



Βρυξέλλες, 29.1.2020  
COM(2020) 50 final

**ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΠΡΟΣ ΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ  
ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ  
ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ**

**Ασφαλής εγκατάσταση του 5G στην ΕΕ - Εφαρμογή της εργαλειοθήκης της ΕΕ**

## **1. Εισαγωγή**

Τα δίκτυα τηλεπικοινωνιών πέμπτης γενιάς (5G) θα διαδραματίσουν αδιαμφισβήτητα κεντρικό ρόλο στην ανάπτυξη της ευρωπαϊκής κοινωνίας και οικονομίας. Αναμένεται ότι θα προσφέρουν τεράστιες οικονομικές ευκαιρίες και ότι θα αποτελέσουν σημαντική βάση για τον ψηφιακό και τον πράσινο μετασχηματισμό σε τομείς, όπως οι μεταφορές, η ενέργεια, η βιομηχανική παραγωγή, η υγεία, η γεωργία και τα μέσα επικοινωνίας.

Κατά συνέπεια, τα δίκτυα 5G είναι πιθανό να επηρεάσουν σχεδόν κάθε πτυχή της ζωής των πολιτών της ΕΕ. Η κυβερνοασφάλεια των δικτύων 5G έχει, επομένως, θεμελιώδη σημασία όχι μόνο για την προστασία των οικονομιών, των κοινωνιών και των δημοκρατικών διαδικασιών μας, αλλά και για να εξασφαλιστεί ένας αξιόπιστος ψηφιακός μετασχηματισμός προς όφελος όλων των πολιτών της ΕΕ.

Το γεγονός ότι πολλές κρίσιμες υπηρεσίες εξαρτώνται από τα δίκτυα 5G συνεπάγεται σοβαρότατες συνέπειες σε περίπτωση συστημικής και εκτεταμένης διαταραχής και, δεδομένου του διασυνδεδεμένου χαρακτήρα των ψηφιακών οικοσυστημάτων, θα μπορούσε να έχει σημαντικές επιπτώσεις πέραν των εθνικών συνόρων. Ως εκ τούτου, η κατοχύρωση της κυβερνοασφάλειας των δικτύων 5G αποτελεί ζήτημα στρατηγικής σημασίας για την Ένωση, σε μια περίοδο κατά την οποία οι κυβερνοεπιθέσεις αυξάνονται συνεχώς, χρησιμοποιούν πιο σύνθετες μεθόδους από ποτέ και προέρχονται από διάφορους παράγοντες απειλής, ιδίως τρίτες χώρες ή παράγοντες που υποστηρίζονται από αυτές. Όσον αφορά την ασφάλεια κρίσιμων υποδομών όπως αυτές των δικτύων 5G, η προσέγγιση που επιλέχθηκε είναι να καθοριστεί για πρώτη φορά κοινή ευρωπαϊκή προσέγγιση. Η προσέγγιση αυτή σέβεται πλήρως τον ανοικτό χαρακτήρα της εσωτερικής αγοράς της ΕΕ, εφόσον τηρούνται οι καθοριζόμενες βάσει επικινδυνότητας απαιτήσεις ασφάλειας της ΕΕ.

Στις 22 Μαρτίου 2019 το Ευρωπαϊκό Συμβούλιο ζήτησε μια εναρμονισμένη προσέγγιση όσον αφορά την ασφάλεια των δικτύων 5G. Στις 26 Μαρτίου 2019 η Επιτροπή εξέδωσε τη σύσταση (ΕΕ) 2019/534 για την κυβερνοασφάλεια δικτύων 5G<sup>1</sup>. Η σύσταση καλεί τα κράτη μέλη να ολοκληρώσουν τις εθνικές εκτιμήσεις επικινδυνότητας και να επανεξετάσουν τα εθνικά μέτρα, ώστε να συνεργαστούν σε επίπεδο ΕΕ για μια συντονισμένη εκτίμηση επικινδυνότητας και να εκπονήσουν εργαλειοθήκη πιθανών μέτρων μετριασμού. Η παρούσα ανακοίνωση αποτελεί αναπόσπαστο μέρος της ολοκληρωμένης ευρωπαϊκής ψηφιακής στρατηγικής της Επιτροπής, σύμφωνα με την έκκληση του Ευρωπαϊκού Συμβουλίου.

## **2. Εισαγωγή των δικτύων 5G στην ΕΕ**

Η εγκατάσταση υποδομών δικτύου 5G στην Ευρώπη έχει κεντρικό ρόλο για την ευρωπαϊκή βιομηχανική στρατηγική και ανταγωνιστικότητα. Η Επιτροπή αναγνωρίζει ότι η εγκατάσταση των τεχνολογιών δικτύου 5G συνιστά σημαντικό παράγοντα διευκόλυνσης των μελλοντικών ψηφιακών υπηρεσιών. Το 2016 η Επιτροπή ενέκρινε το σχέδιο δράσης 5G για να διασφαλίσει ότι η Ένωση θα διαθέτει τις απαραίτητες υποδομές συνδεσιμότητας για τον ψηφιακό μετασχηματισμό της το 2020 και για την πλήρη εγκατάσταση σε αστικές περιοχές και σημαντικές διαδρομές μεταφορών έως το 2025<sup>2</sup>. Η ανακοίνωση για την κοινωνία των Gigabit

<sup>1</sup> Σύσταση (ΕΕ) 2019/534 για την κυβερνοασφάλεια των δικτύων 5G, ΕΕ L 88 της 29.3.2019, σ. 42-47.

<sup>2</sup> COM(2016) 588 της 14ης Ιουνίου 2016 «5G για την Ευρώπη: σχέδιο δράσης».

θέτει τον φιλόδοξο στόχο να υπάρχει πρόσβαση σε συνδεσιμότητα κινητών δεδομένων παντού<sup>3</sup>, συμπεριλαμβανομένων αγροτικών και απομακρυσμένων περιοχών.

Όσον αφορά την εκχώρηση συχνοτήτων, τα κράτη μέλη έχουν εκχωρήσει το 16 % των πρωτοπόρων ζωνών 5G<sup>4</sup>. Τους προσεχείς μήνες θα διεξαχθούν διαβουλεύσεις για ορισμένες διαδικασίες εκχώρησης, λαμβανομένης υπόψη της έννομης υποχρέωσης να καταστεί εφικτή έως το τέλος του έτους η χρήση όλων των πρωτοπόρων ζωνών 5G.

Η Ευρώπη συγκαταλέγεται στις πλέον προηγμένες περιοχές του κόσμου όσον αφορά την εμπορική διάθεση υπηρεσιών 5G<sup>5</sup>. Επί του παρόντος, οι πρώτες υπηρεσίες 5G αναμένεται να είναι διαθέσιμες σε 138 ευρωπαϊκές πόλεις έως το τέλος του 2020. Τα πρώιμα δίκτυα 5G βασίζονται στις υφιστάμενες τεχνολογίες δικτύου 4ης γενιάς (4G) και οι υπηρεσίες 5G παρέχονται κυρίως στο ευρύ κοινό, είτε ως βελτίωση των υπηρεσιών 4G από πλευράς χωρητικότητας και ταχύτητας, είτε ως οικονομικά αποδοτική ασύρματη εναλλακτική λύση αντί των σταθερών δικτύων<sup>6</sup>.

Όσον αφορά τις ευκαιρίες παροχής νέων υπηρεσιών μεταξύ επιχειρήσεων, όπως στους τομείς της ενέργειας, των τροφίμων και της γεωργίας, της υγείας, της βιομηχανικής παραγωγής ή των μεταφορών, η Ευρώπη έχει σημειώσει σημαντική πρόοδο με επενδύσεις της τάξης του 1 δισεκατομμυρίου ευρώ, συμπεριλαμβανομένων 300 εκατομμυρίων ευρώ ενωσιακής χρηματοδότησης υπέρ της σύμπραξης δημόσιου και ιδιωτικού τομέα για το 5G στο πλαίσιο του προγράμματος «Ορίζων 2020». Η επένδυση αυτή περιλαμβάνει περισσότερες από 160 μεγάλης κλίμακας δοκιμές 5G στην Ευρώπη στις οποίες περιλαμβάνονται δέκα διασυνοριακοί διάδρομοι αυτοκινητόδρομων για τη διεξαγωγή δοκιμών μεγάλης κλίμακας σε υπηρεσίες συνδεδεμένης και αυτοματοποιημένης κινητικότητας βασιζόμενες σε δίκτυο 5G. Οι δοκιμές αφορούν, μεταξύ άλλων, εφαρμογές που λειτουργούν σε δίκτυο 5G σε διάφορους τομείς, από βιώσιμη υγειονομική περίθαλψη, αυτοματοποιημένη κινητικότητα και αποδοτική ως προς τη χρήση πόρων γεωργία έως έξυπνα δίκτυα ηλεκτρικής ενέργειας και Βιομηχανία 4.0. Επιπλέον, η ΕΤΕπ, με τη στήριξη του Ευρωπαϊκού Ταμείου Στρατηγικών Επενδύσεων, χορήγησε δάνεια για την επιτάχυνση της έρευνας και της ανάπτυξης της τεχνολογίας 5G.

Ο Ευρωπαϊκός Κώδικας Ηλεκτρονικών Επικοινωνιών (στο εξής: κώδικας)<sup>7</sup> που θα εφαρμόζεται από την 21η Δεκεμβρίου 2020 αποτελεί σημαντική βάση για τη δημιουργία ενός φιλικού προς τις επενδύσεις περιβάλλοντος για τα δίκτυα 5G και πέραν αυτών. Επιπλέον, προγράμματα δημόσιας χρηματοδότησης, όπως ο μηχανισμός «Συνδέοντας την Ευρώπη» — Ψηφιακός τομέας<sup>8</sup> ή τα ευρωπαϊκά διαρθρωτικά και επενδυτικά ταμεία, θα είναι επίσης απαραίτητα προκειμένου να στηριχθεί η μελλοντική εγκατάσταση δικτύων 5G, ιδίως με τη

<sup>3</sup> COM(2016)587 «Συνδεσιμότητα για ανταγωνιστική ψηφιακή ενιαία αγορά - Προς μια ευρωπαϊκή κοινωνία των Gigabit».

<sup>4</sup> <http://www.5GObservatory.eu>

<sup>5</sup> <http://www.5GObservatory.eu>

<sup>6</sup> Ορισμένες από τις νέες λειτουργικές δυνατότητες των δικτύων 5G θα εισαχθούν βάσει σταδιακής προσέγγισης. Κατά το πρώτο (πολύ βραχυπρόθεσμο ή βραχυπρόθεσμο) στάδιο, η εγκατάσταση των δικτύων 5G θα συνίσταται πρωτίστως σε «μη αυτοτελή» δίκτυα, στα οποία μόνο το δίκτυο ραδιοπρόσβασης αναβαθμίζεται σε τεχνολογία 5G και κατά τα λοιπά εξακολουθούν να βασίζονται σε υφιστάμενα κεντρικά δίκτυα 4G, τα οποία θα παρέχουν βελτιωμένες επιδόσεις κινητών ευρυζωνικών υπηρεσιών στους τελικούς χρήστες. Κατά τα επόμενα (βραχυ-/μεσοπρόθεσμα έως μακροπρόθεσμα) στάδια, η εγκατάσταση «αυτοτελών» δικτύων 5G, συμπεριλαμβανομένων λειτουργιών κεντρικού δικτύου 5G, θα έχει ως προϋπόθεση και εν κairώ ως αποτέλεσμα πολύ πιο εκτεταμένες αλλαγές στην αρχιτεκτονική του δικτύου.

<sup>7</sup> Οδηγία (ΕΕ) 2018/1972 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση του Ευρωπαϊκού Κώδικα Ηλεκτρονικών Επικοινωνιών (Αναδιατύπωση).

<sup>8</sup> Πρόταση κανονισμού COM(2018)438, της 6ης Ιουνίου 2018, για τη σύσταση της διευκόλυνσης «Συνδέοντας την Ευρώπη» και την κατάργηση των κανονισμών (ΕΕ) αριθ. 1316/2013 και (ΕΕ) αριθ. 283/2014

σύνδεση κοινοτήτων με υπηρεσίες που λειτουργούν σε δίκτυο 5G, όπως σχολεία, νοσοκομεία, πόλεις και τοπικές διοικήσεις.

Δεδομένων των στρατηγικών ευκαιριών που προσφέρουν στην Ευρώπη οι υπηρεσίες 5G σε διάφορους κλάδους, θα είναι υψίστης σημασίας οι φορείς εκμετάλλευσης και οι πάροχοι υπηρεσιών να επενδύσουν σε προηγμένες λύσεις δικτύων και υπηρεσιών 5G. Για την αξιοποίηση των προαναφερόμενων ευκαιριών απαιτούνται, αφενός, νέα ραδιοδίκτυα 5G και, αφετέρου, νέα αποκαλούμενα «αυτοτελή» κεντρικά δίκτυα 5G, ώστε να παρέχονται προηγμένες λειτουργικές δυνατότητες 5G, όπως ο τεμαχισμός δικτύου<sup>9</sup> και η υπολογιστική παρυφών<sup>10</sup>.

Η Επιτροπή θα εξακολουθήσει να στηρίζει πλήρως την επιτυχή εισαγωγή των δικτύων 5G στην ΕΕ, για παράδειγμα, συνεργαζόμενη με τα κράτη μέλη και τα ενδιαφερόμενα μέρη με στόχο την αξιοποίηση των ευκαιριών των δικτύων 5G. Θα δοθεί η δέουσα προσοχή στις σχετικές με την υγεία πτυχές βάσει της αρχής της προφύλαξης<sup>11</sup>, σε συνεργασία με τους αρμόδιους διεθνείς οργανισμούς και την επιστημονική κοινότητα.

### **3. Η συντονισμένη από την ΕΕ εκτίμηση επικινδυνότητας για την κυβερνοασφάλεια στα δίκτυα 5G**

Συνεργαζόμενο συλλογικά στο πλαίσιο της ομάδας συνεργασίας για την ασφάλεια συστημάτων δικτύου και πληροφοριών (NIS)<sup>12</sup>, κάθε κράτος μέλος ολοκλήρωσε την οικεία εθνική εκτίμηση επικινδυνότητας των εθνικών υποδομών δικτύου 5G και διαβίβασε τα πορίσματα στην Επιτροπή και στον ENISA, τον Οργανισμό της Ευρωπαϊκής Ένωσης για την κυβερνοασφάλεια, έως τις αρχές Ιουλίου του 2019.

Με βάση τις εν λόγω εθνικές εκτιμήσεις επικινδυνότητας, στις 9 Οκτωβρίου 2019 η ομάδα συνεργασίας NIS, η οποία αποτελείται από εκπροσώπους των κρατών μελών, της Επιτροπής και του ENISA, δημοσίευσε έκθεση για τη συντονισμένη από την ΕΕ εκτίμηση επικινδυνότητας όσον αφορά την κυβερνοασφάλεια των δικτύων 5G<sup>13</sup>. Η έκθεση προσδιορίζει τις κύριες απειλές και τους κύριους παράγοντες απειλής, τα πιο ευαίσθητα πάγια στοιχεία και τα κύρια τρωτά σημεία (συμπεριλαμβανομένων των τεχνικών και άλλου είδους τρωτών σημείων) που επηρεάζουν τα δίκτυα 5G. Σε αυτή τη βάση, στην έκθεση προσδιορίζονται επίσης ορισμένες κατηγορίες κινδύνων στρατηγικής από πλευράς ΕΕ σημασίας και παρουσιάζονται με συγκεκριμένα σενάρια κινδύνου, στα οποία σχετικοί συνδυασμοί των διαφόρων παραμέτρων (τρωτά σημεία, απειλές και παράγοντες απειλής) αντιστοιχίζονται με διαφορετικά πάγια στοιχεία (βλ. προσάρτημα).

<sup>9</sup> Ο τεμαχισμός δικτύου 5G καθιστά εφικτό τον υψηλού βαθμού διαχωρισμό μεταξύ στρωμάτων υπηρεσίας εντός του ίδιου φυσικού δικτύου και, ως εκ τούτου, αυξάνει τις δυνατότητες παροχής διαφοροποιημένων υπηρεσιών σε ολόκληρο το δίκτυο.

<sup>10</sup> Η υπολογιστική παρυφών είναι ένα παράδειγμα καταναμημένης πληροφορικής που φέρνει τις υπολογιστικές διεργασίες και την αποθήκευση δεδομένων εγγύτερα στην περιοχή όπου χρειάζονται, με σκοπό τη βελτίωση των χρόνων απόκρισης και την εξοικονόμηση εύρους ζώνης.

<sup>11</sup> Σύσταση του Συμβουλίου, της 12ης Ιουλίου 1999, περί του περιορισμού της έκθεσης του κοινού σε ηλεκτρομαγνητικά πεδία (0 Hz - 300 GHz) (1999/519/EK).

<sup>12</sup> Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (οδηγία NIS). Η ομάδα συνεργασίας NIS συστάθηκε δυνάμει της οδηγίας NIS με στόχο να διασφαλιστούν η στρατηγική συνεργασία και η ανταλλαγή πληροφοριών μεταξύ των κρατών μελών της ΕΕ στον τομέα της κυβερνοασφάλειας.

<sup>13</sup> <https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security>

Για τη συμπλήρωση της εν λόγω έκθεσης ως περαιτέρω συμβολή στην εργαλειοθήκη, ο ENISA προέβη σε ειδική χαρτογράφηση του τοπίου απειλών<sup>14</sup>, η οποία συνίσταται σε λεπτομερή ανάλυση ορισμένων τεχνικών πτυχών και, ειδικότερα, στον προσδιορισμό των πάγιων στοιχείων του δικτύου και των απειλών που τα επηρεάζουν.

Στην έκθεση για τη συντονισμένη από την ΕΕ εκτίμηση επικινδυνότητας επισημαίνονται ορισμένες πτυχές που έχουν σημασία για τα δίκτυα 5G. Συγκεκριμένα:

α) *Οι τεχνολογικές αλλαγές που εισήγαγε η τεχνολογία 5G θα αυξήσουν τη συνολική επιφάνεια έκθεσης σε πιθανές επιθέσεις και τον αριθμό των δυνητικών σημείων εισόδου για τους επιτιθέμενους:*

— *Βελτιωμένη λειτουργικότητα στις παρυφές του δικτύου και περισσότερο αποκεντρωμένη αρχιτεκτονική σε σχέση με τις προηγούμενες γενιές δικτύων κινητών επικοινωνιών σημαίνουν ότι ορισμένες λειτουργίες των κεντρικών δικτύων μπορούν να ενσωματωθούν σε άλλα τμήματα των δικτύων και, κατά συνέπεια, ο αντίστοιχος εξοπλισμός μπορεί να καταστεί πιο ευαίσθητος (π.χ. σταθμοί βάσης ή λειτουργίες διαχείρισης και εντοπισμού).*

— *Το αυξημένο μερίδιο λογισμικού στον εξοπλισμό 5G συνεπάγεται αυξημένους κινδύνους που συνδέονται με τις διαδικασίες ανάπτυξης και ενημέρωσης λογισμικού, δημιουργεί νέους κινδύνους ασφαλείας ρύθμισης παραμέτρων και αυξάνει τη σημασία της ανάλυσης της ασφάλειας όσον αφορά τις επιλογές κάθε μεμονωμένου φορέα εκμετάλλευσης δικτύου κινητών επικοινωνιών κατά το στάδιο εγκατάστασης του δικτύου.*

β) *Αυτά τα νέα τεχνολογικά στοιχεία θα αυξήσουν τη σημασία, αφενός, της εξάρτησης των φορέων εκμετάλλευσης δικτύων κινητών επικοινωνιών από τρίτους προμηθευτές και, αφετέρου, του ρόλου που αυτοί οι προμηθευτές διαδραματίζουν στην αλυσίδα εφοδιασμού 5G.*

*Αυτό, με τη σειρά του, θα αυξήσει, αφενός, τον αριθμό των διαδρομών επιθέσεων τις οποίες θα μπορούσαν να εκμεταλλευθούν παράγοντες απειλής, ιδίως τρίτες χώρες ή παράγοντες που υποστηρίζονται από αυτές, λόγω των ικανοτήτων τους (πρόθεση και πόροι) να εκτελούν επιθέσεις κατά δικτύων τηλεπικοινωνιών των κρατών μελών της ΕΕ και, αφετέρου, τη δυνητική σοβαρότητα των επιπτώσεων των εν λόγω επιθέσεων.*

*Στο πλαίσιο της αυξημένης έκθεσης σε επιθέσεις που διευκολύνονται από τρίτους προμηθευτές, το ατομικό προφίλ κινδύνου των προμηθευτών θα καταστεί ιδιαίτερα σημαντικό, ιδίως όταν ένας προμηθευτής έχει σημαντική παρουσία εντός δικτύων ή περιοχών.*

γ) *Η σημαντική εξάρτηση από έναν και μόνο προμηθευτή αυξάνει την έκθεση σε ενδεχόμενη αστοχία του εν λόγω προμηθευτή και τις αντίστοιχες συνέπειες. Εντείνει επίσης τις πιθανές συνέπειες των αδυναμιών ή των τρωτών σημείων και την πιθανή εκμετάλλευσή τους από παράγοντες απειλής, ιδίως όταν η εξάρτηση αφορά προμηθευτή που παρουσιάζει υψηλό βαθμό επικινδυνότητας.*

δ) *Εάν ευδοιωθούν ορισμένες από τις νέες περιπτώσεις χρήσης που προβλέπονται για τα δίκτυα 5G, αυτά θα αποτελέσουν εντέλει σημαντικό μέρος της αλυσίδας εφοδιασμού πολλών κρίσιμων εφαρμογών ΤΠ και, ως εκ τούτου, θα επηρεαστούν οι απαιτήσεις εμπιστευτικότητας και*

<sup>14</sup> Τοπίο απειλών για τα δίκτυα 5G του ENISA: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks>.

*προστασίας της ιδιωτικής ζωής και, παράλληλα, η ακεραιότητα και η διαθεσιμότητα των εν λόγω δικτύων θα συνιστούν μείζονα ζητήματα εθνικής ασφάλειας καθώς και μείζονα πρόκληση για την ασφάλεια από πλευράς ΕΕ.*

Πηγή: συντονισμένη από την ΕΕ εκτίμηση επικινδυνότητας

Η έκθεση για τη συντονισμένη από την ΕΕ εκτίμηση επικινδυνότητας καταλήγει επίσης στο συμπέρασμα ότι οι προκλήσεις αυτές δημιουργούν ένα νέο πρότυπο ασφάλειας, γεγονός που καθιστά αναγκαίες τόσο την επαναξιολόγηση του ισχύοντος πλαισίου πολιτικής και ασφάλειας που εφαρμόζεται στον τομέα των δικτύων 5G και του οικοσυστήματός του, όσο και τη λήψη των αναγκαίων μέτρων μετριασμού από τα κράτη μέλη.

Για την αποτελεσματική αντιμετώπιση των κινδύνων που διαπιστώθηκαν και για την ενίσχυση της ασφάλειας και της ανθεκτικότητας των δικτύων 5G, απαιτείται συνολική προσέγγιση που συνεπάγεται τη λήψη δέσμης βασικών μέτρων, καθώς και συναφών υποστηρικτικών δράσεων που μπορούν να αντιμετωπίσουν ταυτόχρονα τους κινδύνους. Η συντονισμένη από την ΕΕ εκτίμηση επικινδυνότητας παρείχε τη βάση για τον καθορισμό μέτρων μετριασμού που μπορούν να εφαρμοστούν σε εθνικό και ευρωπαϊκό επίπεδο.

Στα συμπεράσματά του της 3ης Δεκεμβρίου 2019, το Συμβούλιο υποστήριξε τα πορίσματα της συντονισμένης εκτίμησης επικινδυνότητας και τόνισε «τη σημασία μιας συντονισμένης προσέγγισης και αποτελεσματικής υλοποίησης της σύστασης προκειμένου να αποφευχθεί ο κατακερματισμός της ενιαίας αγοράς<sup>15</sup>». Για τον σκοπό αυτόν, το Συμβούλιο κάλεσε τα κράτη μέλη, την Επιτροπή και τον ENISA να «λάβουν όλα τα αναγκαία μέτρα στο πλαίσιο των αρμοδιοτήτων τους για τη διασφάλιση της ασφάλειας και της ακεραιότητας των δικτύων ηλεκτρονικών επικοινωνιών, ιδίως των δικτύων 5G, και να συνεχίσουν να παγιώνουν μια συντονισμένη προσέγγιση για την αντιμετώπιση των προκλήσεων στον τομέα της ασφάλειας που σχετίζονται με τις τεχνολογίες 5G.»

#### **4. Η εργαλειοθήκη της ΕΕ για την κυβερνοασφάλεια των δικτύων 5G**

Στις 29 Ιανουαρίου 2020 η ομάδα συνεργασίας NIS δημοσίευσε την εργαλειοθήκη της ΕΕ για μέτρα μετριασμού των κινδύνων<sup>16</sup>, στην οποία εξετάζονται όλοι οι κίνδυνοι που διαπιστώθηκαν στην έκθεση συντονισμένης εκτίμησης επικινδυνότητας.

Η εργαλειοθήκη της ΕΕ προσδιορίζει και περιγράφει μια δέσμη στρατηγικών και τεχνικών μέτρων, καθώς και αντίστοιχες υποστηρικτικές δράσεις για την ενίσχυση της αποτελεσματικότητάς τους, οι οποίες μπορούν να εφαρμοστούν για τον μετριασμό των κινδύνων που έχουν διαπιστωθεί. Στα **στρατηγικά μέτρα** περιλαμβάνονται μέτρα που αφορούν αυξημένες ρυθμιστικές εξουσίες για τις αρχές ώστε να ελέγχουν τις προμήθειες και την ανάπτυξη δικτύων, ειδικά μέτρα για την αντιμετώπιση των κινδύνων που σχετίζονται με μη τεχνικά τρωτά σημεία, καθώς και πιθανές πρωτοβουλίες για την προώθηση μιας βιώσιμης και διαφοροποιημένης αλυσίδας εφοδιασμού και αξίας στον τομέα των δικτύων 5G, ώστε να αποφεύγονται οι κίνδυνοι συστημικής και μακροπρόθεσμης εξάρτησης. Στα **τεχνικά μέτρα** περιλαμβάνονται μέτρα για την ενίσχυση της ασφάλειας των δικτύων και του εξοπλισμού 5G

<sup>15</sup> Συμπεράσματα του Συμβουλίου σχετικά με τη σημασία του 5G για την ευρωπαϊκή οικονομία και την ανάγκη μετριασμού των κινδύνων ασφάλειας που συνδέονται με το 5G. 3 Δεκεμβρίου 2019, 14517/19 <https://data.consilium.europa.eu/doc/document/ST-14517-2019-INIT/el/pdf>.

<sup>16</sup> Κυβερνοασφάλεια των δικτύων 5G - Εργαλειοθήκη της ΕΕ για μέτρα μετριασμού των κινδύνων, 29 Ιανουαρίου 2020. <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group>.

με την αντιμετώπιση των κινδύνων που απορρέουν από τεχνολογίες, διαδικασίες, ανθρώπινους και φυσικούς παράγοντες. Επιπλέον, για καθέναν από τους τομείς κινδύνου που διαπιστώθηκαν στη συντονισμένη από την ΕΕ εκτίμηση επικινδυνότητας, η εργαλειοθήκη προβλέπει **σχέδια μετριασμού των κινδύνων** βάσει μέτρων ύψιστης αποτελεσματικότητας.

Μεταξύ αυτών, στα συμπεράσματα της εργαλειοθήκης της ΕΕ, όπως συμφωνήθηκε από την ομάδα συνεργασίας NIS, συνιστάται μια δέσμη **βασικών μέτρων** προς εφαρμογή από όλα τα κράτη μέλη και από την Επιτροπή ως εξής:

### **Συμπεράσματα της εργαλειοθήκης της ΕΕ**

*Η εργαλειοθήκη της ΕΕ καθορίζει μια σειρά μέτρων και δράσεων οι οποίες —εάν συνδυαστούν καταλλήλως και εφαρμοστούν αποτελεσματικά— αποτελούν τη βάση για μια συντονισμένη προσέγγιση στον τομέα αυτόν. Πράγματι, δεδομένων του ευρέος φάσματος των τομέων κινδύνου που διαπιστώνονται στη συντονισμένη από την ΕΕ εκτίμηση επικινδυνότητας και του διαφορετικού χαρακτήρα τους, κανένας μεμονωμένος τύπος μέτρου δεν θα είναι επαρκής και, αντ' αυτού, θα είναι αναγκαία μια σειρά μέτρων που θα συνδυάζονται καταλλήλως, προκειμένου να αντιμετωπιστούν όλοι οι βασικοί τομείς κινδύνου.*

*Με βάση την αξιολόγηση των σχεδίων πιθανών μέτρων μετριασμού και τον καθορισμό των μέτρων ύψιστης αποτελεσματικότητας, η εν λόγω εργαλειοθήκη συνιστά τα εξής:*

*1. Όλα τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι έχουν θεσπίσει μέτρα (συμπεριλαμβανομένων των εξουσιών των εθνικών αρχών) για την κατάλληλη και αναλογική αντιμετώπιση των σημερινών και μελλοντικών κινδύνων, και ιδίως να διασφαλίζουν ότι είναι σε θέση να περιορίζουν, να απαγορεύουν και/ή να επιβάλλουν συγκεκριμένες απαιτήσεις ή όρους, σύμφωνα με μια προσέγγιση βάσει επικινδυνότητας, για την προμήθεια, την εγκατάσταση και τη λειτουργία εξοπλισμού δικτύου 5G με βάση μια σειρά από λόγους σχετικούς με την ασφάλεια.*

*Ειδικότερα, θα πρέπει:*

να ενισχύουν τις **απαιτήσεις ασφάλειας** για τους φορείς εκμετάλλευσης δικτύων κινητών επικοινωνιών (π.χ. αυστηροί έλεγχοι πρόσβασης, κανόνες ασφαλούς λειτουργίας και παρακολούθησης, περιορισμοί στην εξωτερική ανάθεση συγκεκριμένων λειτουργιών κ.λπ.)·

να αξιολογούν το προφίλ κινδύνου των προμηθευτών· κατά συνέπεια, **να εφαρμόζουν συναφείς περιορισμούς σε προμηθευτές που θεωρούνται υψηλού κινδύνου — συμπεριλαμβανομένων των απαραίτητων αποκλεισμών ώστε να μετριάσουν αποτελεσματικά τους κινδύνους— για βασικά πάγια στοιχεία που ορίζονται ως κρίσιμης σημασίας και ευαίσθητα στη συντονισμένη από την ΕΕ εκτίμηση επικινδυνότητας (π.χ. λειτουργίες κεντρικού δικτύου, λειτουργίες διαχείρισης και ενορχήστρωσης δικτύου και λειτουργίες δικτύου πρόσβασης)**·

να διασφαλίζουν ότι κάθε φορέας εκμετάλλευσης διαθέτει κατάλληλη στρατηγική πολλαπλών πωλητών για την **αποφυγή ή τον περιορισμό οποιασδήποτε σημαντικής εξάρτησης** από έναν και μόνο προμηθευτή (ή προμηθευτές με παρόμοιο προφίλ κινδύνου), να διασφαλίζουν την κατάλληλη ισορροπία μεταξύ των προμηθευτών σε εθνικό επίπεδο και **να αποφεύγουν την εξάρτηση από προμηθευτές που θεωρούνται υψηλού κινδύνου**· αυτό απαιτεί επίσης να αποφεύγονται καταστάσεις εγκλωβισμού σε έναν μόνο προμηθευτή, μεταξύ άλλων, με την προώθηση μεγαλύτερης διαλειτουργικότητας του εξοπλισμού.

2. Η Ευρωπαϊκή Επιτροπή, από κοινού με τα κράτη μέλη, θα πρέπει να συμβάλλει στα εξής:

στη διατήρηση μιας **διαφοροποιημένης και βιώσιμης αλυσίδας εφοδιασμού 5G**, προκειμένου να αποφευχθεί η μακροπρόθεσμη εξάρτηση, μεταξύ άλλων:

ο με πλήρη αξιοποίηση των υφιστάμενων εργαλείων και μέσων της ΕΕ, ιδίως μέσω του ελέγχου των δυνητικών **άμεσων ξένων επενδύσεων (ΑΞΕ)** που επηρεάζουν βασικά πάγια στοιχεία 5G, καθώς και με αποφυγή των **στρεβλώσεων** στην αγορά προμήθειας 5G που απορρέουν από ενδεχόμενες πρακτικές ντάμπινγκ ή επιδοτήσεις· και

ο με περαιτέρω ενίσχυση **των ικανοτήτων της ΕΕ στις τεχνολογίες 5G και μετά το 5G**, μέσω αξιοποίησης των σχετικών προγραμμάτων και της χρηματοδότησης της ΕΕ·

στη διευκόλυνση του συντονισμού μεταξύ των κρατών μελών όσον αφορά την **τυποποίηση** για την επίτευξη συγκεκριμένων στόχων ασφάλειας και στην ανάπτυξη **συναφών συστημάτων πιστοποίησης σε επίπεδο ΕΕ** για την προώθηση ασφαλέστερων προϊόντων και διαδικασιών.

3. Για να διασφαλιστεί ότι η προαναφερόμενη συντονισμένη προσέγγιση θα έχει αποτελέσματα σε βάθος χρόνου, θα πρέπει να διευρυνθούν η εντολή του άξονα εργασίας της ομάδας συνεργασίας NIS, καθώς και η συνεργασία με άλλους σχετικούς φορείς και οντότητες, με ειδικότερο στόχο:

να επανεξετάζει σε τακτά χρονικά διαστήματα —με την υποστήριξη της Επιτροπής και του ENISA— τις **εθνικές και ενωσιακές εκτιμήσεις επικινδυνότητας** για την ασφάλεια των δικτύων 5G και μετά το 5G, αναπτύσσοντας περαιτέρω και εναρμονίζοντας την ακολουθούμενη μεθοδολογία αξιολόγησης, και προσαρμόζοντάς την στην εξελισσόμενη τεχνολογία 5G·

να διενεργεί αναλυτική και τακτική **παρακολούθηση και αξιολόγηση της εφαρμογής** της εργαλειοθήκης, βάσει δομημένων εκθέσεων από τα κράτη μέλη·

να συντονίζει και να στηρίζει την υλοποίηση **υποστηρικτικών δράσεων**, οι οποίες απαιτούν συνεργασία σε επίπεδο ΕΕ, ιδίως όσον αφορά την εκπόνηση κατευθυντήριων γραμμών και την ανταλλαγή βέλτιστων πρακτικών σχετικά με τα διάφορα μέτρα·

να στηρίζει τον ενδεχόμενο πρόσθετο συντονισμό σε επίπεδο ΕΕ, κατά περίπτωση, ιδίως με στόχο την περαιτέρω σύγκλιση **όσον αφορά τις τεχνικές και οργανωτικές απαιτήσεις ασφάλειας για τους φορείς εκμετάλλευσης δικτύων**.

Πηγή: εργαλειοθήκη της ΕΕ.

Από τα συμπεράσματα της εργαλειοθήκης καθίσταται σαφής η ισχυρή βούληση των κρατών μελών να αντιμετωπίσουν από κοινού τις προκλήσεις στον τομέα της ασφάλειας των δικτύων 5G. Αυτό έχει θεμελιώδη σημασία για την ασφάλεια εντός των κρατών μελών και σε ολόκληρη την ΕΕ, για τις εθνικές οικονομίες, καθώς και για την εσωτερική αγορά της ΕΕ και την τεχνολογική αυτοδυναμία της Ευρώπης. Τόσο η συντονισμένη από την ΕΕ εκτίμηση επικινδυνότητας όσο και η εργαλειοθήκη της ΕΕ αποδεικνύουν την υψηλή αξία των συλλογικών εργασιών που επιτελούνται στο πλαίσιο της ομάδας συνεργασίας NIS, με την εντατική συνεργασία μεταξύ εκπροσώπων από όλα τα κράτη μέλη, την Επιτροπή και τον ENISA.



Η εργαλειοθήκη καθιστά εφικτή μια κοινή ενωσιακή προσέγγιση ως προς την κυβερνοασφάλεια των δικτύων 5G, ενισχύοντας τη συνοχή σε ολόκληρη την εσωτερική αγορά μέσω ενωσιακών πολιτικών και ενωσιακού συντονισμού, καθώς και στην άσκηση των αρμοδιοτήτων των κρατών μελών, ιδίως όσον αφορά την εθνική ασφάλεια. Τα μέτρα και τα σχέδια μετριασμού των κινδύνων που περιέχει η εργαλειοθήκη δίνουν τη δυνατότητα κατάλληλης, αποτελεσματικής και αναλογικής ενωσιακής αντιμετώπισης των κοινών προκλήσεων στον τομέα της κυβερνοασφάλειας των δικτύων 5G.

Η Επιτροπή χαιρετίζει τη δημοσίευση της εργαλειοθήκης της ΕΕ για την κυβερνοασφάλεια των δικτύων 5G και υποστηρίζει πλήρως όλα τα ανωτέρω συμπεράσματα.

Η Επιτροπή καλεί τα κράτη μέλη και τα αρμόδια θεσμικά και λοιπά όργανα ή οργανισμούς της Ένωσης:

- i) να διασφαλίσουν την ταχεία εφαρμογή αποτελεσματικών και κατάλληλων στρατηγικών μετριασμού των κινδύνων σε ολόκληρη την ΕΕ σύμφωνα με την εργαλειοθήκη της ΕΕ και
- ii) να λάβουν όλα τα απαραίτητα περαιτέρω μέτρα για να διασφαλιστεί ο συντονισμός σε επίπεδο Ένωσης, μεταξύ άλλων, με τη συνέχιση των εργασιών στο πλαίσιο της ομάδας συνεργασίας NIS και τη δημιουργία στιβαρού μηχανισμού για την παρακολούθηση της εφαρμογής της εργαλειοθήκης της ΕΕ, ώστε να εξασφαλιστούν η αποτελεσματικότητα των μέτρων και η εύρυθμη λειτουργία της εσωτερικής αγοράς.

## **5. Εφαρμογή της εργαλειοθήκης**

Η αποφασιστικότητα των κρατών μελών να αξιοποιήσουν πλήρως την εργαλειοθήκη είναι απαραίτητη προϋπόθεση για μια αξιόπιστη και επιτυχημένη ευρωπαϊκή προσέγγιση της ασφάλειας των δικτύων 5G. Τα κράτη μέλη θα αποφασίζουν κατά πόσον ένα συγκεκριμένο μέτρο είναι κατάλληλο με βάση τις εθνικές συνθήκες. Ωστόσο, είναι απολύτως απαραίτητο **να εφαρμοστεί μια δέσμη βασικών μέτρων, σύμφωνα με τις συστάσεις της ομάδας συνεργασίας NIS (βλ. συμπεράσματα της εργαλειοθήκης), σε κάθε κράτος μέλος και, στην περίπτωση ορισμένων εκ των εν λόγω μέτρων, σε επίπεδο ΕΕ, προκειμένου να αντιμετωπιστούν οι κίνδυνοι που έχουν διαπιστωθεί.**

Η Επιτροπή είναι πρόθυμη να εξακολουθήσει να παρέχει πλήρη στήριξη στα κράτη μέλη κατά τα επόμενα στάδια και καλεί τα κράτη μέλη:

— **έως τις 30 Απριλίου 2020**, να λάβουν συγκεκριμένα και μετρήσιμα μέτρα για την εφαρμογή της δέσμης βασικών μέτρων που συνιστώνται στα συμπεράσματα της εργαλειοθήκης της ΕΕ·

— **έως τις 30 Ιουνίου 2020**, να εκπονήσουν έκθεση της ομάδας συνεργασίας NIS σχετικά με την κατάσταση εφαρμογής των εν λόγω βασικών μέτρων σε κάθε κράτος μέλος, με βάση την τακτική υποβολή εκθέσεων και παρακολούθηση, ιδίως στο πλαίσιο της ομάδας συνεργασίας NIS, με την υποστήριξη της Επιτροπής και του ENISA.

### **5.1. Εναρμονισμένη προσέγγιση βάσει επικινδυνότητας όσον αφορά τους προμηθευτές 5G**

Δεδομένου του απώτερου στόχου να διασφαλιστούν η ασφάλεια, η ανθεκτικότητα και η βιωσιμότητα των δικτύων 5G, τα κράτη μέλη συμφώνησαν ως προς την ανάγκη να αξιολογείται το προφίλ κινδύνου των επιμέρους προμηθευτών και, ως εκ τούτου, να

εφαρμόζονται κατάλληλοι περιορισμοί σε προμηθευτές που θεωρούνται υψηλού κινδύνου, συμπεριλαμβανομένων των απαραίτητων αποκλεισμών για τον αποτελεσματικό μετριασμό των κινδύνων για τα βασικά πάγια στοιχεία, όπως αναφέρεται στην εργαλειοθήκη. Η Επιτροπή είναι πρόθυμη να στηρίξει τα κράτη μέλη στην εφαρμογή των εν λόγω μέτρων.

Για τη στήριξη της εφαρμογής τους σε ολόκληρη την ΕΕ, η συντονισμένη από την ΕΕ εκτίμηση επικινδυνότητας και η εργαλειοθήκη της ΕΕ παρέχουν καθοδήγηση όσον αφορά (1) την αξιολόγηση του προφίλ κινδύνου των προμηθευτών<sup>17</sup> και (2) την ευαισθησία των στοιχείων και των λειτουργιών δικτύου<sup>18</sup>, καθώς και άλλων πάγιων στοιχείων. Τόσο η συντονισμένη από την ΕΕ εκτίμηση επικινδυνότητας όσο και τα μέτρα της εργαλειοθήκης καλύπτουν τους κινδύνους που συνδέονται με τους προμηθευτές εξοπλισμού δικτύου και υπηρεσιών δικτύου 5G. Δεν καλύπτουν όμως άλλα προϊόντα ή υπηρεσίες που ενδεχομένως παρέχουν αυτοί ή άλλοι προμηθευτές.

Όπως ορίζεται στο σημείο 2.37 της συντονισμένης από την ΕΕ εκτίμησης επικινδυνότητας, το προφίλ κινδύνου των επιμέρους προμηθευτών μπορεί να αξιολογείται με βάση διάφορους παράγοντες.

Η αξιολόγηση των προφίλ κινδύνου των προμηθευτών θα πρέπει να διενεργείται αποκλειστικά για λόγους ασφάλειας και να βασίζεται σε αντικειμενικά κριτήρια. Για τη διευκόλυνση της συντονισμένης προσέγγισης στην εφαρμογή των προαναφερόμενων μέτρων, η εργαλειοθήκη συνιστά στα κράτη μέλη να ανταλλάσσουν πληροφορίες σχετικά με εθνικές προσεγγίσεις και βέλτιστες πρακτικές. Επιπλέον, η Επιτροπή θεωρεί ότι η δράση αυτή θα πρέπει να είναι μία από τις πρώτες προτεραιότητες του επόμενου σταδίου των εργασιών στο πλαίσιο της ομάδας συνεργασίας NIS, από κοινού με την Επιτροπή και τον ENISA.

Είναι σημαντικό να εφαρμόζονται εγκαίρως οι περιορισμοί όσον αφορά προμηθευτές που θεωρούνται υψηλού κινδύνου, συμπεριλαμβανομένων των απαραίτητων αποκλεισμών για τον αποτελεσματικό μετριασμό των κινδύνων, καθώς και τα μέτρα για την αποφυγή της εξάρτησης από τους εν λόγω προμηθευτές. Εάν αυτό γίνεται στο πλέον πρώιμο στάδιο, για παράδειγμα, όπου είναι δυνατόν, κατά τις διαδικασίες αδειοδότησης συχνοτήτων 5G, θα αυξάνεται επίσης η προβλεψιμότητα για τους φορείς της αγοράς και, κατά συνέπεια, θα διευκολύνεται η ταχεία εισαγωγή των δικτύων 5G και θα διασφαλίζονται η μακροπρόθεσμη ασφάλεια των δικτύων 5G και η ανθεκτικότητα της αλυσίδας εφοδιασμού 5G.

Ταυτόχρονα, κατά την εθνική εφαρμογή των εν λόγω μέτρων επιτρέπεται να προβλέπονται διαφορετικά χρονοδιαγράμματα, όπου είναι αναγκαίο και δικαιολογημένο, ιδίως σε περίπτωση υψηλού βαθμού υφιστάμενης εξάρτησης από εξοπλισμό ή υπηρεσίες από προμηθευτές που έχουν αξιολογηθεί ως υψηλού κινδύνου (π.χ. λαμβανομένων υπόψη των κύκλων αναβάθμισης εξοπλισμού, ιδίως της μετάβασης από «μη αυτοτελή» σε «αυτοτελή» δίκτυα 5G). Τα κράτη μέλη μπορούν να εξετάσουν το ενδεχόμενο να καθορίσουν σχέδια εφαρμογής που ενδεχομένως προβλέπουν κατάλληλες μεταβατικές περιόδους για τους ενδιαφερόμενους φορείς εκμετάλλευσης δικτύων. Σε αυτό το πλαίσιο, οι μεταβατικές περίοδοι θα πρέπει να καθορίζονται κατά τρόπο που να διατηρεί ή και να ενισχύει τα κίνητρα για επενδύσεις σε σύγχρονο εξοπλισμό δικτύου, για παράδειγμα, για να επισπευσθεί η

<sup>17</sup> Σημείο 2.37 της συντονισμένης από την ΕΕ εκτίμησης επικινδυνότητας.

<sup>18</sup> Το σημείο 2.21 της συντονισμένης από την ΕΕ εκτίμησης επικινδυνότητας παρουσιάζει τις κύριες κατηγορίες στοιχείων και λειτουργιών και το συνολικό επίπεδο ευαισθησίας τους, και απαριθμεί ορισμένα βασικά στοιχεία που προσδιορίζονται από τα κράτη μέλη για κάθε κατηγορία. Τα σημεία 2.28 και 2.29 καθορίζουν ορισμένους άλλους τύπους ευαίσθητων πάγιων στοιχείων ή περιοχών (π.χ. συγκεκριμένες οντότητες ή γεωγραφικές περιοχές).

εγκατάσταση ολοκληρωμένων («αυτοτελών») κεντρικών δικτύων 5G και να αντικατασταθεί ο υφιστάμενος εξοπλισμός 4G σε άλλα τμήματα των δικτύων ( π.χ. στο δίκτυο ραδιοπρόσβασης), σύμφωνα με τους στόχους του σχεδίου δράσης 5G<sup>19</sup>.

Επιπλέον, λόγω της πολυπλοκότητας των δικτύων 5G που βασίζονται σε λογισμικό, οι φορείς εκμετάλλευσης τηλεπικοινωνιών ενδέχεται να βασίζονται ολοένα και περισσότερο σε τρίτες οντότητες για την εκτέλεση ορισμένων καθηκόντων, όπως η συντήρηση και η αναβάθμιση των δικτύων και του λογισμικού 5G, καθώς και άλλες υπηρεσίες ή διαχείριση των οποίων έχει ανατεθεί εξωτερικά, επιπροσθέτως της παροχής εξοπλισμού δικτύου. Όπως περιγράφεται στη συντονισμένη από την ΕΕ εκτίμηση επικινδυνότητας, αυτό το ενδεχόμενο αποτελεί πηγή σοβαρού κινδύνου για την ασφάλεια. Ως εκ τούτου, θα πρέπει να δοθεί ιδιαίτερη προσοχή στο θέμα αυτό. Είναι σημαντικό να πραγματοποιείται επίσης διεξοδική εκτίμηση ασφάλειας του προφίλ κινδύνου των προμηθευτών που είναι επιφορτισμένοι με τις προαναφερόμενες υπηρεσίες, ιδίως όταν τα καθήκοντα αυτά δεν εκτελούνται εντός της ΕΕ. Θα πρέπει να λαμβάνονται κατάλληλα μέτρα, όπως, μεταξύ άλλων, η εφαρμογή περιορισμών, ιδίως σε ευαίσθητα τμήματα των δικτύων 5G ή ο αναγκαίος αποκλεισμός οντοτήτων υψηλού κινδύνου σύμφωνα με τα μέτρα μετριασμού της εργαλειοθήκης, ώστε να διαφυλάσσεται η μακροπρόθεσμη ακεραιότητα της υποδομής 5G.

### 5.2. Ο ρόλος της Επιτροπής για τη στήριξη της εφαρμογής της εργαλειοθήκης

Η Επιτροπή θα εξακολουθήσει να στηρίζει την εφαρμογή της ενωσιακής προσέγγισης για την κυβερνοασφάλεια των δικτύων 5G γενικά, καθώς και να αναλαμβάνει συγκεκριμένες πρωτοβουλίες σε σχέση με μέτρα και στόχους της εργαλειοθήκης, όπου αυτό μπορεί να αποφέρει προστιθέμενη αξία. Η Επιτροπή θα αξιοποιήσει πλήρως τις αρμοδιότητές της και τα σχετικά μέσα στον βαθμό που απαιτείται για την αντιμετώπιση των διαπιστωθέντων ζητημάτων ασφάλειας. Με τον τρόπο αυτόν, και ενεργώντας συλλογικά από κοινού με τα κράτη μέλη και τον ιδιωτικό τομέα, η Επιτροπή επιδιώκει να στηρίζει στρατηγικά μέτρα που θα συμβάλουν στη διασφάλιση της τεχνολογικής αυτοδυναμίας και της ηγετικής θέσης της ΕΕ στη μελλοντική ανάπτυξη τεχνολογιών δικτύου, στις τεχνολογίες κυβερνοασφάλειας και σε όλα τα συναφή δομικά στοιχεία από τα οποία εξαρτάται το σύνολο της οικονομίας και της ασφάλειάς μας.

Ειδικότερα, η Επιτροπή θα λάβει τα ακόλουθα μέτρα για να εξασφαλίσει την εφαρμογή των αντίστοιχων μέτρων μετριασμού της εργαλειοθήκης στους τομείς που εμπίπτουν στην αρμοδιότητά της:

#### **Διασφάλιση της κυβερνοασφάλειας των δικτύων 5G και μιας διαφοροποιημένης αλυσίδας αξίας στον τομέα των δικτύων 5G:**

**-Συνεργασία στον τομέα της κυβερνοασφάλειας:** Συνεχιζόμενη παροχή στήριξης στα κράτη μέλη για την αποτελεσματική, συντονισμένη και έγκαιρη εφαρμογή των εθνικών μέτρων μέσω της ομάδας συνεργασίας NIS.

**- Κανόνες για τις τηλεπικοινωνίες και την κυβερνοασφάλεια:** Παροχή στήριξης για την εφαρμογή μέτρων της εργαλειοθήκης που σχετίζονται με τις απαιτήσεις ασφάλειας, ιδίως όσον αφορά τις σχετικές διατάξεις δυνάμει των ευρωπαϊκών κανόνων για τις ηλεκτρονικές επικοινωνίες, και εξέταση της προστιθέμενης αξίας πιθανών εκτελεστικών πράξεων για τον

<sup>19</sup> COM(2016)588 της 14ης Σεπτεμβρίου 2016 «5G για την Ευρώπη: σχέδιο δράσης».

αναλυτικό καθορισμό τεχνικών και οργανωτικών μέτρων ασφάλειας, ώστε να συμπληρωθούν οι εθνικοί κανόνες και να ενισχυθούν η αποτελεσματικότητα και η συνοχή των μέτρων ασφάλειας που επιβάλλονται στους φορείς εκμετάλλευσης.

- **Τυποποίηση:** Ανάλυση δράσης για να διατηρηθεί και, όπου χρειάζεται, να αυξηθεί η ευρωπαϊκή συμμετοχή στους αρμόδιους οργανισμούς τυποποίησης, ώστε να επιτευχθούν οι στόχοι ασφάλειας και διαλειτουργικότητας της Ευρώπης. Ειδικότερα, η Επιτροπή, από κοινού με τα κράτη μέλη, θα αξιολογήσει και θα προωθήσει τις τεχνικές προδιαγραφές και τα πρότυπα που θα καταστήσουν εφικτή τη διαλειτουργικότητα μεταξύ προμηθευτών εξοπλισμού 5G σε διαφορετικά τμήματα του δικτύου, όπως, για παράδειγμα, σε παραδοσιακά δίκτυα, ώστε να υλοποιηθεί ένα πραγματικό περιβάλλον πολλαπλών πωλητών, μέσω, για παράδειγμα, ανοικτών και διαλειτουργικών διεπαφών.

- **Πιστοποίηση:** Στήριξη της ανάπτυξης συστημάτων πιστοποίησης 5G για την κάλυψη των αναγκών των δικτύων 5G βάσει του ενωσιακού πλαισίου πιστοποίησης της κυβερνοασφάλειας.

- **Έλεγχος των άμεσων ξένων επενδύσεων (ΑΞΕ):** Στήριξη της εφαρμογής του ενωσιακού πλαισίου ελέγχου με τη χαρτογράφηση της αλυσίδα αξίας των δικτύων 5G, συμπεριλαμβανομένων των ευαίσθητων πάγιων στοιχείων του δικτύου, και την τακτική παρακολούθηση των ΑΞΕ σε ολόκληρη την αλυσίδα αξίας. Σύμφωνα με το χρονοδιάγραμμα ελέγχου των ΑΞΕ (από τον Οκτώβριο του 2020), η Επιτροπή θα εξετάσει ενδελεχώς τις ξένες επενδύσεις στον τομέα των δικτύων 5G σύμφωνα με τις κατευθυντήριες γραμμές που προβλέπονται στον κανονισμό (ΕΕ) 2019/452, λαμβάνοντας υπόψη τη συντονισμένη από την ΕΕ εκτίμηση επικινδυνότητας και την εργαλειοθήκη της ΕΕ.

- **Μέσα εμπορικής άμυνας:** Παρακολούθηση όλων των σχετικών εξελίξεων της αγοράς στην ΕΕ και σε τρίτες χώρες και προστασία των φορέων της ΕΕ στην ευρωπαϊκή αγορά 5G με μέτρα εμπορικής άμυνας που αποσκοπούν στην αντιμετώπιση πιθανών πρακτικών στρέβλωσης του εμπορίου (ντάμπινγκ ή επιδοτήσεων), μεταξύ άλλων, με την κίνηση προκαταρκτικών ερευνών, κατά περίπτωση.

- **Κανόνες ανταγωνισμού:** Παρακολούθηση της λειτουργίας των αγορών προμήθειας υλισμικού και λογισμικού 5G, με σκοπό να εξασφαλίζεται ότι αυτές αποδίδουν ανταγωνιστικά αποτελέσματα, μεταξύ άλλων, σε σχέση με πιθανές καταστάσεις συμβατικού ή τεχνικού «εγκλωβισμού».

- **Προγράμματα ενωσιακής χρηματοδότησης:** Εξασφάλιση ότι η συμμετοχή στα προγράμματα ενωσιακής χρηματοδότησης σε σχετικούς τεχνολογικούς τομείς θα εξαρτάται από την τήρηση απαιτήσεων ασφάλειας, με την πλήρη αξιοποίηση και την περαιτέρω εφαρμογή των όρων ασφάλειας σε προγράμματα E&K, ιδίως στο πλαίσιο του προγράμματος «Ορίζων Ευρώπη», του προγράμματος «Ψηφιακή Ευρώπη» και του μηχανισμού «Συνδέοντας την Ευρώπη 2», καθώς και σε ευρωπαϊκά διαρθρωτικά και επενδυτικά ταμεία και σε άλλα συναφή προγράμματα. Θα πρέπει να εφαρμοστεί παρόμοια προσέγγιση και στα προγράμματα εξωτερικής χρηματοδότησης και τα χρηματοδοτικά μέσα της ΕΕ, για παράδειγμα, όσον αφορά τη χρηματοδότηση που παρέχεται μέσω διεθνών χρηματοδοτικών οργανισμών.

- **Δημόσιες συμβάσεις:** Αξιοποίηση δημόσιων συμβάσεων στον τομέα των δικτύων 5G για την υποστήριξη καθορισμένων στόχων ασφάλειας, διαφοροποίησης των προμηθευτών και μακροπρόθεσμης βιωσιμότητας των δικτύων 5G· ειδικότερα, επιδίωξη να δίνεται η δέουσα

προσοχή στις πτυχές ασφάλειας κατά την ανάθεση δημόσιων συμβάσεων στον τομέα των δικτύων 5G, σύμφωνα με τους κανόνες της ΕΕ για τις δημόσιες συμβάσεις.

- **Αντιμετώπιση συμβάντων και διαχείριση κρίσεων (προσχέδιο) και κυβερνοασκήσεις:** Πλήρης αξιοποίηση της εκπόνησης προσχεδίου της ΕΕ<sup>20</sup> για τη συντονισμένη αντιμετώπιση συμβάντων κυβερνοασφάλειας μεγάλης κλίμακας. Επιπλέον, εξέταση, από κοινού με τον ENISA, του ενδεχόμενου διεξαγωγής κυβερνοασκήσης 5G, μόλις καταστούν ώριμες οι συνθήκες στην αγορά.

Επιπλέον, υπό την ευθύνη του Υπατου Εκπροσώπου της Ένωσης για θέματα εξωτερικής πολιτικής και πολιτικής ασφαλείας και αντιπροέδρου της Επιτροπής, και του Συμβουλίου:

- **Πλαίσιο για κοινή διπλωματική αντίδραση της ΕΕ έναντι κακόβουλων δραστηριοτήτων στον κυβερνοχώρο (εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο)<sup>21</sup>:** Σε περίπτωση κακόβουλων δραστηριοτήτων στον κυβερνοχώρο που απειλούν την ακεραιότητα και την ασφάλεια της ΕΕ, τα κράτη μέλη ενθαρρύνονται να χρησιμοποιούν τα δέοντα μέτρα της κοινής εξωτερικής πολιτικής και πολιτικής ασφαλείας που περιλαμβάνονται στην εργαλειοθήκη της ΕΕ για τη διπλωματία στον κυβερνοχώρο (συμπεριλαμβανομένων, εφόσον απαιτείται, περιοριστικών μέτρων), ώστε να ενθαρρύνουν τη συνεργασία, να διευκολύνουν τον μετριασμό των απειλών και να επηρεάζουν τη συμπεριφορά εν δυνάμει δραστών.

Επιπλέον, ορισμένα προγράμματα θα συμβάλουν στην επίτευξη των στόχων αποφυγής ή περιορισμού του κινδύνου μακροπρόθεσμης εξάρτησης, με την προώθηση της διαφοροποιημένης και βιώσιμης αγοράς δικτύων 5G και, μεταξύ άλλων, με τη διατήρηση των ικανοτήτων της ΕΕ στην αλυσίδα αξίας των δικτύων 5G και τις επενδύσεις στην καινοτομία, σύμφωνα με τις διεθνείς υποχρεώσεις της ΕΕ.

#### **Προώθηση της καινοτομίας και επένδυση στην κυβερνοασφάλεια και στις τεχνολογίες υποδομών δικτύου:**

- **Προγράμματα** ενωσιακής χρηματοδότησης: Αύξηση των επενδύσεων στους τομείς της έρευνας, της καινοτομίας και της εγκατάστασης τεχνολογιών δικτύου και των συναφών δομικών στοιχείων στα οποία αυτές βασίζονται. Η Επιτροπή πρότείνει σχεδόν 3 δισεκατομμύρια ευρώ για επενδύσεις σε τεχνολογίες κυβερνοασφάλειας στο πλαίσιο του επόμενου προϋπολογισμού της ΕΕ για την περίοδο 2021-27. Στις εν λόγω επενδύσεις περιλαμβάνονται η έρευνα και η καινοτομία στο πλαίσιο του προγράμματος «Ορίζων Ευρώπη» και η στήριξη των ικανοτήτων κυβερνοασφάλειας στο πλαίσιο του προγράμματος «Ψηφιακή Ευρώπη». Το πρόγραμμα InvestEU μπορεί επίσης να παράσχει χρηματοδοτική στήριξη της έρευνας και της ανάπτυξης στον τομέα των δικτύων 5G, καθώς και στήριξη της εγκατάστασής τους.

<sup>20</sup> Σύσταση της Επιτροπής για τη συντονισμένη αντιμετώπιση περιστατικών και κρίσεων μεγάλης κλίμακας στον κυβερνοχώρο (ΕΕ 2017/1584).

<sup>21</sup> Συμπεράσματα του Συμβουλίου της 20ής Νοεμβρίου 2017, 9916/17.

Επιπλέον, στο πλαίσιο του επόμενου προγράμματος «Ορίζων Ευρώπη»<sup>22</sup>, η Επιτροπή πρότεινε τη δημιουργία θεσμοθετημένης εταιρικής σχέσης της ΕΕ στον τομέα του Διαδικτύου επόμενης γενιάς (NGI)/ των δικτύων 6G («έξυπνα δίκτυα και υπηρεσίες»), σε συνεργασία με τον κλάδο και σε συντονισμό με τα κράτη μέλη, με σκοπό την ολοκλήρωση της εγκατάστασης των δικτύων 5G και κυρίως **την προετοιμασία για τα δίκτυα 6G**, την επόμενη γενιά τεχνολογιών κινητών επικοινωνιών. Περισσότερα από 2,5 δισεκατομμύρια ευρώ επενδύσεων της ΕΕ προτάθηκαν από τον προϋπολογισμό της ΕΕ (2021-27), σε συνδυασμό με τουλάχιστον 7,5 δισεκατομμύρια ευρώ ιδιωτικών επενδύσεων στην εν λόγω πρωτοβουλία.

- **Ανάπτυξη και εγκατάσταση σε επίπεδο κλάδου:** Αξιολόγηση πιθανών ελλείψεων ή αστοχιών της αγοράς σε ολόκληρη την αλυσίδα αξίας στον τομέα των δικτύων 5G, οι οποίες θα δικαιολογούσαν στοχευμένες παρεμβάσεις στο πλαίσιο του επόμενου μακροπρόθεσμου προϋπολογισμού ή ενδεχόμενου ΣΕΚΕΕ (σημαντικό έργο κοινού ευρωπαϊκού ενδιαφέροντος) για την κυβερνοασφάλεια, σύμφωνα με τις προτάσεις του φόρουμ υψηλού επιπέδου ΣΕΚΕΕ. Η απόφαση για τον σχεδιασμό και τη δημιουργία ΣΕΚΕΕ εναπόκειται στα κράτη μέλη και στις επιχειρήσεις. Οι κανόνες της ΕΕ παρέχουν ευνοϊκό πλαίσιο και η Επιτροπή είναι πρόθυμη να διευκολύνει τις αναγκαίες επαφές και να παράσχει καθοδήγηση.

---

<sup>22</sup> Χρηματοδοτικοί πόροι μπορούν επίσης να αντληθούν από τον μηχανισμό «Συνδέοντας την Ευρώπη 2.0» και το πρόγραμμα «Ψηφιακή Ευρώπη».

## 6. Συμπέρασμα

Τα δίκτυα 5G αναμένεται να προσφέρουν πληθώρα ευκαιριών στους πολίτες, την κοινωνία και την οικονομία της Ευρώπης. Επομένως, είναι ουσιαστικής σημασίας να εξασφαλιστούν η κυβερνοασφάλεια και η ανθεκτικότητα των δικτύων 5G. Ταυτόχρονα, οι απειλές κατά της κυβερνοασφάλειας (συμπεριλαμβανομένου του κινδύνου παρεμβολών από τρίτες χώρες ή παράγοντες που υποστηρίζονται από αυτές) αποτελούν μια εξελισσόμενη πρόκληση, η οποία αποκτά ολοένα και μεγαλύτερη σημασία, παράλληλα με την αυξημένη εξάρτηση από την τεχνολογία και τα δεδομένα. Εάν παραμεληθεί η κυβερνοασφάλεια, θα υπονομευθεί η εμπιστοσύνη στην ανάπτυξη της ψηφιακής οικονομίας και κοινωνίας και η ΕΕ δεν θα μπορέσει να αποκομίσει τα οφέλη της στο σύνολό τους. Για αυτόν τον λόγο, απαιτείται αντιστοίχως εξελισσόμενη και ενισχυμένη αντίδραση.

Η συντονισμένη και συνεπής προσέγγιση ως προς την κυβερνοασφάλεια στην ΕΕ για τις τεχνολογίες και τα δίκτυα κρίσιμης σημασίας έχει θεμελιώδη σημασία, προκειμένου η ΕΕ να κατοχυρώσει την τεχνολογική της αυτοδυναμία, να διατηρήσει και να αναπτύξει τις ικανότητές της στον κλάδο. Η Επιτροπή θα στηρίζει πλήρως την εφαρμογή της προσέγγισης της ΕΕ για την κυβερνοασφάλεια των δικτύων 5G και, παράλληλα, θα διασφαλίσει ότι οι αγορές της ΕΕ θα παραμείνουν ανοικτές σε προϊόντα και υπηρεσίες που τηρούν τις εξελισσόμενες απαιτήσεις κυβερνοασφάλειας και εμπιστοσύνης.

Για τον σκοπό αυτόν, είναι σημαντικό να παραμείνει ισχυρή η δέσμευση όλων των ενδιαφερόμενων μερών όσον αφορά την ασφάλεια των δικτύων 5G και απαιτείται συνεχής συνεργασία μεταξύ των κρατών μελών, της Επιτροπής και του ENISA.

Ως άμεσο επόμενο βήμα, όπως περιγράφεται ανωτέρω, η Επιτροπή καλεί τα κράτη μέλη να αναλάβουν ταχεία δράση για την αποτελεσματική και αντικειμενική εφαρμογή των μέτρων που συμφωνήθηκαν στο πλαίσιο της εργαλειοθήκης, και να συνεχίσουν να συνεργάζονται, με τη στήριξη της Επιτροπής και του ENISA, ώστε να εξασφαλίζεται συντονισμός σε επίπεδο ΕΕ. Παράλληλα, η Επιτροπή θα δρομολογήσει όλες τις απαραίτητες δράσεις που εμπίπτουν στην αρμοδιότητά της για να στηρίζει την εφαρμογή της εργαλειοθήκης από τα κράτη μέλη και να ενισχύσει τον αντίκτυπό της.

Προσάρτημα: Κατηγορίες κινδύνου (πηγή: συντονισμένη από την ΕΕ εκτίμηση επικινδυνότητας).

	<b>Κατηγορίες κινδύνου</b>
<b>Σενάρια κινδύνου που σχετίζονται με ανεπαρκή μέτρα ασφάλειας</b>	<i>K1: Σφάλματα ρύθμισης παραμέτρων δικτύου</i>
	<i>K2: Έλλειψη ελέγχων πρόσβασης</i>
<b>Σενάρια κινδύνου που σχετίζονται με την αλυσίδα εφοδιασμού 5G</b>	<i>K3: Χαμηλή ποιότητα προϊόντος</i>
	<i>K4: Εξάρτηση από οποιονδήποτε μεμονωμένο προμηθευτή εντός επιμέρους δικτύων ή έλλειψη διαφοροποίησης σε εθνικό επίπεδο</i>
<b>Σενάρια κινδύνου που σχετίζονται με τον τρόπο δράσης των κύριων παραγόντων απειλής</b>	<i>K5: Κρατική παρέμβαση μέσω της αλυσίδας εφοδιασμού 5G</i>
	<i>K6: Εκμετάλλευση δικτύων 5G από εγκληματική οργάνωση ή ομάδα οργανωμένου εγκλήματος με στόχο τελικούς χρήστες</i>
<b>Σενάρια κινδύνου που σχετίζονται με τις αλληλεξαρτήσεις μεταξύ δικτύων 5G και άλλων κρίσιμων συστημάτων</b>	<i>K7: Σημαντική διαταραχή υποδομών ή υπηρεσιών κρίσιμης σημασίας</i>
	<i>K8: Γενικευμένη βλάβη δικτύων λόγω διακοπής της παροχής ηλεκτρικής ενέργειας ή άλλων υποστηρικτικών συστημάτων</i>
<b>Σενάρια κινδύνου που σχετίζονται με τις συσκευές τελικών χρηστών</b>	<i>K9: Εκμετάλλευση του διαδικτύου των πραγμάτων (IoT)</i>