ΕΥΡΩΠΑΪΚΗ
ΕΠΙΤΡΟΠΗ

Βρυξέλλες, 12.9.2018
SWD(2018) 404 final

ΕΓΓΡΑΦΟ ΕΡΓΑΣΙΑΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

ΠΕΡΙΛΗΨΗ ΤΗΣ ΕΚΤΙΜΗΣΗΣ ΕΠΙΠΤΩΣΕΩΝ

που συνοδεύει το έγγραφο

ΠΡΟΤΑΣΗ ΚΑΝΟΝΙΣΜΟΥ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ

για τη σύσταση του ευρωπαϊκού βιομηχανικού, τεχνολογικού και ερευνητικού κέντρου ικανοτήτων στον τομέα της κυβερνοασφάλειας και του δικτύου εθνικών κέντρων συντονισμού

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 403 final}

Δελτίο συνοπτικής παρουσίασης

Εκτίμηση επιπτώσεων της πρότασης σχετικά με τη σύσταση δικτύου κέντρων ικανοτήτων και ευρωπαϊκού κέντρου έρευνας και ικανοτήτων στον τομέα της κυβερνοασφάλειας

Α. Ανάγκη ανάληψης δράσης

Γιατί; Ποιο είναι το πρόβλημα;

Σήμερα οι τεχνολογικές και βιομηχανικές ικανότητες στην ΕΕ εξακολουθούν να μην επαρκούν ώστε η ΕΕ να μπορεί να προστατεύει αυτόνομα την οικονομία της και τις οικείες υποδομές κρίσιμης σημασίας και να αποκτήσει ηγετικό ρόλο σε παγκόσμιο επίπεδο στον τομέα της κυβερνοασφάλειας. Στόχος της παρούσας πρωτοβουλίας είναι να συμβάλλει στην αντιμετώπιση των ακόλουθων προβλημάτων και των σχετιζόμενων καθοριστικών παραγόντων της εν λόγω κατάστασης:

Πρόβλημα 1: Το ανεπαρκές επίπεδο στρατηγικού και βιώσιμου συντονισμού και συνεργασίας μεταξύ των επιχειρήσεων, των ερευνητικών κοινοτήτων στον τομέα της κυβερνοασφάλειας και των κυβερνήσεων δεν επιτρέπει την προστασία της οικονομίας, της κοινωνίας και της δημοκρατίας με ευρωπαϊκές λύσεις αιχμής στον τομέα της κυβερνοασφάλειας.

Πρόβλημα 2: Οι επενδύσεις πραγματοποιούνται σε μικρή κλίμακα και η πρόσβαση στην τεχνογνωσία, τις δεξιότητες και τις εγκαταστάσεις κυβερνοασφάλειας σε ολόκληρη την ΕΕ είναι περιορισμένη.

Πρόβλημα 3: Ελάχιστα αποτελέσματα ευρωπαϊκής έρευνας και καινοτομίας στον τομέα της κυβερνοασφάλειας μετατρέπονται σε εμπορικά αξιοποιήσιμες λύσεις και εξαπλώνονται σε ολόκληρη την οικονομία.

Οι παράγοντες που προκαλούν τα εν λόγω προβλήματα είναι διάφοροι, για παράδειγμα, ανεπαρκής εμπιστοσύνη μεταξύ των διαφόρων φορέων της αγοράς κυβερνοασφάλειας, εγγενείς περιορισμοί των υφιστάμενων μηχανισμών συνεργασίας και συγκέντρωσης χρηματοδοτικών πόρων, έλλειψη πλαισίου για την από κοινού σύναψη συμβάσεων στην περίπτωση υποδομών και προϊόντων/λύσεων κυβερνοασφάλειας με υψηλό κόστος, καθώς και ανεπαρκής αξιοποίηση των μηχανισμών ώθησης και έλξης της αγοράς.

Τι αναμένεται να επιτευχθεί με την παρούσα πρωτοβουλία;

Η πρωτοβουλία στοχεύει να διασφαλίσει ότι η ΕΕ θα διατηρήσει και θα αναπτύξει τις απαραίτητες (τεχνολογικές και βιομηχανικές) ικανότητες, ώστε να μπορεί να προστατεύει αυτόνομα την ψηφιακή της οικονομία, την κοινωνία και τη δημοκρατία, και ότι τα κράτη μέλη θα επωφεληθούν από τις πλέον προηγμένες λύσεις κυβερνοασφάλειας και ικανότητες κυβερνοάμυνας. Η πρωτοβουλία στοχεύει επίσης να αυξήσει την ανταγωνιστικότητα των εταιρειών κυβερνοασφάλειας της ΕΕ σε παγκόσμιο επίπεδο και να εξασφαλίσει ότι οι ευρωπαϊκές επιχειρήσεις από διάφορους κλάδους έχουν πρόσβαση στις ικανότητες και τους πόρους που απαιτούνται για να μετατρέψουν την κυβερνοασφάλεια σε ανταγωνιστικό τους πλεονέκτημα. Οι εν λόγω στόχοι θα πρέπει να επιτευχθούν με την ανάπτυξη αποτελεσματικών μηχανισμών μακροπρόθεσμης στρατηγικής συνεργασίας όλων των σχετικών φορέων (δημόσιες αρχές, επιχειρήσεις, ερευνητική κοινότητα από τον μη στρατιωτικό αλλά και από τον αμυντικό τομέα), τη συγκέντρωση γνώσεων και πόρων για την παροχή ικανοτήτων και υποδομών αιχμής, την προώθηση της ευρείας εξάπλωσης ευρωπαϊκών προϊόντων και λύσεων κυβερνοασφάλειας σε ολόκληρη την οικονομία και τον δημόσιο τομέα, τη στήριξη νεοσύστατων επιχειρήσεων και ΜΜΕ κυβερνοασφάλειας, καθώς και με την κάλυψη της έλλειψης δεξιοτήτων στον τομέα της κυβερνοασφάλειας.

Ποια είναι η προστιθέμενη αξία της δράσης σε επίπεδο ΕΕ;

Η πρωτοβουλία αναμένεται ότι θα αποφέρει προστιθέμενη αξία στις υφιστάμενες προσπάθειες που καταβάλλονται σε εθνικό επίπεδο συμβάλλοντας στη δημιουργία ενός διασυνδεδεμένου και πανευρωπαϊκού βιομηχανικού και ερευνητικού οικοσυστήματος κυβερνοασφάλειας. Η πρωτοβουλία αναμένεται ότι θα ενθαρρύνει την καλύτερη συνεργασία μεταξύ των σχετικών ενδιαφερόμενων φορέων (μεταξύ άλλων, του μη στρατιωτικού και του αμυντικού τομέα κυβερνοασφάλειας), με στόχο τη βέλτιστη αξιοποίηση των υφιστάμενων πόρων και της υφιστάμενης εμπειρογνωσίας που βρίσκεται διάσπαρτη σε ολόκληρη την Ευρώπη. Η πρωτοβουλία αναμένεται επίσης ότι θα βοηθήσει την ΕΕ και τα κράτη μέλη να υιοθετήσουν μια προληπτική, μακρόπνοη και στρατηγική προοπτική ως προς τη βιομηχανική πολιτική κυβερνοασφάλειας η οποία δεν θα περιορίζεται αποκλειστικά στην έρευνα και την ανάπτυξη. Αυτή η προσέγγιση αναμένεται ότι θα συμβάλει όχι μόνο στην εξεύρεση πρωτοποριακών λύσεων στις προκλήσεις κυβερνοασφάλειας που αντιμετωπίζουν ο ιδιωτικός και ο δημόσιος τομέας, αλλά και στην

αποτελεσματική εξάπλωση των εν λόγω λύσεων. Επιπλέον, με αυτή την προσέγγιση οι σχετικές ερευνητικές και βιομηχανικές κοινότητες, καθώς και οι δημόσιες αρχές θα μπορέσουν να αποκτήσουν πρόσβαση σε βασικές ικανότητες, όπως εγκαταστάσεις διεξαγωγής δοκιμών και πειραμάτων, οι οποίες συχνά βρίσκονται πέραν των δυνατοτήτων των μεμονωμένων κρατών μελών λόγω ανεπαρκών χρηματοδοτικών και ανθρώπινων πόρων. Αυτή η προσέγγιση θα συμβάλει επίσης στην κάλυψη της έλλειψης δεξιοτήτων και στην αποφυγή της «διαρροής εγκεφάλων», εξασφαλίζοντας ότι τα καλύτερα ταλέντα έχουν πρόσβαση σε ευρωπαϊκά έργα μεγάλης κλίμακας και προσφέροντας, ως εκ τούτου, ενδιαφέρουσες επαγγελματικές προκλήσεις. Όλα τα προαναφερόμενα θεωρούνται επίσης απαραίτητα για την αναγνώριση της Ευρώπης σε παγκόσμιο επίπεδο ως ηγετικού παράγοντα στον τομέα της κυβερνοασφάλειας.

Β. Λύσεις

Ποιες νομοθετικές και μη νομοθετικές επιλογές πολιτικής έχουν εξεταστεί; Υπάρχει προτιμώμενη επιλογή ή όχι; Γιατί;

Εξετάστηκαν διάφορες νομοθετικές και μη νομοθετικές επιλογές πολιτικής. Οι ακόλουθες επιλογές αποτέλεσαν αντικείμενο εις βάθος αξιολόγησης:

1. **Βασικό σενάριο** - Συνεργατική επιλογή: συνέχιση της τρέχουσας προσέγγισης για την ανάπτυξη βιομηχανικών και τεχνολογικών ικανοτήτων στον τομέα της κυβερνοασφάλειας στην ΕΕ, μέσω της υποστήριξης της έρευνας και της καινοτομίας και των οικείων μηχανισμών συνεργασίας στο πλαίσιο του προγράμματος «Ορίζων Ευρώπη».
2. **Επιλογή 1:** Δίκτυο ικανοτήτων στον τομέα της κυβερνοασφάλειας με ένα ευρωπαϊκό βιομηχανικό, τεχνολογικό και ερευνητικό κέντρο ικανοτήτων στον τομέα της κυβερνοασφάλειας, εξουσιοδοτημένο να λαμβάνει μέτρα προς υποστήριξη βιομηχανικών τεχνολογιών, καθώς και στον τομέα της έρευνας και της καινοτομίας.
3. **Επιλογή 2:** Δίκτυο ικανοτήτων στον τομέα της κυβερνοασφάλειας με ένα ευρωπαϊκό κέντρο έρευνας και ικανοτήτων στον τομέα της κυβερνοασφάλειας, περιοριζόμενο αποκλειστικά σε δραστηριότητες έρευνας και καινοτομίας.

Οι επιλογές που απορρίφθηκαν σε πρώιμο στάδιο συμπεριλάμβαναν 1) την επιλογή να μην αναληφθεί καμία δράση, 2) το δίκτυο που αποτελείται μόνο από υφιστάμενα κέντρα ικανοτήτων, και 3) τη χρήση υφιστάμενου οργανισμού (ENISA, REA, ή INEA).

Λαμβανομένων υπόψη της συνολικής δέσμευσης που έχει ήδη αναλάβει η Επιτροπή για την παρούσα πρωτοβουλία και του σημαντικού ρόλου που πρέπει να διαδραματίσουν τα κράτη μέλη, η κύρια διάκριση μεταξύ των δύο επιλογών πολιτικής που αποτέλεσαν αντικείμενο εις βάθος ανάλυσης έγκειται στο πεδίο εφαρμογής τους όπως αποτυπώνεται στην οικεία νομική βάση: μια οντότητα που βασίζεται αποκλειστικά στο άρθρο 187 της ΣΛΕΕ (επιλογή 2) περιορίζει την πρωτοβουλία στον τομέα της έρευνας και της καινοτομίας και συνήθως προϋποθέτει χρηματοδοτική συνεισφορά από ιδιωτικούς φορείς. Αντιθέτως, μια οντότητα που βασίζεται σε διπλή νομική βάση, ήτοι το άρθρο 187 της ΣΛΕΕ και το άρθρο 173 της ΣΛΕΕ (επιλογή 1), συνεπάγεται ευρύτερη εντολή που καλύπτει επίσης, μεταξύ άλλων, την εξάπλωση, τη βιομηχανική στήριξη και τη δημιουργία ισχυρότερων συνεργειών με την κυβερνοάμυνα. Θα ενισχύσει επίσης τον ρόλο των κρατών μελών όσον αφορά τόσο τον ρόλο που επιτελούν στη διακυβέρνηση όσο και τον ρόλο που επιτελούν ως πιθανοί αγοραστές τεχνολογίας κυβερνοασφάλειας.

Από την ανάλυση προέκυψε ότι η επιλογή 1 είναι η πλέον κατάλληλη για την επίτευξη των στόχων της πρωτοβουλίας, ενώ προσφέρει τον υψηλότερο οικονομικό, κοινωνικό και περιβαλλοντικό αντίκτυπο και διαφυλάσσει τα συμφέροντα της Ένωσης. Τα κύρια επιχειρήματα υπέρ της επιλογής αυτής συμπεριλάμβαναν: την ευελιξία να επιτρέπονται διαφορετικά μοντέλα συνεργασίας με την κοινότητα και το δίκτυο κέντρων ικανοτήτων για τη βέλτιστη αξιοποίηση των υφιστάμενων γνώσεων και πόρων· την ικανότητα να αναπτυχθεί συνεργασία μεταξύ των ενδιαφερόμενων μερών του δημόσιου και του ιδιωτικού τομέα από όλους τους συναφείς τομείς, συμπεριλαμβανομένης της άμυνας· και την ικανότητα δημιουργίας μίας πραγματικής βιομηχανικής πολιτικής κυβερνοασφάλειας με την υποστήριξη δραστηριοτήτων που αφορούν όχι μόνον την έρευνα και την ανάπτυξη, αλλά και τη διείσδυση στην αγορά. Τέλος, η επιλογή 1, αφενός, καθιστά εφικτή την αύξηση της συνεκτικότητας, επειδή λειτουργεί ως μηχανισμός υλοποίησης της σχετικής με την κυβερνοασφάλεια χρηματοδότησης που προέρχεται από το πρόγραμμα «Ψηφιακή Ευρώπη» και το πρόγραμμα «Ορίζων Ευρώπη» και, αφετέρου, ενισχύει τις συνέργειες μεταξύ της μη στρατιωτικής και της αμυντικής διάστασης της κυβερνοασφάλειας όσον αφορά το Ευρωπαϊκό Ταμείο Άμυνας.

Ποιος υποστηρίζει την κάθε επιλογή;

Σύμφωνα με τα αποτελέσματα της διαβούλευσης και των διαδικασιών συλλογής αποδεικτικών στοιχείων, διατυπώνεται σαφώς η απαίτηση ότι τόσο οι βιομηχανικές όσο και οι ερευνητικές κοινότητες θα πρέπει να διαθέτουν έναν μηχανισμό που δίνει στην ΕΕ τη δυνατότητα να έχει μια συνεκτική βιομηχανική πολιτική κυβερνοασφάλειας η οποία δεν θα περιορίζεται αποκλειστικά σε δραστηριότητες έρευνας και ανάπτυξης, διότι μόνο με αυτόν τον τρόπο θα μπορέσει η Ευρώπη να καταστεί ηγετική δύναμη σε παγκόσμιο επίπεδο στον τομέα της κυβερνοασφάλειας. Ταυτόχρονα, τα ενδιαφερόμενα μέρη επισήμαναν ότι το καταλυτικό στοιχείο για την επιτυχία θα είναι ο σαφώς καθορισμένος ρόλος του κέντρου ως προς τη στήριξη και τη διευκόλυνση των προσπαθειών του δικτύου και των σχετικών κοινοτήτων, καθώς και η συμμετοχική και συνεργατική προσέγγιση του δικτύου ώστε να μην δημιουργούνται νέα στεγανά. Η δομή θα πρέπει επίσης να είναι ευέλικτη ώστε να μπορεί να προσαρμόζεται εύκολα, δεδομένου ότι η κυβερνοασφάλεια αποτελεί ένα περιβάλλον με ραγδαίους ρυθμούς. Καθόλη τη διάρκεια της διαδικασίας, τα κράτη μέλη επισήμαναν την ανάγκη να μην εισάγονται διακρίσεις έναντι κανενός κράτους μέλους και κανενός οικείου υφιστάμενου κέντρου αριστείας και ικανοτήτων, καθώς και να δοθεί ιδιαίτερη προσοχή στη συμπληρωματικότητα των δράσεων. Ιδίως όσον αφορά το κέντρο, τα κράτη μέλη τόνισαν τη σημασία του συντονιστικού του ρόλου στην υποστήριξη του δικτύου. Επομένως, η πρωτοβουλία της Επιτροπής θα πρέπει να εξασφαλίζει τη δέουσα ισορροπία μεταξύ των δομών διακυβέρνησης και υλοποίησης και να αποτυπώνει αυτή την ισορροπία στις δομές διακυβέρνησης και υλοποίησης, ώστε να διασφαλίζεται αποτελεσματικός ευρωπαϊκός συντονισμός και, παράλληλα, να λαμβάνονται υπόψη οι εξελίξεις σε εθνικό επίπεδο.

Γ. Επιπτώσεις της προτιμώμενης επιλογής

Ποια είναι τα οφέλη της προτιμώμενης επιλογής (ειδάλλως, των κυριότερων επιλογών);

Η προτιμώμενη επιλογή θα επιτρέπει στις δημόσιες αρχές και τις επιχειρήσεις σε όλα τα κράτη μέλη να προλαμβάνουν και να αντιμετωπίζουν αποτελεσματικότερα τις κυβερνοαπειλές με την προσφορά και τη διάθεση ασφαλέστερων προϊόντων και λύσεων. Αυτό είναι ιδιαίτερα σημαντικό για την προστασία της πρόσβασης σε υπηρεσίες ζωτικής σημασίας (π.χ. μεταφορές, υγεία, τραπεζικές και χρηματοοικονομικές υπηρεσίες). Αναμένονται επίσης θετικές επιπτώσεις στην ανταγωνιστικότητα και τις ΜΜΕ της ΕΕ, δεδομένου ότι η επιλογή αυτή προϋποθέτει τη δημιουργία μηχανισμού μέσω του οποίου θα αναπτυχθούν οι βιομηχανικές ικανότητες κυβερνοασφάλειας των κρατών μελών και της Ένωσης και θα μετατραπεί αποτελεσματικά η ευρωπαϊκή επιστημονική αριστεία σε εμπορικά αξιοποιήσιμες λύσεις που μπορούν να εξαπλωθούν σε ολόκληρη την οικονομία. Η εν λόγω επιλογή καθιστά εφικτή τη συγκέντρωση πόρων για την πραγματοποίηση επενδύσεων στις απαραίτητες ικανότητες σε επίπεδο κρατών μελών, την ανάπτυξη κοινών ευρωπαϊκών περιουσιακών στοιχείων και την επίτευξη οικονομιών κλίμακας. Αυτό αναμένεται ότι θα οδηγήσει σε αυξημένη πρόσβαση των ΜΜΕ, των επιχειρήσεων και των ερευνητών στις εν λόγω εγκαταστάσεις, γεγονός που, στη συνέχεια, θα τονώσει την καινοτομία και θα επιταχύνει τις διαδικασίες ανάπτυξης. Με αυτόν τον τρόπο, θα μειωθούν επίσης οι δαπάνες για ορισμένες επιχειρήσεις από την πλευρά της ζήτησης, γεγονός που θα τις βοηθήσει να μετατρέψουν την κυβερνοασφάλεια σε ανταγωνιστικό τους πλεονέκτημα. Η προτιμώμενη επιλογή επιτρέπει την αξιοποίηση των ευκαιριών της αγοράς διπλής χρήσης, καθιστώντας εφικτή τη συνεργασία αμυντικών και μη στρατιωτικών κοινοτήτων επί κοινών προκλήσεων. Είναι επίσης πιθανό να αποφέρει προστιθέμενη αξία στις εθνικές προσπάθειες που καταβάλλονται για την αντιμετώπιση της έλλειψης δεξιοτήτων στον τομέα της κυβερνοασφάλειας. Σε επίπεδο ΕΕ, η εν λόγω επιλογή καθιστά εφικτή τη βελτίωση της συνεκτικότητας και των συνεργειών μεταξύ διαφορετικών μηχανισμών χρηματοδότησης.

Επιπλέον, θα μπορούσε να έχει έμμεση θετική επίπτωση στο περιβάλλον, εάν αναπτυχθούν ειδικές λύσεις κυβερνοασφάλειας για τομείς με δυνητικά τεράστιο περιβαλλοντικό αντίκτυπο (π.χ. μονάδες παραγωγής πυρηνικής ενέργειας) που θα τους βοηθήσουν να αποφύγουν δυνητικά καταστροφικές συνέπειες κυβερνοεπιθέσεων σε αντίστοιχες υποδομές.

Ποιο είναι το κόστος της προτιμώμενης επιλογής (ειδάλλως, των κυριότερων επιλογών);

Το σχετιζόμενο με την προτιμώμενη επιλογή κόστος αφορά κυρίως τις δαπάνες λειτουργίας του κέντρου και των εθνικών κέντρων συντονισμού. Οι δαπάνες που σχετίζονται με την υλοποίηση διαφορετικών χρηματοδοτικών προγραμμάτων (πρόγραμμα «Ψηφιακή Ευρώπη» και πρόγραμμα «Ορίζων Ευρώπη») υπόκεινται σε επιμέρους εκτιμήσεις επιπτώσεων.

Πώς θα επηρεαστούν οι μεγάλες, οι μικρομεσαίες και οι πολύ μικρές επιχειρήσεις;

Μεταξύ των πλέον επηρεαζόμενων ομάδων ενδιαφερόμενων μερών θα είναι οι ευρωπαϊκές εταιρείες, τόσο από την πλευρά της ζήτησης κυβερνοασφάλειας όσο και από την πλευρά της προσφοράς κυβερνοασφάλειας, συμπεριλαμβανομένων των ΜΜΕ και των πολύ μικρών επιχειρήσεων που δραστηριοποιούνται στον τομέα της κυβερνοασφάλειας. Η σύσταση του κέντρου ικανοτήτων και του δικτύου δεν συνεπάγεται την επιβολή κανονιστικών υποχρεώσεων σε αυτές, δημιουργεί δε νέες ευκαιρίες για μείωση των δαπανών σχεδιασμού νέων προϊόντων και τις βοηθά να αποκτούν ευκολότερη πρόσβαση στην κοινότητα των επενδυτών, όπως επίσης και να προσελκύουν την αναγκαία χρηματοδότηση για την εξάπλωση εμπορικά αξιοποιήσιμων λύσεων. Στην περίπτωση των ΜΜΕ και των πολύ μικρών επιχειρήσεων, η πρόσβαση σε χρηματοδοτούμενες από δημόσιους πόρους εγκαταστάσεις διεξαγωγής δοκιμών και πειραμάτων έχει ακόμη μεγαλύτερη σημασία, διότι οι εν λόγω επιχειρήσεις δεν διαθέτουν τους πόρους που απαιτούνται για να αγοράσουν τις απαραίτητες υποδομές ή να ταξιδέψουν εκτός της αγοράς τους (συχνά δε εκτός της ΕΕ), προκειμένου να βρουν τις απαραίτητες υποδομές. Επιπλέον, προσδοκάται ότι με την παρούσα πρωτοβουλία θα ανοίξουν νέες αγορές για τις ευρωπαϊκές ΜΜΕ και τις πολύ μικρές επιχειρήσεις που δραστηριοποιούνται στον τομέα της κυβερνοασφάλειας. Ο επιλεχθείς μηχανισμός θα διασφαλίζει επίσης τον συντονισμό μεταξύ της έρευνας και των επιχειρήσεων και, ως εκ τούτου, θα κατευθύνει τις ερευνητικές προσπάθειες προς συγκεκριμένες βιομηχανικές ανάγκες. Η παροχή εμπειρογνωσίας και εργαλείων αιχμής στον τομέα της κυβερνοασφάλειας θα βοηθήσει έμμεσα τους οικονομικούς φορείς να συμμορφωθούν με την οδηγία για την ασφάλεια δικτύων και πληροφοριών.

Θα υπάρξουν σημαντικές επιπτώσεις στους εθνικούς προϋπολογισμούς και στις εθνικές διοικητικές αρχές;

Η πρωτοβουλία θα δώσει τη δυνατότητα στα κράτη μέλη να συντονίσουν τις επενδύσεις σε απαραίτητες υποδομές κυβερνοασφάλειας σε εθνικό και ευρωπαϊκό επίπεδο. Ο μηχανισμός θα καταστήσει εφικτή τη συγκέντρωση πόρων για εργαλεία και υποδομές που διαφορετικά θα είχαν υψηλότερο κόστος ή δεν θα ήταν οικονομικά προσιτά για τα μεμονωμένα κράτη μέλη. Με αυτή την προσέγγιση θα επιτευχθούν οικονομίες κλίμακας και εξορθολογισμός. Η χρηματοδοτική συνεισφορά των κρατών μελών στο κέντρο ικανοτήτων και τις σχετικές δράσεις θα πρέπει να είναι ανάλογη προς τη χρηματοδοτική συνεισφορά της Ένωσης.

Θα υπάρξουν άλλες σημαντικές επιπτώσεις;

Ναι, η πρωτοβουλία έχει σαφείς θετικές επιπτώσεις, διότι αναμένεται ότι θα αυξήσει σημαντικά τις ικανότητες των κρατών μελών να προστατεύουν αυτόνομα την οικονομία τους και, μεταξύ άλλων, τομείς κρίσιμης σημασίας, και θα αυξήσει την ανταγωνιστικότητα των ευρωπαϊκών επιχειρήσεων και κλάδων που δραστηριοποιούνται στον τομέα της κυβερνοασφάλειας σε διάφορους τομείς, ενώ οι εν λόγω επιχειρήσεις και κλάδοι θα μπορούν ακολούθως να προστατεύουν δεόντως τα υφιστάμενα περιουσιακά τους στοιχεία, να σχεδιάζουν ασφαλή καινοτόμα προϊόντα και, ταυτόχρονα, να περιορίζουν τις σχετιζόμενες με την ασφάλεια δαπάνες Ε&Α. Απώτερος στόχος είναι να καταστεί η ΕΕ ηγετική δύναμη στις ψηφιακές τεχνολογίες και τις τεχνολογίες κυβερνοασφάλειας επόμενης γενιάς.

Δ. Παρακολούθηση

Πότε θα επανεξεταστεί η πολιτική;

Στο νομικό μέσο θα περιλαμβάνεται ρητή ρήτρα παρακολούθησης των βασικών δεικτών επιδόσεων (ΒΔΕ), καθώς και ρήτρα αξιολόγησης και αναθεώρησης, βάσει την οποίας η Επιτροπή θα διενεργήσει ενδιάμεση αξιολόγηση, προκειμένου να εκτιμήσει τις επιπτώσεις του μέσου και την προστιθέμενη αξία του. Η Επιτροπή θα υποβάλει ακολούθως έκθεση στο Ευρωπαϊκό Κοινοβούλιο και στο Συμβούλιο. Έπειτα από αυτή την αξιολόγηση, η Επιτροπή ενδέχεται να προτείνει αναθεώρηση και παράταση της εντολής του κέντρου ικανοτήτων και του δικτύου.