Η κρυπτομηχανή "ON-LINE"

Η άγνωστη ιστορία της ελληνικής απαραβίαστης κρυπτογραφικής συσκευής "DE-59"

Του Ταξιάρχου ε.α. Χρήστου Νοταρίδη

Υπάρχουν κάποιες μοναδικές εφευρέσεις, που ενώ θα μας έκαναν πολύ υπερήφανους, αναγκαστικά έμειναν «αθέατες», στο βωμό της διασφάλισης εθνικών μυστικών.

Η έννοια του κρατικού μυστικού εμφανίστηκε ταυτόχρονα με την ίδρυση των οργανωμένων κρατών. Τότε προέκυψε και η ανάγκη ασφαλούς μετάδοσης εμπιστευτικών μηνυμάτων σε μεγάλες αποστάσεις, αλλά άνθισαν και οι προσπάθειες υποκλοπής τους. Είναι γνωστές οι προσπάθειες διαβίβασης μυστικών στην αρχαία Ελλάδα, με τρόπο που δεν θα επέτρεπε τη~~ν~~ γνώση τους από άλλους εκτός του τελικού τους αποδέκτη. Κλασσικό παράδειγμα η κρυπτεία σκυτάλη των Σπαρτιατών. Με την πάροδο του χρόνου, με την ανάπτυξη της γνώσης και της τεχνολογίας, η κρυπτογράφηση και η αποκρυπτογράφηση απορρήτων πληροφοριών εξελίχθηκε σε κρίσιμο παράγοντα επιτυχίας των επιχειρήσεων και συχνά στη διαδρομή της ιστορίας η διαρροή μυστικών αποδείχθηκε πιο καταστροφική από τις ένοπλες αντιπαραθέσεις.

Η κατασκευή των κρυπτογραφικών μηχανών (ή κρυπτομηχανών) ξεκίνησε από την αρχή της δεκαετίας του 1920, προκειμένου να εξασφαλισθεί το απαραβίαστο των σημάτων **με ταχύτητα κι ευκολία**, ενώ στη συνέχεια κατά τη διάρκεια του Β' ΠΠ εξελίχθηκαν και γνώρισαν ευρεία χρήση μεταξύ των αντίπαλων στρατοπέδων. Αντίστοιχα όμως, αναπτύχθηκαν διατάξεις μηχανικής κρυπτανάλυσης, που τελικά «έσπαγαν» τους κώδικες και αποκάλυπταν τα μυστικά. Είναι πολύ γνωστή, άλλωστε, η εντατική προσπάθεια των Άγγλων σε συνεργασία με τους συμμάχους να «σπάσουν» τη γερμανική κρυπτομηχανή ENIGMA προκειμένου να υποκλέπτουν τα απόρρητα γερμανικά μηνύματα, το οποίο πέτυχαν χωρίς να γίνουν αντιληπτοί, γεγονός που

βοήθησε να συντομευτεί το τέλος του πολέμου κατά μερικά έτη.

Τον Β΄ΠΠ διαδέχθηκε ο Ψυχρός Πόλεμος και η ανάγκη διασφάλισης των επικοινωνιών παρέμεινε αμείωτη από εχθρούς αλλά και από συμμάχους. Μέσα από τους αντίπαλους συνασπισμούς διαπιστώθηκε ότι ήταν πολύ πιο ασφαλές να αναπτύξει η κάθε χώρα τις δικές της εθνικές κρυπτομηχανές, σχεδιασμένες από ανθρώπους που είχαν τις κατάλληλες γνώσεις και κυρίως απολάμβαναν εμπιστοσύνης, παρά να αγοράσουν από το εμπόριο κατασκευασμένες από αγνώστους, με βέβαιο κίνδυνο να υπάρχουν «κεκρόπορτες», που θα επέτρεπαν σε ξένες δυνάμεις να μπορούν να διαβάζουν τα απόρρητα μηνύματα. Η Ελλάδα δεν θα μπορούσε να αποτελεί εξαίρεση.

Στα μέσα της δεκαετίας 1950 η μόλις πρόσφατα ιδρυθείσα ΚΥΠ είχε μυηθεί στο παιχνίδι της υποκλοπής επικοινωνιών άλλων κρατών και των διπλωματικών αποστολών τους κι έτσι αναδείχθηκε η ανάγκη προστασίας και των ελληνικών κρατικών τηλεπικοινωνιών. Εκεί ανέλαβε έργο ο μηχανικός **Δρ. Παναγής Δελμούζος**.

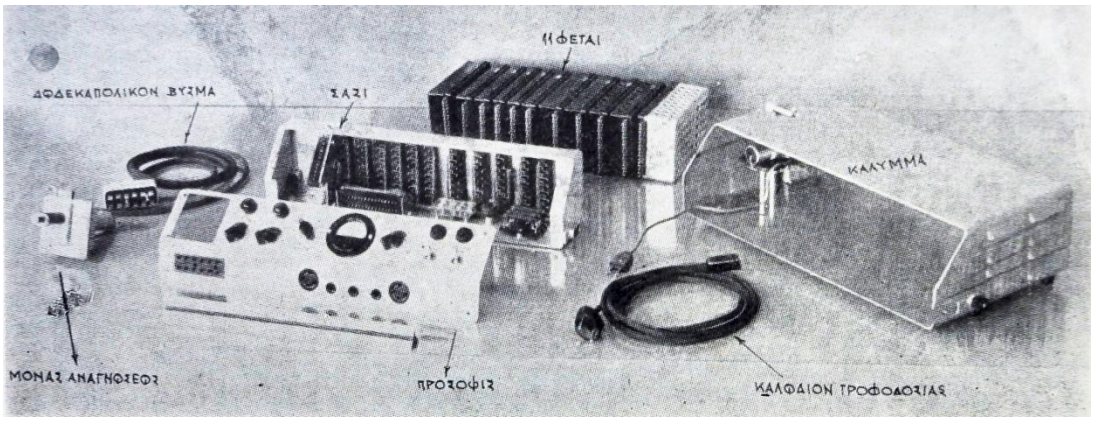
Ο Παναγής, που με τον αδελφό του Άλκη ήταν γιοί του καθηγητού του πανεπιστήμιου Θεσσαλονίκης Αλέξανδρου Δελμούζου, ήταν ήδη καταξιωμένος ηλεκτρονικός τεχνικός, αφού ήδη το 1938 είχε ιδρύσει την εταιρεία **ΕΛΒΙΡΑ** (Ελληνική ΒΙομηχανία ΡΑδιοφώνων), που κατασκεύαζε οικιακά ραδιόφωνα δικής της σχεδίασης με εισαγόμενα εξαρτήματα. Το 1940 η ακμάζουσα ΕΛΒΙΡΑ έφθασε να προτείνει στο Υπουργείο Στρατιωτικών την επιτόπια κατασκευή ραδιοδεκτών για τον Στρατό, μικρότερων-ελαφρύτερων και με καλύτερη ευαισθησία από τους ήδη χρησιμοποιούμενους γερμανικούς LORENZ. Στη διάρκεια της Κατοχής πέτυχαν να παραμείνει σε λειτουργία η ΕΛΒΙΡΑ με προσωπικό 110 άτομα, λόγω της προπολεμικής εμπορικής σχέσης με την γερμανική SIEMENS, αλλά παράλληλα τα αδέλφια συνεργάζονταν κρυφά με τους Συμμάχους και κατασκεύαζαν-επισκεύαζαν ασυρμάτους αντιστασιακών οργανώσεων, όπως η ΑΠΟΛΛΩΝ (ΥΒΟΝΝΗ) όπου είχαν ενταχθεί. Στα μέσα όμως του 1944, προδόθηκε η δράση τους και τα αδέλφια συνελήφθησαν ενώ το εργοστάσιο λεηλατήθηκε, αλλά ευτυχώς κατάφεραν να δραπετεύσουν. Μεταπολεμικά, το 1946 το εργοστάσιο της ΕΛΒΙΡΑ άνοιξε πάλι, με οικονομική βοήθεια που δόθηκε από τους Άγγλους ως αναγνώριση της προσφοράς τους αλλά και ως αποζημίωση των ζημιών που είχαν υποστεί.

Το 1955 η ΕΛΒΙΡΑ είχε πάλι αναπτυχθεί, κατασκεύαζε ποιοτικά ραδιόφωνα και ανταγωνιζόταν επάξια ξένες εταιρείες όπως οι PHILIPS και TELEFUNKEN. Τότε, ανατέθηκε από το Υπουργείο Εξωτερικών στον Δρ. Παναγή Δελμούζο η μελέτη κι ανάπτυξη μίας εθνικής κρυπτομηχανής, με επιδότηση ενός εκατομμυρίου δραχμών.
Ο Δελμούζος ήταν από τους πρώτους που εφήρμοσαν στην πράξη τις θεωρητικές εργασίες του Αμερικανού καθηγητού *C. Shannon* για την ασφάλεια, με τις οποίες αποδείχθηκε ότι το μόνο κρυπτοσύστημα που αντέχει σε οποιαδήποτε κρυπταναλυτική επίθεση, είναι **ο κώδικας μιας χρήσεως *(one-time-pad)*** δηλ. η κλείδα της κρυπτογράφησης να μην επαναλαμβάνεται, αλλά να χρησιμοποιείται μόνο μία φορά, ώστε να μην είναι προβλέψιμη απο εκείνους που θα προσπαθήσουν να υποκλέψουν την επικοινωνία, κάνοντας έτσι αδύνατη τη διάσπαση του κώδικα.

Ο ιδιοφυής Δελμούζος κατάφερε να κάνει πράξη τη θεωρία κι επινόησε μία νέα συσκευή. Το εργαστηριακό πρότυπο τελειοποιήθηκε το 1959 και οδήγησε στη ίδρυση από τον Δελμούζο του ΚΕΕΘΑ (Κέντρου Ερευνών Εθνικής Αμύνης). Η πρώτη δοκιμή των κρυπτομηχανών έγινε σε

γραμμή της Αθήνας με την πρεσβεία μας στη Ρώμη, ενώ ακολούθησε κι άλλη πετυχημένη δοκιμή με τη διπλωματική αποστολή μας στη Νέα Υόρκη. Επρόκειτο για ένα ζεύγος συσκευών, κάθε μία συνδεδεμένη σε τηλέτυπο, δηλ. στις ηλεκτρικές γραφομηχανές αποστολής-λήψης κειμένου μεταξύ δύο μακρινών ανταποκριτών. Η νέα κρυπτοσυσκευή αυτή υποβλήθηκε σε διεξοδικούς ελέγχους από τους Αμερικανούς το 1961, που προσπάθησαν να βρούν τυχόν αδυναμίες της, στο τέλος όμως βρέθηκε απόλυτα απαραβίαστη και το 1962 εγκρίθηκε από το ΝΑΤΟ, ως κατάλληλη για διαβίβαση πληροφοριών **με οποιοδήποτε βαθμό ασφαλείας** (μέγιστη διαβάθμιση).

Η κρυπτομηχανή ονομάσθηκε **«Συσκευή Κρυπτογραφήσεως Επί Γραμμής DE-59»** (προφανώς από το **ΔΕ**λμούζος-19**59**) και σύντομα άρχισε η μαζική παραγωγή της στο ΚΕΕΘΑ. Η κρίσιμη κλείδα της «μιάς-χρήσεως» ήταν σε μορφή χάρτινης διάτρητης ταινίας τηλετύπου, την οποία «διάβαζε» η κρυπτομηχανή ταυτόχρονα με την εκπομπή/λήψη του σήματος, κάνοντας «μίξη» του απόρρητου κειμένου με την κλείδα, ώστε ακόμη κι όταν υποκλαπεί το τελικό κρυπτογραφημένο κείμενο να είναι αδύνατη η διάσπαση του. Η ίδια ακριβώς ταινία-κλείδα (το «σέτ» όπως την έλεγαν οι χειριστές) υπήρχε συγχρονισμένη σε κάθε πλευρά, αποστολέα και παραλήπτη, αλλά μόνον εκεί, αφού είχε παραχθεί μόνον σε 2 αντίτυπα κι έτσι ήταν αδύνατο να διαρρεύσει.
Εσωτερικά, τα εξαρτήματα της συσκευής ήταν τεχνολογίας τρανζίστορ, ξεπερνώντας την εποχή των παρωχημένων λυχνιών, ενώ τα κυκλώματά της ήταν τοποθετημένα σε ένδεκα «φέτες» (βαθμίδες), οπότε αν πάθαινε κάποια βλάβη η επισκευή ήταν εύκολη και ταχεία με την αντικατάσταση της χαλασμένης «φέτας» με εφεδρική. Είχε επίσης επιπρόσθετα συστήματα για έλεγχο ορθής κρυπτογράφησης και καταστολή παρασίτων.



Η λειτουργία της συσκευής **«ON LINE»** όπως την αποκαλούσαν, επειδή κρυπτογραφούσε το σήμα τηλετύπου αυτόματα στη διάρκεια της εκπομπής του, είχε ένα σημαντικό **επιχειρησιακό πλεονέκτημα**: τη ταχύτητα αποστολής-λήψης των διαβαθμισμένων σημάτων, που άλλως θα έπρεπε να κρυπτογραφηθούν με τα ξεπερασμένα χειρογραφικά μέσα, με σημαντική καθυστέρηση ωρών και σοβαρή πιθανότητα σφάλματος από τον κρυπτογράφο.
Σταδιακά εγκαταστάθηκε σε όλα τα Κέντρα Επικοινωνιών των τριών Κλάδων των Ενόπλων Δυνάμεων, της Χωροφυλακής, του Υπουργείου Εξωτερικών και των ελληνικών διπλωματικών αποστολών στο εξωτερικό κι έμεινε **σε χρήση για 35 έτη** τουλάχιστον. Ενώ παραμένει άγνωστη η συνολική ποσότητα συσκευών που κατασκευάσθηκαν, γνωρίζουμε οτι τυπώθηκαν 1.500 τεχνικά εγχειρίδια της. Αξέχαστος σίγουρα στη μνήμη των Χειριστών Τηλετύπου παραμένει ο χαρακτηριστικός ήχος, ΤΑΚ-ΤΑΚ, του αναγνώστη της ταινίας-κλείδας.

Η απόλυτα ασφαλής κρυπτομηχανή του Δελμούζου αποτελούσε πρωτοποριακό τεχνολογικό επίτευγμα εκείνης της εποχής. Απόδειξη του ισχυρισμού αυτού βρίσκουμε στο βιβλίο «*Spycatcher*», του πρώην κορυφαίου υπαλλήλου της βρετανικής υπηρεσίας πληροφοριών Peter Wright. Εκεί ομολογεί ότι οι Βρετανοί είχαν καταφέρει να υποκλέπτουν όλα τα τηλεγραφήματα των ξένων διπλωματών, ακόμη και συμμάχων τους όπως των Γάλλων, σε μία εποχή που υπήρχε ανοιχτή διπλωματική αντιπαράθεση μεταξύ τους που αφορούσε κυρίως την ένταξη της πρώτης στην Ε.Ο.Κ., με τους Γάλλους να αντιδρούν σε αυτή την προοπτική. Δεν πέτυχαν όμως να υποκλέψουν τα τηλεγραφήματα της ελληνικής πρεσβείας, λόγω της εφεύρεσης του Δελμούζου.

Η ραγδαία εξέλιξη της τεχνολογίας οδήγησε στα μέσα της δεκαετίας 1990 στην κατάργηση των τηλετύπων από τις κρατικές τηλεπικοινωνίες, καθώς εμφανίστηκαν τα δίκτυα ψηφιακών δεδομένων υψηλής ταχύτητας, και έτσι η **απαραβίαστη εθνική κρυπτομηχανή DE-59** αποσύρθηκε από την ενεργό υπηρεσία και αποτελεί πλέον ένα από τα μοναδικά εκθέματα στο Μουσείο της Σχολής Διαβιβάσεων. Δυστυχώς, δεν υπήρξε πρόνοια για τον εκσυγχρονισμό της.

Σε όλη τη χρονική περίοδο λειτουργίας της, η ON-LINE κέρδισε την εμπιστοσύνη της πολιτικής και στρατιωτικής ηγεσίας, εξασφαλίζοντας με απόλυτη επιτυχία το απόρρητο των ελληνικών κρατικών επικοινωνιών. Αν δεν είχε εφευρεθεί αυτή η εθνική κρυπτομηχανή, θα ήμασταν αναγκασμένοι είτε να αγοράσουμε συσκευές από κάποια σύμμαχο χώρα, εν γνώσει μας ότι εκείνη θα μπορεί να γνωρίζει τα μυστικά μας, είτε θα ήμασταν δέσμιοι των αργών παλιών κρυπτογραφικών συστημάτων, με συνέπεια δυσκολίες και καθυστερήσεις στην επικοινωνία. Ομως, μετά από τόσα χρόνια, δεν αποδόθηκε ποτέ τιμή ή έστω κάποια στοιχειώδης ένδειξη ευγνωμοσύνης προς τον δημιουργό της Παναγή Δελμούζο (1910-1985), γεγονός που αποτελεί τον κανόνα στη χώρα μας.

Η ελληνική κρυπτομηχανή DE-59 μας έκανε υπερήφανους, αφ' ενός διότι απέδειξε ότι υπάρχουν άξιοι και ικανοί Έλληνες επιστήμονες, αφ' ετέρου διότι διαφύλαξε τα εθνικά μυστικά από εχθρούς και από φίλους, παρέχοντας την ασφάλεια που είχαν ανάγκη όλες οι κρατικές υπηρεσίες, υλοποιώντας το απόφθεγμα ενός εκ των επτά σοφών της αρχαίας Ελλάδος, του Περίανδρου: «λόγων απορρήτων εκφοράν μη ποιού».

Χρήστος Νοταρίδης

Πηγές :

- Π. Αποστολίδη «Μυστική Δράση»
- Ι. Τημενίδη «Κρυπτογράφος στην Πρεσβεία Λονδίνου»
- P. Wright «Spycatcher»
- S. Pinkock «Κρυπτογραφία»
- S. Singh «Κώδικες και Μυστικά»

\