Ερώτηση με αίτημα γραπτής απάντησης E-005820/2020
προς την Επιτροπή
Άρθρο 138 του Κανονισμού
Emmanouil Fragkos (ECR)

Θέμα: Αντιμετώπιση κυβερνοεπιθέσεων της Τουρκίας και του Ιράν

Ομάδες Τούρκων χάκερς έχουν πλήξει τις ιστοσελίδες του ελληνικού Κοινοβουλίου, των υπουργείων Εξωτερικών, Οικονομικών, της Αστυνομίας, της Πυροσβεστικής, της ΕΥΠ, και αρκετών δημόσιων οργανισμών, ενώ πρόσφατα «κατέβηκε» προσωρινά ακόμα και η ιστοσελίδα του Γενικού Επιτελείου Στρατού. Δραστηριότητα παρατηρείται από ομάδες όπως η «Anka Neferler», η «Ayyıldız Tim» και η «APT35».

Ενδεχομένως λόγω έλλειψης εργαλείων, τεχνογνωσίας και πόρων, τα πρόσφατα τουρκικά μηνύματα παρέμειναν στις ιστοσελίδες του Υπουργείου Εσωτερικών και της ΕΡΤ ως δέκα ημέρες. Υπάρχουν σαφείς ενδείξεις πως οι Τούρκοι χάκερς συντονίζονται και χρηματοδοτούνται από την τουρκική κυβέρνηση. Επιπλέον, αποκαλύφθηκε ότι Ιρανοί χάκερς παραβίασαν, για χάρη της Τουρκίας, προσωπικούς λογαριασμούς Ελλήνων αξιωματικών του Πολεμικού Ναυτικού, «χτυπώντας» μάλλον και τα δίκτυα του Πολεμικού Ναυτικού, με πιθανή εγκατάσταση κακόβουλου λογισμικού. Η κυβερνοασφάλεια στην άμυνα αποκτά μεγαλύτερη σημασία.

Λαμβανομένων υπόψη των ανωτέρω, ερωτάται η Επιτροπή:

1. Διαθέτει εργαλεία εντοπισμού παρωχημένου λογισμικού και εξοπλισμού σε δημόσιες υπηρεσίες των κρατών μελών;

2. Υπάρχουν προγράμματα για συντονισμό κοινών δημόσιων διαγωνισμών, ώστε τα κράτη μέλη να εκσυγχρονίσουν τα υλικά και το λογισμικό τους, ελαχιστοποιώντας την ευαλωτότητα έναντι κυβερνοεπιθέσεων, με χαμηλότερο κόστος;

3. Κατόπιν της συμπλήρωσης ενός έτους από την έγκριση της πράξεως για την ασφάλεια στον κυβερνοχώρο, εφόσον έχει αξιολογήσει την παροχή δυνατότητας κυβερνο-πιστοποίησης στον ENISA, σχεδιάζει να του αποδώσει νέο ρόλο για βαθύτερη εμπλοκή των κρατών μελών, μέσα από μια συστηματικότερη προσέγγιση εντοπισμού αδυναμιών και κενών του συστήματος, στοχεύοντας στη βελτιστοποίηση της ανθεκτικότητας, της αποτρεπτικής ικανότητας και της σύγχρονης άμυνας;