Capital.gr

# Η δέσμευση του ΝΑΤΟ για τον κυβερνοχώρο

28/Νοε/2018 11:45

Της**Sophia Besch**

Ηπρωταρχική και πιο επείγουσα εργασία του ΝΑΤΟ στον κυβερνοχώρο είναι η προστασία των δικών του συστημάτων επικοινωνίας και των δικτύων του. Αλλά η συμμαχία επίσης προσφέρει εκπαιδευτικές ευκαιρίες και προσπαθεί να καταστήσει ευκολότερη την ανταλλαγή πληροφοριών μεταξύ των συμμάχων, προκειμένου να βοηθήσει τις πρωτεύουσες να προστατεύσουν τα συστήματά τους και τα "ζωτικής σημασίας" δίκτυά τους από τις επιθέσεις.

ΤοΝΑΤΟ δεν διαθέτει μηχανισμούς για την επιβολή του νόμου και το να πείσει τους συμμάχους να ενισχύσουν τις κυβερνό-άμυνές τους, αποτελεί μια πρόκληση. Στις αμυντικές δαπάνες, ένας πιο παραδοσιακός τομέας ευθύνης του ΝΑΤΟ, η συμμαχία έχει ένα μέσο υψηλού προφίλ στη διάθεσή της για να ασκήσει πιέσεις στους συμμάχους: τη δέσμευση του 2%. Το ΝΑΤΟ έχει αποφασίσει να ακολουθήσει μια ανάλογη προσέγγιση στο έργο της στον κυβερνοχώρο. Η "δέσμευση για την κυβερνο-άμυνα επινοήθηκε το 2016. Καθιστά το ΝΑΤΟ υπεύθυνο όχι μόνο για την προστασία των δικτύων της συμμαχίας αλλά επίσης για τον καθορισμό των καλύτερων πρακτικών και προτύπων και την άντληση πόρων και την ενίσχυση της συνειδητοποίησης στις πρωτεύουσες.

Οισύμμαχοι του ΝΑΤΟ έχουν αρχίσει τώρα να κατανέμουν περισσότερους πόρους για την προστασία των εθνικών δικτύων. Είναι δύσκολο να πούμε πόση απ αυτή την πρόοδο συνδέεται με τη δέσμευση για τον κυβερνοχώρο: οι σύμμαχοι του ΝΑΤΟ έχουν μόλις αρχίσει να διαθέτουν περισσότερους πόρους για την προστασία των εθνικών δικτύων. Είναι δύσκολο να πούμε πόση από αυτή την πρόοδο συνδέεται με την κυβερνό-δέσμευση: επανειλημμένες κυβερνοεπιθέσεις σε συμμάχους του ΝΑΤΟ τα τελευταία χρόνια, έδωσαν σοβαρούς λόγους για να επενδύσουν εθελοντικά. Ωστόσο, όπως και η δέσμευση του 2% για τις αμυντικές δαπάνες, η κυβερνό-δέσμευση μπορεί να είναι χρήσιμη στο να προσδώσει πρόσθετη πολιτική νομιμοποίηση σε όσους προειδοποιούν για την ανάγκη επείγουσας δράσης και για την αύξηση των δαπανών για τον κυβερνοχώρο.

Σεαντίθεση με τη δέσμευση του 2% ωστόσο, μπορεί να είναι δύσκολο να πούμε πόσες δαπάνες είναι αρκετές για τον κυβερνοχώρο. Τα hardware και software των υπολογιστών είναι φθηνά σε σχέση με τα συμβατικά κιτ άμυνας όπως τα μαχητικά αεροσκάφη, ακόμη και εάν το κόστος εκπαίδευσης των ανθρώπων για κυβερνοεργασίες, είναι υψηλό. Ένα πρόβλημα είναι ότι δεν υπάρχει απλή φόρμουλα για το πόση κυβερνό-άμυνα απαιτείται. Το ΝΑΤΟ πάντα δικαιολογεί τις

απαιτήσεις για αμυντικό εξοπλισμό, ζητώντας από τους συμμάχους να συμβαδίζουν με τις προσπάθειες εξοπλισμού των εχθρικών χωρών, ιδιαίτερα της Ρωσίας. Είναι δύσκολο να ποσοτικοποιήσουμε τις απαιτήσεις στον κυβερνοχώρο με τον ίδιο τρόπο.

Αντιθέτως, οι δεσμεύσεις σε αυτόν τον τομέα εστιάζουν στις επιδράσεις των επενδύσεων, όπως εάν μια χώρα-μέλος είναι σε θέση να εποπτεύει ένα δίκτυο 24/7 ή να παρακολουθεί και να εντοπίζει επιθέσεις. Μια απλή σύγκριση της ισχύος στον κυβερνοχώρο μεταξύ ΝΑΤΟ και Ρωσίας, Βόρειας Κορέας ή Κίνας είναι δύσκολη. Αλλά πολλοί επισημαίνουν την ισχύ των δυτικών κρατών σε καινοτόμες τεχνολογίες, ως ένα σημαντικό πλεονέκτημα. Και πάλι, το ΝΑΤΟ δυσκολεύεται να καρπωθεί τα οφέλη των καινοτόμων επιχειρήσεων που βρίσκονται στα κράτη-μέλη του. Η μακρά και συχνά υπερβολική γραφειοκρατική διαδικασία προμηθειών περιορίζει την ικανότητα του ΝΑΤΟ να έχει πρόσβαση στις νεότερες τεχνολογίες άμυνας στον κυβερνοχώρο. Σε έναν τομέα όπου η τεχνολογία προχωράει πολύ γρήγορα, το ΝΑΤΟ πάντα θα βρίσκεται πίσω εάν δεν μπορέσει να μεταρρυθμίσει τον τρόπο με τον οποίο αποκτά ικανότητες στον κυβερνοχώρο.

Ηδέσμευση στον κυβερνοχώρο δεν θα φέρει αποτέλεσμα εάν δεν συμμετάσχει ο ιδιωτικός τομέας: το ΝΑΤΟ θα πρέπει να ενισχύσει το ρόλο του όχι μόνο ως μια πλατφόρμα όπου οι σύμμαχοι μπορούν να ανταλλάσσουν πληροφορίες, αλλά επίσης ως ένα forum για ανταλλαγή (πληροφοριών) με την βιομηχανία. Οι επιχειρήσεις συχνά θα έχουν παρόμοιες ή χειρότερες επιθέσεις στα δίκτυά τους από το ΝΑΤΟ και τα κράτη-μέλη μπορούν να μοιραστούν τις εμπειρίες που διδάχθηκαν. Το ΝΑΤΟ έχει δημιουργήσει μια πλατφόρμα για την ανταλλαγή πληροφοριών με την βιομηχανία, αλλά η βάση δεδομένων χρησιμοποιείται μόνο για μη διαβαθμισμένα τεχνικά χαρακτηριστικά του κακόβουλου λογισμικού προς το παρόν, και ως εκ τούτου έχει περιορισμένη χρησιμότητα για τους χρήστες.

Ησυμμαχία έχει επίσης ένα ξεκάθαρο συμφέρον ασφάλειας στην προώθηση της συνεργασίας πολιτικού-στρατιωτικού και ιδιωτικού-δημοσίου τομέα, στο πεδίο της προστασίας του δικτύου. Δεν είναι όλα τα κρίσιμα δίκτυα υποδομών υπό στρατιωτικό ή κυβερνητικό έλεγχο. Αλλά επί του παρόντος, εάν για παράδειγμα, ένα εργοστάσιο ενέργειες σε ένα κράτος-μέλος του ΝΑΤΟ έκλεινε ξαφνικά, τα γραφεία του ΝΑΤΟ πιθανώς δεν θα ήταν ο πρώτος που θα καλούσε μια εταιρεία, παρόλο που οι επιπτώσεις στην ασφάλεια και στην άμυνα από ένα πεδίο ηλεκτρικής ενέργειας, θα μπορούσαν να είναι σοβαρές. Παρά τη σημασία τους, τα αστικά δίκτυα αυτή τη στιγμή τα "προσέχουν" οι μεμονωμένες χώρες-μέλη του ΝΑΤΟ. Μια επίθεση σε δίκτυα αστικών υποδομών θα μπορούσαν να είναι και οικονομικά επιζήμια και μια απειλή για την άμυνα: για παράδειγμα, εάν κάποιος επιτιθέμενος "χάκαρε" το σιδηροδρομικό δίκτυο της Γερμανίας σε μια στιγμή έντασης, θα μπορούσε να εμποδίσει να κινηθούν γρήγορα οι ενισχύσεις του ΝΑΤΟ και ταυτόχρονα, να παρακωλύσει τη γερμανική οικονομία. Αυτό είναι ένα προφανές πεδίο για συνεργασία μεταξύ ΕΕ-ΝΑΤΟ. Αλλά ενώ το ΝΑΤΟ και η ΕΕ έχουν εντείνει τις προσπάθειές τους για συνεργασία ε σειρά περιπτώσεων τα τελευταία χρόνια, με την κυβερνο-ασφάλεια να είναι ψηλά στη λίστα, αυτά που μοιράζονται μεταξύ τους είναι τυπικά, και περιορίζονται σε μη διαβαθμισμένες πληροφορίες.

Ηανταλλαγή πληροφοριών είναι ένα μεγάλο πρόβλημα για τους συμμάχους του ΝΑΤΟ. Ενώ το ΝΑΤΟ μπορεί να προσφέρει χρήσιμα εργαλεία και ένα ασφαλές περιβάλλον, εξαρτάται πάντα από

τις εθνικές κυβερνήσεις να παράσχουν πληροφορίες σχετικά με τις κυβερνοεπιθέσεις που έχουν βιώσει και τα μέσα που αναπτύσσουν για να αμυνθούν έναντι μελλοντικών περιστατικών, αν μη τι άλλο διότι από τη στιγμή που θα χρησιμοποιηθεί ένα κυβερνο-μέσο και θα αποκαλυφθεί η επίδρασή του, η ισχύς του χάνεται και σε πολλές περιπτώσεις δεν χρησιμοποιείται ξανά.

ΤοΝΑΤΟ θα πρέπει να μεταρρυθμίσει τις διαδικασίες εξαγοράς έτσι ώστε να ταιριάζουν στους κύκλους ανάπτυξης της κυβερνο-τεχνολογίας, να καταστήσει σίγουρο ότι το προσωπικό είναι εκπαιδευμένο ώστε να βλέπει τη διάσταση της κυβερνοασφάλειας στην καθημερινή εργασία, να επιδιώκει συνεργασία με την βιομηχανία, και να βελτιώσει τη σχέση με την ΕΕ μέσω καλύτερων μηχανισμών ανταλλαγής πληροφοριών και περισσότερων κοινών κυβερνο-ασκήσεων. Αλλά για να πείσει τους συμμάχους να αυξήσουν τις εγχώριες προσπάθειές τους και να μάθουν ο ένας από τον άλλο, το ΝΑΤΟ εξακολουθεί να βασίζεται κατά κύριο λόγο στις πιέσεις των ομολόγων. Η ελπίδα είναι ότι η κυβερνο-δέσμευση θα είναι πιο πειστική από ό,τι το ισοδύναμο της αμυντικής δαπάνης.

Μπορείτενα δείτε το κείμενο εδώ: https://www.cer.eu/in-the-press/natos-cyber-pledge

Διαβάστε το άρθρο στο Capital.gr