ΠΡΟΛΟΓΟΣ

Είναι γνωστό ότι από τη μέρα που γεννιόμαστε κάνουμε διαρκώς αξιολόγηση ρίσκου, συνειδητά ή ασυνείδητα. Όλες οι αποφάσεις και ενέργειές μας καθοδηγούνται από το ρίσκο που είμαστε διατεθειμένοι να δεχθούμε, ή καλύτερα, να ανεχθούμε. Όμως η αντίληψη και αξιολόγηση του ρίσκου είναι υποκειμενική και η απόδειξη είναι το ότι όλοι οι οδηγοί δεν οδηγούν με την ίδια επικινδυνότητα. Το ρίσκο γίνεται αντικειμενικό μετά από γεγονός ατυχήματος, οπότε τότε μόνο γνωρίζουμε τις συνέπειες και απώλειες με αξιόλογη ακρίβεια.

Θα μπορούσαμε επομένως να υποστηρίξουμε ότι η αξιολόγηση και γενικότερα η διαχείριση του ρίσκου είναι εν γένει μια τέχνη σε προσωπικό επίπεδο. Με άλλα λόγια, ο κάθε άνθρωπος ανάλογα με τις εμπειρίες και τις αντιλήψεις του σκαρφίζεται τεχνικές για να προστατευτεί. Στον τομέα της επικοινωνίας, η κρυπτογραφία είναι μια από τις τεχνικές αυτές. Από ιστορικής πλευράς, η κρυπτογραφία τοποθετείται χρονικά μετά την κωδικοποίηση. Κωδικοποίηση είναι η χρήση συμβόλων προκειμένου να εξωτερικεύσουμε τις σκέψεις μας και να επικοινωνήσουμε με τους άλλους. Έτσι η πρώτη μορφή κωδικοποίησης ήταν η φυσική γλώσσα, ενώ η δεύτερη μορφή κωδικοποίησης ήταν η αποτύπωση της γλώσσας σε γραπτά μέσα. Όπως όμως γνωρίζουμε, η ιστορία του ανθρώπινου γένους είναι γεμάτη από πολέμους, επομένως έγινε πολύ σύντομα αντιληπτό πως τα γραπτά μέσα κρύβουν πολλούς κινδύνους, γιατί υπάρχει το ενδεχόμενο η πληροφορία που αποτυπώθηκε σ' αυτά να πέσει σε λάθος χέρια. Έτσι γεννήθηκε η κρυπτογραφία που είχε ως σκοπό να αποκρύψει την πληροφορία σε ενδεχόμενη κατοχή του μέσου επικοινωνίας από τον εχθρό. Επειδή όμως σε κάθε δράση υπάρχει και αντίδραση, πολύ σύντομα γεννήθηκε και η κρυπτανάλυση που είχε ως σκοπό να καταρρίψει την κρυπτογραφία.

Σήμερα, στην εποχή της πληροφορίας, της τυποποίησης και της κυριαρχίας των θετικών επιστημών, θα ήταν αδιανόητο να μην προσπαθήσουμε να μοντελοποιήσουμε και να ελέγξουμε το ρίσκο με τον αποτελεσματικότερο τρόπο. Δυστυχώς όμως, όπως θα διαπιστώσουμε, η κρυπτογραφία αδυνατεί να δώσει τις λύσεις που προσμέναμε, ή με άλλα λόγια, η κρυπτογραφία δεν μπορεί να λύσει τα προβλήματα. Αυτό όμως που μπορεί να προσφέρει είναι οι δυνατότητες μετασχηματισμού ενός προβλήματος σε μια πιο διαχειρίσιμη μορφή. Έχοντας ως όπλο τα μαθηματικά μπορούμε να φθάσουμε πιο κοντά στην αντικειμενική αξιολόγηση του

ρίσκου, χωρίς να περιμένουμε πρώτα να συμβεί το γεγονός ατυχήματος, όπως αναφέραμε παραπάνω.

Το βιβλίο αυτό είναι αποτέλεσμα της συντονισμένης προσπάθειας ενός μηχανικού και ενός μαθηματικού με στόχο την ανάδειξη των πραγματικών δυνατοτήτων και διαστάσεων της κρυπτογραφίας. Η κρυπτογραφία εκτός από τέχνη είναι πλέον και επιστήμη. Στο βιβλίο αυτό επιχειρούμε να υποστηρίξουμε αυτήν ακριβώς τη θέση.

Θεσσαλονίκη, Φεβρουάριος 2003 Βασίλης Κάτος, Γιώργος Στεφανίδης