΠΟΛΥΔΙΑΣΤΑΤΟΥΣ ΚΑΙ ΣΥΝΕΧΩΣ ΕΞΕΛΙΣΣΟΜΕΝΟΥΣ ΚΙΝΔΥΝΟΥΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ. ΟΙ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ ΜΠΟΡΟΥΝ ΝΑ ΠΡΟΚΑΛΕΣΟΥΝ ΔΙΑΚΟΠΗ ΛΕΙΤΟΥΡΓΙΑΣ Ή ΠΑΡΑΓΩΓΗΣ. ΤΕΤΟΙΕΣ ΕΠΙΘΕΣΕΙΣ ΕΠΗΡΕΑΖΟΥΝ ΟΧΙ ΜΟΝΟ ΤΗΝ ΙΔΙΑ ΤΗΝ ΕΤΑΙΡΕΙΑ, ΑΛΛΑ ΚΑΙ ΟΛΟΚΛΗΡΗ ΤΗΝ ΕΦΟΔΙΑΣΤΙΚΗ ΑΛΥΣΙΔΑ, ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΜΕΝΩΝ ΠΡΟΜΗΘΕΥΤΩΝ ΚΑΙ ΠΕΛΑΤΩΝ. ΠΑΡΑΛΛΗΛΑ, Η ΚΛΟΠΗ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΟΙ ΔΙΑΡΡΟΕΣ ΠΛΗΡΟΦΟΡΙΩΝ ΑΠΟΤΕΛΟΥΝ ΣΗΜΑΝΤΙΚΟ ΚΙΝΔΥΝΟ. ΟΙ ΠΑΡΑΒΙΑΣΕΙΣ ΜΠΟΡΟΥΝ ΝΑ ΕΚΘΕΣΟΥΝ ΕΥΑΙΣΘΗΤΑ ΕΠΙΧΕΙΡΗΣΙΑΚΑ ΔΕΔΟΜΕΝΑ, ΠΕΛΑΤΟΛΟΓΙΑ Ή ΣΧΕΔΙΑ ΠΡΟΪΟΝΤΩΝ, ΠΡΟΚΑΛΩΝΤΑΣ ΟΙΚΟΝΟΜΙΚΕΣ ΖΗΜΙΕΣ, ΑΠΩΛΕΙΑ ΑΝΤΑΓΩΝΙΣΤΙΚΟΥ ΠΛΕΟΝΕΚΤΗΜΑΤΟΣ ΚΑΙ ΔΙΚΑΣΤΙΚΕΣ ΣΥΝΕΠΕΙΕΣ.

1. ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΕ ΠΕΡΙΒΑΛΛΟΝ « ΤΕΛΕΙΑΣ ΚΑΤΑΙΓΙΔΑΣ »

Μέσο: . . . . . .ΟΙΚΟΝΟΜΙΚΗ ΕΠΙΘΕΩΡΗΣΗ

Ημ. Έκδοσης: . . .01/04/2026 Ημ. Αποδελτίωσης: . . .04/06/2026

Σελίδα: 107

εργαζόμενους, πελάτες και συνεργάτες, πλήττοντας τη φήμη της εταιρείας και την εμπιστοσύνη στην επιχείρηση.

Οι οικονομικές απώλειες είναι συχνά άμεσες και σημαντικές. Επιθέσεις ransomware, phishing ή άλλες μορφές κυβερνοεγκλήματος οδηγούν σε υψηλό κόστος αποκατάστασης, πρόστιμα από ρυθμιστικές αρχές και διακοπή εσόδων. Παράλληλα, οι επιχειρήσεις είναι ευάλωτες μέσω των αλυσίδων εφοδιασμού, καθώς πολλές επιθέσεις δεν στοχεύουν άμεσα τον οργανισμό, αλλά τρίτους συνεργάτες ή παρόχους cloud. Η επίθεση στα botnets του 2026, όταν μολύνθηκαν πάνω από 3 εκατ. συσκευές παγκοσμίως, αποτελεί χαρακτηριστικό παράδειγμα: οι μολυσμένες συσκευές μπορούσαν να χρησιμοποιηθούν για μαζικές επιθέσεις σε τρίτους, αυξάνοντας τον κίνδυνο για ολόκληρο το οικοσύστημα επιχειρήσεων.

Η Τεχνητή Νοημοσύνη προσθέτει νέες προκλήσεις. Οι αυτοματοποιημένες επιθέσεις με AI, τα deepfake emails και video scams, καθώς και η παραγωγή κακόβουλου λογισμικού υψηλής ταχύτητας καθιστούν τον κυβερνοχώρο πιο επικίνδυνο. Σύμφωνα με τους ειδικούς, η Τεχνητή Νοημοσύνη αποτελεί τον πιο σημαντικό παράγοντα αλλαγής στον κυβερνοχώρο για το 2026, καθώς επιταχύνει τόσο τις αμυντικές όσο και τις επιθετικές δυνατότητες.

Τέλος, οι κίνδυνοι δεν είναι πλέον στιγμιαίοι· είναι συνεχείς, πολυδιάστατοι και ασύμμετροι. Η αντιμετώπισή τους απαιτεί στρατηγική προσέγγιση που συνδυάζει τεχνολογική ασφάλεια, εκπαίδευση προσωπικού, επενδύσεις σε ανθεκτικότητα, και συνεργασία με άλλες εταιρείες και κυβερνητικούς φορείς. Η κυβερνοασφάλεια δεν είναι πλέον απλώς τεχνικό θέμα· αποτελεί θεμελιώδη στρατηγική ανάγκη για την επιβίωση και ανάπτυξη των επιχειρήσεων.

ΕΝΙΣΧΥΣΗ ΤΗΣ ΚΥΒΕΡΝΟΑΝΘΕΚΤΙΚΟΤΗΤΑΣ

Στο πλαίσιο αυτό, η κυβερνοασφάλεια παύει να είναι αποκλειστικά τεχνικό ζήτημα και μετατρέπεται σε στρατηγικό, οικονομικό και κοινωνικό θέμα. Απαιτεί τη συνεργασία κυβερνήσεων, επιχειρήσεων και διεθνών οργανισμών, καθώς και την ανάπτυξη κουλτούρας ανθεκτικότητας.

Για τις επιχειρήσεις, και ιδιαίτερα για τον ιδιωτικό τομέα και τις μικρομεσαίες επιχειρήσεις (ΜμΕ), η ενίσχυση της ανθεκτικότητας απέναντι στις ψηφιακές απειλές απαιτεί μια ολιστική προσέγγιση. Η κυβερνοασφάλεια δεν είναι πλέον μόνο τεχνικό ζήτημα· είναι στρατηγική προτεραιότητα που συνδέεται με τη βιωσιμότητα και την ανταγωνιστικότητα της επιχείρησης. Οι ΜμΕ πρέπει να επενδύσουν σε προσιτές τεχνολογίες ασφαλείας, όπως cloud-based λύσεις προστασίας δεδομένων και αυτοματοποίηση ανίχνευσης απειλών, και να αξιοποιήσουν εργαλεία Τεχνητής Νοημοσύνης για πρόληψη επιθέσεων. Παράλληλα, η διαχείριση της εφοδιαστικής αλυσίδας γίνεται κρίσιμη: ακόμα και μικροί προμηθευτές μπορεί να γίνουν δίαυλοι επίθεσης, οπότε απαιτείται αυστηρός έλεγχος και συμφωνίες ασφάλειας με συνεργάτες.

Ιδιαίτερη σημασία έχει η εκπαίδευση και ευαισθητοποίηση του προσωπικού, καθώς οι εργαζόμενοι συχνά αποτελούν τον πιο ευάλωτο κρίκο. Η καλλιέργεια κουλτούρας ασφάλειας μειώνει τον κίνδυνο ανθρώπινου λάθους, όπως phishing ή κακόβουλα email. Τέλος, η ανθεκτικότητα ενισχύεται μέσω συνεργασίας με άλλες επιχειρήσεις, τοπικούς φορείς και οργανισμούς του κλάδου, συμμετοχής σε κοινές βάσεις πληροφοριών απειλών και ακολουθώντας διεθνή πρότυπα ασφάλειας. Για τις ΜμΕ, αυτές οι πρακτικές δεν είναι πολυτέλεια· αποτελούν ουσιαστική επένδυση για να μπορέσουν να επιβιώσουν και να αναπτυχθούν σε έναν κόσμο όπου οι κυβερνοαπειλές είναι συνεχείς, ασύμμετρες και παγκόσμιες.

* Ο ΤΡΙΑΝΤΑΦΥΛΛΟΣ ΚΑΡΑΤΡΑΝΤΟΣ ΕΙΝΑΙ ΔΡ ΕΥΡΩΠΑΪΚΗΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΝΕΩΝ ΑΠΕΙΛΩΝ ΚΑΙ ΕΠΙΣΤΗΜΟΝΙΚΟΣ ΣΥΝΕΡΓΑΤΗΣ ΕΛΙΑΜΕΠ.

ΓΙΑ ΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ, ΚΑΙ ΙΔΙΑΙΤΕΡΑ ΓΙΑ ΤΟΝ ΙΔΙΩΤΙΚΟ ΤΟΜΕΑ ΚΑΙ ΤΙΣ ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ (ΜμΕ), Η ΕΝΙΣΧΥΣΗ ΤΗΣ ΑΝΘΕΚΤΙΚΟΤΗΤΑΣ ΑΠΕΝΑΝΤΙ ΣΤΙΣ ΨΗΦΙΑΚΕΣ ΑΠΕΙΛΕΣ ΑΠΑΙΤΕΙ ΜΙΑ ΟΛΙΣΤΙΚΗ ΠΡΟΣΕΓΓΙΣΗ. Η ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΔΕΝ ΕΙΝΑΙ ΠΛΕΟΝ ΜΟΝΟ ΤΕΧΝΙΚΟ ΖΗΤΗΜΑ· ΕΙΝΑΙ ΣΤΡΑΤΗΓΙΚΗ ΠΡΟΤΕΡΑΙΟΤΗΤΑ ΠΟΥ ΣΥΝΔΕΕΤΑΙ ΜΕ ΤΗ ΒΙΩΣΙΜΟΤΗΤΑ ΚΑΙ ΤΗΝ ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ ΤΗΣ ΕΠΙΧΕΙΡΗΣΗΣ. ΟΙ ΜμΕ ΠΡΕΠΕΙ ΝΑ ΕΠΕΝΔΥΣΟΥΝ ΣΕ ΠΡΟΣΙΤΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΑΣΦΑΛΕΙΑΣ, ΟΠΩΣ CLOUD-BASED ΛΥΣΕΙΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΑΥΤΟΜΑΤΟΠΟΙΗΣΗ ΑΝΙΧΝΕΥΣΗΣ ΑΠΕΙΛΩΝ, ΚΑΙ ΝΑ ΑΞΙΟΠΟΙΗΣΟΥΝ ΕΡΓΑΛΕΙΑ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ ΓΙΑ ΠΡΟΛΗΨΗ ΕΠΙΘΕΣΕΩΝ.