ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ

1999 *2004*

Προσωρινή επιτροπή για το σύστημα Echelon

ΠΡΟΣΩΡΙΝΟ

18 Μαΐου 2001

ΣΧΕΔΙΟ ΕΚΘΕΣΗΣ

σχετικά με την ύπαρξη ενός παγκοσμίου συστήματος παρακολούθησης της ιδιωτικής και οικονομικής επικοινωνίας (σύστημα παρακολούθησης ECHELON)

Προσωρινή επιτροπή για το σύστημα Echelon

Εισηγητής: Gerhard Schmid

ΠΕΡΙΕΧΟΜΕΝΑ

Σελίδα

ΙΣΤΟΡΙΚΟ ΤΗΣ ΔΙΑΔΙΚΑΣΙΑΣ

Κατά τη συνεδρίαση της 5ης Ιουλίου 2000 το Ευρωπαϊκό Κοινοβούλιο αποφάσισε τη συγκρότηση μιας προσωρινής επιτροπής για το σύστημα παρακολούθησης Echelon. Για την εκπλήρωση της εντολής της η προσωρινή επιτροπή όρισε κατά τη συνεδρίασή της συγκρότησης σε σώμα στις 5 Ιουλίου 2000 τον κ. Gerhard Schmid ως εισηγητή.

Κατά τη συνεδρίασή της/τις συνεδριάσεις της στις …. η επιτροπή εξέτασε το σχέδιο έκθεσης.

Κατά την τελευταία ως άνω συνεδρίαση, η επιτροπή ενέκρινε την πρόταση ψηφίσματος με ... ψήφους υπέρ, ... ψήφους κατά και ... αποχές(ή)/ομόφωνα.

Ήσαν παρόντες κατά την ψηφοφορία οι βουλευτές ... (πρόεδρος/ασκών/ασκούσα την προεδρία), ... (αντιπρόεδρος), ... (αντιπρόεδρος), ... (εισηγητής/ήτρια), ..., ... (αναπλ. ...), ... (αναπλ. ... σύμφωνα με το άρθρο 153, παράγραφος 2, του Κανονισμού), ... και ... .

Η έκθεση κατατέθηκε στις …

Η προθεσμία για την κατάθεση τροπολογιών θα αναγράφεται στο σχέδιο ημερήσιας διάταξης της περιόδου συνόδου κατά την οποία θα εξετασθεί η έκθεση/ορίσθηκε για τις …, … .

ΠΡΟΤΑΣΗ ΨΗΦΙΣΜΑΤΟΣ

Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου σχετικά με την ύπαρξη ενός παγκοσμίου συστήματος παρακολούθησης της ιδιωτικής και οικονομικής επικοινωνίας (σύστημα παρακολούθησης ECHELON)

Το Ευρωπαϊκό Κοινοβούλιο,

– έχοντας υπόψη την απόφαση του Ευρωπαϊκού Κοινοβουλίου της 5ης Ιουλίου 2000, περί συστάσεως προσωρινής επιτροπής για το σύστημα παρακολούθησης Echelon και τη σχετική εντολή της,

– έχοντας υπόψη τη Συνθήκη ΕΚ, η οποία στοχεύει στην οικοδόμηση μιας κοινής αγοράς με υψηλό βαθμό ανταγωνιστικότητας,

– έχοντας υπόψη τη Συνθήκη της Ευρωπαϊκής Ένωσης, ιδίως το άρθρο της 6, παράγραφος 2, το οποίο καθορίζει την υποχρέωση της ΕΕ για το σεβασμό των θεμελιωδών δικαιωμάτων, και τον τίτλο της V, που περιέχει διατάξεις για την κοινή εξωτερική πολιτική και πολιτική ασφάλειας,

– έχοντας υπόψη το Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, του οποίου το άρθρο 7 προστατεύει το σεβασμό της ιδιωτικής και οικογενειακής ζωής και ορίζει ρητά το δικαίωμα στο σεβασμό της επικοινωνίας,

– έχοντας υπόψη την Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου, ιδίως το άρθρο της 8 που προστατεύει την ιδιωτική ζωή, και τις πολυάριθμες άλλες διεθνείς συνθήκες που προβλέπουν την προστασία της ιδιωτικής ζωής,

– έχοντας υπόψη την έκθεση σχετικά με την ύπαρξη ενός παγκοσμίου συστήματος παρακολούθησης της ιδιωτικής και οικονομικής επικοινωνίας (σύστημα παρακολούθησης Echelon) της προσωρινής επιτροπής για το σύστημα παρακολούθησης Echelon (A5-..../2001),

ως προς την ύπαρξη ενός παγκοσμίου συστήματος παρακολούθησης της ιδιωτικής και οικονομικής επικοινωνίας (Σύστημα παρακολούθησης ECHELON)

Α. εκτιμώντας ότι η ύπαρξη ενός λειτουργούντος σε παγκόσμιο επίπεδο συστήματος παρακολούθησης των επικοινωνιών, το οποίο λειτουργεί με τη σύμμετρη συμμετοχή των ΗΠΑ, του Ηνωμένου Βασιλείου, του Καναδά, της Αυστραλίας και της Νέας Ζηλανδίας, στο πλαίσιο της συμφωνίας UKUSA, δεν είναι δυνατόν πλέον να αμφισβητηθεί· ότι βάσει των υφισταμένων ενδείξεων φαίνεται πιθανό ότι η μυστική ονομασία του είναι πραγματικά "ECHELON", το τελευταίο όμως είναι ωστόσο δευτερεύουσας σημασίας,

Β. γνωρίζοντας ότι το σύστημα χρησιμεύει στην παρακολούθηση όχι στρατιωτικής, αλλά ιδιωτικής και οικονομικής επικοινωνίας, αλλά ότι η στην έκθεση πραγματοποιούμενη ανάλυση κατέδειξε ότι το μέγεθος αυτού του συστήματος σε κάθε περίπτωση δεν μπορεί να είναι τόσο εκτεταμένο όσο υποθέτουν εν μέρει τα μέσα ενημέρωσης,

ως προς τα όρια του συστήματος παρακολούθησης

Γ. εκτιμώντας ότι το σύστημα παρακολούθησης στηρίζεται στην παγκόσμια παρακολούθηση δορυφορικής επικοινωνίας, αλλά ότι όμως η επικοινωνία σε περιοχές με υψηλή πυκνότητα επικοινωνίας μεταδίδεται μόνο σε πολύ μικρό τμήμα μέσω δορυφόρων· ότι κατ' αυτό τον τρόπο το μεγαλύτερο μέρος της επικοινωνίας δεν είναι δυνατόν να παρακολουθηθεί από επίγειους σταθμούς, αλλά μόνο με λαθροσύνδεση καλωδίων και αναχαίτιση ραδιοσημάτων, πράγμα το οποίο – όπως απέδειξαν οι εις την έκθεση πραγματοποιηθείσες εξετάσεις – είναι δυνατόν μόνο εντός στενών ορίων· ότι το κόστος σε προσωπικό για την τελική αξιολόγηση αναχαιτισθείσας επικοινωνίας προϋποθέτει περαιτέρω περιορισμούς· ότι, κατά συνέπεια, οι χώρες του ECHELON έχουν πρόσβαση σε ένα πολύ περιορισμένο τμήμα της καλωδιακής και ασύρματης επικοινωνίας και μπορούν να αξιοποιήσουν μόνο ένα περιορισμένο τμήμα της επικοινωνίας,

ως προς την πιθανή ύπαρξη άλλων συστημάτων παρακολούθησης

Δ. με τη σκέψη ότι η παρακολούθηση επικοινωνίας αποτελεί ένα σύνηθες για τις μυστικές υπηρεσίες πληροφοριών μέσο κατασκοπείας και ότι ένα τέτοιο σύστημα θα μπορούσε να χρησιμοποιηθεί και από άλλες χώρες, εφόσον αυτές διαθέτουν τα ανάλογα οικονομικά μέσα και τις γεωγραφικές προϋποθέσεις· ότι η Γαλλία, τουλάχιστον σε ό,τι αφορά στις γεωγραφικές προϋποθέσεις – λόγω των υπερποντίων εδαφών της θα ήταν το μοναδικό κράτος μέλος της ΕΕ που θα ήταν σε θέση να εγκαταστήσει από μόνη της ένα παγκόσμιο σύστημα παρακολούθησης, και ότι πέραν αυτού υπάρχουν ενδείξεις ότι και η Ρωσία θα μπορούσε να χρησιμοποιήσει ένα τέτοιο σύστημα,

ως προς τη συμβατότητα με το δίκαιο της ΕΕ

Ε. με τη σκέψη ότι όσον αφορά το ζήτημα της συμβατότητας ενός συστήματος τύπου ECHELON με το δίκαιο της ΕΕ πρέπει να υπάρξει διάκριση μεταξύ δύο περιπτώσεων: αν το σύστημα χρησιμοποιείται μόνο για τους σκοπούς των υπηρεσιών πληροφοριών, δεν προκύπτει αντίθεση προς το δίκαιο της Ένωσης, καθώς οι δραστηριότητες που βρίσκονται στην υπηρεσία της κρατικής ασφάλειας δεν καλύπτονται από τη Συνθήκη ΕΚ, αλλά εμπίπτουν στον τίτλο V της Συνθήκης ΕΕ (ΚΕΠΠΑ), όπου όμως προς το παρόν δεν υπάρχουν σχετικές ρυθμίσεις και συνεπώς λείπουν τα σημεία επαφής. Αν αντιθέτως γίνεται κατάχρηση του συστήματος για την κατασκοπεία των ανταγωνιστών, τότε το σύστημα βρίσκεται σε αντίθεση με την υποχρέωση πίστης των κρατών μελών και με την έννοια της κοινής αγοράς που διέπεται από τον ελεύθερο ανταγωνισμό, κατά τρόπο που ένα κράτος που συμμετέχει σε αυτό παραβιάζει το κοινοτικό δίκαιο,

ως προς τη συμβατότητα με το θεμελιώδες δικαίωμα στο σεβασμό της ιδιωτικής ζωής (άρθρο 8 ΕΣΔΑ)

ΣΤ. έχοντας επίγνωση ότι κάθε παρακολούθηση επικοινωνίας συνιστά βαθιά επέμβαση στην ιδιωτική ζωή του ατόμου· ότι το άρθρο 8 της ΕΣΔΑ που προστατεύει την ιδιωτική ζωή, επιτρέπει επεμβάσεις μόνο προς διασφάλιση της εθνικής ασφάλειας, εφόσον οι σχετικές ρυθμίσεις προβλέπονται από το εσωτερικό δίκαιο, είναι κοινώς προσιτές, και καθορίζουν υπό ποίες προϋποθέσεις και συνθήκες μπορεί η δημόσια αρχή να προβαίνει σε αυτές· ότι οι επεμβάσεις πέραν αυτού πρέπει να είναι ανάλογες, ότι πρέπει να διενεργείται κατά συνέπεια μία στάθμιση συμφερόντων, και, σύμφωνα με τη νομολογία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου, ένα απλό "να είναι χρήσιμες ή επιθυμητές", δεν αρκεί,

Ζ. εκτιμώντας ότι ένα σύστημα των υπηρεσιών πληροφοριών, το οποίο θα παρακολουθούσε

δίχως καμία διασφάλιση της τήρησης της αρχής της αναλογικότητας κάθε επικοινωνία δεν θα συμβιβαζόταν με την ΕΣΔΑ· ότι κατά τον ίδιο τρόπο θα υπήρχε παραβίαση της ΕΣΔΑ, αν η ρύθμιση ήταν μεταγενέστερη της παρακολούθησης της επικοινωνίας, αν αυτή δεν είχε νομική βάση, αν δεν ήταν δημοσίως προσιτή ή αν ήταν διατυπωμένη κατά τέτοιο τρόπο, ώστε οι συνέπειές της να μην είναι προβλέψιμες για τον καθένα· ότι οι ρυθμίσεις, σύμφωνα με τις οποίες δραστηριοποιούνται οι αμερικανικές υπηρεσίες πληροφοριών στην αλλοδαπή, είναι στο μεγαλύτερό τους μέρος χαρακτηρισμένες ως εμπιστευτικές, και κατά συνέπεια η τήρηση της αρχής της αναλογικότητας είναι κατ' αυτό τον τρόπο τουλάχιστον αμφίβολη, και ότι πράγματι υπάρχει παραβίαση των εις της ΕΣΔΑ θεσπιζόμενων αρχών της πρόσβασης στο δίκαιο και της δυνατότητας πρόβλεψης των επιπτώσεών του,

Η. εκτιμώντας ότι τα κράτη μέλη δεν μπορούν να απαλλαγούν των υποχρεώσεών τους που απορρέουν από την ΕΣΔΑ, αφήνοντας τις υπηρεσίες πληροφοριών άλλων κρατών, οι οποίες υπόκεινται σε λιγότερο αυστηρές διατάξεις, να δραστηριοποιούνται στην επικράτειά τους, διότι άλλως θα απογυμνωνόταν η αρχή της νομιμότητας με τις δύο συνιστώσες της πρόσβασης στο δίκαιο και της δυνατότητας πρόβλεψης των επιπτώσεών του και θα απεστερείτο η νομολογία του Δικαστηρίου των Ανθρωπίνων Δικαιωμάτων του περιεχομένου της,

Θ. ενόψει του γεγονότος ότι η συμβατότητα μιας νομοθετικά προβλεπόμενης δραστηριότητας των υπηρεσιών πληροφοριών προϋποθέτει επιπλέον ότι υπάρχουν επαρκή συστήματα ελέγχου προκειμένου να δημιουργείται μία εξισορρόπηση του κινδύνου που συνεπάγεται η μυστική δράση ενός μέρους της διοίκησης· ότι το Ευρωπαϊκό Δικαστήριο των Ανθρωπίνων Δικαιωμάτων εξήρε ρητά τη σημασία ενός αποτελεσματικού συστήματος ελέγχου στον τομέα της δράσης των υπηρεσιών πληροφοριών, και ότι για το λόγο αυτό φαίνεται προβληματικό το ότι ορισμένα κράτη μέλη δεν διαθέτουν δικά τους κοινοβουλευτικά όργανα ελέγχου των μυστικών υπηρεσιών,

ως προς το ερώτημα, αν οι πολίτες προστατεύονται επαρκώς από τις υπηρεσίες πληροφοριών

Ι. εκτιμώντας ότι η προστασία των πολιτών της ΕΕ εξαρτάται από την έννομη κατάσταση των επιμέρους κρατών μελών, αυτά όμως είναι πολύ διαφορετικά διαμορφωμένα, ορισμένα μάλιστα δεν έχουν καθόλου κοινοβουλευτικά όργανα ελέγχου, και για το λόγο αυτό δεν είναι δυνατόν να γίνει λόγος για επαρκή προστασία· ότι οι ευρωπαίοι πολίτες έχουν θεμελιώδες συμφέρον όπως τα εθνικά τους κοινοβούλια διαθέτουν μία ρητά διαρθρωμένη ειδική επιτροπή ελέγχου, η οποία εποπτεύει και ελέγχει τις δραστηριότητες των υπηρεσιών πληροφοριών· ότι ακόμη και εκεί όπου υπάρχουν όργανα ελέγχου, υπάρχουν γι' αυτά μεγάλα κίνητρα, να ασχολούνται περισσότερο με τη δραστηριότητα υπηρεσιών πληροφοριών της ημεδαπής παρά με αυτήν των υπηρεσιών πληροφοριών της αλλοδαπής, λόγω του ότι, κατά κανόνα, μόνο στην πρώτη περίπτωση θίγονται οι πολίτες της ίδιας της χώρας,

ΙΑ. έχοντας επίγνωση του γεγονότος ότι στην περίπτωση συνεργασίας μεταξύ των υπηρεσιών πληροφοριών στο πλαίσιο της ΚΕΠΠΑ, τα όργανα καλούνται να θεσπίσουν επαρκείς προστατευτικές διατάξεις προς όφελος των ευρωπαίων πολιτών,

ως προς την οικονομική κατασκοπεία

ΙΒ. έχοντας επίγνωση του γεγονότος ότι αποτελεί μέρος του τομέα καθηκόντων των υπηρεσιών πληροφοριών της αλλοδαπής να ενδιαφέρονται για οικονομικά δεδομένα, όπως

είναι οι εξελίξεις σε επιχειρησιακούς κλάδους, η εξέλιξη των αγορών πρώτων υλών, η τήρηση οικονομικών αποκλεισμών, η τήρηση των κανόνων παράδοσης για αγαθά διττής χρήσης κλπ.· και ότι, για τους λόγους αυτούς, παρακολουθούνται συχνά ενεχόμενες επιχειρήσεις,

ΙΓ. εκτιμώντας ότι εν πάση περιπτώσει δεν είναι ανεκτό όταν υπηρεσίες πληροφοριών χρησιμοποιούνται για κατασκοπεία ανταγωνιστών, κατασκοπεύοντας αλλοδαπές επιχειρήσεις, προκειμένου να παράσχουν σε ημεδαπές επιχειρήσεις ανταγωνιστικό πλεονέκτημα, ότι ωστόσο, δεν υπάρχει καμία αποδεδειγμένη περίπτωση ότι το παγκόσμιο σύστημα παρακολούθησης χρησιμοποιήθηκε για αυτό το σκοπό, αν και αυτό υποστηρίχθηκε επανειλημμένα,

ΙΔ. έχοντας υπόψη ότι ευαίσθητα δεδομένα μιας επιχείρησης βρίσκονται συχνά μέσα στην ίδια την επιχείρηση, έτσι ώστε η κατασκοπεία στους ανταγωνιστές να επιχειρείται κατά πρώτο λόγο δια της προσπάθειας να ληφθούν οι πληροφορίες από συνεργάτες ή λάθρα εισχωρήσαντα πρόσωπα ή μέσω εισβολής στα εσωτερικά δίκτυα υπολογιστών· ότι μόνον αν κάποια ευαίσθητα στοιχεία διαβιβασθούν ενσύρματα ή ασύρματα (δορυφόρος) προς τα έξω, μπορεί να χρησιμοποιηθεί ένα σύστημα παρακολούθησης των επικοινωνιών για το σκοπό της ανταγωνιστικής κατασκοπείας και αυτό ισχύει συστηματικά μόνο στις ακόλουθες τρεις περιπτώσεις:
- σε επιχειρήσεις οι οποίες λειτουργούν σε τρεις ωριαίες ατράκτους, έτσι ώστε τα προσωρινά αποτελέσματα να αποστέλλονται από την Ευρώπη στην Αμερική και στη συνέχεια στην Ασία·
- στην περίπτωση τηλεδιασκέψεων σε πολυεθνικές εταιρίες οι οποίες μεταδίδονται μέσω δορυφόρου ή καλωδιακά·
- όταν γίνεται επί τόπου διαπραγμάτευση σημαντικών αναθέσεων (όπως συμβαίνει στην κατασκευή εγκαταστάσεων, κατασκευή υποδομών τηλεπικοινωνιών, ανακατασκευή συστημάτων μεταφοράς, κλπ) και πρέπει από το σημείο αυτό να γίνεται συνεννόηση με τις κεντρικές υπηρεσίες της επιχείρησης,

ως προς τις δυνατότητες αυτοπροστασίας

ΙΕ. έχοντας υπόψη ότι η ασφάλεια για τις επιχειρήσεις τότε μόνο μπορεί να επιτευχθεί, όταν ολόκληρο το περιβάλλον εργασίας έχει διασφαλισθεί καθώς και όλες οι οδοί επικοινωνίας προστατεύονται, δια των οποίων μεταβιβάζονται ευαίσθητες πληροφορίες· ότι υπάρχουν επαρκώς ασφαλή συστήματα κρυπτογράφησης σε προσιτές τιμές στην ευρωπαϊκή αγορά· ότι πρέπει να συσταθεί και στους ιδιώτες επειγόντως να κρυπτογραφούν τα μηνύματα ηλεκτρονικού ταχυδρομείου· ότι ένα μη κρυπτογραφημένο μήνυμα είναι το ίδιο με μία επιστολή χωρίς φάκελο· ότι στο διαδίκτυο υπάρχουν σχετικά φιλικά προς τον χρήστη συστήματα τα οποία διατίθενται μάλιστα δωρεάν για ιδιωτική χρήση,

ως προς μια συνεργασία των υπηρεσιών πληροφοριών εντός της ΕΕ

ΙΣΤ. εκτιμώντας ότι η ΕΕ έχει συμφωνήσει να συντονίσει τη συλλογή πληροφοριών των υπηρεσιών πληροφοριών στο πλαίσιο της ανάπτυξης μιας οικείας πολιτικής ασφάλειας και άμυνας, εν προκειμένω όμως να συνεχίσει τη συνεργασία με άλλους εταίρους σ' αυτούς τους τομείς,

ΙΖ. εκτιμώντας ότι μια συνεργασία των υπηρεσιών πληροφοριών στο εσωτερικό της ΕΕ φαίνεται και επιθυμητή επειδή, αφενός, μια κοινή πολιτική ασφάλειας δίχως την

ενσωμάτωση των υπηρεσιών πληροφοριών θα ήταν παράλογη, αφετέρου θα συνδέονταν με αυτήν πολυάριθμα πλεονεκτήματα από επαγγελματική, οικονομική και πολιτική άποψη· ότι επίσης θα αντιστοιχούσε περισσότερο στην ιδέα ενός ισότιμου εταίρου των ΗΠΑ και θα μπορούσε να συμπεριλάβει όλα τα κράτη μέλη σε ένα σύστημα, το οποίο θα δημιουργηθεί σε πλήρη συμφωνία με την ΕΣΔΑ· ότι θα πρέπει φυσικά να διασφαλισθεί ένας αντίστοιχος έλεγχος της συνεργασίας από το Ευρωπαϊκό Κοινοβούλιο,

ΙΗ. εκτιμώντας ότι το Ευρωπαϊκό Κοινοβούλιο πρόκειται να θεσπίσει ίδιες ρυθμίσεις σχετικά με την πρόσβαση σε εμπιστευτικές και ευαίσθητες πληροφορίες και έγγραφα,

όσον αφορά τη σύναψη και τροποποίηση διεθνών συνθηκών για την προστασία των πολιτών και επιχειρήσεων

1. καλεί το Γενικό Γραμματέα του Συμβουλίου της Ευρώπης να υποβάλει στην Επιτροπή Υπουργών μία μελέτη, κατά πόσον είναι λογική η προσαρμογή της εις το άρθρο 8 της ΕΣΔΑ κατοχυρωμένης προστασίας της ιδιωτικής ζωής στις σύγχρονες μεθόδους επικοινωνίας και δυνατότητες παρακολούθησης σε ένα πρόσθετο πρωτόκολλο ή από κοινού με τη ρύθμιση της προστασίας δεδομένων στο πλαίσιο της αναθεώρησης της σύμβασης για την προστασία δεδομένων, υπό την προϋπόθεση ότι κατ' αυτό τον τρόπο δεν θα υπάρξει ούτε υποβάθμισή του από το Δικαστήριο αναπτυχθέντος επιπέδου νομικής προστασίας ούτε μείωση της για την προσαρμογή σε περαιτέρω εξελίξεις αναγκαίας ευελιξίας·

2. καλεί τα κράτη μέλη να δημιουργήσουν ένα ευρωπαϊκό πλαίσιο, προκειμένου να επανεξετάσουν τις νομοθετικές ρυθμίσεις για τη διασφάλιση του απορρήτου της αλληλογραφίας και τηλεπικοινωνίας, να συμφωνήσουν επιπλέον σε ένα κοινό κείμενο, το οποίο διασφαλίζει στο σύνολό της και εγγυάται πέραν αυτής την προστασία της ιδιωτικής ζωής, όπως αυτή ορίζεται στο άρθρο 7 του Ευρωπαϊκού Χάρτη των Θεμελιωδών Δικαιωμάτων, σε όλους τους ευρωπαίους πολίτες στην επικράτεια των κρατών μελών, ότι η δραστηριότητα των υπηρεσιών πληροφοριών πραγματοποιείται σύμφωνα με τα θεμελιώδη δικαιώματα, καθώς και ότι αντιστοιχεί στο κεφάλαιο 8 της έκθεσης, ιδίως στο 8.3.4 στις από το άρθρο 8 της ΕΣΔΑ απορρέουσες προϋποθέσεις·

3. καλεί τα κράτη μέλη του Συμβουλίου της Ευρώπης να θεσπίσουν ένα πρόσθετο πρωτόκολλο το οποίο καθιστά δυνατή την προσχώρηση των Ευρωπαϊκών Κοινοτήτων στην ΕΣΔΑ, ή να προβληματισθούν σχετικά με άλλα μέτρα, τα οποία αποκλείουν συγκρούσεις της νομολογίας των Δικαστηρίων του Στρασβούργου και του Λουξεμβούργου·

4. καλεί τον Γενικό Γραμματέα του ΟΗΕ να αναθέσει στην αρμόδια επιτροπή την υποβολή προτάσεων, οι οποίες στοχεύουν στην προσαρμογή του άρθρου 17 του Διεθνούς Συμφώνου για τα Αστικά και Πολιτικά Δικαιώματα, το οποίο εγγυάται την προστασία της ιδιωτικής ζωής στις τεχνολογικές καινοτομίες·

5. καλεί τις ΗΠΑ να υπογράψουν το Πρόσθετο Πρωτόκολλο του Διεθνούς Συμφώνου για τα Αστικά και Πολιτικά Δικαιώματα, προκειμένου να καταστούν δυνατές ατομικές προσφυγές κατά των ΗΠΑ λόγω της παραβίασής του, ενώπιον της Συμβατικής Επιτροπής Ανθρωπίνων Δικαιωμάτων· οι σχετικές αμερικανικές ΜΚΟ, ιδίως η ACLU (American Civil Liberties Union) και EPIC (Electronic Privacy Information Center) καλούνται να ασκήσουν αντίστοιχη πίεση στην αμερικανική κυβέρνηση·

όσον αφορά εθνικά νομοθετικά μέτρα για την προστασία πολιτών και επιχειρήσεων

6. καλεί τα κράτη μέλη να επανεξετάσουν τη σχετική με τη δραστηριότητα των υπηρεσιών πληροφοριών νομοθεσία τους ως προς τη συμβατότητά της με τα θεμελιώδη δικαιώματα·

7. καλεί τα κράτη μέλη να επιδιώξουν ένα κοινό επίπεδο προστασίας από τη δραστηριότητα των υπηρεσιών πληροφοριών, το οποίο προσδιορίζεται από το ανώτατο επίπεδο που υπάρχει σε κάποιο κράτος μέλος, καθώς οι θιγόμενοι από τη δραστηριότητα μιας αλλοδαπής υπηρεσίας πληροφοριών πολίτες είναι κατά κανόνα πολίτες άλλων κρατών και κατά συνέπεια και άλλων κρατών μελών·

8. καλεί τα όργανα της ΕΕ στην περίπτωση συνεργασίας των υπηρεσιών πληροφοριών στο πλαίσιο της ΚΕΠΠΑ, να θεσπίσουν επαρκείς διατάξεις προστασίας των ευρωπαίων πολιτών· το Ευρωπαϊκό Κοινοβούλιο, το οποίο λογικά θα αποτελέσει το ελεγκτικό όργανο, πρέπει να θέσει τις απαραίτητες για την εποπτεία αυτού του ευαίσθητου τομέα προϋποθέσεις, προκειμένου να είναι ρεαλιστικό αλλά και υπεύθυνο να απαιτήσει τα αναγκαία ελεγκτικά δικαιώματα·

όσον αφορά ειδικά νομικά μέτρα για την καταπολέμηση της οικονομικής κατασκοπείας

9. καλεί τα κράτη μέλη να αναλογισθούν σε ποιο βαθμό μπορούν να καταπολεμηθούν με ρυθμίσεις στο ευρωπαϊκό και διεθνές δίκαιο η οικονομική κατασκοπεία και η δωροδοκία για το σκοπό της αποκόμησης ανάθεσης συμβάσεων, ιδίως αν θα ήταν εφικτή μια ρύθμιση στα πλαίσια του Παγκόσμιο Οργανισμού Εμπορίου, η οποία λαμβάνει υπόψη της την στρεβλωτική για τον ανταγωνισμό επίπτωση μιας τέτοιας συμπεριφοράς, π.χ. ορίζοντας ότι τέτοιες συμβάσεις είναι άκυρες·

10. καλεί τα κράτη μέλη να αναλάβουν σε μία κοινή ρητή δήλωση την υποχρέωση να μην διενεργούν οικονομική κατασκοπεία μεταξύ τους, και με τον τρόπο αυτό να σηματοδοτήσουν τη συμφωνία τους με το πνεύμα και τις διατάξεις της Συνθήκης ΕΚ·

όσον αφορά μέτρα εφαρμογής του δικαίου και ελέγχου της

11. καλεί τα εθνικά κοινοβούλια, τα οποία δεν διαθέτουν ίδια κοινοβουλευτικά όργανα ελέγχου για την εποπτεία των υπηρεσιών πληροφοριών, να προβούν στη σύσταση τέτοιων οργάνων·

12. καλεί τις εθνικές επιτροπές ελέγχου των μυστικών υπηρεσιών να αποδίδουν κατά την άσκηση των ελεγκτικών αρμοδιοτήτων που τους έχουν ανατεθεί μεγάλη σημασία στην προστασία της ιδιωτικής ζωής, ανεξαρτήτως του εάν πρόκειται για την παρακολούθηση των δικών τους πολιτών, άλλων πολιτών της ΕΕ ή πολιτών τρίτων χωρών·

13. καλεί τη Γερμανία και την Αγγλία να εξαρτήσουν την περαιτέρω άδεια παρακολούθησης επικοινωνιών από υπηρεσίες πληροφοριών των ΗΠΑ στην επικράτειά τους, από το εάν οι δραστηριότητες αυτές συμβιβάζονται με την ΕΣΔΑ, δηλαδή ότι ανταποκρίνονται στην αρχή της αναλογικότητας, υπάρχει πρόσβαση στη νομική βάση και είναι δυνατόν να προβλεφθεί η επίπτωση για το μεμονωμένο άτομο, καθώς και ότι υπάρχει αντίστοιχος αποτελεσματικός έλεγχος, λόγω του ότι είναι υπεύθυνες για τη συμβατότητα με τα ανθρώπινα δικαιώματα της επιτρεπόμενης ή απλώς ανεκτής δραστηριότητας των υπηρεσιών πληροφοριών στην επικράτειά τους·

όσον αφορά μέτρα ενίσχυσης της αυτοπροστασίας πολιτών και επιχειρήσεων

14. καλεί την Επιτροπή και τα κράτη μέλη να αναπτύξουν προγράμματα με τα οποία θα ενισχύεται η συνειδητοποίηση πολιτών και επιχειρήσεων της προβληματικής σχετικά με την ασφάλεια και συγχρόνως θα προσφέρουν πρακτική βοήθεια για το σχεδιασμό και την υλοποίηση ολοκληρωμένων λύσεων προστασίας·

15. καλεί την Επιτροπή και τα κράτη μέλη να επεξεργασθούν κατάλληλα μέτρα για την προώθηση, την ανάπτυξη και την κατασκευή ευρωπαϊκής τεχνολογίας και λογισμικού κρυπτογράφησης, και ιδίως να υποστηρίξουν προγράμματα που έχουν ως στόχο την ανάπτυξη φιλικού προς τον χρήστη λογισμικού κρυπτογράφησης, του οποίου ο πηγαίος κώδικας θα είναι προσιτός σε όλους·

16. καλεί την Επιτροπή και τα κράτη μέλη να ενισχύσουν σχέδια λογισμικού, των οποίων ο πηγαίος κώδικας θα είναι προσιτός σε όλους, λόγω του ότι έτσι μόνο μπορεί να διασφαλισθεί ότι δεν έχουν ενσωματωθεί "κερκόπορτες" (αποκαλούμενο: "open-source Software")·

17. καλεί τα ευρωπαϊκά όργανα καθώς και τις δημόσιες διοικήσεις των κρατών μελών να εφαρμόζουν συστηματικά την κρυπτογράφηση των μηνυμάτων ηλεκτρονικού ταχυδρομείου, προκειμένου η κρυπτογράφηση να καταστεί μακροπρόθεσμα η συνήθης πρακτική·

όσον αφορά άλλα μέτρα

18. καλεί τις επιχειρήσεις να συνεργάζονται στενότερα με τις υπηρεσίες αντικατασκοπίας, ιδίως να γνωστοποιούν σε αυτές επιθετικές ενέργειες που προέρχονται από την αλλοδαπή και έχουν σκοπό την οικονομική κατασκοπεία προκειμένου να αυξήσουν την αποτελεσματικότητα των υπηρεσιών·

19. καλεί την Επιτροπή να υποβάλει πρόταση για τη σύσταση μιας ευρωπαϊκής συμβουλευτικής υπηρεσίας για ζητήματα ασφάλειας επιχειρηματικών πληροφοριών, η οποία παράλληλα με την αύξηση της συνειδητοποίησης του προβλήματος έχει ως αποστολή και την παροχή πρακτικής βοήθειας·

20. θεωρεί ως λογικό να οργανωθεί ένα πέραν της Ευρώπης συνέδριο για την προστασία της ιδιωτικής ζωής από την παρακολούθηση των τηλεπικοινωνιών, προκειμένου να δημιουργηθεί ένα πλαίσιο για ΜΚΟ από την Ευρώπη, τις ΗΠΑ και άλλα κράτη, όπου θα μπορέσουν να συζητηθούν διασυνοριακές και διεθνείς πτυχές και θα συντονισθούν τομείς δραστηριότητας και συμπεριφορές·

21. αναθέτει στην Πρόεδρό του να διαβιβάσει το παρόν ψήφισμα στο Συμβούλιο, την Επιτροπή, τις κυβερνήσεις και κοινοβούλια των κρατών μελών καθώς και στις υποψήφιες προς ένταξη χώρες και το Συμβούλιο της Ευρώπης.

ΑΙΤΙΟΛΟΓΙΚΗ ΕΚΘΕΣΗ

1. Εισαγωγή:

1.1. Αφορμή για τη σύσταση της Επιτροπής

Στις 5 Ιουλίου 2000, το Ευρωπαϊκό Κοινοβούλιο ψήφισε τη σύσταση μιας προσωρινής επιτροπής για το σύστημα ECHELON. Αφορμή υπήρξε η συζήτηση για τη μελέτη που είχε ζητήσει η STOA[1] σχετικά με το σύστημα ECHELON[2], την οποία παρουσίασε ο συντάκτης της Duncan Campbell στα πλαίσια μίας ακρόασης της Επιτροπής Ελευθεριών και Δικαιωμάτων των Πολιτών, Δικαιοσύνης και Εσωτερικών Υποθέσεων για το θέμα "Ευρωπαϊκή Ένωση και Προστασία Δεδομένων".

1.2. Οι ισχυρισμοί που εμπεριέχονται και στις δύο μελέτες της STOA σχετικά με την ύπαρξη ενός παγκοσμίου συστήματος παρακολούθησης με την ονομασία ECHELON

1.2.1. Η πρώτη έκθεση της STOA του 1997

Σε μία έκθεση, την οποία είχε ζητήσει η STOA[3] το 1997 για λογαριασμό του Ευρωπαϊκού Κοινοβουλίου από το ίδρυμα Omega Foundation με θέμα "Αξιολόγηση τεχνολογιών πολιτικού Ελέγχου", στο κεφάλαιο "εθνικά και διεθνή δίκτυα παρακολούθησης επικοινωνιών" περιέχονταν και περιγραφή του ECHELON. Ο συντάκτης της μελέτης ισχυριζόταν εν προκειμένω, ότι η NSA (η Εθνική Υπηρεσία Ασφάλειας των ΗΠΑ) υποκλέπτει συστηματικά την επικοινωνία στην Ευρώπη που διενεργείται με ηλεκτρονικό ταχυδρομείο, τηλέφωνο και τηλεομοιοτυπία[4]. Με την έκθεση αυτή, το ECHELON έγινε γνωστό σε ολόκληρη την Ευρώπη ως ένα σύστημα παρακολούθησης ευρέως φάσματος.

1.2.2. Οι εκθέσεις της STOA του 1999

Για την καλύτερη ενημέρωσή της για τα εν λόγω ζητήματα, η STOA ζήτησε το 1999 τη διεξαγωγή μίας μελέτης αποτελούμενης από πέντε μέρη, η οποία ασχολείται με την "ανάπτυξη τεχνολογιών παρακολούθησης και τους κινδύνους της κατάχρησης πληροφοριών οικονομικού περιεχομένου". Ο τόμος 2/5, που συντάχθηκε από τον Duncan Campbell, ήταν αφιερωμένος

[1] Η STOA (Scientific and Technological Options Assesment) είναι μία υπηρεσία της Γενικής Διεύθυνσης Έρευνας του Ευρωπαϊκού Κοινοβουλίου, αρμόδια για την ανάθεση ερευνών.

[2] Η παρούσα κατάσταση όσον αφορά σε θέματα τηλεπικοινωνιακής αναγνώρισης (COMINT) στην αυτοματοποιημένη επεξεργασία για σκοπούς συλλογής πληροφοριών από ελεγχόμενα πολύγλωσσα συστήματα ευρυζωνικών μισθωμένων κυκλωμάτων και από τα δημόσια δίκτυα μετάδοσης καθώς και η δυνατότητα εφαρμογής στον ορισμό και την επιλογή του προορισμού του COMINT συμπεριλαμβανομένης της γλωσσικής αναγνώρισης (Οκτώβριος 1999)

[3] Scientific and Technological Options Assesment

[4] Steve Wright, An appraisal of technologies for political control (1998), 20

στην εξέταση των δυνατοτήτων των υπηρεσιών πληροφοριών και ιδίως στον τρόπο λειτουργίας του ECHELON.[5]

Μεγάλη αναστάτωση προκάλεσε ο ισχυρισμός, ότι το ECHELON έχει ξεφύγει από τον αρχικό του σκοπό, που ήταν η άμυνα κατά του Ανατολικού Συνασπισμού, και σήμερα χρησιμοποιείται ως μέσο οικονομικής κατασκοπείας. Η θέση αυτή ενισχύεται στην έκθεση με την παράθεση παραδειγμάτων υποτιθέμενης οικονομικής κατασκοπείας. Συγκεκριμένα, αναφέρεται ότι οι εταιρίες Airbus και Thomsom CFS έχουν υποστεί ζημία.

Ως αποτέλεσμα της έκθεσης της STOA, το ECHELON συζητήθηκε σχεδόν στο σύνολο των κοινοβουλίων των κρατών μελών και μάλιστα στη Γαλλία και το Βέλγιο συντάχθηκαν σχετικές εκθέσεις.

1.3. Η εντολή της Επιτροπής

Συγχρόνως με την απόφαση σχετικά με τον διορισμό μιας επιτροπής με χρονικά περιορισμένη διάρκεια, το Ευρωπαϊκό Κοινοβούλιο προσδιόρισε και τα καθήκοντά της, δηλαδή ανέθεσε στην προσωρινή επιτροπή

"- να διερευνήσει την ύπαρξη ενός συστήματος παρακολούθησης επικοινωνιών με την ονομασία ECHELON, η δραστηριότητα του οποίου περιγράφεται στην έκθεση της STOA σχετικά με την ανάπτυξη τεχνολογίας παρακολούθησης και τους κινδύνους από την κατάχρηση πληροφοριών οικονομικού περιεχομένου,

- να αξιολογήσει τη συμβατότητα ενός τέτοιου συστήματος με το κοινοτικό δίκαιο, ιδίως με το άρθρο 286 της συνθήκης ΕΚ καθώς και τις οδηγίες 95/46/ΕΚ και 97/66/ΕΚ και το άρθρο 6 παράγραφος 2 της συνθήκης ΕΕ, λαμβανομένων υπόψη των ακόλουθων ερωτημάτων:
  - Προστατεύονται τα δικαιώματα των πολιτών της Ευρωπαϊκής Ένωσης από τις ενέργειες των υπηρεσιών πληροφοριών;
  - Η κρυπτογράφηση προσφέρει προσήκουσα και επαρκή προστασία για την εγγύηση της ιδιωτικής ζωής των πολιτών, ή πρέπει να ληφθούν πρόσθετα μέτρα, και αν ναι, τι είδους μέτρα;
  - - Πώς μπορούν να επισημανθούν καλύτερα στα όργανα της ΕΕ οι κίνδυνοι αυτών των μεθόδων, και ποια μέτρα δύνανται να ληφθούν;

- να διαπιστώσει αν η ευρωπαϊκή βιομηχανία κινδυνεύει λόγω της παγκόσμιας παρακολούθησης πληροφοριών

- ενδεχομένως, την υποβολή προτάσεων για πολιτικές και νομοθετικές πρωτοβουλίες."

1.4. Για ποιο λόγο δεν συστάθηκε εξεταστική επιτροπή;

Το Ευρωπαϊκό Κοινοβούλιο τάχθηκε υπέρ της σύστασης προσωρινής επιτροπής, διότι ο διορισμός εξεταστικής επιτροπής προβλέπεται στα πλαίσια της συνθήκης ΕΚ (άρθρο 193 συνθήκη ΕΚ) μόνον όταν πρόκειται για τον έλεγχο παραβιάσεων του κοινοτικού δικαίου, και συνεπώς η εξεταστική επιτροπή μπορεί να ασχοληθεί μόνον με θέματα που ρυθμίζονται σε αυτό. Τα θέματα που υπάγονται στο άρθρο 5 (Κοινή Εξωτερική Πολιτική και Πολιτική Ασφαλείας)

[5] Η παρούσα κατάσταση όσον αφορά σε θέματα τηλεπικοινωνιακής αναγνώρισης (COMINT) στην αυτοματοποιημένη επεξεργασία για σκοπούς συλλογής πληροφοριών από ελεγχόμενα πολύγλωσσα συστήματα ευρυζωνικών μισθωμένων κυκλωμάτων και από τα δημόσια δίκτυα μετάδοσης καθώς και η δυνατότητα εφαρμογής στον ορισμό και την επιλογή του προορισμού του COMINT συμπεριλαμβανομένης της γλωσσικής αναγνώρισης (Οκτώβριος 1999), PE 168.184.

και 6 συνθήκη ΕΕ (Αστυνομία και δικαστική συνεργασία σε ποινικές αποφάσεις) εξαιρούνται. Πέραν τούτου, οι ιδιαίτερες εξουσίες της εξεταστικής επιτροπής σχετικά με την κλήση για εξέταση και τη λήψη γνώσης εγγράφων υφίστανται κατά τη διοργανική απόφαση[6] τότε μόνον, αν δεν υπάρχουν αντίθετοι προς αυτές λόγοι απορρήτου ή δημόσιας ή εθνικής ασφάλειας, που σε κάθε περίπτωση αποκλείουν την κλήση των μυστικών υπηρεσιών προς εξέταση. Επίσης, η εξεταστική επιτροπή δεν μπορεί να διευρύνει τις εργασίες της σε τρίτες χώρες, διότι αυτές εξ ορισμού δεν μπορούν να παραβιάσουν το δίκαιο της ΕΕ. Η σύσταση εξεταστικής επιτροπής θα σήμαινε συνεπώς μόνον έναν περιορισμό ως προς το περιεχόμενο, δίχως να συνεπάγεται πρόσθετα δικαιώματα, και γι' αυτό το λόγο απορρίφθηκε από την πλειοψηφία των μελών του Ευρωπαϊκού Κοινοβουλίου.

1.5. Η μέθοδος και το σχέδιο εργασίας

Προκειμένου να καλύψει πλήρως και καθ' ολοκληρία την εντολή της, η επιτροπή επέλεξε την ακόλουθη μεθοδολογία. Σε ένα πρόγραμμα εργασίας, που προτάθηκε από τον εισηγητή και έγινε αποδεκτό από την επιτροπή, υπήρχε μία λίστα των παρακάτω σχετικών θεμάτων: 1. Βέβαια γνώση σχετικά με το ECHELON, 2. Διάλογος σε κοινοβουλευτικό και κυβερνητικό επίπεδο, 3. Υπηρεσίες πληροφοριών και δράση τους, 4. Συστήματα επικοινωνίας και η δυνατότητα παρακολούθησης τους, 5. Κρυπτογράφηση, 6. Οικονομική κατασκοπεία, 7. Στόχοι κατασκοπείας και μέτρα προστασίας και 8. Νομικό πλαίσιο και προστασία της ιδιωτικής ζωής του ατόμου. Τα θέματα συζητήθηκαν διαδοχικά στις επιμέρους συνεδριάσεις, ενώ η σειρά καθορίστηκε βάσει πρακτικών κριτηρίων και συνεπώς δεν υποδήλωνε κάποια αξιολόγηση των επιμέρους βασικών θεμάτων. Για την προετοιμασία των επιμέρους συνεδριάσεων, ο εισηγητής επεξεργαζόταν συστηματικά και αξιολογούσε το υφιστάμενο υλικό. Στις συνεδριάσεις προσκαλούνταν στη συνέχεια, ανάλογα με τις απαιτήσεις του εκάστοτε βασικού θέματος, εκπρόσωποι των εθνικών διοικήσεων (ιδίως των μυστικών υπηρεσιών) και των κοινοβουλίων με την ιδιότητά τους ως όργανα ελέγχου των μυστικών υπηρεσιών, επίσης νομικοί εμπειρογνώμονες και εμπειρογνώμονες σε θέματα επικοινωνιακής τεχνολογίας και τεχνικής παρακολούθησης, ασφάλειας επιχειρήσεων και τεχνικής κρυπτογράφησης, ως εκπρόσωποι της επιστήμης και της πράξης. Επίσης, έγινε ακρόαση δημοσιογράφων, οι οποίοι είχαν διερευνήσει το θέμα αυτό. Οι συνεδριάσεις ήταν κατά κανόνα δημόσιες, διεξάγονταν όμως κάποιες φορές κεκλεισμένων των θυρών, όταν αυτό κρινόταν σκόπιμο για λόγους άντλησης πληροφοριών. Πέραν τούτου, ο πρόεδρος της επιτροπής και ο εισηγητής μετέβησαν στο Λονδίνο και το Παρίσι για να συναντήσουν εκεί πρόσωπα, τα οποία για διάφορους λόγους δεν ήταν σε θέση να συμμετάσχουν στις συνεδριάσεις της επιτροπής, η συμπερίληψη των οποίων όμως στις εργασίες της επιτροπής κρινόταν σκόπιμη. Για τους ίδιους λόγους ο πρόεδρος της επιτροπής, οι συντονιστές και ο εισηγητής μετέβησαν στις ΗΠΑ. Επίσης, ο εισηγητής προέβη σε πολυάριθμες, εν μέρει εμπιστευτικές κατ' ιδίαν συζητήσεις.

1.6. Οι ιδιότητες που αποδίδονται στο ECHELON

Το σύστημα παρακολούθησης που ονομάζεται "ECHELON" διαφέρει από άλλα συστήματα των υπηρεσιών πληροφοριών λόγω δύο χαρακτηριστικών που του προσδίδονται:
Πρώτον, στο σύστημα αυτό αποδίδεται η δυνατότητα για μια, τρόπον τινά, απόλυτη παρακολούθηση. Υποστηρίζεται, ότι μπορεί κανείς, κυρίως με τη βοήθεια δορυφορικών

[6] Απόφαση του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου και της Επιτροπής από 19 Απριλίου 1995 σχετικά με τις λεπτομέρειες της άσκησης του δικαιώματος εξέτασης του Ευρωπαϊκού Κοινοβουλίου (95/167/ ΕΚ), άρθρο 3 παράγραφος 3-5

σταθμών λήψης και κατασκοπευτικών δορυφόρων, να υποκλέψει οποιαδήποτε πληροφορία που μεταβιβάζεται από οποιοδήποτε πρόσωπο, μέσω τηλεφώνου, τηλεομοιοτυπίας, διαδικτύου ή ηλεκτρονικού ταχυδρομείου, προκειμένου να λάβει γνώση του περιεχομένου της.

Ως δεύτερο χαρακτηριστικό του ECHELON που αναφέρεται είναι ότι το συγκεκριμένο σύστημα λειτουργεί με τη συνεργασία αρκετών κρατών (του Ηνωμένου Βασιλείου, των ΗΠΑ, του Καναδά, της Αυστραλίας και της Νέας Ζηλανδίας), γεγονός που του προσδίδει προστιθέμενη αξία σε σχέση με τα εθνικά συστήματα: τα κράτη μπορούν να θέτουν το ένα στη διάθεση του άλλου τις εγκαταστάσεις παρακολούθησης, να καλύπτουν από κοινού τις δαπάνες και να αξιοποιούν από κοινού τις πληροφορίες που αποκτούν. Η διεθνής αυτή συνεργασία είναι απαραίτητη ειδικά για την παρακολούθηση δορυφορικών συστημάτων τηλεπικοινωνίας σε παγκόσμια κλίμακα, επειδή μόνο έτσι είναι δυνατό να λαμβάνονται οι πληροφορίες και των δύο συνομιλητών. Είναι προφανές ότι οι σταθμοί δορυφορικής λήψης, εξαιτίας του μεγέθους τους, δεν είναι δυνατόν να εγκατασταθούν στην επικράτεια ενός κράτους χωρίς τη συναίνεσή του. Στη συγκεκριμένη περίπτωση απαιτείται η αμοιβαία συναίνεση και συνεργασία περισσότερων κρατών που θα βρίσκονται σε διάφορα σημεία του πλανήτη.

Ωστόσο, δεν πρέπει να βλέπουμε την απειλή που συνιστά το ECHELON μόνο στο ότι είναι ένα εξαιρετικά ισχυρό σύστημα παρακολούθησης, αλλά και στο γεγονός ότι δρα μέσα σε ένα χώρο που στερείται δικαίου. Μέσω ενός συστήματος διεθνούς παρακολούθησης σαν το ECHELON, στις περισσότερες περιπτώσεις η παρακολούθηση ενός κράτους δεν θα έπληττε τους κατοίκους του ίδιου του κράτους. Κατά συνέπεια, το θύμα της παρακολούθησης, ως αλλοδαπός, δεν διαθέτει κανενός είδους νομική προστασία εντός της χώρας και κατά συνέπεια το θύμα βρίσκεται απόλυτα στο έλεος του συγκεκριμένου συστήματος. Ο κοινοβουλευτικός έλεγχος στον εν λόγω τομέα είναι επίσης ανεπαρκής, εφ' όσον οι ψηφοφόροι, οι οποίοι θεωρούν δεδομένο ότι δεν πλήττονται οι ίδιοι αλλά "μόνο" άτομα που βρίσκονται στο εξωτερικό, δεν ενδιαφέρονται ιδιαίτερα για το ζήτημα αυτόν, ενώ οι εκλεγμένοι αντιπρόσωποί τους φροντίζουν πρώτα απ' όλα για όσα ενδιαφέρουν τους ψηφοφόρους του. Έτσι, δεν προξενεί επίσης έκπληξη το γεγονός ότι οι ακροάσεις που γίνονται στο αμερικανικό Κογκρέσο σχετικά με τις δραστηριότητες της NSA περιορίζονται απλώς στο ερώτημα αν πλήττονται από αυτό και Αμερικανοί πολίτες, ενώ αντίθετα αυτή καθ' εαυτή η ύπαρξη ενός τέτοιου συστήματος δεν προξενεί καμία αγανάκτηση. Έτσι εμφανίζεται ακόμη πιο σημαντική η εξέταση του θέματος σε ευρωπαϊκό επίπεδο.

2. Οι δραστηριότητες των υπηρεσιών πληροφοριών εξωτερικού

2.1. Εισαγωγή

Οι περισσότερες κυβερνήσεις για την εγγύηση της ασφάλειας της χώρας τους, διαθέτουν εκτός από αστυνομία και υπηρεσίες πληροφοριών. Καθώς η δράση τους είναι συνήθως μυστική, οι υπηρεσίες αυτές ονομάζονται και μυστικές. Οι εν λόγω υπηρεσίες χρησιμεύουν

- στην άντληση πληροφοριών για τη διατήρηση της εθνικής ασφάλειας
- στην αντικατασκοπία γενικότερα
- στην αντιμετώπιση κινδύνων που θα μπορούσαν να απειλήσουν τις ένοπλες δυνάμεις
- - στην άντληση πληροφοριών σχετικά με τα διαδραματιζόμενα στην αλλοδαπή

2.2. Τι είναι κατασκοπεία;

Οι κυβερνήσεις έχουν ανάγκη συστηματικής συλλογής και αξιολόγησης πληροφοριών σχετικά με συγκεκριμένα δρώμενα σε άλλες χώρες. Πρόκειται για βασικά στοιχεία για τη λήψη αποφάσεων στους τομείς της άμυνας, της εξωτερικής πολιτικής κλπ. Για το λόγο αυτό, διατηρούν υπηρεσίες πληροφοριών εξωτερικού. Οι υπηρεσίες αυτές αξιολογούν καταρχήν πληροφορίες, οι οποίες είναι προσιτές στο κοινό. Σύμφωνα με καταθέσεις, που έχει υπόψη του ο εισηγητής, αυτό αποτελεί κατά μέσο όρο τουλάχιστο το 80% της δραστηριότητας των υπηρεσιών πληροφοριών.[7] Όμως οι ιδιαίτερα σημαντικές πληροφορίες των προαναφερόμενων τομέων τηρούνται από τις κυβερνήσεις ή τις εταιρίες μυστικές, και για το λόγο αυτό δεν είναι προσπελάσιμες από το κοινό. Όποιος παρόλα αυτά θέλει να τις αποκτήσει, πρέπει να τις κλέψει. Κατασκοπεία δεν είναι άλλο παρά η οργανωμένη κλοπή πληροφοριών.

2.3. Στόχοι της κατασκοπείας

Οι συνήθεις στόχοι της κατασκοπείας είναι τα στρατιωτικά μυστικά, άλλα κυβερνητικά μυστικά ή πληροφορίες σχετικά με τη σταθερότητα ή τον κίνδυνο κυβερνήσεων. Αυτό αφορά π.χ. σε νέα οπλικά συστήματα, στρατιωτικές στρατηγικές ή πληροφορίες σχετικά με στρατιωτικές βάσεις. Οι πληροφορίες σχετικά με επικείμενες αποφάσεις στην εξωτερική πολιτική, τη νομισματική πολιτική ή οι εμπιστευτικές πληροφορίες στρατολογημένων προσώπων σχετικά με εντάσεις στο εσωτερικό μιας κυβέρνησης είναι επίσης σημαντικές. Πέραν αυτών, υπάρχει και ενδιαφέρον για πληροφορίες οικονομικής σημασίας. Σε αυτές συγκαταλέγονται, εκτός από τις πληροφορίες που αφορούν στους επιμέρους εμπορικούς κλάδους, και οι λεπτομέρειες σχετικά με νέες τεχνολογίες ή επαφές με την αλλοδαπή.

2.4. Μέθοδοι κατασκοπείας

Κατασκοπεία είναι η δημιουργία πρόσβασης σε πληροφορίες, τις οποίες ο κάτοχός τους ουσιαστικά θέλει να προστατέψει από την πρόσβαση ξένων σε αυτές. Συνεπώς, η προστασία πρέπει να υπερκεραστεί και να παραβιαστεί. Αυτό συμβαίνει τόσο στην πολιτική κατασκοπεία όσο και στην οικονομική. Για το λόγο αυτό, σε αμφότερους τους τομείς τίθενται τα ίδια

[7] Η "Commission on the Roles and Capabilities of the US Intelligence Community" διαπιστώνει στην έκθεσή της "Preparing for the 21st Century: An Appraisal of U.S. Intelligence" ότι το 95 % όλων των οικονομικών πληροφοριών προέρχονται από δημόσια προσιτές πηγές (κεφάλαιο 2 "The Role of intelligence").

προβλήματα και εφαρμόζονται οι ίδιες τεχνικές κατασκοπείας. Από λογική άποψη δεν υπάρχει καμία διαφορά, απλώς το επίπεδο προστασίας είναι στην οικονομία συνήθως μικρότερο και συνεπώς η οικονομική κατασκοπεία είναι καμιά φορά ευκολότερο να πραγματοποιηθεί. Ιδίως, η συνείδηση του κινδύνου κατά την χρήση μέσων επικοινωνίας που δύνανται να παρακολουθηθούν, στην οικονομία είναι συνήθως μειωμένη σε σχέση με ότι ισχύει για το κράτος σε εμπιστευτικούς τομείς.

2.4.1. Η συμμετοχή ανθρώπων στην κατασκοπεία

Η προστασία των εμπιστευτικών πληροφοριών οργανώνεται πάντοτε κατά τον ίδιο τρόπο:
- Μόνο λίγα, επιλεγμένα πρόσωπα έχουν πρόσβαση στις εμπιστευτικές πληροφορίες
- Για τη διάθεση των πληροφοριών αυτών υπάρχουν απαραβίαστοι κανόνες
- Οι πληροφορίες δεν εξέρχονται κατά κανόνα από την περιοχή προστασίας, και αν αυτό συμβεί, τότε μόνον κατά τρόπο ασφαλή ή κρυπτογραφημένο. Για το λόγο αυτό, η οργανωμένη κατασκοπεία επιδιώκει καταρχήν να αποκτήσει άμεση, και χωρίς διαμεσολαβητές, πρόσβαση στις επιθυμητές πληροφορίες (η λεγόμενη human intelligence). Πρόκειται για
    - Πρόσωπα της ίδιας της υπηρεσίας ή επιχείρησης (πράκτορες), που διεισδύουν,
    - Για στρατολογημένα πρόσωπα από τον ίδιο χώρο

Τα στρατολογημένα πρόσωπα εργάζονται για ξένες επιχειρήσεις ή εταιρίες συνήθως για τους παρακάτω λόγους:
- Σεξουαλική αποπλάνηση
- Δωροδοκία με χρήματα ή άλλου είδους παροχές
- Εκβιασμό
- Αναφορά σε ιδεολογίες
- Απόδοση μιας ιδιαίτερης σημασίας ή τιμής (επίκληση ανικανοποίητων αισθημάτων και αισθημάτων μειονεξίας)

Ειδική περίπτωση αποτελεί η μέθοδος εκμαίευσης πληροφοριών κατά την οποία υπό φαινομενικά αθώες περιστάσεις (συζητήσεις στο περιθώριο συνελεύσεων, σε ειδικά συνέδρια, στα μπαρ ξενοδοχείων) οι συνεργάτες υπηρεσιών, εταιριών κλπ. παραπλανούνται, με επίκληση στη ματαιοδοξία τους κλπ., ώστε να προβούν σε αποκαλύψεις.
Η συμμετοχή προσώπων έχει το πλεονέκτημα της άμεσης πρόσβασης στις επιθυμητές πληροφορίες. Έχει όμως και μειονεκτήματα:
- η αντικατασκοπία επικεντρώνεται πάντοτε σε πρόσωπα ή πράκτορες
- σε στρατολογημένα άτομα, οι αδυναμίες που αποτέλεσαν το βασικό λόγο της στρατολόγησης μπορεί να αποδεχθούν μοιραίες
- οι άνθρωποι κάνουν πάντα λάθη και ως εκ τούτου βρίσκονται κάποτε εμπλεκόμενοι σε θέματα αντικατασκοπίας

Για το λόγο αυτό γίνεται η προσπάθεια, να αντικατασταθεί, όπου είναι δυνατό, η χρησιμοποίηση πρακτόρων ή στρατολογημένων ατόμων από έναν ανώνυμο και ανεξάρτητο από πρόσωπα τρόπο κατασκοπείας. Το πιο απλό είναι εν προκειμένω η αποτίμηση ραδιοσημάτων που εκπέμπονται από εγκαταστάσεις ή οχήματα στρατιωτικής σημασίας.

2.4.2. Η αποτίμηση ηλεκτρομαγνητικών σημάτων

Η πλέον γνωστή στο κοινό μορφή κατασκοπείας με τεχνικά μέσα είναι η χρησιμοποίηση της δορυφορικής φωτογράφησης. Πέραν αυτής όμως, αναχαιτίζονται και αποτιμούνται κάθε είδους ηλεκτρομαγνητικά σήματα (η λεγόμενη signal intelligence, SIGNINT).

2.4.2.1. Ηλεκτρομαγνητικά σήματα που δεν εξυπηρετούν τις επικοινωνίες

Κάποια ηλεκτρομαγνητικά σήματα, π.χ. οι εκπομπές σταθμών ραντάρ, μπορεί να προσφέρουν στον στρατιωτικό τομέα πολύτιμες πληροφορίες σχετικά με την οργάνωση της αεροπορικής άμυνας του αντιπάλου (η λεγόμενη electronic intelligence, ELINT). Επίσης, οι ηλεκτρομαγνητικές εκπομπές, που μπορούν να δώσουν πληροφορίες σχετικά με τη θέση ομάδων, αεροπλάνων, πλοίων ή υποβρυχίων, αποτελούν πολύτιμη πηγή πληροφοριών για τις μυστικές υπηρεσίες. Επίσης έχει σημασία η παρακολούθηση κατασκοπευτικών δορυφόρων απεικόνισης, που ανήκουν σε άλλες χώρες, όπως και η εγγραφή ή η αποκωδικοποίηση των σημάτων τους.

Τα σήματα λαμβάνονται από σταθερούς σταθμούς, από χαμηλά περιφερόμενους δορυφόρους ή από οιονεί γεωστατικούς δορυφόρους SIGINT. Αυτό το μέρος της δραστηριότητας των μυστικών υπηρεσιών, που σχετίζεται με ηλεκτρομαγνητικά σήματα, καλύπτει ένα σημαντικό μέρος των δυνατοτήτων παρακολούθησης των υπηρεσιών αυτών, δίχως όμως να εξαντλούνται τα τεχνικά μέσα.

2.4.2.2. Η αποτίμηση αναχαιτισθείσας επικοινωνίας

Οι υπηρεσίες πληροφοριών εξωτερικού πολλών χωρών υποκλέπτουν τις στρατιωτικές και διπλωματικές επικοινωνίες άλλων κρατών. Κάποιες από τις υπηρεσίες αυτές παρακολουθούν μάλιστα, στο βαθμό που έχουν πρόσβαση, και τις πολιτικές επικοινωνίες άλλων κρατών. Σε αρκετές χώρες, οι υπηρεσίες έχουν το δικαίωμα να παρακολουθούν και την επικοινωνία που εισέρχεται στη χώρα ή εξέρχεται από αυτή. Στα δημοκρατικά κράτη, η παρακολούθηση της επικοινωνίας των **ιδίων** πολιτών από τις υπηρεσίες πληροφοριών υπόκειται σε συγκεκριμένους περιοριστικούς όρους και ελέγχους. Οι εθνικές νομοθεσίες προστατεύουν όμως μόνον τους πολίτες που διαμένουν στο έδαφος της δικής τους χώρας (βλ. κεφάλαιο 8).

2.5. Η δραστηριότητα ορισμένων υπηρεσιών πληροφοριών

Η δημόσια συζήτηση πυροδοτήθηκε κυρίως από τις δραστηριότητες παρακολούθησης των αμερικανικών και βρετανικών μυστικών υπηρεσιών. Η κριτική επικεντρώνεται στην παρακολούθηση και αποτίμηση επικοινωνίας (ήχος, τηλεομοιοτυπία, ηλεκτρονικό ταχυδρομείο). Για να γίνει **πολιτική** αποτίμηση, απαιτείται ένα μέτρο, βάσει του οποίου να μπορεί να αξιολογηθεί η δραστηριότητα αυτή. Ως μέτρο σύγκρισης προσφέρεται η δραστηριότητα παρακολούθησης των μυστικών υπηρεσιών στην ΕΕ. Ο παρακάτω πίνακας 1 προσφέρει μία συνοπτική εικόνα. Από αυτόν προκύπτει, ότι η παρακολούθηση ιδιωτικής επικοινωνίας από υπηρεσίες πληροφοριών εξωτερικού δεν αποτελεί ιδιαιτερότητα των αμερικανικών ή βρετανικών υπηρεσιών πληροφοριών.

Χώρα	επικοινωνίες εξωτερικού	κρατικές επικοινωνίες	πολιτικές επικοινωνίες
Βέλγιο	+	+	-
Δανία	+	+	+
Φιλανδία	+	+	+
Γαλλία	+	+	+
Γερμανία	+	+	+
Ελλάδα	+	+	-
Ιρλανδία	-	-	-
Ιταλία	+	+	+

Λουξεμβούργο	-	-	-
Ολλανδία	+	+	+
Αυστρία	+	+	-
Πορτογαλία	+	+	-
Σουηδία	+	+	+
Ισπανία	+	+	+
Ηνωμένο Βασίλειο	+	+	+
ΗΠΑ	+	+	+
Καναδάς	+	+	+
Αυστραλία	+	+	+
Νέα Ζηλανδία	+	+	+

Πίνακας 1: Δραστηριότητα παρακολούθησης των υπηρεσιών πληροφοριών της ΕΕ και των χωρών του ECHELON

Όπου οι επιμέρους στήλες υποδηλώνουν:
Στήλη 1: η εκάστοτε χώρα
Στήλη 2: παρακολούθηση επικοινωνίας εξωτερικού
Στήλη 3: παρακολούθηση κρατικών επικοινωνιών (στρατός, πρεσβείες κλπ.)
Στήλη 4: παρακολούθηση πολιτικών επικοινωνιών

3. Τεχνικοί περιορισμοί για την παρακολούθηση τηλεπικοινωνιών

3.1. Η δυνατότητα παρακολούθησης διαφόρων φορέων επικοινωνιών

Για την εξ αποστάσεως επικοινωνία μεταξύ ατόμων, απαιτείται ένας φορέας επικοινωνίας. Αυτός μπορεί να είναι:

- Αέρας (ήχος)
- Φως (συσκευή οπτικών σημάτων μορς, καλώδια οπτικών ινών)
- Ηλεκτρικό ρεύμα (τηλέγραφος, τηλέφωνο)
- Ηλεκτρομαγνητικό κύμα (ραδιοεπικοινωνίες στις πιο ετερόκλητες μορφές τους)

Ένα τρίτο πρόσωπο που αποκτά πρόσβαση στον φορέα της επικοινωνίας, μπορεί να την υποκλέψει. Η πρόσβαση μπορεί να είναι εύκολη ή δύσκολη, να είναι δυνατή από οποιονδήποτε τόπο ή μόνο από συγκεκριμένες θέσεις. Στη συνέχεια εξετάζονται δύο ακραίες περιπτώσεις: αφ' ενός οι τεχνικές δυνατότητες ενός επιτόπιου κατασκόπου και αφ' ετέρου οι δυνατότητες ενός συστήματος παρακολούθησης που λειτουργεί σε παγκόσμια κλίμακα.

3.2. Οι δυνατότητες της επιτόπιας παρακολούθησης[8]

Οποιαδήποτε επικοινωνία μπορεί να υποκλαπεί επί τόπου, εφ' όσον αυτός που κάνει την παρακολούθηση είναι αποφασισμένος να παραβεί το νόμο και το θύμα της παρακολούθησης δεν λαμβάνει μέτρα προστασίας.

- **Οι συνομιλίες** σε κλειστούς χώρους μπορούν να υποκλαπούν με την τοποθέτηση μικροφώνων (των λεγόμενων κοριών) ή με την σάρωση των δονήσεων των υαλοπινάκων των παραθύρων με την βοήθεια λέιζερ.
- **Οι οθόνες** εκπέμπουν ακτινοβολία, η οποία μπορεί να συλλεχθεί έως και σε απόσταση 30 μέτρων. Έτσι γίνεται ορατό το περιεχόμενο μιας οθόνης.
- **Το τηλέφωνο, η τηλεομοιοτυπία και το ηλεκτρονικό ταχυδρομείο** μπορούν να υποκλαπούν, εάν αυτός που κάνει την παρακολούθηση διασυνδεθεί λαθραία με τα καλώδια που εξέρχονται από το εκάστοτε κτίριο.
- Ένα **κινητό τηλέφωνο** μπορεί να υποκλαπεί από μία απόσταση έως και ..... χιλιομέτρων.
- Οι **ιδιωτικές ραδιοεπικοινωνίες VHF** μπορούν να υποκλαπούν εντός της εμβέλειας του ασυρμάτου VHF.

Οι συνθήκες για την χρήση τεχνικών μέσων κατασκοπείας επί τόπου είναι βέλτιστες, διότι οι ενέργειες παρακολούθησης μπορούν να περιοριστούν σε ένα πρόσωπο-στόχο ή αντικείμενο-στόχο και πρακτικά μπορεί να καλυφθεί σχεδόν κάθε είδος επικοινωνίας. Μειονέκτημα αποτελεί μόνον κάποιος σχετικός κίνδυνος ανακάλυψης κατά την τοποθέτηση "κοριών" ή της λαθραίας σύνδεσης στα καλώδια.

[8] Manfred Fink, Lauschziel Wirtschaft – Abhφrgefahren und –techniken, Vorbeugung und Abwehr, Richard Boorberg Verlag St??τγάρδη 1996

3.3. Οι δυνατότητες ενός συστήματος παρακολούθησης που λειτουργεί σε παγκόσμια κλίμακα

Για την διηπειρωτική επικοινωνία υπάρχουν σήμερα διάφοροι φορείς επικοινωνίας για όλα τα είδη επικοινωνίας (συνομιλία, τηλεομοιοτυπία και μετάδοση δεδομένων). Οι δυνατότητες ενός συστήματος παρακολούθησης που δρα σε παγκόσμια κλίμακα περιορίζονται από δύο παράγοντες:

- Η περιορισμένη πρόσβαση στον φορέα της επικοινωνίας
- Η αναγκαιότητα επιλεκτικού φιλτραρίσματος της επιθυμητής επικοινωνίας από μια τεράστια ποικιλία επικοινωνιών που λαμβάνουν χώρα

3.3.1. Η πρόσβαση στους φορείς επικοινωνίας

3.3.1.1. Καλωδιακή επικοινωνία

Μέσω καλωδίων λαμβάνουν χώρα όλα τα είδη επικοινωνίας (συνομιλία, τηλεομοιοτυπία, ηλεκτρονικό ταχυδρομείο, μετάδοση δεδομένων). Η καλωδιακή επικοινωνία μπορεί να υποκλαπεί μόνο όταν είναι δυνατή η πρόσβαση στο καλώδιο. Η πρόσβαση σε κάθε περίπτωση είναι εφικτή στο άκρο μιας καλωδιακής σύνδεσης, όταν αυτό το άκρο βρίσκεται εντός της επικράτειας του κράτους που κάνει την παρακολούθηση. Εντός των κρατικών συνόρων μπορούν λοιπόν **από τεχνική άποψη** να υποκλαπούν όλα τα καλώδια, εφ' όσον η παρακολούθηση επιτρέπεται από τον νόμο. Συνήθως όμως οι ξένες υπηρεσίες πληροφοριών δεν έχουν νόμιμη πρόσβαση σε καλώδια που βρίσκονται εντός της επικράτειας άλλων κρατών. Παράνομα, στην καλύτερη περίπτωση μπορούν να πραγματοποιήσουν σημειακή πρόσβαση, ενώ υφίσταται σημαντικός κίνδυνος ανακάλυψης.

Διηπειρωτικές καλωδιακές συνδέσεις υλοποιήθηκαν από την εποχή του τηλέγραφου με την βοήθεια υποθαλάσσιων καλωδίων. Η πρόσβαση σε αυτά τα καλώδια είναι πάντοτε εφικτή στο σημείο όπου αυτά εξέρχονται πάλι από το νερό. Σε περίπτωση συνεργασίας πολλών κρατών σε μια ομάδα παρακολούθησης, υπάρχει πρόσβαση σε όλα τα άκρα των καλωδιακών συνδέσεων τα οποία υπάρχουν σε αυτά τα κράτη. Το γεγονός αυτό διαδραμάτισε σημαντικό ιστορικό ρόλο, διότι το σημείο όπου τόσο τα υποθαλάσσια τηλεγραφικά καλώδια, όσο και τα πρώτα υποθαλάσσια τηλεφωνικά ομοαξονικά καλώδια μεταξύ Ευρώπης και Αμερικής εξέρχονταν από το νερό, βρισκόταν στην Νέα Γη (Newfoundland, στην καναδική επικράτεια), ενώ οι συνδέσεις με την Ασία διέρχονταν από την Αυστραλία, διότι απαιτούνταν ενδιάμεσοι ενισχυτές. Σήμερα τα καλώδια οπτικών ινών τοποθετούνται χωρίς να λαμβάνεται υπ' όψιν η τυχόν διαμόρφωση υποβρύχιων ορεινών τοπίων και χωρίς την ανάγκη ενδιάμεσων ενισχυτών, απ' ευθείας χωρίς να γίνεται ενδιάμεση στάση στην Αυστραλία και την Νέα Ζηλανδία.

Στα ηλεκτρικά καλώδια μπορεί να γίνει παρείσφρηση και μεταξύ των δύο άκρων μιας σύνδεσης επαγωγικά (δηλ. ηλεκτρομαγνητικά με την βοήθεια ενός πηνίου που έρχεται σε επαφή με το καλώδιο) χωρίς να δημιουργηθεί απ' ευθείας ηλεκτρικά αγώγιμη σύνδεση. Αυτό είναι επίσης δυνατόν να γίνει μέσω υποβρυχίων σε ηλεκτρικά υποθαλάσσια καλώδια, υπό ιδιαίτερα υψηλή δαπάνη μέσων και χρήματος. Η τεχνική αυτή χρησιμοποιήθηκε από τις ΗΠΑ για την παρείσφρηση σε ένα συγκεκριμένο υποβρύχιο καλώδιο της ΕΣΣΔ, μέσω του οποίου διέρχονταν μη κρυπτογραφημένες διαταγές για τα ρωσικά πυρηνικά υποβρύχια. Η χρήση της τεχνικής αυτής προς κάλυψη εκτάσεων είναι απαγορευτική και μόνο για οικονομικούς λόγους.

Στις χρησιμοποιούμενες σήμερα οπτικές ίνες παλαιότερης γενιάς η επαγωγική παρείσφρηση είναι δυνατή μόνο στους ενδιάμεσους ενισχυτές. Σ' αυτούς τους ενισχυτές το οπτικό σήμα μετατρέπεται σε ηλεκτρικό σήμα, το οποίο ενισχύεται και ξαναμετατρέπεται σε οπτικό σήμα. Τίθεται όμως το ερώτημα, για το πώς οι τεράστιες ποσότητες δεδομένων, οι οποίες θα μεταφερθούν από ένα τέτοιο καλώδιο από τον τόπο της παρακολούθησης στον τόπο αξιολόγησης, χωρίς να τοποθετηθεί ούτε ένα καλώδιο οπτικών ινών. Η χρήση ενός υποβρυχίου εξοπλισμένου με τις ανάλογες τεχνικές εγκαταστάσεις αξιολόγησης, εξ αιτίας της εξαιρετικής δαπάνης σε μέσα και χρήμα, προσφέρεται ως εναλλακτική δυνατότητα μόνο σε πολύ σπάνιες περιπτώσεις, όπως για παράδειγμα κατά την διάρκεια πολέμου, για την υφαρπαγή στρατηγικών στρατιωτικών επικοινωνιών του εχθρού. Όσον αφορά στην παρακολούθηση ρουτίνας των διεθνών τηλεπικοινωνιών μέσω υποβρυχίων, η γνώμη του εισηγητή είναι ότι δεν αποτελεί ενδεχόμενη εναλλακτική λύση. Τα καλώδια οπτικών ινών νέας γενιάς χρησιμοποιούν λέιζερ ερβίου ως ενδιάμεσο ενισχυτή – η ηλεκτρομαγνητική διασύνδεση με σκοπό την παρακολούθηση σε αυτούς τους ενισχυτές δεν είναι πλέον δυνατή! Η παρακολούθηση σε τέτοιου είδους καλώδια οπτικών ινών μπορεί να γίνει μόνο στα άκρα της σύνδεσης.

Στην πρακτική του εφαρμογή, για την ομάδα παρακολούθησης των λεγόμενων **χωρών του ECHELON** αυτό σημαίνει ότι στα πλαίσια εύλογων δαπανών μπορούν να υποκλέψουν μόνον στα άκρα των υποθαλάσσιων καλωδίων τα οποία καταλήγουν στην επικράτειά τους. Ουσιαστικά μπορούν λοιπόν να υφαρπάξουν μόνον καλωδιακές επικοινωνίες οι οποίες αφικνούνται ή φεύγουν από την χώρα τους! Αυτό σημαίνει, ότι η πρόσβασή τους στις καλωδιακές επικοινωνίες που εισέρχονται στην ή εξέρχονται από την χώρα **στην Ευρώπη** περιορίζεται **στην επικράτεια του Ηνωμένου Βασιλείου!** Διότι οι επικοινωνίες εσωτερικού περιορίζονται μέχρι στιγμής στο καλωδιακό δίκτυο εσωτερικού. Με την ιδιωτικοποίηση των τηλεπικοινωνιών μπορεί να υπάρχουν εξαιρέσεις – αυτές όμως είναι τμηματικές και μη προβλέψιμες!

Αυτό συνήθως ισχύει για το τηλέφωνο και την τηλεομοιοτυπία. Για την επικοινωνία μέσω του Διαδικτύου με καλώδια ισχύουν άλλοι περιορισμοί. Συνοψίζοντας μπορούν όμως να αναφερθούν οι παρακάτω περιορισμοί:

- Η επικοινωνία στο Διαδίκτυο διεκπεραιώνεται μέσω πακέτων δεδομένων, όπου τα απευθυνόμενα σε ένα παραλήπτη πακέτα μπορούν να κινηθούν μέσω διαφορετικών διαδρομών εντός του δικτύου.

- Στην αρχή της εποχής του Διαδικτύου χρησιμοποιούνταν τυχόν κενά στο ποσοστό κάλυψης του δημοσίου επιστημονικού δικτύου για την μεταβίβαση μηνυμάτων ηλεκτρονικού ταχυδρομείου. Γι' αυτό η πορεία ενός μηνύματος ήταν εντελώς απρόβλεπτη. Τα επί μέρους πακέτα κινούνταν μέσα από χαοτικές και μη προβλέψιμες διόδους. Η σημαντικότερη διεθνής σύνδεση εκείνη την εποχή ήταν το "επιστημονικό δίκτυο κορμού" μεταξύ Ευρώπης και Αμερικής.

- Με την εμπορευματοποίηση του Διαδικτύου και την εδραίωση των παροχέων υπηρεσιών Διαδικτύου προέκυψε στη συνέχεια και μια εμπορευματοποίηση του δικτύου. Οι παροχείς υπηρεσιών Διαδικτύου εκμεταλλεύονταν ή μίσθωναν δικά τους δίκτυα. Γι' αυτό επιχείρησαν σε αυξημένο βαθμό να κρατήσουν την επικοινωνία εντός του δικού τους δικτύου, για να αποφύγουν την καταβολή τελών χρήσης σε άλλους χρήστες δικτύων. Η διαδρομή επομένως ενός πακέτου δεδομένων εντός του δικτύου δεν καθορίζεται αποκλειστικά από το ποσοστό κίνησης του δικτύου, αλλά εξαρτάται επίσης και από παράγοντες κόστους.

- Ένα μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο αποστέλλεται από έναν πελάτη ενός παροχέα στον πελάτη ενός άλλου παροχέα, κατά κανόνα παραμένει στο εταιρικό δίκτυο, ακόμη και αν αυτή δεν είναι η γρηγορότερη διαδρομή. Υπολογιστές οι οποίοι αποφασίζουν σχετικά με την μεταφορά των πακέτων δεδομένων και οι οποίοι βρίσκονται στους κόμβους των δικτύων (οι λεγόμενοι "δρομολογητές", "router"), οργανώνουν την μετάβαση σε άλλα δίκτυα μέσα από συγκεκριμένα σημεία παράδοσης (τα λεγόμενα "σημεία διακλάδωσης", "switches").
- Κατά την περίοδο του επιστημονικού δικτύου κορμού, τα σημεία διακλάδωσης της παγκόσμιας επικοινωνίας του Διαδικτύου ήταν στις ΗΠΑ. Ως εκ τούτου, οι κατά τόπους υπηρεσίες πληροφοριών είχαν πρόσβαση σε σημαντικό όγκο της ευρωπαϊκής επικοινωνίας του Διαδικτύου. Σήμερα η επικοινωνία του Διαδικτύου διεκπεραιώνεται κατά πολύ μικρό μέρος μόνο μέσω των ΗΠΑ.
- Η ενδοευρωπαϊκή επικοινωνία διεκπεραιώνεται κατά μικρό μέρος μέσω ενός σημείου διακλάδωσης στο Λονδίνο, στο οποίο έχει πρόσβαση η βρετανική υπηρεσία πληροφοριών GCHQ. Το μεγαλύτερο μέρος της επικοινωνίας παραμένει εντός της ευρωπαϊκής ηπείρου. Έτσι για παράδειγμα, περισσότερο από το 95% της γερμανικής επικοινωνίας μέσω Διαδικτύου διεκπεραιώνεται μέσα από ένα σημείο διακλάδωσης στην Φρανκφούρτη.

Πρακτικά αυτό σημαίνει ότι οι χώρες του ECHELON διαθέτουν πρόσβαση μόνο σε ένα **πολύ περιορισμένο μέρος** της καλωδιακής επικοινωνίας του Διαδικτύου.

3.3.1.2. Ραδιοεπικοινωνίες[9]

Η δυνατότητα παρακολούθησης των ραδιοεπικοινωνιών εξαρτάται από την εμβέλεια των χρησιμοποιούμενων ηλεκτρομαγνητικών κυμάτων. Εάν τα ραδιοκύματα της εκπομπής έχουν πορεία κατά μήκος της επιφάνειας της γης (τα λεγόμενα **κύματα εδάφους** ή **επιφανείας**), τότε η εμβέλειά τους είναι περιορισμένη και εξαρτάται από το είδος του τοπίου, από τα κτίσματα και τη βλάστηση. Εάν τα ραδιοκύματα μεταδίδονται προς το διάστημα (τα λεγόμενα **έμμεσα ραδιοκύματα** ή **κύματα χώρου**), τότε το κύμα χώρου, μετά από ανάκλαση σε στρώματα της ιονόσφαιρας, μπορεί να καλύψει σημαντικές αποστάσεις. Η εμβέλεια αυξάνεται σε σημαντικό βαθμό με πολλαπλές ανακλάσεις.

Η εμβέλεια εξαρτάται από το μήκος κύματος:

- Τα κύματα πολύ χαμηλών συχνοτήτων και τα μακρά κύματα (3kHz – 300kHz) μεταδίδονται μόνο μέσω κύματος εδάφους, διότι το κύμα χώρου δεν ανακλάται. Έχουν μικρές εμβέλειες
- Τα μεσαία κύματα (300kHz-3 MHz) διαδίδονται μέσω κύματος εδάφους και τη νύχτα επίσης μέσω κύματος χώρου. Έχουν μεσαίες εμβέλειες.
- Τα βραχέα κύματα (3MHz-30 MHz) διαδίδονται κατά κύριο λόγο μέσω του κύματος χώρου και εξ αιτίας των πολλαπλών ανακλάσεων επιτρέπουν την **παγκόσμια** λήψη.
- Τα κύματα πολύ υψηλών συχνοτήτων (30 MHz-300MHz) διαδίδονται μόνον ως κύμα εδάφους, διότι το κύμα χώρου δεν ανακλάται. Διαδίδονται κατά σχετικά ευθύγραμμο

[9] U. Freyer, Nachrichtenóbertragungstechnik, Hanser Verlag 2000

τρόπο, όπως το φως, και γι' αυτό η εμβέλειά τους εξαρτάται λόγω της καμπυλότητας της γης από το ύψος των κεραιών του πομπού και του δέκτη. Ανάλογα με την ισχύ, έχουν εμβέλειες μέχρι και 100 χλμ. (στα κινητά τηλέφωνα περίπου 30 χλμ.).

- Τα δεκατομετρικά κύματα και τα εκατοστομετρικά κύματα (30MHz-30 GHz) διαδίδονται περισσότερο από τα κύματα πολύ υψηλών συχνοτήτων οιονεί οπτικά. Μπορούν εύκολα να διαμορφωθούν σε δέσμες κυμάτων και επιτρέπουν κατευθυντικές μεταδόσεις με χαμηλή ισχύ (εδαφοπαγείς κατευθυντικές ραδιοζεύξεις). Η λήψη τους γίνεται μόνο με κεραία η οποία βρίσκεται πολύ κοντά και παράλληλα προς την διαδρομή των κυμάτων της κατευθυντικής ραδιοζεύξης ή βρίσκεται εντός της διαδρομής των κυμάτων της κατευθυντικής ραδιοζεύξης ή στην προέκτασή της.

Τα μακρά και τα μεσαία κύματα χρησιμοποιούνται μόνο σε πομπούς ραδιοφωνικών σταθμών, ραδιοφάρους, κ.λπ. Οι στρατιωτικές και πολιτικές ραδιοεπικοινωνίες λαμβάνουν χώρα μέσω βραχέων κυμάτων και προ πάντων μέσω κυμάτων πολύ υψηλών συχνοτήτων και δεκατομετρικών/εκατοστομετρικών κυμάτων.

Από τα παραπάνω προκύπτει ότι ένα σύστημα παρακολούθησης επικοινωνιών που δρα σε παγκόσμια κλίμακα, μπορεί να χρησιμοποιήσει μόνο τις ραδιοεπικοινωνίες των βραχέων κυμάτων. Σε όλα τα άλλα είδη ραδιοεπικοινωνιών ο σταθμός παρακολούθησης θα πρέπει να βρίσκεται σε απόσταση 100 χλμ. ή και μικρότερη (π.χ. σε ένα πλοίο ή σε μια πρεσβεία).

Πρακτικά αυτό σημαίνει ότι οι χώρες του ECHELON έχουν πρόσβαση μόνο σε ένα πολύ περιορισμένο τμήμα των ραδιοεπικοινωνιών.

3.3.1.3. Επικοινωνίες που μεταδίδονται με γεωστατικούς τηλεπικοινωνιακούς δορυφόρους[10]

Τα δεκατομετρικά και εκατοστομετρικά κύματα όπως προαναφέρθηκε μπορούν να συμπτυχθούν εύκολα σε λεπτές δέσμες για κατευθυντικές ραδιοζεύξεις. Εάν δημιουργήσει κανείς μια κατευθυντική ραδιοζεύξη με έναν στατικό τηλεπικοινωνιακό δορυφόρο υψηλής τροχιάς, ο οποίος λαμβάνει τα σήματα της κατευθυντικής ραδιοζεύξης, τα μετατρέπει και τα επανεκπέμπει στη γη, μπορεί έτσι χωρίς την χρήση καλωδίων να καλύψει μεγάλες αποστάσεις. Η εμβέλεια μιας τέτοιας σύνδεσης περιορίζεται ουσιαστικά μόνο από το γεγονός ότι ο δορυφόρος δεν μπορεί να λαμβάνει και να εκπέμπει παρακάμπτοντας την υδρόγειο σφαίρα. Ως εκ τούτου, για να εξασφαλιστεί η παγκόσμια κάλυψη χρησιμοποιούνται περισσότεροι δορυφόροι (σχετικές λεπτομέρειες στο κεφάλαιο 4). Εάν οι χώρες του ECHELON διατηρούν σταθμούς παρακολούθησης στις απαραίτητες περιοχές του πλανήτη, κατ' αρχήν είναι σε θέση να υποκλέψουν το σύνολο των διακινούμενων μέσα από τέτοιους δορυφόρους επικοινωνίες τηλεφωνίας, τηλεομοιοτυπίας και μετάδοσης δεδομένων.

3.3.1.4. Οι δυνατότητες παρακολούθησης από αεροπλάνα και πλοία

Είναι γνωστό εδώ και πολύ καιρό ότι τα ειδικά αεροσκάφη του τύπου AWACS χρησιμοποιούνται για τον εντοπισμό άλλων αεροσκαφών. Το ραντάρ αυτών των σκαφών διαθέτει ένα σύστημα εντοπισμού για την ταυτοποίηση αναγνωρισθέντων στόχων, το οποίο είναι σε θέση να εντοπίζει, να ταξινομεί και να συσχετίζει ηλεκτρονικές εκπομπές με επαφές ραντάρ. Δεν υπάρχει ειδική δυνατότητα παρακολούθησης σημάτων (SIGNINT)[11]. Αντιθέτως, το κινούμενο με χαμηλές ταχύτητες κατασκοπευτικό αεροσκάφος του αμερικανικού ναυτικού EP-

[10] Hans Dodel, Satellitenkommunikation, Hóthig Verlag 1999

[11] Επιστολή του Υφυπουργού του Ομοσπονδιακού Υπουργείου Άμυνας Walter Kolbow από 14.2.2001

3, διαθέτει δυνατότητες παρακολούθησης μικροκυμάτων, κυμάτων πολύ υψηλών συχνοτήτων Υ, όπως επίσης και βραχέων κυμάτων. Τα σήματα αξιολογούνται άμεσα πάνω στο αεροσκάφος, το οποίο είναι για καθαρά στρατιωτική χρήση[12].

Πέραν αυτού χρησιμοποιούνται και ναυτικά σκάφη επιφανείας, όπως επίσης και υποβρύχια σκάφη για παράκτιες αποστολές κοντά στα κράτη-στόχους προς παρακολούθηση των στρατιωτικών ραδιοεπικοινωνιών[13].

3.3.1.5. Οι δυνατότητες παρακολούθησης από κατασκοπευτικούς δορυφόρους

Τα ραδιοκύματα, εφ' όσον δεν διαμορφώνονται με την βοήθεια αντίστοιχων κεραιών σε δέσμες, εκπέμπουν προς όλες τις κατευθύνσεις, δηλαδή και προς το διάστημα. Δορυφόροι Παρακολούθησης Σημάτων (Signal Intelligence Satellites) κινούμενοι σε χαμηλές τροχιές είναι σε θέση να παρακολουθήσουν τον προς αναγνώριση πομπό μόνο για λίγα λεπτά κάθε φορά. Σε πυκνοκατοικημένες, υψηλής βιομηχανικής ανάπτυξης περιοχές, εξ αιτίας της μεγάλης συγκέντρωσης πομπών της ίδιας συχνότητας η παρακολούθηση δυσχεραίνεται σε τόσο μεγάλο βαθμό, ώστε είναι δύσκολο να φιλτραριστούν μεμονωμένα σήματα.[14] Οι δορυφόροι αυτοί δεν είναι κατάλληλοι για την συνεχή παρακολούθηση πολιτικών ραδιοεπικοινωνιών.
Παράλληλα υπάρχουν οι υψηλά σταθμευμένοι (στα 42.000 χλμ.), λεγόμενοι οιονεί στατικοί δορυφόροι παρακολούθησης σημάτων SIGNIT των ΗΠΑ.[15] Σε αντίθεση με τους γεωστατικούς τηλεπικοινωνιακούς δορυφόρους, αυτοί οι δορυφόροι έχουν μια κλίση 3 έως 10 βαθμών, απόγειο 39.000 έως 42.000 χλμ. και περίγειο από 30.000 έως 33.000 χλμ. Για το λόγο αυτό, οι δορυφόροι δεν βρίσκονται ακίνητοι σε τροχιά γύρω από την γη, αλλά κινούνται σε μια πολύπλοκη ελλειπτική τροχιά. Έτσι κατά την διάρκεια μια ημέρας καλύπτουν μεγαλύτερη περιοχή και επιτρέπουν τον προσδιορισμό της θέσης πηγών ραδιοσημάτων. Αυτό, όπως επίσης και τα άλλα δημόσια προσβάσιμα χαρακτηριστικά των δορυφόρων παραπέμπουν σε καθαρά στρατιωτική χρήση τους.

Τα ληφθέντα σήματα μεταβιβάζονται μέσω κατερχόμενης κατευθυντικής ζεύξης που εστιάζεται στενά σε ένα συγκεκριμένο σημείο με 24 GHz στον σταθμό λήψης.

3.3.2. Δυνατότητες αυτόματης αξιολόγησης της υποκλαπείσας επικοινωνίας: η χρήση φίλτρων

Στην παρακολούθηση των επικοινωνιών εξωτερικού δεν παρακολουθείται μια συγκεκριμένη τηλεφωνική σύνδεση. Μάλλον καταγράφεται η πλήρης ή ένας μέρος της μεταβιβαζόμενης από τον παρακολουθούμενο δορυφόρο ή το παρακολουθούμενο καλώδιο επικοινωνίας και φιλτράρεται από ηλεκτρονικούς υπολογιστές με την χρήση λέξεων κλειδιών. Διότι η αξιολόγηση όλης της καταγεγραμμένης επικοινωνίας είναι εντελώς αδύνατη.

Το φιλτράρισμα των επικοινωνιών συγκεκριμένων συνδέσεων γίνεται εύκολα. Με την βοήθεια λέξεων κλειδιών μπορούν να εντοπιστούν εξειδικευμένα επίσης μηνύματα τηλεομοιοτυπίας και ηλεκτρονικού ταχυδρομείου. Ακόμη και μια συγκεκριμένη φωνή μπορεί να εντοπιστεί, εφ' όσον

[12] Sóddeutsche Zeitung ??. 80, ap? 5.4.2001, s. 6

[13] Jeffrey T. Richelson, The U.S. Intelligence Community, Ballinger, Νέα Υόρκη 1989, σ. 188 , σ. 190

[14] Επιστολή του Υφυπουργού του Ομοσπονδιακού Υπουργείου Άμυνας Walter Kolbow από 14.2.2001

[15]Major Andronov, Zarubezhnoye voyennoye obozreniye, αριθ. 12, 1993, σ. 37-43

το σύστημα έχει εκπαιδευτεί στην αναγνώριση της φωνής αυτής[16] Αντιθέτως, σύμφωνα με τα δεδομένα που διαθέτει ο εισηγητής προς το παρόν δεν υπάρχει η δυνατότητα προς αυτόματη αναγνώριση λέξεων οι οποίες εκφέρονται από μια τυχαία φωνή. Οι δυνατότητες του φιλτραρίσματος πέραν αυτού περιορίζονται και από άλλους παράγοντες: από την πεπερασμένη δυναμικότητα των ηλεκτρονικών υπολογιστών, από το γλωσσικό πρόβλημα, και προ πάντων από τον περιορισμένο αριθμό ειδικών αξιολογητών, οι οποίοι είναι σε θέση να διαβάσουν και να αξιολογήσουν τα φιλτραρισμένα μηνύματα.

Κατά την αξιολόγηση των δυνατοτήτων των συστημάτων φιλτραρίσματος θα πρέπει να συνυπολογιστεί επίσης ότι οι συνολικές τεχνικές δυνατότητες ενός τέτοιου συστήματος παρακολούθησης, το οποίο λειτουργεί βάσει της "αρχής της ηλεκτρικής σκούπας", κατανέμονται σε διάφορα θέματα. Ένα μέρος των λέξεων-κλειδιών σχετίζεται με την στρατιωτική ασφάλεια, ένα μέρος με το εμπόριο ναρκωτικών και με άλλες μορφές του διεθνούς εγκλήματος, ένα μέρος προέρχεται από το λεξιλόγιο εννοιών του εμπορίου εμπορευμάτων διπλής χρήσης (dual-use), ενώ ένα άλλο μέρος έχει να κάνει με την τήρηση διαφόρων εμπάργκο. Ένα μέρος των εννοιών-κλειδιών έχει να κάνει επίσης με την οικονομία. Αυτό σημαίνει, ότι οι δυνατότητες του συστήματος εκτείνονται σε πολλαπλούς τομείς. Ο περιορισμός των λέξεων-κλειδιών μόνο στον τομέα που παρουσιάζει οικονομικό ενδιαφέρον δεν θα αντιτίθονταν μόνον στις απαιτήσεις της πολιτικής ηγεσίας από τις υπηρεσίες. Ακόμη και μετά το τέλος του ψυχρού πολέμου δεν πραγματοποιήθηκε κάτι παρόμοιο[17]

3.3.3. Το παράδειγμα της γερμανικής Ομοσπονδιακής Υπηρεσίας Πληροφοριών

Το τμήμα 2 της γερμανικής ομοσπονδιακής υπηρεσίας πληροφοριών προμηθεύεται πληροφορίες μέσω της παρακολούθησης επικοινωνιών εξωτερικού. Αυτό υπήρξε αντικείμενο ελέγχου από το γερμανικό συνταγματικό δικαστήριο. Οι δημοσιοποιημένες κατά την δίκη λεπτομέρειες[18] μαζί με τις δηλώσεις του Ernst Uhrlau, συντονιστή των Μυστικών Υπηρεσιών στην Ομοσπονδιακή Καγκελαρία ενώπιον της επιτροπής ECHELON στις 21.11.2000 παρέχουν μια εικόνα των δυνατοτήτων των υπηρεσιών πληροφοριών κατά την παρακολούθηση δορυφορικών επικοινωνιών.

Οι δυνατότητες άλλων υπηρεσιών πληροφοριών, εξ αιτίας του δικαιώματος πρόσβασης στις καλωδιακές επικοινωνίες ή λόγω μεγαλύτερου αριθμού προσωπικού αξιολόγησης μπορεί να είναι εν μέρει μεγαλύτερες σε επί μέρους σημεία. Ειδικότερα, όταν συμπεριλαμβάνονται οι καλωδιακές μεταφορές, αυξάνεται η στατιστική πιθανότητα επιτυχίας αναγνώρισης, όχι οπωσδήποτε όμως και ο αριθμός των αξιολογήσιμων κινήσεων. Ουσιαστικά, βάσει του παραδείγματος της γερμανικής Ομοσπονδιακής Υπηρεσίας Πληροφοριών είναι εμφανές για τον εισηγητή κατά παραδειγματικό τρόπο, ποιες είναι οι δυνατότητες και στρατηγικές των υπηρεσιών πληροφοριών του εξωτερικού κατά την παρακολούθηση της επικοινωνίας εξωτερικού, ακόμη και αν δεν αποκαλύπτονται από αυτές.

Η ομοσπονδιακή υπηρεσία πληροφοριών προσπαθεί με **στρατηγικό** έλεγχο των τηλεπικοινωνιών να προμηθευτεί από το εξωτερικό πληροφορίες σχετικά με το εξωτερικό. Γι'

[16] Ιδιωτική πληροφορία προς τον εισηγητή, η πηγή προστατεύεται

[17] Ιδιωτική πληροφορία προς τον εισηγητή, πηγή προστατεύεται

[18] BverfG, 1 BvR 2226/94 από 14.7.1999, Εδάφιο 1

αυτό τον σκοπό με την χρήση μιας σειράς λέξεων αναζήτησης (οι οποίες θα πρέπει στην Γερμανία να εγκριθούν από την λεγόμενη επιτροπή G10[19]) γίνεται αναχαίτιση και διερεύνηση της δορυφορικής επικοινωνιακής κίνησης. Η σύνθεσή της παρουσιάζεται περίπου ως εξής (αριθμοί του έτους 2000): από τις περίπου 10 εκατομμύρια διεθνείς ζεύξεις επικοινωνίας ημερησίως, οι οποίες πραγματοποιούνται από και προς τη Γερμανία, περίπου 800.000 διεκπεραιώνονται μέσω δορυφόρου. Από αυτές σχεδόν το 10% (75.000) φιλτράρονται από μια μηχανή αναζήτησης. Ο περιορισμός αυτός κατά την γνώμη του εισηγητή δεν προκύπτει από το νόμο (θεωρητικά, τουλάχιστον πριν από την δίκη ενώπιον του συνταγματικού δικαστηρίου θα ήταν δυνατή η χρήση του 100%), αλλά τεχνικά, εξ αιτίας άλλων περιορισμών, π.χ. της περιορισμένης δυναμικότητας αξιολόγησης.

Και ο αριθμός των λέξεων αναζήτησης που επιδέχονται χειρισμό περιορίζεται από τεχνικής απόψεως, όπως και λόγω της επιφύλαξης έγκρισης. Στο σκεπτικό της αποφάσεως του ομοσπονδιακού συνταγματικού δικαστηρίου παράλληλα με τις καθαρά τυπικές λέξεις αναζήτησης (συνδέσεις αλλοδαπών ή εταιριών στο εξωτερικό), αναφέρονται 2.000 λέξεις αναζήτησης στον τομέα της παράνομης διάδοσης πυρηνικών όπλων, 1.000 λέξεις αναζήτησης στον τομέα του εμπορίου στρατιωτικού εξοπλισμού, 500 λέξεις αναζήτησης στον τομέα της τρομοκρατίας και 400 λέξεις στον τομέα του εμπορίου ναρκωτικών. Στην τρομοκρατία και το εμπόριο ναρκωτικών πάντως η διαδικασία δεν αποδείχτηκε ως πολύ επιτυχής.

Η μηχανή αναζήτησης ελέγχει αν υπάρχει επιτυχής αναγνώριση των εγκεκριμένων εννοιών αναζήτησης στα μηνύματα τηλεομοιοτυπίας και τέλεξ. Προς το παρόν δεν υπάρχει δυνατότητα για την αυτόματη αναγνώριση λέξεων μέσα από συνδυασμούς γλωσσών. Εφ' όσον δεν γίνει επιτυχής αναγνώριση των λέξεων αναζήτησης τεχνικά τα μηνύματα ρίχνονται στον κάδο απορριμμάτων. Δεν επιτρέπεται να αξιολογηθούν, καθότι δεν υπάρχει νομική βάση γι' αυτό. Ημερησίως προκύπτουν περίπου 5 επικοινωνίες συμμετεχόντων στις τηλεπικοινωνίες που εμπίπτουν στην προστασία του γερμανικού συντάγματος. Η στρατηγική αναγνώριση της ομοσπονδιακής υπηρεσίας πληροφοριών αποβλέπει στην εύρεση επί μέρους τμημάτων ενός μωσαϊκού, ως ενδείξεις προς περαιτέρω διερεύνηση. Ο στόχος της δεν είναι η απόλυτη παρακολούθηση των επικοινωνιών εξωτερικού. Σύμφωνα με τα δεδομένα που βρίσκονται στην διάθεση του εισηγητή το ίδιο ισχύει επίσης για την δραστηριότητα παρακολούθησης σημάτων άλλων υπηρεσιών πληροφοριών του εξωτερικού.

[19] Νόμος περί περιορισμού του απορρήτου επιστολών, του ταχυδρομικού απορρήτου και του απορρήτου των τηλεπικοινωνιών (Νόμος του άρθρου 10 του Θεμελιώδους Νόμου) από 13.8.1968

4. Η τεχνολογία των δορυφορικών επικοινωνιών

4.1. Η σημασία των τηλεπικοινωνιακών δορυφόρων

Οι τηλεπικοινωνιακοί δορυφόροι αποτελούν σήμερα ένα αναπόσπαστο μέρος του παγκόσμιου δικτύου τηλεπικοινωνιών και της τροφοδοσίας με τηλεοπτικά και ραδιοφωνικά προγράμματα, όπως επίσης και υπηρεσιών πολυμέσων. Παρ' όλα αυτά το μερίδιο της δορυφορικής κίνησης στην διεθνή επικοινωνία κατά τα τελευταία έτη μειώθηκε έντονα στην κεντρική Ευρώπη. Σε μερικές περιοχές σήμερα είναι μάλιστα κάτω από 10 %[20]. Αυτό σχετίζεται με τα προτερήματα των καλωδίων οπτικών ινών, τα οποία μπορούν να διεκπεραιώσουν ασύγκριτα μεγαλύτερη ποσότητα κινήσεων με καλύτερη ποιότητα σύνδεσης.

Η επικοινωνία σήμερα και στον τομέα της ομιλίας είναι ψηφιακή. Η χωρητικότητα των ψηφιακών συνδέσεων μέσω δορυφόρων περιορίζεται ανά αναμεταδότη σε **1.890** κανάλια ομιλίας με το πρότυπο ISDN (64 kbits/δευτ.). Συγκριτικά, μπορούν σήμερα σε μια μοναδική οπτική ίνα να μεταδοθούν **241.920** κανάλια ομιλίας με το ίδιο πρότυπο. Αυτό αντιστοιχεί σε αναλογία **1:128**!

Σ' αυτό προστίθεται ότι η ποιότητα μέσω δορυφόρου είναι χειρότερη απ' αυτή μέσω των θαλάσσιων καλωδίων οπτικών ινών. Οι απώλειες ποιότητας λόγω της μεγάλης καθυστέρησης των σημάτων που ανέρχεται σε μερικές εκατοντάδες χιλιοστά του δευτερολέπτου δεν γίνονται αντιληπτές σε κανονική μετάδοση ομιλίας – παρότι γίνονται αισθητές. Σχετικά με τις συνδέσεις μετάδοσης δεδομένων και τηλεομοιοτυπίας, οι οποίες διεκπεραιώνονται μέσω μιας περίπλοκης "διαδικασίας χειραψίας", όσον αφορά στην ασφάλεια της σύνδεσης το καλώδιο έχει φανερά πλεονεκτήματα. Την ίδια στιγμή όμως μόνο το 15% του παγκόσμιου πληθυσμού είναι συνδεδεμένο στο παγκόσμιο καλωδιακό δίκτυο[21].

Γι' αυτό σε μερικές εφαρμογές τα δορυφορικά συστήματα μακροπρόθεσμα θα είναι πιο συμφέροντα από το καλώδιο. Αναφέρονται μερικά παραδείγματα από τον πολιτικό τομέα:

- Εθνικές, περιφερειακές και διεθνείς επικοινωνίες τηλεφωνίας και μετάδοσης δεδομένων σε περιοχές με μικρό επικοινωνιακό όγκο, δηλ. εκεί όπου η υλοποίηση μιας καλωδιακής σύνδεσης δεν θα ήταν συμφέρουσα λόγω έλλειψης κίνησης.
- Χρονικά περιορισμένη επικοινωνία σε αποστολές επέμβασης σε περίπτωση καταστροφών, εκδηλώσεις, μεγάλα εργοτάξια, κ.λπ.
- Αποστολές του ΟΗΕ σε περιοχές με υπανάπτυκτη τηλεπικοινωνιακή υποδομή.
- Ευέλικτη/κινητή επικοινωνία οικονομικών εφαρμογών, με τερματικά που διαθέτουν κεραίες πολύ μικρού ανοίγματος (V-SATs, βλ. παρακάτω)

Αυτό το φάσμα χρήσεων των δορυφόρων στην επικοινωνία προκύπτει από τα παρακάτω χαρακτηριστικά: Η εκπομπή ενός και μοναδικού γεωστατικού δορυφόρου μπορεί να καλύψει σχεδόν το 50% της επιφάνειας της γης. Ακόμη και δύσβατα εδάφη μπορούν να καλυφθούν. Σε αυτή την περιοχή καλύπτεται τότε το 100% των χρηστών, ανεξάρτητα εάν αυτοί βρίσκονται στη

[20] Βλ. αιτιολόγηση σχετικά με την αλλαγή του νόμου G10 στη Γερμανία

[21] Αρχική σελίδα της Deutsche Telekom: www.detesat.com/deutsch/

στεριά, στη θάλασσα ή στον αέρα. Οι δορυφόροι μέσα σε λίγους μήνες είναι έτοιμοι προς λειτουργία, ανεξάρτητα από την επιτόπια υποδομή, είναι πιο αξιόπιστοι από το καλώδιο και μπορούν αν αντικατασταθούν ευκολότερα.

Αρνητικά θα πρέπει να εκτιμηθούν τα παρακάτω χαρακτηριστικά της δορυφορικής επικοινωνίας: οι σχετικά μεγάλες καθυστερήσεις του σήματος, η απώλεια διάδοσης, ο συγκριτικά με το καλώδιο μικρότερος χρόνος ζωής 12 έως 15 ετών, η μεγαλύτερη πιθανότητα βλαβών, όπως επίσης και η ευκολία παρακολούθησης.

4.2. Ο τρόπος λειτουργίας μιας δορυφορικής ζεύξης

Τα μικροκύματα όπως προαναφέρθηκε (βλ. κεφάλαιο 3) με τη βοήθεια των αντίστοιχων κεραιών μπορούν εύκολα να διαμορφωθούν σε στενές δέσμες κυμάτων. Γι' αυτό υπάρχει η δυνατότητα αντικατάστασης των καλωδίων με διαδρομές κατευθυντικής ραδιοζεύξης. Εάν η κεραία εκπομπής και λήψης δεν βρίσκονται πάνω στο ίδιο επίπεδο, αλλά όπως στην περίπτωση της γης πάνω στην επιφάνεια μιας σφαίρας, τότε η κεραία λήψης, από μια ορισμένη απόσταση και πάνω, εξ αιτίας της καμπυλότητας της γης "χάνεται" κάτω από τον ορίζοντα. Οι δύο κεραίες τότε δεν "βλέπονται" πια μεταξύ τους. Αυτό θα συνέβαινε επί παραδείγματι σε μια διηπειρωτική διαδρομή κατευθυντικής ραδιοζεύξης μεταξύ Ευρώπης και ΗΠΑ. Οι κεραίες θα έπρεπε να είναι τοποθετημένες σε ιστούς ύψους 1,8 χλμ. για να μπορέσουν να αποκαταστήσουν μια σύνδεση. Και μόνο γι' αυτόν το λόγο δεν μπορεί να υλοποιηθεί μια τέτοια διηπειρωτική διαδρομή κατευθυντικής ραδιοζεύξης, χωρίς να λαμβάνεται υπ' όψιν η απώλεια από τον αέρα και τους υδρατμούς κατά μήκος της διαδρομής των κυμάτων. Εάν αντίθετα υπάρχει η δυνατότητα να στηθεί σε μεγάλο ύψος στο διάστημα σε μια "σταθερή θέση" ένα είδος κατόπτρου για την κατευθυντική ραδιοζεύξη, τότε παρά την ύπαρξη της καμπυλότητας της γης μπορούν να καλυφθούν μεγάλες αποστάσεις, κατά τον ίδιο τρόπο όπως με την βοήθεια ενός σταθερού καθρέφτη οδικής κυκλοφορίας μπορεί κανείς να ελέγξει πίσω από στροφές. Η θεωρητική αρχή που μόλις περιγράφηκε υλοποιείται με τη χρήση των λεγόμενων γεωστατικών δορυφόρων.

4.2.1. Γεωστατικοί δορυφόροι

Ένας δορυφόρος που περιστρέφεται παράλληλα προς τον ισημερινό σε κυκλική τροχιά μιας περιστροφής γύρω από τη γη ανά 24 ώρες, ακολουθεί ακριβώς την περιστροφική πορεία της γης. Σε σχέση με την επιφάνεια της γης, παραμένει ακίνητος σε ύψος 36.000 χιλιομέτρων, δηλ. βρίσκεται σε **γεωστατική** θέση. Σε αυτό τον τύπο δορυφόρων ανήκουν οι περισσότεροι τηλεπικοινωνιακοί και τηλεοπτικοί δορυφόροι

4.2.2. Η διαδρομή του σήματος μιας δορυφορικής επικοινωνιακής σύνδεσης

Η μετάδοση σημάτων μέσω δορυφόρων μπορεί να περιγραφεί ως εξής:

Το προερχόμενο από αγωγό σήμα μεταδίδεται στον δορυφόρο από έναν σταθμό εδάφους με παραβολική κεραία μέσω μιας προσανατολισμένης προς τα πάνω σύνδεσης κατευθυντικής ραδιοζεύξης, το λεγόμενο **uplink** (ανερχόμενη ζεύξη). Ο δορυφόρος λαμβάνει το σήμα, το ενισχύει και το μεταδίδει μέσω μιας προσανατολισμένης προς τα κάτω σύνδεσης κατευθυντικής ραδιοζεύξης, το λεγόμενο **downlink** (κατερχόμενη ζεύξη), πίσω σε έναν άλλο σταθμό εδάφους. Από εκεί το σήμα μεταφέρεται πάλι πίσω σε ένα καλωδιακό δίκτυο.

Στις κινητές επικοινωνίες το σήμα μεταδίδεται απευθείας από την κινητή μονάδα επικοινωνίας στο δορυφόρο και από εκεί μπορεί μέσω ενός σταθμού εδάφους να τροφοδοτηθεί πάλι σε έναν αγωγό, ή και να μεταδοθεί πάλι απευθείας σε άλλη κινητή μονάδα.

4.2.3. Τα σημαντικότερα υφιστάμενα δορυφορικά επικοινωνιακά συστήματα

Οι προερχόμενες από τα **καλωδιακά δίκτυα δημόσιας πρόσβασης** (όχι απαραιτήτως κρατικά) επικοινωνίες μεταδίδονται, αν χρειαστεί, μέσω δορυφορικών συστημάτων διαφορετικής έκτασης από και προς σταθερούς σταθμούς εδάφους και στην συνέχεια τροφοδοτούνται πάλι σε καλωδιακά δίκτυα. Διακρίνουμε ανάμεσα σε:

- παγκόσμια (π.χ. INTELSAT)

- περιφερειακά (ηπειρωτικά) (π.χ. EUTELSAT)

- εθνικά (π.χ. ITALSAT)

δορυφορικά συστήματα.

Οι περισσότεροι από αυτούς τους δορυφόρους βρίσκονται σε γεωστατική θέση. Σε παγκόσμια κλίμακα 120 ιδιωτικές εταιρίες διατηρούν στο σημείο αυτό περίπου 1.000 δορυφόρους[22].

Παράλληλα, για τις περιοχές μεγάλου γεωγραφικού πλάτους κοντά στο Βορρά, υπάρχουν δορυφόροι σε ειδική τροχιά μεγάλης εκκεντρικότητας (ρωσικές τροχιές Molnyia), στην οποία οι δορυφόροι κατά το ήμισυ του χρόνου περιφοράς τους είναι ορατοί από τον χρήστη στις περιοχές μεγάλου γεωγραφικού πλάτους κοντά στον Βορρά. Έτσι με δύο δορυφόρους επιτυγχάνεται τοπική κάλυψη, η οποία δεν είναι δυνατόν να υλοποιηθεί από μια γεωστατική θέση πάνω από τον Ισημερινό.

Πέραν αυτού υπάρχει στο παγκόσμιας κλίμακας σύστημα INMARSAT ένα **σύστημα κινητών επικοινωνιών**, το οποίο αρχικά δημιουργήθηκε για χρήση στην θάλασσα, με το οποίο μπορούν να δημιουργηθούν δορυφορικές συνδέσεις παντού στον κόσμο. Λειτουργεί επίσης με γεωστατικούς δορυφόρους.

Το σύστημα δορυφορικής κινητής τηλεφωνίας το οποίο λειτουργεί σε παγκόσμια κλίμακα με τη χρήση πολλαπλών περιφερόμενων με χρονική μετατόπιση σε χαμηλές τροχιές δορυφόρων με το όνομα IRIDIUM διέκοψε πριν λίγο καιρό τη λειτουργία του για οικονομικούς λόγους ελλείψει κίνησης.

Πέραν τούτου, υπάρχει μια ταχέως αναπτυσσόμενη αγορά για τις λεγόμενες συνδέσεις VSAT (very small aperture terminal, τερματικό με κεραία πολύ μικρού ανοίγματος). Πρόκειται για ραδιοσταθμούς με κεραίες διαμέτρου μεταξύ 0,9 και 3,7 μέτρων, οι οποίοι διατηρούνται από εταιρίες για την κάλυψη των αναγκών τους (π.χ. τηλε-εικονοδιασκέψεις) ή από παροχείς υπηρεσιών κινητής τηλεφωνίας για την κάλυψη χρονικά περιορισμένων αναγκών σύνδεσης (π.χ. συνέδρια). Το 1996 βρίσκονταν σε λειτουργία 200.000 τερματικά με κεραίες πολύ μικρού ανοίγματος. Η Volkswagen AG διατηρεί 3.000, η Renault 4,000, η General Motors 100.000 και ο μεγαλύτερος ευρωπαϊκός όμιλος επιχειρήσεων ορυκτών καυσίμων διατηρεί 12.000 μονάδες VSAT. Σε περίπτωση που ο ίδιος ο πελάτης δεν φροντίζει για την κρυπτογράφηση, η επικοινωνία διεκπεραιώνεται ανοιχτά[23].

---

[22] G. Thaller, Satelliten im Erdorbit, Franzisverlag, Μόναχο 1999

[23] H. Dodel, ιδιωτική πληροφορία

4.2.3.1. Δορυφορικά συστήματα που λειτουργούν σε παγκόσμια κλίμακα

Τα εν λόγω δορυφορικά συστήματα, με την κατανομή πολλαπλών δορυφόρων στην περιοχή του Ατλαντικού, του Ινδικού και του Ειρηνικού, καλύπτουν όλη την υδρόγειο.

INTELSAT[24]

Η INTELSAT (International Telecomunications Satellite Organisation) ιδρύθηκε το 1964 ως αρχή με οργανωτική δομή παρόμοια με αυτή του ΟΗΕ και σκοπός των εργασιών της ήταν η διεκπεραίωση της διεθνούς επικοινωνίας. Μέλη της ήταν εθνικοί ταχυδρομικοί οργανισμοί κρατικής ιδιοκτησίας. Σήμερα, 144 κυβερνήσεις είναι μέλη της INTELSAT . Το έτος 2001 η INTELSAT θα ιδιωτικοποιηθεί.

Εν τω μεταξύ η INTELSAT διατηρεί στόλο 19 γεωστατικών δορυφόρων, οι οποίοι συνδέουν μεταξύ τους περισσότερα από 200 κράτη, και οι παροχές των οποίων μισθώνονται προς τα μέλη της INTELSAT. Τα μέλη διατηρούν δικούς τους σταθμούς εδάφους. Μέσω της INTELSAT Business Service (IBS) από το 1984 οι δορυφόροι μπορούν να χρησιμοποιηθούν και από μη-μέλη (π.χ. τηλεπικοινωνιακούς οργανισμούς, μεγάλες εταιρίες, διεθνείς ομίλους). Η INTELSAT προσφέρει σε παγκόσμια κλίμακα διάφορες υπηρεσίες όπως στον τομέα των επικοινωνιών, της τηλεόρασης, κ.λπ. Η τηλεπικοινωνιακή μετάδοση γίνεται στις ζώνες συχνοτήτων C και Ku (βλ. παρακάτω).

Οι δορυφόροι INTELSAT είναι οι σημαντικότεροι διεθνείς τηλεπικοινωνιακοί δορυφόροι. Μέσω αυτών διεκπεραιώνεται το μεγαλύτερο μέρος των δορυφορικών διεθνών επικοινωνιών.

Οι δορυφόροι καλύπτουν την περιοχή του Ατλαντικού, του Ινδικού και του Ειρηνικού (βλ. Πίνακα, κεφ·αλαιο 5,5.3).

Πάνω από τον Ατλαντικό μεταξύ 304°E και 359°E βρίσκονται 10 δορυφόροι, την περιοχή του Ινδικού καλύπτουν 6 δορυφόροι μεταξύ 62°E και 110,5°E, τον χώρο του Ειρηνικού 3 δορυφόροι μεταξύ 174°E και 180°E. Η αυξημένη κίνηση στην περιοχή του Ατλαντικού καλύπτεται με μια σειρά από μεμονωμένους δορυφόρους.

INTERSPUTNIK[25]

Το 1971 ιδρύθηκε η διεθνής οργάνωση δορυφορικών επικοινωνιών INTERSPUTNIK από 9 κράτη ως πρακτορείο της πρώην Σοβιετικής Ένωσης με καθήκοντα παρόμοια με την INTELSAT. Σήμερα η INTERSPUTNIK είναι μια διακυβερνητική οργάνωση, μέλη της οποίας μπορούν να γίνουν κυβερνήσεις οποιωνδήποτε κρατών. Εν τω μεταξύ αριθμεί 24 κράτη μέλη (μεταξύ αυτών και η Γερμανία) και περίπου 40 χρήστες (μεταξύ άλλων η Γαλλία και η Αγγλία), οι οποίοι εκπροσωπούνται από τις διοικήσεις των ταχυδρομείων ή τους τηλεπικοινωνιακούς οργανισμούς τους. Η έδρα της είναι στην Μόσχα.

Η τηλεπικοινωνιακή μετάδοση γίνεται στις ζώνες συχνοτήτων C και Ku (βλ. παρακάτω).
Με τους δορυφόρους (Gorizont, Express, Express A της ρωσικής Ομοσπονδίας και LMI-1 της κοινοπραξίας Lockhead-Martin), καλύπτεται επίσης ολόκληρη η υδρόγειος: στην περιοχή του Ατλαντικού υπάρχει 1 δορυφόρος ενώ υπάρχουν σχέδια για δεύτερο, στην περιοχή του Ινδικού υπάρχουν 3 δορυφόροι, στην περιοχή του Ειρηνικού 2 (βλ. πίνακα, κεφάλαιο 5,5.3).

[24] Ιστοσελίδα INTELSAT http://www.intelsat.com

[25] Ιστοσελίδα της INTERSPUTNIK: http://www.intersputnik.com

INMARSAT

Η INMARSAT (Interim International Maritime Satellite) από το 1979 με το δορυφορικό σύστημά της διαθέτει παγκοσμίως **κινητή** επικοινωνία στη θάλασσα, στον αέρα και στην ξηρά, όπως επίσης και ένα σύστημα ραδιοεπικοινωνίας έκτακτης ανάγκης. Η INMARSAT δημιουργήθηκε με πρωτοβουλία της "International Maritime Organisation" ως διακρατική οργάνωση. Εν τω μεταξύ η INMARSAT έχει ιδιωτικοποιηθεί και η έδρα της είναι στο Λονδίνο.

Το σύστημα INMARSAT αποτελείται από εννέα δορυφόρους σε γεωστατικές τροχιές. Τέσσερις από τους δορυφόρους - η γενιά INMARSAT III – καλύπτουν, εκτός από τις ακραίες περιοχές των πόλων, ολόκληρη την υδρόγειο. Κάθε ένας από αυτούς καλύπτει περίπου το 1/3 της επιφάνειας της γης. Εξ αιτίας της τοποθέτησής τους στις τέσσερις περιοχές των ωκεανών (Δυτικός και Ανατολικός Ατλαντικός, Ειρηνικός, Ινδικός Ωκεανός) επιτυγχάνεται παγκόσμια κάλυψη. Παράλληλα, κάθε δορυφόρος INMARSAT διαθέτει και μια σειρά δεσμών κηλίδας "Spot-Beams", γεγονός το οποίο παρέχει τη δυνατότητα διαμόρφωσης δεσμών ενέργειας σε περιοχές αυξημένης τηλεπικοινωνιακής κίνησης.

Η τηλεπικοινωνιακή μετάδοση γίνεται στις ζώνες συχνοτήτων L και Ku (βλ. στο 4,2.4.).

4.2.3.2. Τοπικά δορυφορικά συστήματα

Οι περιοχές κάλυψης τοπικών δορυφορικών συστημάτων καλύπτονται μεμονωμένες περιοχές/ήπειροι. Η μεταδιδόμενη από αυτούς επικοινωνία συνεπώς μπορεί να ληφθεί μόνο σε αυτές τις περιοχές.

EUTELSAT[26]

Η EUTELSAT ιδρύθηκε το 1977 από 17 ευρωπαϊκές διοικήσεις ταχυδρομείων, με στόχο την κάλυψη των ειδικών αναγκών της Ευρώπης όσον αφορά στη δορυφορική επικοινωνία και στην υποστήριξη της ευρωπαϊκής βιομηχανίας διαστήματος. Έχει την έδρα της στο Παρίσι και αριθμεί περίπου 40 κράτη-μέλη. Η EUTELSAT πρόκειται να ιδιωτικοποιηθεί το έτος 2001.

Η EUTELSAT διατηρεί 18 γεωστατικούς δορυφόρους, οι οποίοι καλύπτουν την Ευρώπη, την Αφρική και ένα μεγάλο μέρος της Ασίας και παρέχουν σύνδεση με την Αμερική. Οι δορυφόροι βρίσκονται μεταξύ 12,5°W και 48°E. Η EUTELSAT προσφέρει κυρίως τηλεοπτικά προγράμματα (850 ψηφιακά και αναλογικά κανάλια) και ραδιοφωνικά προγράμματα (520 κανάλια), πέραν αυτού όμως εξυπηρετεί και τις επικοινωνίες, και κυρίως εντός της Ευρώπης (συμπεριλαμβανομένης της Ρωσίας): π.χ. για τηλε-εικονοδιασκέψεις, για ιδιωτικά δίκτυα μεγάλων επιχειρήσεων (μεταξύ άλλων η General Motors και η Fiat), για ειδησεογραφικά πρακτορεία (Reuters, AFP), για παροχείς οικονομικών δεδομένων, όπως επίσης και για κινητές υπηρεσίες μετάδοσης δεδομένων.

Η τηλεπικοινωνιακή μετάδοση γίνεται στην ζώνη συχνοτήτων Ku.

ARABSAT[27]

Η ARABSAT είναι το αντίστοιχο της EUTELSAT στην αραβική περιοχή, και ιδρύθηκε το 1976. Τα μέλη της είναι 21 αραβικά κράτη. Οι δορυφόροι ARABSAT χρησιμοποιούνται τόσο για μετάδοση τηλεοπτικών προγραμμάτων, όσο και για επικοινωνία.

[26] Ιστοσελίδα της EUTELSAT: http://www.com

[27] Ιστοσελίδα της ARABSAT: http://www.arabsat.

Η τηλεπικοινωνιακή μετάδοση γίνεται κυρίως στην ζώνη συχνοτήτων C.

PALAPA[28]

Το ινδονησιακό σύστημα PALAPA έχει τεθεί σε λειτουργία από το 1995 και αποτελεί το νοτιοασιατικό αντίστοιχο του EUTELSAT. Η ζώνη κάλυψής του περιλαμβάνει τη Μαλαισία, την Κίνα, την Ιαπωνία, την Ινδία, το Πακιστάν και άλλα κράτη της περιοχής.
Η τηλεπικοινωνιακή μετάδοση γίνεται στις ζώνες συχνοτήτων C και Ku.

4.2.3.3. Εθνικά δορυφορικά συστήματα[29]

Πολλά κράτη χρησιμοποιούν για την κάλυψη εθνικών αναγκών, δικά τους δορυφορικά συστήματα με περιορισμένες περιοχές κάλυψης.

Ο γαλλικός τηλεπικοινωνιακός δορυφόρος **TELECOM**, χρησιμεύει μεταξύ άλλων, για την σύνδεση των γαλλικών νομών της Αφρικής και της Νότιας Αμερικής με την μητρόπολη. Η τηλεπικοινωνιακή μετάδοση γίνεται στις ζώνες συχνοτήτων C και Ku.

Η **ITALSAT** διατηρεί τηλεπικοινωνιακούς δορυφόρους, οι οποίοι με περιορισμένες περιοχές κάλυψης, διατεταγμένες σε σειρά περιλαμβάνουν ολόκληρη τη γεωγραφική περιοχή της Ιταλίας σε σχήμα "μπότας". Γι' αυτό η λήψη είναι δυνατή μόνο στην Ιταλία. Η τηλεπικοινωνιακή μετάδοση γίνεται στην ζώνη συχνοτήτων Ku.

Ο **AMOS** είναι ένας ισραηλινός δορυφόρος κυρίως για σταθερή επικοινωνία, του οποίου η περιοχή κάλυψης (footprint) εκτείνεται σε περιοχή της Μέσης Ανατολής. Η τηλεπικοινωνιακή μετάδοση γίνεται στην ζώνη συχνοτήτων Ku.

Οι ισπανικοί δορυφόροι **HISPASAT** καλύπτουν την Ισπανία και Πορτογαλία (Ku-Spots) και μεταφέρουν ισπανικά τηλεοπτικά προγράμματα στη Βόρειο και Νότιο Αμερική.

4.2.4. Η εκχώρηση συχνοτήτων

Αρμόδια για την διανομή συχνοτήτων είναι η International Telecommunication Union. Για την εξασφάλιση μιας σχετικής τάξης ο κόσμος διαιρέθηκε για τον σκοπό των ραδιοεπικοινωνιών σε τρεις περιοχές:

1. Ευρώπη, Αφρική, πρώην Σοβιετική Ένωση, Μογγολία
2. Βόρειος και Νότιος Αμερική, καθώς και Γροιλανδία
3. Ασία εκτός των κρατών της περιοχής 1, Αυστραλία και Νότιος Ειρηνικός

Αυτή η υποδιαίρεση η οποία ωρίμασε ιστορικά, υιοθετήθηκε και για τους σκοπούς των δορυφορικών επικοινωνιών και έχει ως αποτέλεσμα τη συσσώρευση δορυφόρων σε ορισμένες γεωστατικές ζώνες.

Οι σημαντικότερες ζώνες συχνοτήτων για τις δορυφορικές επικοινωνίες είναι:

- η ζώνη συχνοτήτων L (0,4 – 1,6 GHz) για κινητές δορυφορικές επικοινωνίες, π.χ. μέσω INMARSAT.

[28] H.Dodel, Satellitenkommunikation, Hóthigverlag 1999

[29] H.Dodel και έρευνες στο Διαδίκτυο

- η ζώνη συχνοτήτων C (3,6 - 6,6 GHz) για επίγειους σταθμούς, π.χ. μέσω INTELSAT

- η ζώνη συχνοτήτων Ku (10 - 20GHz) για επίγειους σταθμούς, π.χ. INTELSAT-Ku-Spot και EUTELSAT

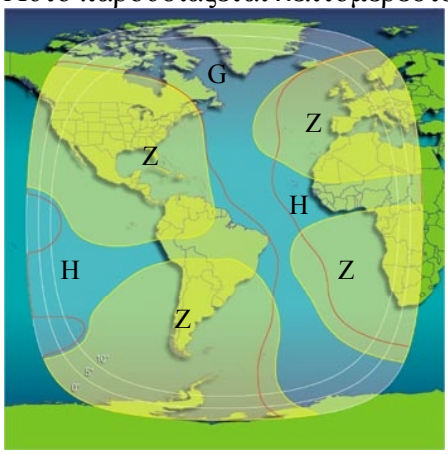
- η ζώνη συχνοτήτων Ka (20 - 46 GHz) για επίγειους σταθμούς, π.χ. μέσω εθνικών δορυφόρων όπως ITALSAT

- η ζώνη συχνοτήτων V (46 – 56 GHz) για τερματικά με κεραίες πολύ μικρού ανοίγματος (V-SATs)

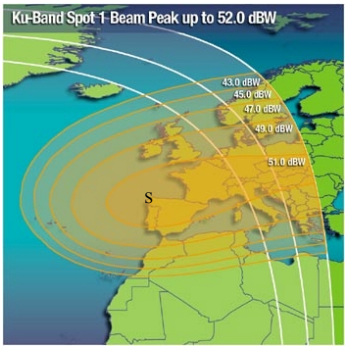
4.2.5. Περιοχές κάλυψης των δορυφόρων (footprints)

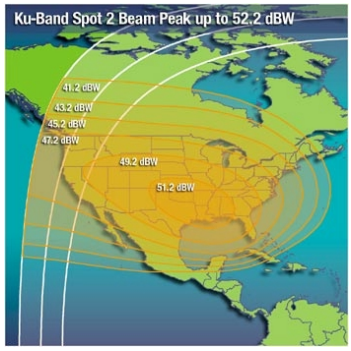
Ως περιοχή κάλυψης ή "footprint" χαρακτηρίζεται η περιοχή πάνω στην γη, η οποία καλύπτεται από την κεραία του δορυφόρου. Μπορεί να περιλαμβάνει μέχρι και το 50 % της επιφάνειας της γης ή να περιορίζεται μέσω σύμπτυξης του σήματος σε μικρές, τοπικά περιορισμένες κηλίδες (spots).
Όσο μεγαλύτερη είναι η συχνότητα του εκπεμπόμενου σήματος, τόσο περισσότερο μπορεί να συμπτυχθεί σε δέσμη, και συνεπώς τόσο μικρότερη θα είναι η περιοχή κάλυψης. Με τη σύμπτυξη (διαμόρφωση σε λεπτή δέσμη) του εκπεμπόμενου δορυφορικού σήματος σε μικρότερες περιοχές κάλυψης μπορεί να αυξηθεί η ενέργεια του σήματος. Όσο μικρότερη είναι η περιοχή κάλυψης, τόσο ισχυρότερο μπορεί να είναι το σήμα και συνεπώς τόσο μικρότερες μπορεί να είναι οι κεραίες λήψης.

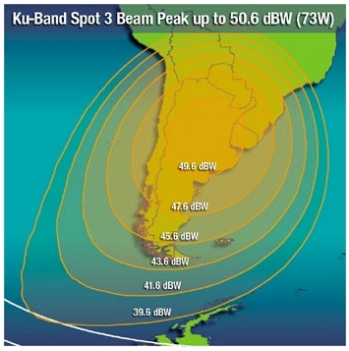
Αυτό παρουσιάζεται λεπτομερέστερα εν συντομία για τους δορυφόρους INTELSAT:



Οι περιοχές κάλυψης των δορυφόρων INTELSAT είναι διαιρεμένες σε διάφορες δέσμες (Beams):
Η παγκόσμια δέσμη (Global-Beam) (G) κάθε δορυφόρου καλύπτει περίπου ένα τρίτο της επιφάνειας της γης,
Οι ημι-δέσμες (Hemi-Beams) (H) καλύπτουν η καθεμία μια επιφάνεια λίγο μικρότερη από το ήμισυ της παγκόσμιας δέσμης.
Οι δέσμες ζώνης (Zone-Beams) (Z) είναι κηλίδες (Spots) σε ορισμένες περιοχές της γης. Είναι μικρότερες από τις ημι-δέσμες.
Εκτός αυτού υπάρχουν οι λεγόμενες δέσμες κηλίδας (Spot-Beams), οι οποίες είναι ακριβείς, μικρές περιοχές κάλυψης (βλ. παρακάτω).







Οι συχνότητες της ζώνης συχνοτήτων C υπάρχουν στις παγκόσμιες δέσμες, τις ημι-δέσμες και της δέσμες ζώνης. Οι συχνότητες της ζώνης συχνοτήτων Ku υπάρχουν στις δέσμες κηλίδας (Spot-Beams).

4.2.6. Τα απαραίτητα για έναν επίγειο σταθμό μεγέθη κεραιών

Ως κεραίες λήψης πάνω στη γη χρησιμοποιούνται παραβολικές κεραίες. Το παραβολικό κάτοπτρο ανακλά όλα τα προσπίπτοντα κύματα και τα συμπτύσσει στο εστιακό σημείο του. Στην εστία αυτή υπάρχει το αυτό καθ' αυτό σύστημα λήψης. Όσο μεγαλύτερη είναι η ενέργεια του σήματος στο σημείο της λήψης, τόσο μικρότερη μπορεί να είναι η διάμετρος της παραβολικής κεραίας.

Για τον σκοπό της διενεργούμενης με αυτή την έκθεση έρευνας, έχει σημασία ότι ένα μέρος της διηπειρωτικής επικοινωνίας διεκπεραιώνεται μέσω της ζώνης συχνοτήτων C στις παγκόσμιες δέσμες των δορυφόρων INTELSAT και άλλων δορυφόρων (π.χ. INTERSPUTNIK), για την οποία εν μέρει απαιτούνται κάτοπτρα δορυφορικών κεραιών διαμέτρου περίπου 30 μέτρων (βλ. κεφάλαιο 5). Οι κεραίες των 30 μέτρων απαιτούνταν επίσης για τους πρώτους σταθμούς παρακολούθησης των τηλεπικοινωνιακών δορυφόρων, αφού η πρώτη γενιά INTELSAT Spots διέθετε μόνο παγκόσμιες δέσμες και η μετάδοση των σημάτων δεν ήταν τόσο εκλεπτυσμένης τεχνολογίας όπως σήμερα. Αυτά τα κάτοπτρα που έχουν εν μέρει διαμέτρους άνω των 30 μέτρων χρησιμοποιούνται στους αντίστοιχους σταθμούς ακόμη και όταν από τεχνική άποψη δεν είναι απαραίτητα.

Οι συνήθεις κεραίες που απαιτούνται σήμερα για την επικοινωνία INTELSAT στην ζώνη συχνοτήτων C, έχουν διάμετρο 13 έως 18 μέτρων. Σε μεμονωμένες περιπτώσεις (π.χ. στον INTELSAT 511) απαιτείται για την παγκόσμια δέσμη μεγαλύτερη κεραία. Στους νεότερους δορυφόρους INTELSAT για τις δέσμες ζώνης της ζώνης συχνοτήτων C επαρκούν κεραίες με διάμετρο έως και 5 μέτρα.

Γι8α την λήψη της επικοινωνίας της ζώνης συχνοτήτων C της Intersputnik απαιτούνται κεραίες διαμέτρου από 2 έως 25 μέτρων.

Για τις κηλίδες Ku των δορυφόρων INTELSAT, αλλά και άλλων δορυφόρων (EUTELSAT ζώνη συχνοτήτων KU, AMOS ζώνη συχνοτήτων Ku, κ.λπ.) απαιτούνται κεραίες διαμέτρου 2 έως 10 μέτρων.

Για τερματικά με κεραίες πολύ μικρού ανοίγματος τα οποία λειτουργούν στην ζώνη συχνοτήτων V και το σήμα των οποίων λόγω της υψηλής συχνότητας μπορεί να συμπτυχθεί σε πιο ισχυρή δέσμη απ' ότι στην ζώνη συχνοτήτων Ku, επαρκούν διάμετροι κεραιών 0,9-3,7 μέτρων (π.χ. VSATs της EUTELSAT ή INMARSAT).

5. Η δια τεκμηρίων απόδειξη της ύπαρξης ενός τουλάχιστο παγκοσμίου συστήματος παρακολούθησης

5.1. Για ποιο λόγο απόδειξη δια τεκμηρίων;

Οι μυστικές υπηρεσίες είναι φυσικό να μην αποκαλύπτουν τις λεπτομέρειες των εργασιών τους. Για το λόγο αυτό δεν υπάρχει, τουλάχιστον επίσημη, δήλωση των υπηρεσιών πληροφοριών εξωτερικού των χωρών του ECHELON σχετικά με τη συνεργασία σε ένα παγκόσμιο σύστημα παρακολούθησης. Ως εκ τούτου, η απόδειξη πρέπει να αναζητηθεί δια της συγκέντρωσης όσο το δυνατόν περισσοτέρων τεκμηρίων, τα οποία θα συμπυκνώνονται σε μία πειστική δια τεκμηρίων απόδειξη.
Το σύνολο των τεκμηρίων που θα αποτελέσουν μία τέτοια απόδειξη αποτελείται από τρία στοιχεία:

- την απόδειξη, ότι υπηρεσίες πληροφοριών εξωτερικού υποκλέπτουν στις χώρες του ECHELON ιδιωτικές και επαγγελματικές επικοινωνίες.
- την απόδειξη, ότι λόγω του τρόπου λειτουργίας του πολιτικού δορυφορικού συστήματος επικοινωνίας, εντοπίζονται σε διάφορες περιοχές της γης σταθμοί παρακολούθησης, οι οποίοι επιβλέπονται από κάποια από τις χώρες του ECHELON .
- την απόδειξη, ότι οι χώρες αυτές συνεργάζονται όσον αφορά στις υπηρεσίες πληροφοριών, σε πολύ μεγάλο βαθμό. Εάν αυτό σημαίνει ότι, οι συνεργάτες αναλαμβάνουν εντολές παρακολούθησης και στη συνέχεια διαβιβάζουν άμεσα το μη επεξεργασμένο υλικό, δίχως οι ίδιοι να προβαίνουν σε αποτίμηση, δεν είναι σημαντικό για την απόδειξη της μεταξύ τους συνεργασίας. Το γεγονός αυτό έχει σημασία μόνο εφόσον πρόκειται για τη διασάφηση των ιεραρχιών που υπάρχουν εντός ενός τέτοιου συστήματος παρακολούθησης.

5.1.1. Η απόδειξη της υποκλεπτικής δράσης υπηρεσιών πληροφοριών εξωτερικού

Τουλάχιστον στα δημοκρατικά κράτη, οι μυστικές υπηρεσίες εργάζονται βάσει νόμων, στους οποίους περιγράφονται ο σκοπός ή και οι εξουσίες τους. Για το λόγο αυτό, είναι εύκολο να αποδειχθεί, ότι σε πολλά από αυτά τα κράτη υπάρχουν υπηρεσίες πληροφοριών εξωτερικού, οι οποίες παρακολουθούν τις επικοινωνίες των πολιτών. Αυτό ισχύει και για τις πέντε λεγόμενες χώρες του ECHELON, που στο σύνολό τους διατηρούν τέτοιες υπηρεσίες. Σε κάθε μία από τις εν λόγω χώρες δεν χρειάζεται κάποια πρόσθετη απόδειξη για τη διενέργεια παρακολούθησης επικοινωνιών που εισέρχονται στη χώρα ή εξέρχονται από αυτή. Στις δορυφορικές επικοινωνίες, μπορεί κανείς από την επικράτειά του να αναχαιτίσει και ένα μέρος των επικοινωνιών, οι οποίες προορίζονται για παραλήπτες στο εξωτερικό. Σε καμία από τις πέντε χώρες του ECHELON δεν υπάρχουν νομικοί προορισμοί που θα εμπόδιζαν κάτι τέτοιο. Η λογική στην οποία βασίζεται η μέθοδος του στρατηγικού ελέγχου των τηλεπικοινωνιών εξωτερικού και ο στόχος της, αφήνουν να εννοηθεί, ότι οι υπηρεσίες πράγματι ενεργούν κατά τον τρόπο αυτό.[30]

[30] Ο εισηγητής έχει πληροφορίες από προστατευμένη πηγή, ότι αυτό ισχύει.

5.1.2. Η απόδειξη της ύπαρξης σταθμών στις γεωγραφικά σημαίνουσες περιοχές

Ο μοναδικός περιορισμός που τίθεται στην προσπάθεια οικοδόμησης ενός συστήματος παρακολούθησης επικοινωνιών σε παγκόσμια κλίμακα που υποστηρίζεται από δορυφόρους, προέρχεται από την ίδια την τεχνική της επικοινωνίας αυτής. Δεν υπάρχει σημείο, από τον οποίο να μπορούν να παρακολουθηθούν **όλες** οι δορυφορικές επικοινωνίες σε ολόκληρο τον κόσμο (βλ. κεφάλαιο 4,2.5.).

Ένα παγκόσμιο σύστημα παρακολούθησης θα μπορούσε να οικοδομηθεί υπό τρεις προϋποθέσεις:

- ο λειτουργός διαθέτει σε όλα τα προς τούτο απαραίτητα μέρη του κόσμου ιδία κυριαρχικά εδάφη
- ο λειτουργός διαθέτει σε όλα τα προς τούτο απαραίτητα μέρη του κόσμου εν μέρει ιδία κυριαρχικά εδάφη και επιπλέον δικαιώματα ως φιλοξενούμενος στα λοιπά μέρη του κόσμου και μπορεί εκεί να λειτουργεί ή να χρησιμοποιεί από κοινού σταθμούς .
- ο λειτουργός είναι ένας σύνδεσμος των υπηρεσιών πληροφοριών περισσοτέρων χωρών και λειτουργεί το σύστημα στα προς τούτο απαραίτητα μέρη του κόσμου.

Καμία από τις χώρες του ECHELON δεν θα μπορούσε να θέσει μόνη της σε λειτουργία ένα παγκόσμιο σύστημα. Οι ΗΠΑ δεν έχουν επίσημες αποικίες. Ο Καναδάς, η Αυστραλία και η Νέα Ζηλανδία επίσης δεν διαθέτουν ιδία κυριαρχικά εδάφη εκτός της επικράτειάς τους. Επίσης, το Ηνωμένο Βασίλειο δεν θα μπορούσε να θέσει από μόνο του σε λειτουργία ένα παγκόσμιο σύστημα παρακολούθησης (βλ. κεφάλαιο 6).

5.1.3. Η απόδειξη ενός στενού συνδέσμου υπηρεσιών πληροφοριών

Δεν έχει γίνει γνωστό, αν και σε πιο βαθμό οι χώρες του ECHELON συνεργάζονται μεταξύ τους σε επίπεδο υπηρεσιών πληροφοριών. Συνήθως, η συνεργασία των υπηρεσιών είναι διμερής και διεξάγεται βάσει της ανταλλαγής αποτιμημένου υλικού. Η ύπαρξη και μόνο παρόμοιας συνεργασίας είναι ήδη πολύ ασυνήθιστο γεγονός. Αν μάλιστα προστεθεί και η τακτική ανταλλαγή μη επεξεργασμένου υλικού, προκύπτει μία τελείως νέα ποιότητα. Μία συνεργασία αυτού του είδους μπορεί να αποδειχθεί μόνον με τεκμήρια.

5.2. Πώς αναγνωρίζεται ένας σταθμός παρακολούθησης δορυφορικής επικοινωνίας;

5.2.1. Κριτήριο 1: η δυνατότητα της πρόσβασης στις εγκαταστάσεις

Οι μεγάλες εγκαταστάσεις του οργανισμού τηλεπικοινωνιών, του ραδιοφώνου ή και ερευνητικών οργανισμών, που διαθέτουν μεγάλες κεραίες, είναι προσιτές σε επισκέπτες, κατόπιν προηγούμενης ειδοποίησης. Αυτό δεν ισχύει για τους σταθμούς παρακολούθησης. Τέτοιους σταθμούς λειτουργεί συνήθως ο στρατός, ο οποίος διενεργεί και την παρακολούθηση από τεχνικής άποψης. Έτσι για παράδειγμα, τη λειτουργία του σταθμού αναλαμβάνουν για την NSA οι Naval Security Group (NAVSECGRU) ή Air Intelligence Agency της US Airforce (AIA). Στους βρετανικούς σταθμούς, η βρετανική Royal Airforce είναι υπεύθυνη των εγκαταστάσεων για την βρετανική υπηρεσία πληροφοριών GCHQ. Αυτός ο διακανονισμός επιτρέπει την αυστηρή στρατιωτική φύλαξη της εγκατάστασης και ταυτοχρόνως εξυπηρετεί λόγους συγκάλυψης.

5.2.2. Κριτήριο 2: το είδος της κεραίας

Σε εγκαταστάσεις που πληρούν το κριτήριο 1, χρησιμοποιούνται διάφοροι τύποι κεραιών, οι οποίες διαφέρουν χαρακτηριστικά ως προς τη μορφή τους. Η μορφή τους δίνει πληροφορίες για το σκοπό της εγκατάστασης παρακολούθησης. Έτσι, διαρθρώσεις επιμηκών ραβδοειδών κεραιών σε δακτύλιο μεγάλης διαμέτρου χρησιμοποιούνται για την ραδιογωνιομετρία σημάτων. Οι επίσης δακτυλιοειδείς διαρθρώσεις ρομβικά μορφοποιημένων κεραιών (οι λεγόμενες κεραίες Pusher) εξυπηρετούν τον ίδιο σκοπό. Οι κεραίες λήψης από όλες τις κατευθύνσεις ή κατευθυντικές κεραίες, που μοιάζουν με τεράστιες κλασσικές κεραίες τηλεόρασης, χρησιμοποιούνται για την παρακολούθηση μη κατευθυντικών ραδιοσημάτων. **Όμως για την λήψη δορυφορικών σημάτων χρησιμοποιούνται μόνον παραβολικές κεραίες**. Αν οι παραβολικές κεραίες βρίσκονται ανοιχτά εκτεθειμένες στην ύπαιθρο, μπορεί κανείς γνωρίζοντας την τοποθεσία τους, την γωνία ανύψωσής τους (elevation) και το αζιμούθιό τους, να υπολογίσει ποιού δορυφόρου γίνεται λήψη. Αυτό θα ήταν δυνατό να γίνει π.χ. στο Morwenstow (Ηνωμένο Βασίλειο) ή στην Yakima (ΗΠΑ) και στο Sugar Grove (ΗΠΑ). Συνήθως όμως, οι παραβολικές κεραίες καλύπτονται κάτω από άσπρες σφαιροειδείς καλύπτρες, τα Radome, προκειμένου να προστατεύονται, αλλά και για την κάλυψη της κατεύθυνσής τους.

Αν οι παραβολικές κεραίες ή οι καλύπτρες βρίσκονται στον υπαίθριο χώρο ενός σταθμού παρακολούθησης, τότε σίγουρα γίνεται με αυτές λήψη σημάτων από δορυφόρους. Παρόλα αυτά δεν διευκρινίζεται κατ αυτόν τον τρόπο ακόμη, για τι είδους σήματα πρόκειται.

5.2.3. Κριτήριο 3: το μέγεθος της κεραίας

Οι κεραίες δορυφορικής λήψης μιας εγκατάστασης του κριτηρίου 1 μπορεί να επιτελούν διάφορους σκοπούς :
- σταθμός λήψης στρατιωτικών επικοινωνιών
- σταθμός λήψης κατασκοπευτικών δορυφόρων (εικόνες, ραντάρ)
- σταθμός λήψης στρατιωτικών δορυφόρων SIGINT
- σταθμός λήψης παρακολούθησης πολιτικών δορυφόρων επικοινωνίας

Εξωτερικά, δεν διακρίνεται από τις κεραίες ή τις καλύπτρες ο σκοπός που εξυπηρετούν. Υπάρχουν όμως τεχνικά επιβαλλόμενα ελάχιστα μεγέθη για κεραίες, οι οποίες θέλουν να λαμβάνουν το λεγόμενο “global beam” στην ζώνη C της διεθνούς επικοινωνίας που στηρίζεται σε δορυφόρους. Στην πρώτη γενιά αυτών των δορυφόρων, απαιτούνταν κεραίες με διάμετρο 25 έως 30 μέτρων περίπου, ενώ σήμερα μια διάμετρος 15 έως 18 μέτρων είναι επαρκής. Το αυτόματο φιλτράρισμα των αναχαιτιζόμενων σημάτων μέσω ηλεκτρονικού υπολογιστή απαιτεί μία όσο το δυνατόν καλύτερη ποιότητα σήματος, για το λόγο αυτό επιλέγονται ανάλογα κεραίες με μέγεθος που αγγίζει τα ανώτατα από τα παραπάνω όρια. Επειδή οι κεραίες είναι συναρμολογημένες επάνω σε βάσεις, οι διάμετροι των καλύπτρων είναι ακόμη μεγαλύτερες από τις διαμέτρους των κεραιών.

5.2.1. Συμπεράσματα

Εξ όσων γνωρίζει ο εισηγητής, δεν υπάρχουν οποιεσδήποτε στρατιωτικές εφαρμογές για κεραίες του μεγέθους αυτού. Συνεπώς, όταν εντοπίζονται κεραίες σε υπαίθριο χώρο που πληροί το κριτήριο 1, πρόκειται για παρακολούθηση πολιτικής δορυφορικής επικοινωνίας.

5.3. Πορίσματα που έχουν δημοσιοποιηθεί σχετικά με γνωστούς σταθμούς παρακολούθησης

5.3.1. Μέθοδος

Προκειμένου να διαπιστωθεί ποιοι σταθμοί ανταποκρίνονται στα κριτήρια που αναφέρονται στο κεφάλαιο 5.2. και αποτελούν τμήμα του παγκόσμιου συστήματος παρακολούθησης και ποιες αποστολές έχουν, αξιολογήθηκαν η επί του παρόντος αντιφατική βιβλιογραφία (Hager[31], Richelson[32], Campbell[33]), αποχαρακτηρισμένα έγγραφα [34], η Homepage της Federation of American Scientists[35] καθώς και Homepages των φορέων εκμετάλλευσης [36] (NSA, AIA, κ.ά.) και άλλες δημοσιεύσεις του Ιντερνέτ. Πέραν αυτών συλλέχθηκαν οι ζώνες φωτισμού των δορυφόρων επικοινωνιών, υπολογίσθηκαν τα αναγκαία μεγέθη των κεραιών, και καταχωρήθηκαν από κοινού με τους πιθανούς σταθμούς σε παγκόσμιους χάρτες.

5.3.2. Ακριβής ανάλυση

Για την εκμετάλλευση ισχύουν οι ακόλουθες αρχές που συνδέονται με τη φυσική της δορυφορικής επικοινωνίας (βλ. και κεφάλαιο 4):

- μία δορυφορική κεραία μπορεί να συλλάβει μόνο αυτό το οποίο ευρίσκεται εντός της ζώνης φωτισμού, στην οποία αυτή ευρίσκεται. Προκειμένου να μπορέσει να λάβει επικοινωνία που τρέχει κυρίως στις ζώνες C και Ku, πρέπει μία κεραία να βρίσκεται εντός των ζωνών φωτισμού που περιέχουν τις ζώνες C ή Ku.
- Για κάθε παγκόσμια ακτίνα είναι αναγκαία μία δορυφορική κεραία, ακόμη και όταν οι ακτίνες δύο δορυφόρων επικαλύπτονται.
- Εάν ένας δορυφόρος έχει περισσότερες ζώνες φωτισμού από την παγκόσμια ακτίνα μόνο, πράγμα το οποίο είναι χαρακτηριστικό για τις σημερινές γενεές δορυφόρων, δεν είναι δυνατόν με μία μοναδική δορυφορική κεραία πλέον να συλληφθεί η συνολικά τρέχουσα επικοινωνία μέσω αυτών των δορυφόρων, λόγω του ότι μία μόνη δορυφορική κεραία δεν μπορεί να βρίσκεται σε όλες τις ζώνες φωτισμού του δορυφόρου. Για τη σύλληψη της Hemi-Beams και της Global-Beams ενός δορυφόρου είναι κατά συνέπεια αναγκαίες δύο δορυφορικές κεραίες σε διαφορετικές περιοχές (βλ. παράσταση των ζωνών φωτισμού στο κεφάλαιο 4). Εφόσον προστεθούν και άλλες ακτίνες (Zonebeam και Spotbeam) είναι αναγκαίες περαιτέρω δορυφορικές κεραίες. Ορισμένες είναι επικαλυπτόμενες ακτίνες ενός

---

[31] Hager, Nicky: EXPOSING THE GLOBAL SURVEILLANCE SYSTEM http://www.ncoic.com/echelon1.htm
Hager, Nicky: Secret Power. New Zealands´s Role in the international Spy Network, New Zealand 1996

[32] Richelson, Jeffrey, Desperately seeking Signals, 4 2000, The Bulletin of the Atomic Scientists, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html
Richelson,T.Jeffrey, The U.S. Intelligence Community, Westview Press 1999

[33] Campbell, Duncan, Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5, 10 1999, STOA, http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf
Campbell, Duncan: Inside Echelon, 25.7.2000http://www.heise.de/tp/deutsch/special/ech/6928/1.html
Campbell, Duncan: Interception Capabilities n- Impact and Exploitation – Echelon and its role in COMINT, που υποβλήθηκε στην προσωρινή επιτροπή Echelon του Ευρωπαϊκού Κοινοβουλίου στις 22 Ιανουαρίου 2001
Federation of American Scientists, http://www.fas.org/irp/nsa/nsafacil.html

[34] Richelson, Jeffrey: Newly released documents on the restrictions NSA places on reporting the identities of US-persons: Αποχαρακτηρισμένα: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

[35] Federation of American Scientists

[36] Military.com; *.mil-Homepages

δορυφόρου. Μπορούν ωστόσο να συλληφθούν από μία δορυφορική κεραία, λόγω του ότι είναι δυνατόν από τεχνική άποψη να διαχωρισθούν ορισμένες ζώνες συχνοτήτων κατά την υποδοχή.

Πέραν αυτού ισχύουν οι προϋποθέσεις που έχουν αναφερθεί στο κεφάλαιο 5.2.: η μη πρόσβαση των εγκαταστάσεων λόγω του ότι αυτές λειτουργούν από τον στρατό[37], λόγω του ότι για την υποδοχή σημάτων δορυφόρων είναι αναγκαίες δορυφορικές κεραίες και ότι το μέγεθος των δορυφορικών κεραιών για τη σύλληψη της ζώνης C στην Global-Beam για την πρώτη γενεά INTELSAT πρέπει να έχει μέγεθος μεγαλύτερο των 25 μέτρων, για τις επόμενες γενεές περισσότερο από 15 έως 18 μέτρα.

5.3.2.1. Η παράλληλη πορεία της ανάπτυξης του INTELSAT με την κατασκευή σταθμών

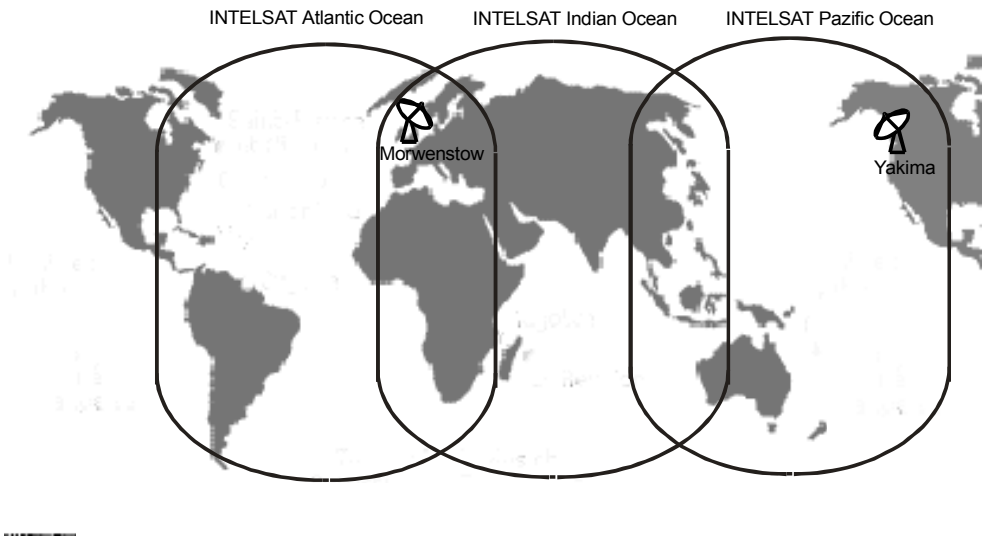
Ένα παγκόσμιο σύστημα παρακολούθησης πρέπει να διευρύνεται με την πρόοδο της επικοινωνίας. Με την αρχή της δορυφορικής επικοινωνίας πρέπει κατά συνέπεια να συμβαδίζει η δημιουργία σταθμών, και με την εισαγωγή νέων γενεών δορυφόρων η δημιουργία νέων σταθμών καθώς και η κατασκευή νέων δορυφορικών κεραιών, που ανταποκρίνονται στις εκάστοτε απαιτήσεις. Ο αριθμός των σταθμών και ο αριθμός των δορυφορικών κεραιών πρέπει τότε πάντοτε να μεγαλώνει, όταν είναι αναγκαίος για τη σύλληψη της επικοινωνίας.
Αντιθέτως, όταν λοιπόν εκεί όπου προστίθενται νέες ζώνες φωτισμού δημιουργούνται νέοι σταθμοί και κατασκευάζονται νέες δορυφορικές κεραίες, δεν πρόκειται για σύμπτωση, αλλά είναι δυνατόν να θεωρηθεί ως ένδειξη για την ύπαρξη νέων σταθμών παρακολούθησης για επικοινωνίες.
Λόγω του ότι οι δορυφόροι INTELSAT ήταν οι πρώτοι δορυφόροι επικοινωνιών οι οποίοι, πέραν αυτού, κάλυψαν όλη την υδρόγειο σφαίρα, είναι λογικό ότι η δημιουργία και μεγέθυνση των σταθμών συμβαδίζει με τις γενεές του INTELSAT.

Η πρώτη γενεά

Ήδη το 1965 τέθηκε ο πρώτος δορυφόρος INTELSAT (Early Bird) σα γεωστατική τροχιά. Η ικανότητά του μετάδοσης ήταν ακόμη μικρή και το αποτύπωμα δέσμης του εκτιμώταν μόνο πάνω από το βόρειο ημισφαίριο.
Με τις γενεές INTELSAT II και III, που τέθηκαν σε λειτουργία το 1967 και το 1968, επιτεύχθηκε για πρώτη φορά μία παγκόσμια κάλυψη. Οι Global-Beams των δορυφόρων κάλυπταν τον τομέα του Ατλαντικού, του Ειρηνικού και του Ινδικού. Μικρότερα αποτυπώματα δέσμης δεν υπήρχαν ακόμη. Για τη σύλληψη του συνόλου της επικοινωνίας ήταν, κατά συνέπεια, απαραίτητες τρεις δορυφορικές κεραίες. Λόγω του ότι επικαλύπτονταν πάνω από τον ευρωπαϊκό χώρο δύο Global-Beams, ήταν δυνατόν να συλληφθούν σ' αυτή την περιοχή σε ένα σταθμό με δύο δορυφορικές κεραίες διαφορετικής κατεύθυνσης τα παγκόσμια αποτυπώματα δέσμης δύο δορυφόρων.

[37] Χρησιμοποιούμενες συντμήσεις: NAVSECGRU: Naval Security Group, INSCOM: United States Army Intelligence And Security Command, AIA: Air Intelligence Agency, IG: Intelligence Group, IS: Intelligence Sqadron, IW: Intelligence Wing, IOG: Information Operation Group, MIG: Military Intelligence Group

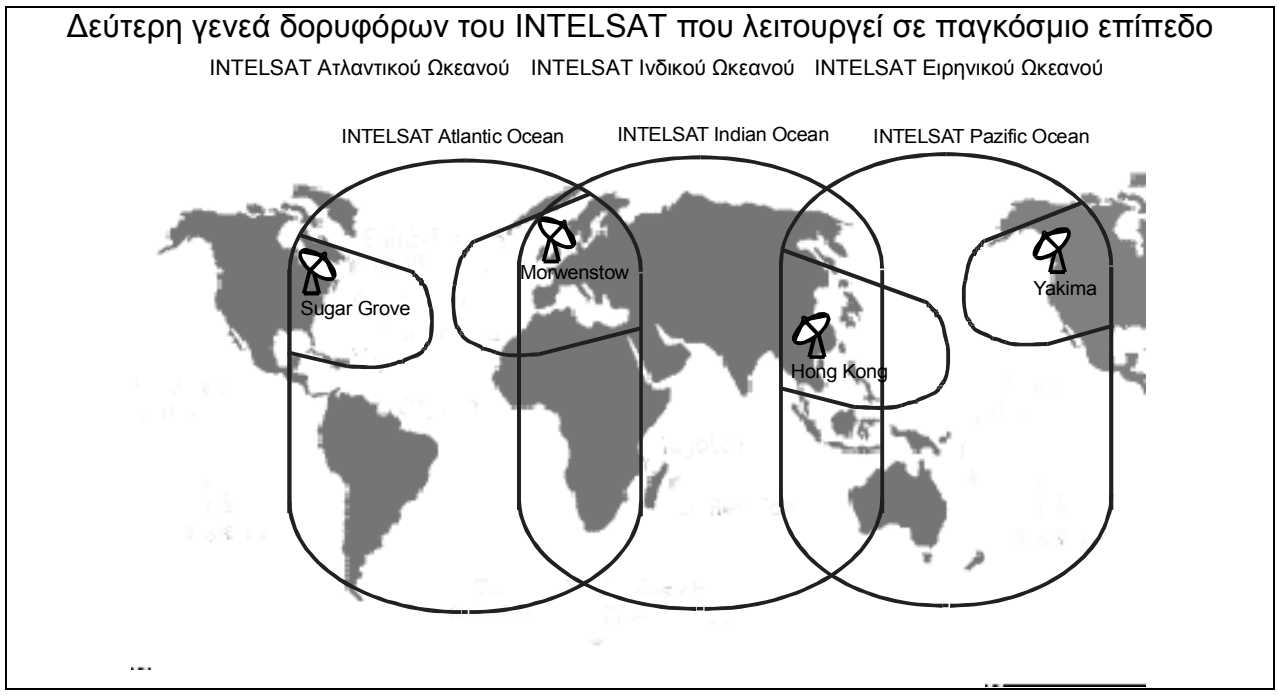
Πρώτη γενεά δορυφόρων του INTELSAT που λειτουργούν σε παγκόσμιο επίπεδο



Το 1970 ιδρύθηκε ο σταθμός **Yakima** στο βορειοδυτικό τμήμα των ΗΠΑ, το 1972/73 ο σταθμός **Morwenstow** στη Νότια Αγγλία. Ο σταθμός Yakima είχε τότε μία μεγάλη κεραία (προς την κατεύθυνση του Ειρηνικού), ο σταθμός Morwenstow είχε δύο μεγάλες κεραίες (μία προς την κατεύθυνση του Ατλαντικού και μία προς την κατεύθυνση του Ινδικού Ωκεανού). Λόγω της θέσης των δύο σταθμών ήταν δυνατή η σύλληψη του συνόλου των επικοινωνιών. Πέραν αυτού, το 1974 κατασκευάσθηκε στο Menwith Hill η πρώτη μεγάλη δορυφορική κεραία.

Η δεύτερη παγκόσμια γενεά

Η δεύτερη γενεά των δορυφόρων INTELSAT (IV και IVA) αναπτύχθηκε κατά τη δεκαετία του '70 και τέθηκε σε γεωστατική τροχιά (1971 και 1975). Οι νέοι δορυφόροι οι οποίοι διασφάλιζαν επίσης μια παγκόσμια κάλυψη και διέθεταν σημαντικά περισσότερες διαύλους επικοινωνίας (4000 – 6000), είχαν παράλληλα με την Global-Beam και Zone-Beams στο βόρειο ημισφαίριο (βλέπε κεφάλαιο 4). Μία Zone-Beam κάλυπτε το ανατολικό τμήμα των ΗΠΑ, μία το δυτικό των ΗΠΑ, μία τη Δυτική Ευρώπη και μία άλλη την Ανατολική Ασία. Με δύο σταθμούς με τρεις δορυφορικές κεραίες δεν ήταν πλέον δυνατή η σύλληψη του συνόλου των επικοινωνιών. Με τους υπάρχοντες σταθμούς στην Yakima μπορούσε να καλυφθεί η Zone-Beam στο δυτικό τμήμα των ΗΠΑ, με το σταθμό Morwenstow η Zone-Beam πάνω από την Ευρώπη. Για τη σύλληψη των δύο περαιτέρω Zone-Beams ήταν αναγκαίος ένας σταθμός στο ανατολικό τμήμα των ΗΠΑ και ένας άλλος στο χώρο της Ανατολικής Ασίας.



Κατά το τέλος της δεκαετίας του '70 κατασκευάστηκε ο σταθμός **Sugar Grove** στις ανατολικές ΗΠΑ (ο σταθμός υπήρχε ήδη για την παρακολούθηση ρωσικών επικοινωνιών)· τέθηκε σε λειτουργία το 1980. Επίσης κατά το τέλος της δεκαετίας του '70 ιδρύθηκε ένας σταθμός στο **Χογκ Κογκ**.
Κατ' αυτό τον τρόπο, με τους τέσσερις σταθμούς – Yakima, Morwenstow, Sugar Grove και HongKong – ήταν δυνατή κατά τη δεκαετία του '80 η παγκόσμια παρακολούθηση των επικοινωνιών INTELSAT.

Οι μεταγενέστεροι δορυφόροι INTELSAT με Zone-Beams και Spot-Beams συμπληρωματικά με τους δορυφόρους των Global-Beams και Hemi-Beams κατέστησαν αναγκαίους περαιτέρω σταθμούς σε διάφορα σημεία του κόσμου. Εν προκειμένω είναι πολύ δύσκολο να συνδεθεί η δημιουργία περαιτέρω σταθμών ή η τοποθέτηση περαιτέρω δορυφορικών κεραιών.
Λόγω του ότι πέραν αυτού είναι πολύ δύσκολη η πρόσβαση σε πληροφορίες σχετικά με σταθμούς, δεν είναι δυνατόν να διερευνηθεί ακριβώς ποιοι δορυφόροι συλλαμβάνονται με ποιες δέσμες. Είναι όμως ωστόσο δυνατόν να διαπιστωθεί σε ποιες δέσμες βρίσκονται γνωστοί σταθμοί.

5.3.2.2. Η παγκόσμια κάλυψη από σταθμούς που είναι προφανές ότι παρακολουθούν δορυφόρους επικοινωνιών

Σήμερα διασφαλίζεται παγκόσμια δορυφορική επικοινωνία με δορυφόρους της INTELSAT, INMARSAT και INTERSPUTNIK. Ο καταμερισμός σε τρία αποτυπώματα δέσμης (ινδικός, ειρηνικός και ατλαντικός τομέας) διατηρήθηκε όπως και κατά τις πρώτες γενεές δορυφόρων.
Σε καθένα από τα αποτυπώματα δέσμης υπάρχουν σταθμοί για τους οποίους συμπίπτουν τα για τους σταθμούς παρακολούθησης χαρακτηριστικά κριτήρια:

Δορυφόροι υπεράνω του Ινδικού Ωκεανού:

INTELSAT 604 (60°Ανατολικά), 602 (62°Ανατολικά), 804 (64°Ανατολικά), 704 (66°Ανατολικά) EXPRESS 6A (80°Ανατολικά) INMARSAT τομέας Ινδικού Ωκεανού	Geraldton, Αυστραλία Pine Gap, Αυστραλία Morwenstow, Αγγλία Menwith Hill, Αγγλία
INTELSAT APR1 (83°), APR-2 (110,5°)	Geraldton, Αυστραλία Pine Gap, Αυστραλία Misawa, Ιαπωνία

Δορυφόροι υπεράνω του Ειρηνικού :

INTELSAT 802 (174°), 702 (176°), 701 (180°) GORIZONT 41 (130°Ανατολικά), 42 (142°Ανατολικά), LM-1 (75°Ανατολικά) INMARSAT τομέας Ειρηνικού Ωκεανού	Waihopai, Νέα Ζηλανδία Geraldton, Αυστραλία Pine Gap, Αυστραλία Misawa, Ιαπωνία Yakima, USA – μόνο Intelsat και Inmarsat

Δορυφόροι υπεράνω του Ατλαντικού :

INTELSAT 805 (304,5°), 706 (307°), 709 (310°) 601 (325,5°), 801 (328°), 511(330,5°), 605 (332,5°), 603 (335,5°), 705 (342°) EXPRESS 2 (14°Δυτικά), 3A (11°Δυτικά) INMARSAT τομέας Ατλαντικού Ωκεανού	Sugar Grove, ΗΠΑ Buckley Field, ΗΠΑ Sabana Seca, Πόρτο Ρίκο Morwenstow, Αγγλία Menwith Hill, Αγγλία
INTELSAT 707 (359°)	Morwenstow, Αγγλία Menwith Hill, Αγγλία

Με αυτόν τον τρόπο καταδεικνύεται ότι είναι δυνατή μια παγκόσμια παρακολούθηση των τηλεπικοινωνιών.

Πέραν αυτών, υπάρχουν δύο ακόμη σταθμοί στους οποίους μεν δεν συμπίπτει το κριτήριο του μεγέθους της κεραίας, οι οποίοι όμως είναι δυνατόν να αποτελούν παρόλα αυτά τμήμα του παγκόσμιου συστήματος παρακολούθησης. Με τους σταθμούς αυτούς θα ήταν δυνατόν π.χ. να συλληφθούν οι Zone-Beams ή Spot-Beams δορυφόρων, των οποίων οι Global-Beams παρακολουθούνται από άλλους σταθμούς, ή για την Global-Beam των οποίων είναι αναγκαίες μεγάλες δορυφορικές κεραίες.

5.3.2.3. Οι σταθμοί λεπτομερειακά

Στην λεπτομερή περιγραφή σταθμών γίνεται διάκριση μεταξύ σταθμών οι οποίοι παρακολουθούν σαφώς δορυφόρους επικοινωνιών (κριτήρια από το κεφάλαιο 5.2) και σταθμών των οποίων η αποστολή δεν μπορεί να τεκμηριωθεί με τη βοήθεια των ανωτέρω κριτηρίων.

Σταθμοί για την παρακολούθηση δορυφόρων επικοινωνιών

Τα εις το κεφάλαιο 5.2. περιγραφόμενα κριτήρια τα οποία μπορούν να αξιολογηθούν ως ενδείξεις για ένα σταθμό παρακολούθησης δορυφόρων επικοινωνιών αποδεικνύονται αληθή για τους ακόλουθους σταθμούς:

Yakima, ΗΠΑ (120°Δυτικά, 46°Βόρεια)
Ο σταθμός ιδρύθηκε το 1970 συγχρόνως με την πρώτη γενεά δορυφόρων. Από το 1995 σταθμεύει εκεί η Intelligence Agency (AIA) με την 544η Intelligence Group (Detachment 4). Σταθμεύει επίσης εκεί η Naval Security Group (NAVSECGRU). Στον χώρο αυτό έχουν εγκατασταθεί έξι δορυφορικές κεραίες, για το μέγεθος των οποίων δεν προκύπτει τίποτα από τις πηγές. Ο Hager περιγράφει τις δορυφορικές κεραίες ως μεγάλες και δίνει την κατεύθυνσή τους προς δορυφόρους Intelsat υπεράνω του Ειρηνικού Ωκεανού (2 δορυφορικές κεραίες) και προς τον δορυφόρο Intelsat υπεράνω του Ατλαντικού, καθώς και την κατεύθυνση προς τον δορυφόρο Inmarsat 2.
Η ημερομηνία ίδρυσης του σταθμού Yakima συγχρόνως με την πρώτη γενεά δορυφόρων ersten Intelsat καθώς και η γενική περιγραφή καθηκόντων της 544ης Intelligence Group συνηγορούν για το ρόλο του σταθμού Yakima όσον αφορά την παγκόσμια παρακολούθηση των επικοινωνιών. Μία άλλη σχετική ένδειξη είναι η εγγύτητα του σταθμού Yakima προς ένα σταθμό υποδοχής δορυφόρων, ο οποίος βρίσκεται 100 μίλια βορειότερα.

Sugar Grove, USA (80°Δυτικά, 39°Βόρεια)
Ο σταθμός Sugar Grove ιδρύθηκε συγχρόνως με τη θέση σε λειτουργία της δεύτερης γενεάς δορυφόρων Intelsat κατά το τέλος της δεκαετίας του "70. Σταθμεύουν εδώ οι NAVSECGRU καθώς και η AIA με την 544η Intelligence Group (Detachment 3). Ο σταθμός διαθέτει, σύμφωνα με στοιχεία διαφόρων συγγραφέων, 10 δορυφορικές κεραίες, εκ των οποίων τρεις είναι μεγαλύτερες από 18 μέτρα (18,2 μέτρα, 32,3 μέτρα και 46 μέτρα) και κατ' αυτό τον τρόπο είναι σαφές ότι έχουν την αρμοδιότητα της παρακολούθησης δορυφόρων επικοινωνιών. Μία αποστολή του Detachment 3 της 544ης IG στο σταθμό είναι να διαθέτει "υποστήριξη πληροφοριών" για τη συλλογή πληροφοριών δορυφόρων επικοινωνιών από τους σταθμούς εκστρατείας του Ναυτικού.[38]
Πέραν αυτού, ο σταθμός Sugar Grove βρίσκεται κοντά (60 μίλια) στον δορυφορικό σταθμό στο Etam.

Sabana Seca, Πόρτο Ρίκο (66°Δυτικά, 18°Βόρεια)
Το 1952 εγκαταστάθηκε η NAVSECGRU στη Sabana Seca. Από το 1995 ευρίσκεται εκεί και η AIA με την 544η IG (Detachment 2). Ο σταθμός έχει τουλάχιστον μία δορυφορική κεραία διαμέτρου 32μέτρων και 4 άλλες δορυφορικές κεραίες.
Αποστολή του σταθμού είναι, σύμφωνα με επίσημα στοιχεία, η επεξεργασία δορυφορικής επικοινωνίας ("performing satellite communication processing"), "κρυπτογραφική και υπηρεσία επικοινωνιών " καθώς και η υποστήριξη του Ναυτικού και αποστολών της DoD (μεταξύ άλλων, συλλογή πληροφοριών του COMSAT (από περιγραφή της 544ης IG)). Στο μέλλον η Sabana Seca θα καταστεί ο πρώτος σταθμός εκστρατείας για την ανάλυση και επεξεργασία δορυφορικής επικοινωνίας.

Morwenstow, Αγγλία (4°Δυτικά, 51°Βόρεια)
Ο σταθμός Morwenstow ιδρύθηκε συγχρόνως με τον Yakima με την πρώτη γενεά δορυφόρων Intelsat κατά τις αρχές της δεκαετίας του '70. Φορέας λειτουργίας του Morwenstow είναι η βρετανική υπηρεσία πληροφοριών (GCHQ). Στο Morwenstow είναι εγκατεστημένες περίπου .

[38] "Παρέχει ενισχυμένη υποστήριξη πληροφοριών σε επιχειρησιακούς διοικητές της Πολεμικής Αεροπορίας και άλλους καταναλωτές πληροφοριών δορυφορικών επικοινωνιών που συλλέγονται από σταθμούς εκστρατείας που διοικούνται από το Ναυτικό." Από την ιστοσελίδα της 44ης Intelligence Group http://www.aia.af.mil

30 δορυφορικές κεραίες, δύο εκ των οποίων με διάμετρο 30 μέτρων· όσον αφορά το μέγεθος των άλλων κεραιών δεν υπάρχουν στοιχεία.
Όσον αφορά την αποστολή του σταθμού, δεν είναι τίποτα γνωστό από επίσημη πλευρά, το μέγεθος και ο αριθμός των δορυφορικών κεραιών καθώς και η θέση της μόνο 110 χλμ. από το σταθμό της Telekom στο Goonhilly δεν αφήνουν καμία αμφιβολία για τη λειτουργία του σταθμού ως σταθμού παρακολούθησης για δορυφόρους επικοινωνιών.

Menwith Hill, Αγγλία (2°Δυτικά, 53°Βόρεια)
Ο σταθμός του Menwith Hill ιδρύθηκε το 1956, και το 1974 διετίθεντο ήδη 8 δορυφορικές κεραίες. Εν τω μεταξύ έχουν εγκατασταθεί εκεί περίπου 30 δορυφορικές κεραίες, από τις οποίες ορισμένες έχουν διάμετρο μεγαλύτερη των 20 μέτρων. Στο Menwith Hill συνεργάζονται Βρετανοί και Αμερικανοί. Από την αμερικανική πλευρά βρίσκονται εκεί η NAVSECGRU, η AIA (451η IOS) καθώς και το INSCOM, που έχει τη διοίκηση του σταθμού. Το γήπεδο στο οποίο είναι εγκατεστημένος ο σταθμός Menwith Hill ανήκει στο Υπουργείο Άμυνας της Αγγλίας και έχει εκμισθωθεί στην αμερικανική κυβέρνηση. Σύμφωνα με επίσημα στοιχεία αποστολή του Menwith Hill είναι "να παρέχει ταχεία ραδιοεπικοινωνία και να διενεργεί έρευνα επικοινωνιών". Σύμφωνα με δηλώσεις του Richelson και της Federation of American Scientists είναι ο Menwith Hill τόσο επίγειος σταθμός για κατασκοπευτικούς δορυφόρους όσο και επίγειος σταθμός για ρωσικούς δορυφόρους επικοινωνιών.

Geraldton, Αυστραλία (114°Ανατολικά, 28°Νότια)
Ο σταθμός υπάρχει από τις αρχές της δεκαετίας του '90. Η διοίκηση του σταθμού ανήκει στις μυστικές υπηρεσίες της Αυστραλίας (DSD), οι Βρετανοί, οι οποίοι προηγουμένως ήταν σταθμευμένοι στο Χονγκ Κονγκ (βλ. ανωτέρω) ανήκουν τώρα στο προσωπικό αυτού του σταθμού. Έξι δορυφορικές κεραίες, εκ των οποίων τουλάχιστον μία έχει διάμετρο περίπου 20 μέτρων (εκτίμηση), είναι σύμφωνα με δήλωση του Hager στραμμένη σε δορυφόρους υπεράνω του Ινδικού Ωκεανού και σε δορυφόρους υπεράνω του Ειρηνικού Ωκεανού.
Σύμφωνα με στοιχεία που κατέθεσε ενόρκως εμπειρογνώμων από το Κοινοβούλιο της Αυστραλίας, παρακολουθούνται στο Geraldton δορυφόροι επικοινωνιών.[39]

Pine Gap, Αυστραλία (133°Ανατολικά, 23°Νότια)
Ο σταθμός στο Pine Gap ιδρύθηκε το 1966. Τη διοίκηση την έχουν οι μυστικές υπηρεσίες της Αυστραλίας (DSD)· τα μισά από τα εκεί σταθμεύοντα περίπου 900 πρόσωπα είναι Αμερικανοί της CIA και της NAVSECGRU.[40]
Ο σταθμός Pine Gap έχει 18 δορυφορικές κεραίες, εκ των οποίων μία με διάμετρο . 30 περίπου μέτρων και μία με διάμετρο 20 περίπου μέτρων. Σύμφωνα με επίσημα στοιχεία καθώς και στοιχεία διαφόρων συγγραφέων, ο σταθμός είναι από την έναρξη λειτουργίας του επίγειος σταθμός για δορυφόρους SIGINT. Από εδώ ελέγχονται και καθοδηγούνται διάφοροι κατασκοπευτικοί δορυφόροι καθώς και λαμβάνονται, γίνεται η επεξεργασία τους και αναλύονται τα σήματά τους. Οι μεγάλες δορυφορικές κεραίες συνηγορούν όμως και για την παρακολούθηση δορυφόρων επικοινωνιών, λόγω του ότι για τους δορυφόρους SIGINT δεν απαιτούνται μεγάλες δορυφορικές κεραίες. Έως το 1980 αποκλείονταν Αυστραλοί από το τμήμα

[39] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; http://www.aph.gov.au/hansard

[40] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; http://www.aph.gov.au/hansard

ανάλυσης των σημάτων, αλλά έκτοτε έχουν ελεύθερη πρόσβαση σε όλα εκτός από τον εθνικό κρυπτογραφικό χώρο των Αμερικανών.

Misawa, Ιαπωνία (141°Ανατολικά, 40°Βόρεια)
Ο σταθμός στη Misawa υπάρχει από το 1948· σταθμεύουν εκεί Ιάπωνες και Αμερικανοί. Από την αμερικανική πλευρά είναι εγκατεστημένες εκεί η NAVSECGRU, η INSCOM καθώς και ορισμένες ομάδες της AIA (544ξ IG, 301η IS,). Στο χώρο του σταθμού υπάρχουν περίπου 14 δορυφορικές κεραίες, από τις οποίες ορισμένες έχουν διάμετρο 20 περίπου μέτρων (εκτίμηση). Η Misawa χρησιμεύει επισήμως ως "Κέντρο Κρυπτογραφικών Επιχειρήσεων" Σύμφωνα με στοιχεία του Richelson παρακολουθούνται με τη βοήθεια της Misawa οι ρωσικοί δορυφόροι Molnyia καθώς και άλλοι ρωσικοί δορυφόροι επικοινωνιών.

Waihopai, Νέα Ζηλανδία (173°Ανατολικά, 41°Νότια)
Ο σταθμός Waihopai υπάρχει από το 1989. Έκτοτε υπάρχει μία μεγάλη κεραία με 18 μέτρα διάμετρο, μία δεύτερη μικρότερη κατασκευάστηκε αργότερα επιπλέον. Σύμφωνα με τον Hager η μεγάλη κεραία είναι στραμμένη προς τον Intelsat 701 πάνω από τον Ειρηνικό Ωκεανό.

Buckley Field, ΗΠΑ, Denver Κολοράντο (104°Δυτικά, 40°Βόρεια)
Ο σταθμός ιδρύθηκε το 1972. Σταθμεύει εκεί η 544η IG (Det. 45). Στο γήπεδο του σταθμού υπάρχουν περίπου 5 δορυφορικές κεραίες εκ των οποίων 4 έχουν διάμετρο περίπου 20 μέτρων. Επίσημη αποστολή του σταθμού είναι να συλλέγει δεδομένα για πυρηνικά γεγονότα από τους δορυφόρους SIGINT, να τα αξιολογεί και να τα αναλύει. Το μέγεθος των δορυφορικών κεραιών αποτελεί ένδειξη ότι διαδραματίζουν ρόλο κατά την παρακολούθηση μη στρατιωτικών επικοινωνιών.

Χονγκ Κονγκ (22°Βόρεια, 114°Ανατολικά)
Ο σταθμός ιδρύθηκε κατά το τέλος της δεκαετίας του '70 συγχρόνως με τη δεύτερη γενεά INTELSAT και είχε εξοπλισθεί με μεγάλες δορυφορικές κεραίες. Όσον αφορά τα ακριβή μεγέθη δεν υπάρχουν στοιχεία. Το 1994 άρχισε η διάλυση του σταθμού του Χονγκ Κονγκ και οι κεραίες μεταφέρθηκαν στην Αυστραλία. Ποιοι σταθμοί ανέλαβαν την αποστολή του Χονγκ Κονγκ δεν είναι σαφές: Geraldton, Pine Gap ή όμως ο σταθμός Misawa στην Ιαπωνία.
Ενδεχομένως, καταμερίστηκαν οι αποστολές σε διάφορους σταθμούς.

5.3.2.3.1.Άλλοι σταθμοί

Στους ακόλουθους σταθμούς δεν είναι δυνατόν με τη βοήθεια των ανωτέρω αναφερθέντων κριτηρίων να τεκμηριωθεί σαφώς η λειτουργία τους:

Leitrim, Καναδάς (75°Δυτικά, 45°Βόρεια)
Ο σταθμός Leitrim είναι τμήμα ενός προγράμματος ανταλλαγών μεταξύ καναδικών και αμερικανικών στρατιωτικών μονάδων. Για το λόγο αυτό σταθμεύουν στο Leitrim, σύμφωνα με στοιχεία του Ναυτικού, περίπου 30 πρόσωπα. Το 1985 εγκαταστάθηκε η πρώτη από 4 δορυφορικές κεραίες, από τις οποίες οι δύο μεγαλύτερες έχουν διάμετρο μόνο 12 μέτρα περίπου (εκτίμηση).
Αποστολή του σταθμού είναι, σύμφωνα με επίσημα στοιχεία, "η κρυπτογραφική βαθμολόγηση" και η παρακολούθηση διπλωματικών επικοινωνιών.

Bad Aibling, Γερμανία (12°Ανατολικά, 47°Βόρεια)

Ο σταθμός κοντά στο Bad Aiblings, στον οποίο εργάζονται περίπου 750 Αμερικανοί, αναλήφθηκε το 1952 από τον Αμερικανικό στρατό (από το 1972 έως το 1994 βρισκόταν στα χέρια του Υπουργείου Αμύνης). Σταθμεύουν στο Bad Aibling οι NAVSECGRU, INSCOM (66η IG, η 718 IG) καθώς και διάφορες ομάδες της AIA (402nd IG, 26th IOG). Υπάρχουν εκεί εγκατεστημένες 14 δορυφορικές κεραίες, από τις οποίες καμία δεν είναι μεγαλύτερη από 18 μέτρα. Σύμφωνα με επίσημα στοιχεία, έχει το Bad Aibling τις ακόλουθες αποστολές: "ταχεία ραδιοζεύξη και ασφαλείς επικοινωνίες, υποστήριξη στο Υπουργείο Άμυνας και ενοποιημένες διοικήσεις, μεσαίες και μακρές επικοινωνίες HFκαι επικοινωνίες δορυφόρων, έρευνα στη φυσική των επικοινωνιών, εξοπλισμός δοκιμών και αξιολόγηση επικοινωνιών". Σύμφωνα με τον Richelson είναι το Bad Aibling επίγειος σταθμός για δορυφόρους SIGINT και για ρωσικούς δορυφόρους επικοινωνιών.

Άγιος Νικόλαος, Κύπρος (32°Ανατολικά, 35°Βόρεια)
Ο Άγιος Νικόλαος στην Κύπρο είναι ένας βρετανικός σταθμός. Οι αποστολές του σταθμού με 9 δορυφορικές κεραίες, των οποίων το μέγεθος είναι άγνωστο, κατανέμονται σε δύο μονάδες, στην "Signals Regiment Radio και στην Signals Unit (RAF)".
Η θέση του Αγίου Νικολάου πλησίον των αραβικών κρατών και το γεγονός ότι ο Άγιος Νικόλαος είναι ο μοναδικός σταθμός εντός ορισμένων αποτυπωμάτων δέσμης (κυρίως Spot-Beams) σ' αυτόν τον τομέα, συνηγορούν για έναν σημαντικό ρόλο αυτού του σταθμού στην απόκτηση πληροφοριών.

Shoal Bay, Αυστραλία (134°Ανατολικά, 13°Νότια)
Ο σταθμός Shoal Bay είναι σταθμός που λειτουργεί μόνο από την Υπηρεσία Πληροφοριών της Αυστραλίας. Εικάζεται ότι ο σταθμός έχει 10 δορυφορικές κεραίες των οποίων το μέγεθος δεν περιγράφεται εγγύτερα. Σε φωτογραφίες που φαίνονται οι δορυφορικές κεραίες έχουν οι μεγαλύτερες 5 διάμετρο 8 μέτρων κατ' ανώτατο όριο, η διακρινόμενη έκτη κεραία είναι ακόμη μικρότερη. Σύμφωνα με στοιχεία του Richelson οι κεραίες είναι στραμμένες στον δορυφόρο της Ινδονησίας PALAPA. Εάν ο σταθμός αποτελεί τμήμα του παγκοσμίου συστήματος παρακολούθησης μη στρατιωτικών επικοινωνιών είναι ασαφές.

Guam, Ειρηνικός Ωκεανός (144°Ανατολικά, 13°Νότια)
Ο σταθμός του Guam υπάρχει από το 1898. Τώρα υπάρχει εκεί ένας ναυτικός σταθμός πληροφορικής και τηλεπικοινωνιών, στον οποίο σταθμεύουν οι 544th IG της AIA καθώς και ναύτες.
Υπάρχουν στο σταθμό τουλάχιστον δύο δορυφορικές κεραίες που, όσον αφορά το μέγεθός τους, τίποτα δεν είναι γνωστό. Για το λόγο αυτό η λειτουργία του Guam παραμένει ασαφής.

Kunia, Χαβάη (158°Δυτικά, 21°Βόρεια)
Ο σταθμός αυτός είναι από το 1993 περιφερειακό κέντρο επιχειρήσεων ασφάλειας (RSOC) σε λειτουργία, και λειτουργεί από την NAVSECGRU και την AIA. Στις αποστολές του συμπεριλαμβάνεται η διάθεση πληροφοριών και επικοινωνίας καθώς και κρυπτογραφική υποστήριξη. Η λειτουργία της Kunia παραμένει ασαφής.

Medina Annex, ΗΠΑ Τέξας (98°Δυτικά, 29°Βόρεια)
Η Medina είναι, όπως και η Kunia, ένα περιφερειακό κέντρο επιχειρησιακής ασφάλειας – που ιδρύθηκε το 1993 – που λειτουργεί με μονάδες της NAVSECGRU και της AIA με αποστολές στην Καραϊβική.

Fort Gordon (81°Δυτικά, 31°Βόρεια)
Ο σταθμός Fort Gordon είναι επίσης ένα περιφερειακό κέντρο επιχειρησιακής ασφάλειας, που λειτουργεί από την INSCOM και την AIA (702nd IG, 721st IB, 202nd IB, 31st IS) με ασαφείς αποστολές.

Fort Mead, ΗΠΑ (76°Δυτικά, 39°Βόρεια)
Ο σταθμός Fort Mead είναι το επιτελείο της NSA.

5.3.3. Σύνοψη των αποτελεσμάτων

Τα ακόλουθα συμπεράσματα συνάγονται από τα συλλεγέντα δεδομένα σχετικά με τους σταθμούς, τους δορυφόρους και τις ανωτέρω περιγραφείσες προϋποθέσεις:

1. Υπάρχουν σε κάθε αποτύπωμα δέσμης σταθμοί παρακολούθησης για τουλάχιστον ορισμένες από τις Global-Beams με εκάστοτε τουλάχιστον μία κεραία με διάμετρο μεγαλύτερη των 18 μέτρων, οι οποίες λειτουργούν με Αμερικανούς ή Βρετανούς ή όπου Αμερικανοί ή Βρετανοί ασκούν δραστηριότητες μυστικών υπηρεσιών. Αυτό αποτελεί μία σοβαρή ένδειξη για την ύπαρξη ενός παγκόσμιου συστήματος παρακολούθησης.

2. Η ανάπτυξη των επικοινωνιών INTELSAT και η σύγχρονη δημιουργία αντίστοιχων σταθμών παρακολούθησης τεκμηριώνουν τον παγκόσμιο προσανατολισμό του συστήματος.

3. Από το σημείο 1 και 2 είναι δυνατόν να αναγνωρισθούν ορισμένοι σταθμοί σαφώς ως σταθμοί οι οποίοι παρακολουθούν διεθνή δορυφορική επικοινωνία.

4. Στοιχεία στα αποχαρακτηρισμένα έγγραφα και αυτά των φορέων εκμετάλλευσης (AIA, NSA, Ναυτικό, κλπ.) πρέπει να αξιολογηθούν ως απόδειξη για τους εκεί αναφερθέντες σταθμούς.

5. Ορισμένοι σταθμοί βρίσκονται συγχρόνως σε Beams καθώς και Spots διαφόρων δορυφόρων, κατά τρόπο που μεγάλο τμήμα των επικοινωνιών είναι δυνατόν να συλληφθεί.

6. Υπάρχουν ορισμένοι άλλοι σταθμοί, που δεν διαθέτουν μεγάλες κεραίες, οι οποίοι όμως είναι δυνατόν να αποτελούν τμήμα του συστήματος. λόγω του ότι είναι δυνατόν να λαμβάνουν επικοινωνίες από τα Beams και τα Spots. Εν προκειμένω, πρέπει κανείς να μην χρησιμοποιήσει την ένδειξη του μεγέθους των κεραιών αλλά να χρησιμοποιήσει άλλες ενδείξεις.

7. Ορισμένοι από τους αναφερθέντες σταθμούς βρίσκονται αποδεδειγμένα σε άμεση εγγύτητα κανονικών επίγειων σταθμών δορυφόρων επικοινωνιών.

5.4. Η συμφωνία UKUSA (Ηνωμένου Βασιλείου-ΗΠΑ)

Ως συμφωνία UKUSA χαρακτηρίζεται μία συμφωνία SIGINT που υπεγράφη μεταξύ της Μεγάλης Βρετανίας και των Ηνωμένων Πολιτειών καθώς και της Αυστραλίας, του Καναδά και της Νέας Ζηλανδίας.

5.4.1. Ιστορική εξέλιξη της συμφωνίας UKUSA[41]

Η συμφωνία ΗΒΗΠΑ αποτελεί τη συνέχεια της ήδη κατά τον Β' Παγκόσμιο Πόλεμο πολύ στενής συνεργασίας των Ηνωμένων Πολιτειών και της Μεγάλης Βρετανίας, η οποία είχε ήδη σημειωθεί κατά τον Α' Παγκόσμιο Πόλεμο.

Η πρωτοβουλία για τη δημιουργία μιας συμμαχίας SIGINT προέκυψε τον Αύγουστ του 1940 σε μία συνάντηση Αμερικανών και Βρετανών στο Λονδίνο εκ μέρους των Αμερικανών.[42] Το Φεβρουάριο του 1941 οι αμερικανοί κρυπτοαναλυτές παρέδωσαν στην Βρετανία μια συσκευή Cipher (PURPLE). Την άνοιξη του 1941 άρχισε η συνεργασία στην κρυπτογραφική ανάλυση.[43] Η συνεργασία των μυστικών υπηρεσιών ενισχύθηκε με την κοινή επιχείρηση των στόλων στο Βόρειο Ατλαντικό κατά το καλοκαίρι του 1941. Τον Ιούνιο του 1941 μπόρεσαν οι Βρετανοί να σπάσουν τον γερμανικό κώδικα του στόλου ENIGMA:

Η είσοδος της Αμερικής στον πόλεμο ενίσχυσε περαιτέρω τη συνεργασία SIGINT. Το 1942 άρχισαν να εργάζονται Αμερικανοί κρυπτογράφοι της "Ναυτικής Υπηρεσίας SIGINT" στη Μεγάλη Βρετανία.[44] Η επικοινωνία μεταξύ των αιθουσών εντοπισμού υποβρυχίων στο Λονδίνο, Ουάσιγκτον και, από το Μάιο του 1943, στην Οττάβα του Καναδά, ήταν τόσο στενή, ώστε σύμφωνα με δήλωση κάποιου που συμμετείχε τότε, εργάζονταν ως μία μοναδική οργάνωση.[45]

Το πρώτο εξάμηνο του 1943 υπεγράφη η συμφωνία BRUSA-SIGINT και πραγματοποιήθηκε ανταλλαγή προσωπικού. Το περιεχόμενο της συμφωνίας αφορά κυρίως τον καταμερισμό της εργασίας και συνοψίζεται στις πρώτες τρεις παραγράφους της: περιέχουν την ανταλλαγή οιωνδήποτε πληροφοριών από την ανακάλύψη, εντοπισμό και παρακολούθηση σημάτων καθώς και την λύση κωδίκων και κρυπτογραφήσεων. Οι Αμερικανοί ήταν κυρίως υπεύθυνοι για την Ιαπωνία, οι Βρετανοί για τη Γερμανία και Ιταλία.[46]

Μετά τον πόλεμο, η πρωτοβουλία για τη διατήρηση της συμμαχίας SIGINT ξεκίνησε κυρίως από τη Μεγάλη Βρετανία. Η βάση γι' αυτό το σκοπό συμφωνήθηκε σε μία παγκόσμια περιοδεία βρετανών πρακτόρων μυστικών υπηρεσιών (μεταξύ άλλων ο Sir Harry Hinsley, του οποίου τα βιβλία αποτελούν τη βάση του αναφερόμενου άρθρου) κατά το πρώτο εξάμηνο του 1945. Ένας στόχος ήταν να αποσταλεί προσωπικό του SIGINT από την Ευρώπη προς τον Ειρηνικό Ωκεανό

---

[41] Christopher Andrew, "The making of the Anglo-American SIGINT Alliance" in E. Hayden, h. Peake and S. Halpern eds, In the Name of Inteligence. Essays in honor of Washington Pforzheimer (Washington NIBC Press 1995) σελ. 95 -109

[42] όπου ανωτέρω, σελ. 99: „At a metteing in London on 31 August 1940 between the British Chiefs of Staff and the American Military Observer Mission, the US Army representative, Brigadier General George V. Strong, reported that ´it had recently been arranged in principle between the British and the United States Governments that periodic exchange of information would be desirable,´ and said that ´the time had come or a free exchange of intelligence´. (COS (40)289, CAB 79/6, PRO. Smith, The Ultra Magic Deals, pp. 38, 43-4. Sir F.H. Hinsley, et al., British Intellgence in the Second Worls War, vol.I, pp.312-13)

[43] όπου ανωτέρω, σελ.. 100: „ In the spring of 1941, Steward Menzies, the Chief of SIS, appointed an SIS liason officer to the British Joint Services Missin in Washington, Tim O´Connor, …, to advice him on cryptologic collaboration" (

[44] όπου ανωτέρω, σελ. 100 (Sir F.H. Hinsley, et al., British Intellgence in the Second Worls War, vol II, p.56)

[45] όπου ανωτέρω, σελ. 101 (Sir F.H. Hinsley, et al., British Intellgence in the Second Worls War, vol. II, p 48)

[46] όπου ανωτέρω, σελ. 101-2: Interivews mit Sir F.H. Hinsley, „Operations of the Military Intelligence Service War Department London (MIS WD London)," 11 June 1945, Tab A, RG 457 SRH-110, NAW

για τον πόλεμο με την Ιαπωνία. Στο πλαίσιο αυτό συμφωνήθηκε με την Αυστραλία, να διατεθούν στις υπηρεσίες της Αυστραλίας πόροι και προσωπικό (Βρετανοί). Κατά την επιστροφή στις Ηνωμένες Πολιτείες ο δρόμος οδήγησε στη Νέα Ζηλανδία και τον Καναδά.

Το Σεπτέμβριο του 1945 υπέγραψε ο Τρούμαν ένα άκρως απόρρητο μνημόνιο, το οποίο αποτελεί τον ακρογωνιαίο λίθο της συμμαχίας SIGINT σε ειρηνική περίοδο.[47] Αμέσως κατόπιν ξεκίνησαν διαπραγματεύσεις μεταξύ Βρετανών και Αμερικανών για μια συμφωνία. Μία βρετανική αντιπροσωπεία ήρθε πέραν αυτού σε επαφή με τους Καναδούς και τους Αυστραλούς, προκειμένου να συζητήσει μια ενδεχόμενη συμμετοχή. Το Φεβρουάριο και το Μάρτιο του 1946 πραγματοποιήθηκε μία άκρως απόρρητη αγγλοαμερικανική διάσκεψη SIGINT, προκειμένου να συζητηθούν λεπτομέρειες. Οι Βρετανοί είχαν εξουσιοδοτηθεί από τους Καναδούς και τους Αυστραλούς. Προϊόν της διάσκεψης υπήρξε μία ακόμη χαρακτηρισμένη συμφωνία 25 περίπου σελίδων, που επισφράγισε τις λεπτομέρειες μιας συμφωνίας SIGINT μεταξύ των ΗΠΑ και της Βρετανικής Κοινοπολιτείας. Περαιτέρω διαπραγματεύσεις ακολούθησαν τα επόμενα δύο χρόνια, ώστε το τελικό κείμενο της αποκαλούμενης Συμφωνίας UKUSA να υπογραφεί τον Ιούνιο του 1948.[48]

5.4.2. Αποδείξεις για την ύπαρξη της συμφωνίας

Μέχρι τώρα δεν υπάρχει καμία επίσημη αναγνώριση της συμφωνίας UKUSA από τις υπογράφουσες χώρες. Ωστόσο, υπάρχουν πολλές σαφείς αποδείξεις για την ύπαρξή της.

5.4.2.1. Ο κατάλογος ακρωνυμίων του Ναυτικού

Το ακρωνύμιο UKUSA σημαίνει, σύμφωνα με το Ναυτικό των ΗΠΑ[49] "Ηνωμένο Βασίλειο-ΗΠΑ" και χαρακτηρίζει μία "συμφωνία SIGINT 5 κρατών".

5.4.2.2. Δήλωση του Διευθυντή της DSD

Ο Διευθυντής της Υπηρεσίας Πληροφοριών της Αυστραλίας (DSD) επιβεβαίωσε την ύπαρξη αυτής της συμφωνίας σε μία συνέντευξη: σύμφωνα με τις πληροφορίες που έδωσε, εργάζονται οι μυστικές υπηρεσίες της Αυστραλίας με άλλες υπερπόντιες υπηρεσίες πληροφοριών στο πλαίσιο της συμφωνίας UKUSA.[50]

---

[47] Truman, Memorandum for the Secretaries of the State, War and the Navy, 12 Sept. 1945: „The Secretary of War and the Secretary of the Navy are hereby authorised ti direct the Chief of Staff, U.S. Army and the Commander in Chief, U.S. Fleet; and Chief of Naval Oerations to continue collaboration in the field of communication intelligence between the United States Army and Navy and the British, and to extend, modify or discontinue this collaboration, as determined to be in the best interests of the United States.“ (from Bradley F. Smith, The Ultra-Magic Deals and the Most Secret Special Relationship (Novato, Ca: Presidio 1993))

[48] Christopher Andrew, “The making of the Anglo-American SIGINT Alliance” in E. Hayden, h. Peake and S. Halpern eds, In the Name of Inteligence. Essays in honor of Washington Pforzheimer (Washington NIBC Press 1995) pp. 95 –109: Interviews with Sir Harry Hinsley, March/April 1994, who did a part of the negotiations; Interviews with Dr. Louis Tordella, Deputy Director of NSA from 1958 to 1974, who was present at the signing

[49] „Όροι/Συντμήσεις/Ακρωνύμια“ που δημοσιεύθηκε από το Κέντρο Εκπαίδευσης Πληροφοριών του Ναυτικού και του Σώματος Πεζοναυτών των ΗΠΑ (NMITC) στην θέση http://www.cnet.navy.mil/nmitc/training/u.html

[50] Martin Brady, Διευθυντής της DSD, Καμπέρα 16 Μαρτίου 2000

5.4.2.3. Έκθεση της Κοινοβουλευτικής Επιτροπής για την Ασφάλεια και τις Πληροφορίες του Καναδικού Κοινοβουλίου

Στην έκθεση αυτή περιγράφεται ότι ο Καναδάς με ορισμένους από τους στενότερους και παλαιότερους συμμάχους του συνεργάζεται σε θέματα πληροφοριών. Η έκθεση κατονομάζει αυτούς τους συμμάχους: Ηνωμένες Πολιτείες (NSA), Μεγάλη Βρετανία (GCHQ), Αυστραλία (DSD) και Νέα Ζηλανδία (GCSB). Το όνομα της συμφωνίας δεν αναφέρεται στην έκθεση.

5.4.2.4. Δήλωση του πρώην Αναπληρωτή Διευθυντή της NSA, Δρ. Louis Torella

Σε μία συνέντευξη με τον Christopher Andrew, Καθηγητή στο Πανεπιστήμιο του Κέιμπριτζ, το Νοέμβριο του 1987 και τον Απρίλιο του 1992, επιβεβαιώνει ο πρώην Αναπληρωτής Διευθυντής της NSA, Δρ. Louis Torella, ο οποίος ήταν παρών κατά την υπογραφή, την ύπαρξη της συμφωνίας.[51]

5.4.2.5. Επιστολή του πρώην Διευθυντή της GCHQ, Joe Hooper

Ο πρώην Διευθυντής της GCHQ Joe Hooper αναφέρει σε μια επιστολή προς τον πρώην Διευθυντή της NSA Στρατάρχη S.Carter τη συμφωνία UKUSA.

5.4.2.6. Συνομιλητές του εισηγητή

Ο εισηγητής μίλησε με πολλά πρόσωπα, τα οποία λόγω των καθηκόντων τους πρέπει να γνωρίζουν τη συμφωνία UKUSA και το περιεχόμενό της, για τη συμφωνία. Εν προκειμένω επιβεβαιώθηκε έμμεσα εν πάση περιπτώσει η ύπαρξή της, λόγω του είδους των απαντήσεων.

5.5. Αξιολόγηση αμερικανικών αποχαρακτηρισμένων εγγράφων

5.5.1. Το είδος των εγγράφων

Στα πλαίσια του "Freedom of Information Acts" του 1966 (5 U.S.C. § 552) και των ρυθμίσεων του Υπουργείου Άμυνας (Κανονισμός DoD FOIA 5400.7-R του 1997) για πρώτη φορά αποχαρακτηρίσθηκαν και κατέστησαν με τον τρόπο αυτό προσβάσιμα στο κοινό έγγραφα, που πριν ήταν απόρρητα.
Η δημόσια πρόσβαση στα έγγραφα αυτά γίνεται δια του 1985 ιδρυθέντος Εθνικού Αρχείου Ασφαλείας του Πανεπιστημίου George Washington στην Washington. Ο συντάκτης Jeffrey Richelson, πρώην μέλος του Εθνικού Αρχείου Ασφαλείας, κατέστησε προσιτά μέσω Διαδικτύου 16 έγγραφα, τα οποία προσφέρουν γνώση για την γέννηση, την εξέλιξη, την διοίκηση και την εντολή της NSA.[52] Πέραν αυτών, σε δύο από τα έγγραφα αναφέρεται το"ECHELON". Οι διάφοροι συντάκτες, που έχουν γράψει για το σύστημα ECHELON, αναφέρονται επανειλημμένα στα έγγραφα αυτά και τα χρησιμοποιούν ως απόδειξη για την ύπαρξη του παγκόσμιου κατασκοπευτικού δικτύου ECHELON. Περαιτέρω, στα έγγραφα που διατέθηκαν από τον Richelson συγκαταλέγονται κάποια, που επιβεβαιώνουν την ύπαρξη της NRO (National

[51] Andrew, Christopher „The growth of the Australian Intelligence Community and the Anglo-American Connection", σελ. 223-4

[52] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

Reconnaissance Office) και περιγράφουν τη λειτουργία της ως διαχειριστή και λειτουργό δορυφόρων SIGINT.[53]

5.5.2. Περιεχόμενο των εγγράφων

Τα έγγραφα περιέχουν αποσπασματικές περιγραφές ή αναφορές των ακόλουθων θεμάτων:

5.5.2.1 Αποστολή και σχεδιασμός της NSA (έγγραφα 1, 4, 10, 11, 16)

Από την 10η Μαρτίου 1950 προσδιορίζεται στο Εθνικό Συμβούλιο Ασφαλείας Πληροφορικών Οδηγία 9 (NSCID 9), για τους σκοπούς της COMINT, η έννοια της επικοινωνίας εξωτερικού. Σύμφωνα με τον ορισμό αυτό, η **επικοινωνία εξωτερικού συμπεριλαμβάνει κάθε είδους κυβερνητική επικοινωνία με την ευρεία έννοια (όχι μόνον τη στρατιωτική) καθώς και κάθε άλλη επικοινωνία, η οποία θα μπορούσε να περιέχει πληροφορίες στρατιωτικής, πολιτικής, επιστημονικής ή οικονομικής αξίας**.

Η οδηγία (NSCID 9 αναθ., 29. 12. 52) διευκρινίζει ρητά, ότι αρμόδιο για την εσωτερική ασφάλεια είναι μόνον το Ομοσπονδιακό Γραφείο Ερευνών.
Το Υπουργείο Εθνικής Άμυνας (DoD) οδηγία από 23 Δεκεμβρίου 1091 σχετικά με την NSA και την Κεντρική Υπηρεσία Ασφαλείας (CSS) ορίζει τον σχεδιασμό για την NSA ως εξής:

- Η NSA είναι μία αυτόνομα οργανωμένη υπηρεσία εντός του Υπουργείου Εθνικής Ασφάλειας υπό την διεύθυνση του Αναπληρωτή Υπουργού Εθνικής Άμυνας.
- Η NSA αφενός μεριμνά για την εκπλήρωση της αποστολής SIGINT των ΗΠΑ, αφετέρου διαθέτει ασφαλή συστήματα επικοινωνίας σε όλα τα τμήματα και τις υπηρεσίες.
- Οι δραστηριότητες SIGINT της NSA δεν περιλαμβάνουν τη δημιουργία και τη διανομή έτοιμων πληροφοριών. Αυτό υπάγεται στις αρμοδιότητες άλλων τμημάτων και υπηρεσιών

Επίσης, η Οδηγία του Υπουργείου Εθνικής Ασφαλείας του 1991 περιγράφει τη δομή της NSA και του CSS.
Στο υπόμνημά του ενώπιον της μόνιμης ειδικής επιτροπής ελέγχου των υπηρεσιών πληροφοριών της Βουλής των Αντιπροσώπων στις 12 Απριλίου 2000, ο διευθυντής της NSA Hayden ορίζει τα καθήκοντα της NSA ως εξής:

- Μέσω ηλεκτρονικής παρακολούθησης συλλέγεται επικοινωνία εξωτερικού για στρατιωτικούς και πολιτικούς σκοπούς
- η NSA παρέχει πληροφορίες σε αξιωματούχους της αμερικανικής κυβέρνησης σχετικά με τη διεθνή τρομοκρατία, τα ναρκωτικά, την προμήθεια όπλων
- δεν υπάγεται στα καθήκοντα της NSA η συλλογή όλων των επικοινωνιών
- η NSA μπορεί να παραδίδει πληροφορίες μόνον σε παραλήπτες εξουσιοδοτημένους από την κυβέρνησης, όχι όμως άμεσα σε αμερικανικές εταιρίες

Σε ένα μνημόνιο του υποναυάρχου του αμερικανικού ναυτικού W.O. Studeman από 8 Απριλίου 1992 εξ ονόματος της κυβέρνησης, γίνεται αναφορά στο καθήκον της NSA σε διεθνές επίπεδο, εκτός της υποστήριξης στρατιωτικών επιχειρήσεων.

5.5.2.2. Εξουσίες των Υπηρεσιών Πληροφοριών (έγγραφο 7)

Από την αμερικανική οδηγία 18 περί σημάτων πληροφοριών (USSID 18) προκύπτει, ότι γίνεται παρακολούθηση καλωδίων και ραδιοσημάτων.

[53] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/index.html

5.5.2.3. Καταγραφή ενεργών σε σταθμούς “ECHELON” μονάδων (έγγραφα 9, 12)

Στις αρμοδιότητες του Συμβουλίου Πληροφοριών Επικοινωνιών των ΗΠΑ ανήκει εκτός των άλλων η παρακολούθηση όλων των διακανονισμών (“arrangements”) με αλλοδαπές κυβερνήσεις στον τομέα COMINT. Ένα από τα καθήκοντα του διευθυντή της NSA είναι, να διαχειρίζεται όλες τις σχέσεις με αλλοδαπές υπηρεσίες COMINT.

5.5.2.4. Καταγραφή ενεργών σε σταθμούς “ECHELON” μονάδων (έγγραφα 9, 12)

Στις οδηγίες της NAVSECGRU C5450.48A περιγράφονται η αποστολή, η λειτουργία και ο σκοπός της Naval Security Group Activity (NAVSECGRUACT), η 544η ομάδα πληροφοριών στη Sugar Grove, Δυτική Βιρτζίνια. Εδώ αναφέρεται, ότι μία ιδιαίτερη αρμοδιότητα είναι: η διατήρηση και η λειτουργία ενός σταθμού ECHELON. Επίσης, ως καθήκον αναφέρεται η επεξεργασία πληροφοριών μυστικών υπηρεσιών.

Στο έγγραφο “History of the Air Intelligence Agency – 1η Ιανουαρίου έως 31 Δεκεμβρίου 1994 (RCS: HAF-HO(A&SA)7101 τόμος 1) αναφέρεται στο σημείο “Ενεργοποίηση των μονάδων Echelon” η Υπηρεσία Πληροφοριών της Αεροπορίας (AIA), αποσπάσματα 2 και 3:

Τα έγγραφα δεν παρέχουν πληροφορίες σχετικά με το τι είναι οι σταθμοί “ECHELON”, τι γίνεται με έναν σταθμό “ECHELON” και τι σημαίνει το ψευδώνυμο ECHELON. Από τα έγγραφα δεν προκύπτει τίποτα σχετικά με τη συμφωνία UKUSA.

5.5.2.5. Καταγραφή σταθμών (έγγραφα 6, 9, 12)

- Sugar Grove, Δυτική Βιρτζίνια στις οδηγίες NAVSECGRU C5450.48A
- Αεροπορική Βάση Misawa, Ιαπωνία στην History of the Air Intelligence Agency - Ιανουάριος - 31 Δεκεμβρίου 1994 (RCS: HAF-HO(A&SA)7101 τόμος 1)
- Πουέρτο Ρίκο (i.e. Sabana Seca), ibid.
- Γκουάμ, ibid.
- Yakima, στην πολιτεία Washington, ibid.
- Fort Meade, Maryland, μία αναφορά COMINT της NSA από το οχυρό George G. Meade, Maryland από 31 Αυγούστου 1972 αποδεικνύει τις εκεί δραστηριότητες COMINT.

5.5.2.6. Προστασία του ιδιωτικού βίου των αμερικανών πολιτών (έγγραφα 7, 7α έως στ, 11,16)

Στις οδηγίες NAVSECGRU C5450.48A ορίζεται, ότι πρέπει να διασφαλίζεται ο ιδιωτικός βίος των πολιτών.
Στα διάφορα έγγραφα αναφέρεται με ποιον τρόπο πρέπει να προστατεύεται ο ιδιωτικός βίος των αμερικανών πολιτών (Baker, General Counsel, NSA, έγγραφο από 9 Σεπτεμβρίου 1992, Οδηγία των ΗΠΑ για τις πληροφορίες από σήματα (USSID) 18, 20 Οκτωβρίου 1980, και διάφορες συμπληρώσεις.[54]

[54] Dissemination of U.S. Government Organizations and Officials, μνημόνιο 5 Φεβρουαρίου 1993; Reporting Guidance on References to the First Lady, 8 Ιουλίου 1993; Reporting Guidance on Former President Carter’s Involvement in the Bosnian Peace Process, 15 Δεκεμβρίου 1994; Understanding USSID 18, 30 Σεπτεμβρίου 1997; οδηγία USSID 18, 14 Φεβρουαρίου 1998;
NSA/US IDENTITIES IN SIGINT, Μάρτιος 1994; Statement for the record of NSA Director Lt Gen Michael V. Hayden, USAF, 12 Απριλίου 2000)

5.5.2.7. Ορισμοί (έγγραφα 4, 5α,7)

Η οδηγία του Υπουργείου Εθνικής Άμυνας από 23 Δεκεμβρίου 1991 προσφέρει ακριβείς ορισμούς των πληροφοριών από σήματα, των πληροφοριών επικοινωνιών, των ηλεκτρονικών πληροφοριών και των πληροφοριών τηλεπικοινωνιών, όπως επίσης και η οδηγία του Εθνικού Συμβουλίου για την Ασφάλεια Πληροφοριών αριθ. 6 από 17 Φεβρουαρίου1972.

Σύμφωνα με αυτές, COMINT σημαίνει η συλλογή και η επεξεργασία επικοινωνιών εξωτερικού (με ηλεκτρομαγνητικά μέσα) εκτός από την παρακολούθηση και την επεξεργασία μη κρυπτογραφημένης επικοινωνίας, ΜΜΕ, προπαγάνδας, εκτός και αν είναι κρυπτογραφημένα.

5.5.3. Συγκεφαλαίωση

1. Ήδη 50 χρόνια πριν, το ενδιαφέρον δεν στρεφόταν μόνον σε πληροφορίες προερχόμενες από τους τομείς της πολιτικής και της ασφάλειας, αλλά αφορούσε και στην επιστήμη και στην οικονομία.
2. Τα έγγραφα αποδεικνύουν ότι η NSA συνεργάζεται με άλλες υπηρεσίες COMINT.
3. Τα έγγραφα που παρέχουν πληροφορίες σχετικά με το πώς είναι οργανωμένη η NSA και ποια είναι τα καθήκοντά της, καθώς και ότι υπάγεται στο Υπουργείο Εθνικής Άμυνας, ουσιαστικά δεν προσφέρουν κάτι περισσότερο από αυτά που μπορεί κανείς να μάθει από την ιστοσελίδα της NSA που είναι προσπελάσιμη από όλους.
4. Η παρακολούθηση καλωδίων επιτρέπεται.
5. Η 544η ομάδα πληροφοριών και τα τμήματα 2 και 3 της Υπηρεσίας Πληροφοριών Αεροπορίας συμμετέχουν στη συλλογή πληροφοριών για τις μυστικές υπηρεσίες.
6. Ο όρος "ECHELON" εμφανίζεται σε διαφορετικά πλαίσια.
7. Οι τοποθεσίες Sugar Grove στη Δυτική Βιρτζίνια, Αεροπορική Βάση Misawa στην Ιαπωνία, Πουέρτο Ρίκο (δηλ. Sabana Seca), Γκουάμ, Yakima στην Πολιτεία Washington αναφέρονται ως σταθμοί SIGINT
8. Τα έγγραφα παρέχουν πληροφορίες για το πως πρέπει να προστατευθεί ο ιδιωτικός βίος των αμερικανών πολιτών.

Τα έγγραφα δεν αποτελούν απόδειξη, αποτελούν όμως ισχυρές ενδείξεις, οι οποίες, σε συνδυασμό με άλλες ενδείξεις, επιτρέπουν την εξαγωγή συμπερασμάτων.

5.6. Στοιχεία ειδικών συντακτών και δημοσιογράφων

5.6.1. Το βιβλίο του Nicky Hager

Στο βιβλίο του Nicky Hager "Secret Powers – New Zealand's role in the international spy network", που δημοσιεύτηκε το 1996, περιγράφεται για πρώτη φορά λεπτομερώς το σύστημα ECHELON. Σύμφωνα με το βιβλίο αυτό, το σύστημα τέθηκε σε λειτουργία το 1947, όταν το Ηνωμένο Βασίλειο και οι Ηνωμένες Πολιτείες συμφώνησαν, σε συνέχεια της συνεργασίας τους κατά τη διάρκεια του πολέμου, να εξακολουθήσουν από κοινού τις μέχρι τότε δραστηριότητες COMINT σε παγκόσμιο επίπεδο. Τα κράτη θα συνεργάζονταν με σκοπό τη δημιουργία ενός παγκοσμίου συστήματος παρακολούθησης, διαχωρίζοντας τον απαιτούμενο ειδικό εξοπλισμό και τις σχετικές προκύπτουσες δαπάνες και θα αποκτούσαν από κοινού πρόσβαση στα

αποτελέσματα. Στη συνέχεια προσχώρησαν στη συμφωνία μεταξύ Ηνωμένου Βασιλείου και Ηνωμένων Πολιτειών ο Καναδάς, η Αυστραλία και η Νέα Ζηλανδία.

Σύμφωνα με όσα αναφέρει ο Hager, η παρακολούθηση δορυφορικής επικοινωνίας αποτελεί τον πυρήνα του σημερινού συστήματος. Ήδη τη δεκαετία του 1970 άρχισε η παρακολούθηση μέσω επίγειων σταθμών τις πληροφορίες που διαβιβάζονταν μέσω του δορυφόρου Intel – το πρώτο παγκόσμιο σύστημα δορυφορικής επικοινωνίας[55]. Οι πληροφορίες αυτές ελέγχονταν στη συνέχεια μέσω ηλεκτρονικού υπολογιστή, με τη χρήση λέξεων κλειδιών ή διευθύνσεων, προκειμένου να φιλτραριστούν οι ενδιαφέρουσες πληροφορίες. Αργότερα, η παρακολούθηση επεκτάθηκε και σε άλλους δορυφόρους, π.χ. στον Inmarsat[56], που επικεντρωνόταν στις θαλάσσιες επικοινωνίες.

Ο Hager επισημαίνει στο βιβλίο του ότι η παρακολούθηση δορυφορικής επικοινωνίας αποτελεί μόνον ένα, αν και σημαντικό, στοιχείο του συστήματος παρακολούθησης. Ισχυρίζεται ότι πέρα από αυτό υπάρχουν και πολλές άλλες εγκαταστάσεις παρακολούθησης ραδιοαναμεταδόσεων και καλωδίων, οι οποίες όμως είναι λιγότερο τεκμηριωμένες και δυσκολότερο να αποδειχθούν, καθότι, σε αντίθεση με τους επίγειους σταθμούς, δεν διακρίνονται σχεδόν καθόλου. Έτσι, το "ECHELON" καθίσταται συνώνυμο του παγκόσμιου συστήματος παρακολούθησης .

5.6.2. Αναφορές του Duncan Campbell

Ο Duncan Campbell εξηγεί στην μελέτη της STOA από 2/5/1999, η οποία ασχολείται διεξοδικά με την τεχνική πτυχή του ζητήματος, τον τρόπο που χρησιμοποιείται κάθε μέσο για τη μετάδοση επικοινωνίας μπορεί να παρακολουθηθεί. Σε μία από τις τελευταίες του εκθέσεις διευκρινίζει πάντως, ότι και το ECHELON έχει τα όριά του, και ότι η αρχική άποψη, που έλεγε ότι είναι δυνατή μία πλήρης παρακολούθηση, έχει αποδειχθεί λανθασμένη. "Ούτε το ECHELON ούτε το κατασκοπευτικό σύστημα του οποίου αποτελεί μέρος, έχουν τη δυνατότητα αυτή. Δεν υπάρχει άλλωστε ο εξοπλισμός, ο οποίος θα είχε την ισχύ να αναγνωρίσει και να επεξεργαστεί το περιεχόμενο κάθε γλωσσικού μηνύματος ή κάθε τηλεφωνικής κλήσης." [57]

5.6.3. Αναφορές του Jeff Richelson

Ο συγγραφέας Jeffrey Richelson, πρώην μέλος των Εθνικών Αρχείων Ασφαλείας, κατέστησε με το διαδίκτυο προσπελάσιμα 16 παλαιότερα χαρακτηρισμένα έγγραφα, που δίνουν μία επισκόπηση στη δημιουργία, ανάπτυξη, διοίκηση και εντολή της NSA (National Security Agency).[58]
Πέραν αυτού έχει συγγράψει διάφορα βιβλία και άρθρα σχετικά με δραστηριότητες υπηρεσιών πληροφοριών των ΗΠΑ. Στο βιβλίο του που κυκλοφόρησε το 1985 "The Ties That Bind"[59] περιγράφει εκτεταμένα τη σύσταση της συμφωνίας UKUSA και τις δραστηριότητες των εις αυτή τη συμφωνία συμμετεχουσών μυστικών υπηρεσιών των ΗΠΑ, Μεγάλης Βρετανίας, Καναδά, Αυστραλίας και Νέας Ζηλανδίας.

---

[55] βλ. σχετικά http://www.intelsat.int/index.htm

[56] βλ. σχετικά http://www.inmarsat.org/index3.html

[57] Duncan Campbell, Inside Echelon. Ως προς την ιστορία, τεχνική και λειτουργία του γνωστού ως ECHELON συστήματος παρακολούθησης και φιλτραρίσματος, 1

[58] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

[59] Jeffrey T. Richelson, Desmond Ball 1985: The Ties That Bind, Boston UNWIN HYMAN, Sydney Wellington London

Στο πολύ εκτεταμένο βιβλίο του "The U.S. Intelligence Community"[60] του 1999, δίδει μία επισκόπηση όσον αφορά τις δραστηριότητες των υπηρεσιών πληροφοριών των ΗΠΑ, περιγράφει τις οργανωτικές δομές των υπηρεσιών, τις μεθόδους τους συλλογής και ανάλυσης πληροφοριών. Στο κεφάλαιο 8 του βιβλίου εξετάζει λεπτομερειακά το δυναμικό SIGINT των υπηρεσιών πληροφοριών και περιγράφει ορισμένους επίγειους σταθμούς. Στο κεφάλαιο 13 περιγράφει τις σχέσεις των ΗΠΑ προς άλλες υπηρεσίες πληροφοριών, μεταξύ άλλων της Συμφωνίας UKUSA. Το όνομα ECHELON το αναφέρει σε ένα σημείο ως κωδική λέξη για ένα σύστημα ανταλλαγών βασιζόμενο σε ηλεκτρονικούς υπολογιστές.
Στο άρθρο του, που δημοσιεύθηκε το 2000, "Desperately seeking Signals"[61] περιγράφει σε συντομία τη συμφωνία UKUSA, αναφέρει δορυφορικές εγκαταστάσεις παρακολούθησης για επικοινωνιακούς δορυφόρους και περιγράφει δυνατότητες και όρια της παρακολούθησης μη στρατιωτικής επικοινωνίας.

5.6.4. Αναφορές του James Bamford

Θα υποβληθούν συμπληρωματικά

5.6.5. Αναφορές των Bo Elkjaer και Kenan Seeberg,

Οι δύο Δανοί δημοσιογράφοι Bo Elkjaer και Kenan Seeberg ανέφεραν στις 22 Ιανουαρίου 2001 ενώπιον της Επιτροπής, ότι το ECHELON ήδη κατά την δεκαετία του 1980 είχε εξελιχθεί σημαντικά, και ότι η Δανία συνεργάζεται με τις ΗΠΑ από τον 1984.

5.7. Μαρτυρίες πρώην συνεργατών υπηρεσιών πληροφοριών

5.7.1. Margaret Newsham (πρώην συνεργάτης της NSA)

Η Margaret Newsham[62] υπήρξε από το 1974 μέχρι το 1984 υπάλληλος των εταιριών Ford και Lockheed και εργάστηκε κατά το διάστημα αυτό κατά δήλωσή της για την NSA. Είχε εκπαιδευτεί στο κέντρο της NSA στο Fort George Meade στην πολιτεία των Maryland ΗΠΑ, και είχε τοποθετηθεί το 1977-1978 στο Menwith Hill, τον αμερικάνικο επίγειο σταθμό σε βρετανικό έδαφος. Εκεί αναφέρει ότι διαπίστωσε, ότι παρακολουθούνταν μία συνομιλία του αμερικανού γερουσιαστή Strohm Thurmond. Ήδη από το 1978, το ECHELON μπορούσε να παρακολουθήσει τις τηλεπικοινωνίες ενός ορισμένου προσώπου, που διαβιβάζονταν μέσω δορυφόρου.

Σε ό,τι αφορά τον δικό της ρόλο στην NSA, αναφέρει ότι ήταν υπεύθυνη για την δημιουργία συστημάτων και προγραμμάτων, τη διάρθρωσή τους και τη θέση τους σε λειτουργία σε μεγάλους υπολογιστές. Όπως ισχυρίζεται, τα λογισμικά προγράμματα ονομάστηκαν SILKWORTH και SIRE, ενώ ECHELON ήταν η ονομασία του δικτύου.

[60] Jeffrey T. Richelson 1999 (4th ed.): „The U.S. Intelligence Community“, Westview Press

[61] Jeffrey T. Richelson 2000: „Desperately seeking Signals“ The Bulletin of the Atomic Scientists, March/April 2000, Vol. 56, No. 2, pp. 47-51

[62] βλ. για τα παρακάτω Bo Elkjaer, Kenan Seeberg, Echelon was my baby – Interview with Margaret Newsham, Ekstra Bladet, 17.1.1999

5.7.2. Wayne Madsen (Πρώην συνεργάτης της NSA)

Ο Wayne Madsen[63], πρώην συνεργάτης της NSA, επιβεβαιώνει επίσης την ύπαρξη του ECHELON. Κατά τη γνώμη του, η συλλογή οικονομικών πληροφοριών έχει μέγιστη προτεραιότητα και χρησιμοποιείται προς όφελος αμερικανικών εταιριών. Εκφράζει ιδίως τον φόβο ότι το ECHELON ενδεχομένως παρακολουθεί μη κυβερνητικές οργανώσεις όπως την Διεθνή Αμνηστία ή την Greenpeace. Αναφέρει σχετικά ότι η NSA αναγκάστηκε να παραδεχτεί ότι διέθετε περισσότερες από 1.000 σελίδες με πληροφορίες σχετικά με την Πριγκίπισσα Νταϊάνα, η οποία, με την εκστρατεία της κατά των ναρκών, είχε έλθει σε αντίθεση με την πολιτική των ΗΠΑ.

5.7.3. Mike Frost (πρώην συνεργάτης των καναδικών μυστικών υπηρεσιών)

Ο Mike Frost απασχολήθηκε για περισσότερα από 20 χρόνια στην καναδική μυστική υπηρεσία CSE[64]. Ο σταθμός παρακολούθησης στη Οτάβα είναι, όπως λέει, μόνον ένα μέρος του παγκόσμιου δικτύου σταθμών κατασκοπείας.[65] Σε μία συνέντευξη στο σταθμό CBS δήλωσε ότι "παντού στον κόσμο, παρακολουθούνται κάθε μέρα από το ECHELON, ένα μυστικό δίκτυο παρακολούθησης της κυβέρνησης, οι τηλεφωνικές συνδιαλέξεις, τα ηλεκτρονικά μηνύματα και τα φαξ".[66] Αυτό αφορά και στις επικοινωνίες των πολιτών. Ως παράδειγμα αναφέρει σε μία συνέντευξη με ένα αυστραλιανό κανάλι, ότι η CSE είχε πράγματι καταχωρήσει σε μία τράπεζα δεδομένων για πιθανούς τρομοκράτες το όνομα και τον τηλεφωνικό αριθμό μιας γυναίκας, η οποία σε μία αθώα συζήτηση με έναν φίλο της είχε χρησιμοποιήσει μία διφορούμενη έννοια. Ο υπολογιστής είχε ανακαλύψει, κατά την διερεύνηση επικοινωνιών βάσει λέξεων κλειδιών αυτή την έννοια και είχε επαναλάβει την επικοινωνία, ενώ ο υπεύθυνος ανάλυσης, που δεν ήταν σίγουρος για τι επρόκειτο, καταχώρησε τα προσωπικά στοιχεία της γυναίκας αυτής.[67]

Όπως διατείνεται, οι υπηρεσίες πληροφοριών των χωρών του ECHELON αλληλοβοηθούνται και κατασκοπεύοντας η μία για την άλλη, έτσι ώστε να μην μπορεί να κατηγορηθεί τουλάχιστο η εγχώρια υπηρεσία πληροφοριών. Έτσι, η GCHQ παρακάλεσε την καναδική CSE να κατασκοπεύσει για λογαριασμό της δύο άγγλους υπουργούς, όταν η πρωθυπουργός ζήτησε από τους πρώτους να μάθει, αν αυτοί βρίσκονταν με το μέρος της.[68]

5.7.4. Fred Stock (πρώην συνεργάτης των καναδικών μυστικών υπηρεσιών)

Ο Fred Stock αποκλείστηκε, σύμφωνα με όσα δηλώνει ο ίδιος, το 1993 από την καναδική υπηρεσία πληροφοριών CSE, διότι είχε εκφραστεί κατά της μετατόπισης του κέντρου βάρους στις οικονομικές πληροφορίες και πολιτικούς στόχους. Ισχυρίζεται, ότι η επικοινωνία που προέκυψε από υποκλοπές περιείχε επιχειρηματικές πληροφορίες σχετικά με άλλες χώρες,

---

[63] Τηλεοπτική συνέντευξη από την εκπομπή του NBC "60 Minutes" από 27.2.2000; http://cryptome.org/echelon-60min.htm

[64] Communication Security EstΕπίσημη Εφημερίδαishment, υπάγεται στο καναδικό υπουργείο άμυνας, λειτουργεί Sigint

[65] Τηλεοπτική συνέντευξη του NBC "60 Minutes" από 27.2.2000; http://cryptome.org/echelon-60min.htm

[66] Rötzer, Die NSA geht wegen Echelon an die Öffentlichkeit; http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special

[67] Τηλεοπτική συνέντευξη του NBC "60 Minutes" από 27.2.2000; http://cryptome.org/echelon-60min.htm

[68] Συνέντευξη του αυστραλιανού τηλεοπτικού σταθμού Channel 9 από 23..3.1999; http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm

μεταξύ των οποίων και διαπραγματεύσεις στο πλαίσιο της Βορειοαμερικανικής Ζώνης Ελεύθερου Εμπορίου (NAFTA), αγορά σιτηρών από την Κίνα, γαλλικές πωλήσεις όπλων. Σύμφωνα με τον Stock, η υπηρεσία ελάμβανε συστηματικά και πληροφορίες σχετικά με ενέργειες περιβαλλοντικής διαμαρτυρίας πλοίων της Greenpeace σε ανοιχτή θάλασσα.[69]

5.8. Κυβερνητικές πληροφορίες

5.8.1. Αναφορές από αμερικανική πλευρά

Ο πρώην διευθυντής της CIA James Woolsey δήλωσε σε μία συνέντευξη τύπου,[70] την οποία έδωσε μετά από αίτημα του Υπουργού Εξωτερικών των ΗΠΑ, ότι οι ΗΠΑ διενεργούν κατασκοπεία στην ηπειρωτική Ευρώπη. Όμως κατά τα λεγόμενά του, οι "οικονομικές πληροφορίες" (Economic Intelligence) όμως αποκτάται κατά 95% από την αποτίμηση δημοσίως προσιτών πηγών πληροφόρησης, και μόνον το 5% είναι μυστικές πληροφορίες που έχουν υποκλαπεί. Σύμφωνα με τον Woolsey, τα οικονομικά στοιχεία άλλων κρατών αποτελούν αντικείμενο παρακολούθησης μόνον στις περιπτώσεις όπου πρόκειται για την τήρηση κυρώσεων ή για αγαθά διπλής χρήσης, καθώς και σε περιπτώσεις δωροδοκίας κατά την προσκύρωση δημόσιων διαγωνισμών. Οι πληροφορίες αυτές δεν μεταδίδονται όμως περαιτέρω σε αμερικανικές επιχειρήσεις. Ο Woolsey τονίζει ότι ακόμη και αν κατά την κατασκοπεία οικονομικών στοιχείων ανακαλυφθούν οικονομικά αξιοποιήσιμες πληροφορίες, θα ήταν πολύ χρονοβόρο για τους αναλυτές να αναλύσουν σχετικά τον μεγάλο όγκο των υφιστάμενων δεδομένων, και ότι θα συνιστούσε κατάχρηση να αναλώνουν τον χρόνο τους για την κατασκοπεία φίλων εμπορικών εταίρων. Επίσης επισημαίνει ότι, ακόμη και αν αυτό συνέβαινε, θα ήταν λόγω της διεθνούς διαπλοκής δύσκολο να αποφασιστεί ποιες επιχειρήσεις θα θεωρηθούν αμερικανικές επιχειρήσεις και ως εκ τούτου θα πρέπει να λάβουν τις πληροφορίες.

Σε ένα μεταγενέστερο άρθρο για την εφημερίδα The Wall Street Journal Europe[71], oWoolsey επαναλαμβάνει ότι οι ΗΠΑ κατασκοπεύουν την Ευρώπη, αλλά ότι αυτό συμβαίνει μόνον για να αποκαλυφθούν ενδεχόμενες δωροδοκίες. Στο άρθρο αυτό αναφέρει επίσης ρητά, ότι οι ΗΠΑ χρησιμοποιούν υπολογιστές, προκειμένου να διερευνήσουν δεδομένα βάσει λέξεων – κλειδιών.

5.8.2. Αναφορές από αγγλική πλευρά

Από τις διάφορες επερωτήσεις στη Βουλή των Κοινοτήτων[72] προκύπτει ότι ο σταθμός της Βασιλικής Πολεμικής Αεροπορίας στο Menwith Hill ανήκει μεν στο αγγλικό υπουργείο άμυνας, χρησιμοποιείται όμως από το αμερικανικό υπουργείο άμυνας, και ιδίως από την NSA[73], η οποία διορίζει τον διοικητή του σταθμού,[74] ως εγκατάσταση επικοινωνιών.[75] Κατά τα μέσα του 2000, στον σταθμό του Menwith Hill εργάζονταν 415 μέλη του αμερικανικού στρατού, 5 άτομα του

[69] Bronskill, Canada a key snooper in huge spy network, Ottawa citizen, 24.10.2000, http://www.ottawacitizen.com/national/990522/2630510.html

[70] Transcript, 7.3.2000, http://cryptome.org/echelon-cia.htm

[71] James Woolsey, Why America Spies on its Allies, The Wall Street Journal, 22.3.2000, 31

[72] Commons Written Answers, House of Commons Hansard Debares

[73] 12.7.1995.

[74] 25.10.1994

[75] 3.12.1997

στρατού του Ηνωμένου Βασιλείου, καθώς και 989 αμερικανοί και 392 άγγλοι πολίτες, χωρίς να συνυπολογίζονται οι παρόντες συνεργάτες της GCHQ.[76] Η παρουσία των αμερικανικών ομάδων ρυθμίζεται από το NATO και από ειδικές μυστικές[77] συμφωνίες οι οποίες, ενόψει των υφιστάμενων σχέσεων μεταξύ των κυβερνήσεων του Ηνωμένου Βασιλείου και των ΗΠΑ για μία κοινή άμυνα, χαρακτηρίζονται ως προσήκουσες.[78] Ο σταθμός αποτελεί ένα ακέραιο στοιχείο του παγκόσμιου δικτύου του αμερικανικού υπουργείου εξωτερικών, που στηρίζει τα συμφέροντα του Ηνωμένου Βασιλείου, των ΗΠΑ και του NATO.[79]

Στην ετήσια έκθεση 1999/2000 τονίζεται ρητά η αξία, η οποία θα προκύψει από μία στενή συνεργασία βάσει της συμφωνίας μεταξύ ΗΠΑ και Ηνωμένου Βασιλείου, και η οποία αντικατοπτρίζεται στην ποιότητα των αποτελεσμάτων τω υπηρεσιών πληροφοριών. Ιδίως επισημαίνεται το γεγονός ότι όταν οι εγκαταστάσεις της NSA τέθηκαν για τρεις ημέρες εκτός λειτουργίας, η GCHQ εξυπηρετούσε αμέσως μετά τους βρετανούς πελάτες και τους πελάτες της από τις ΗΠΑ.[80]

5.8.3. Αναφορές από αυστραλιανή πλευρά[81]

Ο Martin Brady, Διευθυντής της αυστραλιανής υπηρεσίας πληροφοριών DSD[82], επιβεβαίωνε σε μία επιστολή προς την εκπομπή "Sunday" του αυστραλιανού τηλεοπτικού σταθμού "Channel 9", ότι υπάρχει μία συνεργασία της DSD με άλλες υπηρεσίες πληροφοριών βάσει της σχέσης ΗΠΑ & Ηνωμένου Βασιλείου. Στην ίδια επιστολή τονίζεται ότι όλες οι εγκαταστάσεις των υπηρεσιών πληροφοριών της Αυστραλίας λειτουργούν υπό την επιμέλεια των αυστραλιανών υπηρεσιών ή από κοινού με αμερικάνικες υπηρεσίες. Στις περιπτώσεις στις οποίες οι εγκαταστάσεις χρησιμοποιούνται από κοινού, η αυστραλιανή κυβέρνηση έχει πλήρη γνώση όλων των δραστηριοτήτων και σε όλα τα επίπεδα συμμετέχει αυστραλιανό προσωπικό.[83]

5.8.4. Αναφορές από ολλανδική πλευρά

Στις 19 Ιανουαρίου 2001, ο ολλανδός υπουργός άμυνας παρουσίασε στο ολλανδικό κοινοβούλιο μία έκθεση σχετικά με την τεχνική και την νομική πλευρά της παγκόσμιας παρακολούθησης που διενεργείται με τη βοήθεια σύγχρονων συστημάτων επικοινωνίας.[84] Η ολλανδική κυβέρνηση υποστηρίζει στην έκθεση αυτή την άποψη ότι, παρότι δεν κατέχει σχετικά ιδία γνώση, βάσει διαθεσίμων πληροφοριών από τρίτους, φαίνεται καθ' όλα πιθανό ότι το δίκτυο ECHELON

---

[76] 12.5.2000

[77] 12.7.1995

[78] 8.3.1999, 6.7.1999

[79] 3.12.1997

[80] Intelligence and Security Committee, Annual Report 1999-2000, Z. 14, η οποία υποβλήθηκε στο Κοινοβούλιο και τον Πρωθυπουργό τον Νοέμβριο του 2000.

[81]http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp;
http://sunday.ninemsn.com/01_cover_stories/article_335.asp

[82] Defence Signals Directorate, Australischer Nachrichtendienst der SIGINT betreibt

[83] Brief von Martin Brady, Direktor der DSD vom 16.März 1999 an Ross Coulthart, Sunday Program; Vgl dazu auch: http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp;
http://sunday.ninemsn.com/01_cover_stories/article_335.asp

[84] Brief aan de Tweede Kamer betreffende "Het grootschalig afluisteren van moderne telecommunicatiesystemen" από 19.01.01

υπάρχει, όπως και άλλα συστήματα με τις ίδιες δυνατότητες. Σύμφωνα με όσα αναφέρονται στην έκθεση, η ολλανδική κυβέρνηση συμπεραίνει, ότι η παγκόσμια παρακολούθηση συστημάτων επικοινωνιών δεν περιορίζεται στις χώρες που συμμετέχουν στο σύστημα ECHELON, αλλά ότι διενεργείται και από κυβερνητικές υπηρεσίες άλλων χωρών.

5.8.5. Αναφορές από ιταλική πλευρά

Ο Luigi Ramponi, πρώην διευθυντής της ιταλικής υπηρεσίας πληροφοριών SISMI, σε μία συνέντευξή του στην εφημερίδα "il mondo" δεν αφήνει αμφιβολίες για την ύπαρξη του "ECHELON".[85] Ο Ramponi δηλώνει ρητά, ότι, υπό την ιδιότητά του ως αρχηγός της SISMI, γνώριζε για την ύπαρξη του ECHELON,και ότι από το 1992 ήταν ενήμερος σχετικά με μία μεγάλη δραστηριότητα παρακολούθησης κυμάτων χαμηλής, μεσαίας και υψηλής συχνότητας. Όπως λέει, όταν το 1991 ανέλαβε στην SISMI, κυρίως ασχολούνταν με το Ηνωμένο Βασίλειο και τις Ηνωμένες Πολιτείες.

5.9. Κοινοβουλευτικές εκθέσεις

5.9.1. Εκθέσεις της μόνιμης εξεταστικής επιτροπής του Βελγίου

Η μόνιμη εξεταστική επιτροπή του Βελγίου έχει ήδη λάβει θέση ως προς το θέμα ECHELON σε δύο εκθέσεις της.

Στην έκθεση "Rapport d'activitıs 1999", το 3^{o} κεφάλαιο ήταν αφιερωμένο στο ερώτημα με ποιον τρόπο αντιδρούν οι βελγικές μυστικές υπηρεσίες στη δυνατότητα παρακολούθησης των επικοινωνιών εκ μέρους ενός υποτιθέμενου συστήματος ECHELON. Η έκθεση, που αποτελείται από σχεδόν 15 σελίδες, καταλήγει στο συμπέρασμα ότι οι δύο βελγικές υπηρεσίες πληροφοριών Süreté de l'Etat ?αι Service gınéral du Renseignement (SGR) ?άμβαναν πληροφορίες για το ECHELON μόνον μέσω δημοσίων εγγράφων.
Η δεύτερη έκθεση "Rapport complémentaire d'activités 1999" ασχολείται πολύ διεξοδικότερα με το σύστημα ECHELON. Λαμβάνει θέση ως προς τις μελέτες του STOA και αφιερώνει ένα μέρος στην ανάλυση της περιγραφής των βασικών τεχνικών και νομικών προϋποθέσεων για την παρακολούθηση τηλεπικοινωνιών. Η ουσία των συμπερασμάτων της έκθεσης είναι ότι το ECHELON υπάρχει πραγματικά και ότι είναι σε θέση να υποκλέπτει όλες τις πληροφορίες που μεταδίδονται με δορυφόρο (περίπου το 1% του συνόλου των διεθνών συνδιαλέξεων), εφόσον η αναζήτηση γίνεται με λέξεις – κλειδιά, και ότι οι δυνατότητές του ως προς την αποκρυπτογράφηση είναι πολύ μεγαλύτερες από ό,τι παρουσιάζονται από την αμερικανική πλευρά. Ως προς τις δηλώσεις ότι στο Menwith Hill δεν διενεργείται βιομηχανική κατασκοπεία, διατηρούνται αμφιβολίες. Τονίζεται ρητά, ότι είναι αδύνατο να διαπιστωθεί με βεβαιότητα το τι μπορεί ή δεν μπορεί να κάνει το ECHELON.

5.9.2. Εκθεση της επιτροπής εθνικής άμυνας της γαλλικής Εθνοσυνέλευσης

Στη Γαλλία, κατατέθηκε στην Εθνοσυνέλευση από την επιτροπή εθνικής άμυνας μία έκθεση σχετικά με το ζήτημα των συστημάτων παρακολούθησης.[86]

---

[85] Francesco Sorti, Dossier. exclusivo. caso Echelon. parla Luigi Ramponi. Anche I politici sapevano, il mondo, 17.4.1998

[86] Rapport d'information déposé en application de l'article 145 du règlement par la commission de la défense nationale et des forces armées, sur les systèmes de surveillance et d'interception électroniques pouvant mettre en

Μετά από εκτενή επεξήγηση των διαφόρων πτυχών, ο εισηγητής Arthur Paecht καταλήγει στο συμπέρασμα, ότι το ECHELON υπάρχει και ότι αποτελεί το μόνο γνωστό υπερεθνικό σύστημα παρακολούθησης. Σύμφωνα με την έκθεση, οι δυνατότητες του συστήματος είναι πραγματικές, έχουν όμως φτάσει τα όριά τους, όχι μόνον επειδή το κόστος της λειτουργίας του δεν είναι πια ανάλογο προς την επικοινωνιακή έκρηξη, αλλά και επειδή πλέον κάποιοι στόχοι προστατεύονται.

Αναφέρεται ότι το σύστημα ECHELON έχει ξεφύγει από τους αρχικούς του στόχους, οι οποίοι συνδέονταν με το πλαίσιο του ψυχρού πολέμου, οπότε δεν είναι πλέον απίθανο οι συλλεχθείσες πληροφορίες να χρησιμοποιούνται για πολιτικούς και οικονομικούς σκοπούς κατά άλλων χωρών του NATO.

Το ECHELON θα μπορούσε κάλλιστα να αποτελέσει κίνδυνο για τις θεμελιώδεις ελευθερίες και δημιουργεί σχετικά πολυάριθμα προβλήματα τα οποία χρήζουν μιας κατάλληλης απάντησης. Είναι λάθος να φαντάζεται κανείς ότι οι χώρες μέλη του ECHELON θα παραιτηθούν από τη δραστηριότητά τους. Μάλιστα, υπάρχουν πολλές ενδείξεις για το ότι δημιουργήθηκε ένα νέο σύστημα με νέους εταίρους, προκειμένου να ξεπεραστούν τα όρια του ECHELON με τη βοήθεια νέων μέσων.

---

cause la sécurit´nationale, N° 2623 Assemblöe nationale, enregisté à la Présidence de l'Assemblée nationale le 11 octobre 2000.

6. Είναι δυνατή η ύπαρξη παγκοσμίων συστημάτων παρακολούθησης;

6.1. Οι προϋποθέσεις ενός συστήματος τέτοιου είδους

6.1.1. Τεχνικές – γεωγραφικές προϋποθέσεις

Με στόχο την παρακολούθηση διεθνών και, μέσω δορυφόρων, πρώτης γενιάς επικοινωνιών, είναι απαραίτητη η εγκατάσταση σταθμών λήψης στις περιοχές του Ατλαντικού, του Ινδικού Ωκεανού και του Ειρηνικού. Στην νεότερη γενιά δορυφόρων, η οποία επιτρέπει την εκπομπή σε υποπεριοχές, πρέπει να τηρούνται περαιτέρω όροι σχετικά με την γεωγραφική τοποθέτηση σταθμών παρακολούθησης, αν επιδιώκεται η κάλυψη του συνόλου της επικοινωνίας που μεταδίδεται μέσω δορυφόρων.

Ένα ευρύ, διεθνές σύστημα παρακολούθησης είναι υποχρεωμένο, να εγκαθιστά τους σταθμούς του εκτός των επικρατειών των χωρών του ECHELON.

6.1.2. Πολιτικές – οικονομικές προϋποθέσεις

Η δημιουργία ενός τέτοιου διεθνούς δράσης συστήματος παρακολούθησης πρέπει όμως επιπλέον να επιφέρει οικονομικά και πολιτικά οφέλη στον υπεύθυνο λειτουργίας. Ο επικαρπωτής ή οι επικαρπωτές ενός τέτοιου συστήματος πρέπει να έχουν παγκόσμια οικονομικά, στρατιωτικά ή άλλα συμφέροντα ασφάλειας, ή τουλάχιστο να θεωρούν, ότι ανήκουν στις λεγόμενες παγκόσμιες δυνάμεις. Συνεπώς, ο κύκλος περιορίζεται ουσιαστικά, πέραν από τις ΗΠΑ και το Ηνωμένο Βασίλειο, στην Κίνα και τις χώρες του G8.

6.2. Γαλλία

Η Γαλλία διαθέτει σε και στις τρεις περιοχές που προαναφέρθηκαν δικά της εδάφη, υπηρεσίες και περιφερειακούς οργανισμούς.

Στην περιοχή του Ατλαντικού, ανατολικά του Καναδά βρίσκεται το Σαιν Πιέρ και Μικελόν (65° W / 47° N), βορειοανατολικά της Νοτίου Αμερικής η Γουαδελούπη (61° W / 16° N) και η Μαρτινίκα (60° W / 14° N) και επίσης, στην βορειοανατολική ακτή της Νοτίου Αμερικής, η Γαλλική Γουϊάνα (52° W / 5° N).

Στην περιοχή του Ινδικού Ωκεανού βρίσκονται ανατολικά της Νοτίου Αφρικής η Μαγιότ (45° O / 12° S) και η Ρεουνιόν (55° O / 20° S) καθώς και τελείως νότια τα Γαλλικά Νότια Εδάφη και η Γαλλική Ανταρκτική. Στην περιοχή του Ειρηνικού βρίσκονται η Νέα Καληδονία (165° O / 20° S), Βαλίς και Φουτούνα (176° W / 12° S) καθώς και η Γαλλική Πολυνησία (150° W / 16° S).

Σχετικά με τους πιθανούς σταθμούς της γαλλικής υπηρεσίας πληροφοριών DGSE σε αυτές τις υπερπόντιες περιοχές δεν γνωρίζουμε πολλά. Σύμφωνα με αναφορές γάλλων[87] υπάρχουν σταθμοί στο Kourou της Γαλλικής Γουιάνα καθώς και στην Μαγιότ. Σε σχέση με το μέγεθος των σταθμών, τον αριθμό των δορυφορικών κεραιών και το μέγεθός τους δεν υπάρχουν περαιτέρω στοιχεία. Υποτίθεται, ότι υπάρχουν επίσης σταθμοί στη Γαλλία στο Domme, κοντά στο Μπορντό, καθώς και στο Alluetts-le-Roi κοντά στο Παρίσι. Ο Jauvert υπολογίζει τον αριθμό των δορυφορικών πιάτων σε 30 συνολικά. Ο συντάκτης Schmidt-Enboom[88] ισχυρίζεται, ότι και στην Νέα Καληδονία λειτουργεί ένας σταθμός.

Θεωρητικά, και η Γαλλία θα μπορούσε να θέσει σε λειτουργία ένα διεθνές σύστημα παρακολούθησης. Ο εισηγητής δεν έχει όμως επαρκείς δημοσιευμένες πληροφορίες προκειμένου να υποστηρίξει κάτι τέτοιο με βεβαιότητα.

6.3. Ρωσσία

Η αρμόδια για την ασφάλεια των επικοινωνιών και για SIGINT ρωσική υπηρεσία πληροφοριών GRU διατηρεί επίγειους σταθμούς στην Λετονία, το Βιετνάμ και την Κούβα.

Στην περιοχή του Ατλαντικού βρίσκεται, σύμφωνα με τα στοιχεία της Αμερικανικής Ομοσπονδίας Επιστημόνων, ο σταθμός της Lourdes στην Κούβα (82°W, 23°N), ο οποίος λειτουργείται από κοινού με την κουβανική υπηρεσία πληροφοριών. Στην περιοχή του Ινδικού Ωκεανού υπάρχουν σταθμοί στη Ρωσία, για τους οποίους δεν έχουμε περαιτέρω πληροφορίες, καθώς και ένας σταθμός στην Skrunda της Λετονίας. Στην περιοχή του Ειρηνικού υποστηρίζεται ότι υπάρχει ένας σταθμός στην ακτή Cam Rank Bay του Βόρειου Βιετνάμ. Λεπτομέρειες σχετικά με τους σταθμούς, τον αριθμό και το μέγεθος των κεραιών τους δεν είναι γνωστές.

Πάντως, αν συνυπολογιστούν οι σταθμοί που βρίσκονται στην επικράτεια της Ρωσίας, θα ήταν θεωρητικά εφικτή μία παγκόσμια κάλυψη. Όμως και εδώ οι διαθέσιμες πληροφορίες δεν επαρκούν για αξιόπιστους ισχυρισμούς.

---

[87] Jean Guisnel, Léspionage nést plus un secret, The Tocqueville Connection, 10.7.1998

Vincent Jauvert, Espionnage comment la France, Le Nouvel Observateur, 5.4.2001, 1900, σ. 14 επ.

[88] E.Schmidt-Eenboom, στο: Streng Geheim, Museumsstiftung Post und Telekommunikation, Χαϊδελβέργη 1999, σ. 180

6.4. Οι υπόλοιπες χώρες του G-8 και η Κίνα

Ούτε οι υπόλοιπες χώρες του της ομάδας G8, ούτε η Κίνα διαθέτουν δικά τους εδάφη ή στενούς συμμάχους στις απαραίτητες περιοχές του κόσμου, ώστε να λειτουργήσουν ένα παγκόσμιο σύστημα παρακολούθησης.

7. Η συμβατότητα ενός συστήματος παρακολούθησης επικοινωνιών τύπου "ECHELON" με το ευρωπαϊκό δίκαιο

7.1. Διευκρινήσεις ως προς τον προβληματισμό

Η εντολή που έλαβε η Επιτροπή συμπεριλαμβάνει εκτός άλλων και την ρητή ανάθεση του ελέγχου της συμβατότητας ενός συστήματος παρακολούθησης τύπου "ECHELON" με το ευρωπαϊκό δίκαιο.[89] Ιδίως πρέπει να αξιολογηθεί, αν ένα τέτοιο σύστημα είναι συμβατό με τις δύο οδηγίες 95/46 ΕΚ και 97/66 ΕΚ περί προστασίας δεδομένων, καθώς και τα άρθρα 286 συνθήκη ΕΚ και 8 παρ. 2 συνθήκη ΕΕ.

Είναι απαραίτητο, ο έλεγχος να διενεργηθεί βάσει δύο διαφορετικών κριτηρίων. Το ένα κριτήριο είναι η δια τεκμηρίων απόδειξη, όπως αναπτύχθηκε στο κεφάλαιο 5, από την οποία προκύπτει ότι το σύστημα που χαρακτηρίζεται ως "ECHELON" είχε σχεδιαστεί ως σύστημα αναχαίτισης επικοινωνιών, προκειμένου να παρέχει στις αμερικανικές, καναδικές, αυστραλιανές και νεοζηλανδικές μυστικές υπηρεσίες πληροφορίες μέσω της συλλογής και της αξιολόγησης δεδομένων επικοινωνιών. Πρόκειται για ένα κλασσικό κατασκοπευτικό εργαλείο υπηρεσιών πληροφοριών εξωτερικού.[90] Έτσι, σε πρώτο στάδιο πρόκειται να ελεγχθεί η συμβατότητα ενός τέτοιου συστήματος υπηρεσιών πληροφοριών με το ευρωπαϊκό δίκαιο.

Παράλληλα, σε μία από τις εκθέσεις της STOA που κατατέθηκε από τον Campbell εγείρεται η κατηγορία ότι γίνεται κατάχρηση του συστήματος αυτού για λόγους ανταγωνιστικής κατασκοπείας, και ότι η οικονομία των ευρωπαϊκών χωρών υπέστη ως εκ τούτου σημαντικές ζημίες. Επίσης, υπάρχουν δηλώσεις του πρώην διευθυντή της CIA R. James Woolsey, ότι οι ΗΠΑ ναι μεν κατασκοπεύουν ευρωπαϊκές εταιρίες, αυτό όμως συμβαίνει μόνον χάριν της δικαιοσύνης στην αγορά, καθώς η ανάθεση των συμβάσεων γίνεται ενδεχομένως, όπως υποστηρίζει, μόνο βάσει δωροδοκίας.[91] Αν είναι αλήθεια ότι τα συστήματα χρησιμοποιούνται για την ανταγωνιστική κατασκοπεία, το ερώτημα της συμβατότητας με το ευρωπαϊκό δίκαιο τίθεται εκ νέου. Για το λόγο αυτό, η δεύτερη αυτή πτυχή θα εξεταστεί ξεχωριστά σε δεύτερο στάδιο.

7.2. Η συμβατότητα ενός συστήματος υπηρεσιών πληροφοριών με το ευρωπαϊκό δίκαιο

7.2.1. Συμβατότητα με το κοινοτικό δίκαιο

Οι δραστηριότητες και τα μέτρα που εφαρμόζονται στην υπηρεσία της κρατικής ασφάλειας ή και της ποινικής δίωξης, καταρχήν δεν εμπίπτουν στο πεδίο ρύθμισης της συνθήκης των Ευρωπαϊκών Κοινοτήτων. Καθώς η Ευρωπαϊκή Κοινότητα, σύμφωνα με την αρχή περί περιορισμένων αρμοδιοτήτων, μπορεί να δραστηριοποιείται μόνον εκεί όπου έχει την ανάλογη αρμοδιότητα, εξαίρεσε από το πεδίο εφαρμογής των οδηγιών περί προστασίας δεδομένων που στηρίζονται στην συνθήκη ΕΚ, ιδίως στο άρθρο 95 (πρώην άρθρο 100^{α}) της συνθήκης αυτής,

[89] βλ. Σχετικά παραπάνω, κεφάλαιο 1, 1.3

[90] βλ. Σχετικά παραπάνω, κεφάλαιο 2

[91] βλ. Σχετικά παραπάνω, κεφάλαιο 5, 5.6. και 5.8.

τους εν λόγω τομείς. Η οδηγία 59/46/ΕΚ σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών[92], καθώς και η οδηγία 97/66/ΕΚ σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των τηλεπικοινωνιών[93] "σε καμία περίπτωση δεν εφαρμόζονται όταν πρόκειται για επεξεργασία/δραστηριότητα που αφορά τη δημόσια ασφάλεια, την εθνική άμυνα, την ασφάλεια του κράτους(συμπεριλαμβανομένης της οικονομικής ευημερίας, αν η επεξεργασία/δραστηριότητα άπτεται της ασφάλειας της χώρας) και για δραστηριότητές του σε τομείς ποινικού δικαίου". Η ίδια διατύπωση χρησιμοποιήθηκε και στο σχέδιο οδηγίας για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τομέα των τηλεπικοινωνιών, που κατατέθηκε τότε στο Κοινοβούλιο[94]. Συνεπώς, η συμμετοχή ενός κράτους μέλους σε σύστημα παρακολούθησης που τίθεται στην υπηρεσία της κρατικής ασφάλειας δεν μπορεί να αντίκειται στις οδηγίες περί προστασίας δεδομένων.

Κατά τον ίδιο τρόπο δεν μπορεί να υπάρχει παραβίαση του άρθρου 186 συνθήκη ΕΚ, που επεκτείνει το πεδίο εφαρμογής των περί προστασίας δεδομένων οδηγιών και στην επεξεργασία δεδομένων από τα όργανα και τους οργανισμούς της Κοινότητας. Το ίδιο ισχύει για τον Κανονισμό 45/2001 σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και για την ελεύθερη κυκλοφορία δεδομένων.[95] Και αυτός ο Κανονισμός εφαρμόζεται μόνον στο βαθμό που τα όργανα ενεργούν μέσα στο πλαίσιο της συνθήκης ΕΚ.[96] Προς αποφυγή παρεξηγήσεων πρέπει όμως να τονιστεί στο σημείο αυτό ρητά, ότι ποτέ δεν έχει υποστηριχτεί από καμία πλευρά, ότι τα κοινοτικά όργανα και οι οργανισμοί συμμετέχουν σε σύστημα παρακολούθησης, και ο εισηγητής δεν έχει καμία ένδειξη για κάτι τέτοιο.

7.2.2. Συμβατότητα με το λοιπό ευρωπαϊκό δίκαιο

Για τον τομέα του τίτλου V (Κοινή εξωτερική πολιτική και πολιτική ασφάλειας) και VI (Αστυνομική και δικαστική συνεργασία σε ποινικές υποθέσεις) δεν υπάρχουν διατάξεις προστασίας δεδομένων αντίστοιχες με εκείνες των κοινοτικών οδηγιών. Εκ μέρους του Ευρωπαϊκού Κοινοβουλίου έχει επισημανθεί ήδη επανειλημμένως, ότι στον τομέα αυτό η ανάγκη για ανάληψη δράσης είναι επιτακτική.[97]

---

[92] Επίσημη Εφημερίδα 1995 L 281/31

[93] Επίσημη Εφημερίδα 1998 L 24/1

[94] COM (2000) 385 τελικό, Επίσημη Εφημερίδα C 365 E/223

[95] Κανονισμός (ΕΚ) αρ. 45/2001, Επίσημη Εφημερίδα 2001 L 8/1

[96] Άρθρο 3 παρ. 1; βλ. και την εκτίμηση 15 "Όταν η επεξεργασία αυτή διενεργείται από τα όργανα και τους οργανισμούς της Κοινότητας για την άσκηση δραστηριοτήτων που δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος κανονισμού, ιδίως εκείνων που προβλέπονται στους τίτλους V και VI της συνθήκης για την Ευρωπαϊκή Ένωση, η προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών εξασφαλίζεται, τηρουμένου του άρθρου 6 της συνθήκης για την Ευρωπαϊκή Ένωση."

[97] Βλ. Για παράδειγμα υπό στοιχείο 25 της απόφασης για το σχέδιο δράσης του Συμβουλίου και της Επιτροπής, προκειμένου για την καλύτερη δυνατή υλοποίηση των διατάξεων της Συνθήκης του Άμστερνταμ σχετικά με τη δημιουργία ενός χώρου ελευθερίας, ασφάλειας και δικαίου (13844/98 - C4-0692/98 - 98/0923(CNS), Επίσημη Εφημερίδα C 219 από 30.7.1999, 61 επ.

Η προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών του ατόμου εξασφαλίζονται στους τομείς αυτούς μόνον μέσω των άρθρων 6 και 7, και ιδίως του άρθρου 6 παρ. 2 της συνθήκης ΕΕ, στο οποίο η Ένωση αναλαμβάνει την υποχρέωση να σέβεται τα θεμελιώδη δικαιώματα, όπως κατοχυρώνονται από την Ευρωπαϊκή Σύμβαση για την Προστασία των Δικαιωμάτων του Ανθρώπου και όπως προκύπτουν από τις κοινές συνταγματικές παραδόσεις των κρατών μελών. Έτσι, στην δεσμευτική ισχύ των θεμελιωδών δικαιωμάτων, και ιδίως της ΕΣΔΑ, για τα κράτη μέλη (βλ. και κατωτέρω, κεφάλαιο 8) δημιουργείται και μία δεσμευτική ισχύς των θεμελιωδών δικαιωμάτων για την Ένωση, κατά την άσκηση της νομοθετικής και διοικητικής της εξουσίας. Επειδή όμως μέχρι σήμερα δεν υπήρχε σε επίπεδο Ευρωπαϊκής Ένωσης κάποια ρύθμιση σχετικά με την παρακολούθηση των τηλεπικοινωνιών για λόγους ασφάλειας ή υπηρεσιών πληροφοριών,[98] δεν ανακύπτει προς το παρόν ζήτημα παραβίασης του άρθρου 6 παρ. 2 της συνθήκης ΕΕ.

7.3. Το ζήτημα της συμβατότητας στην περίπτωση της κατάχρησης του συστήματος για λόγους οικονομικής κατασκοπείας

Σε περίπτωση, που ένα κράτος μέλος προήγαγε ένα σύστημα παρακολούθησης, το οποίο εκτός των άλλων θα διενεργούσε ανταγωνιστική κατασκοπεία, επιτρέποντας στις δικές του υπηρεσίες πληροφοριών να ενεργούν ανάλογα, ή διαθέτοντας σε ξένες υπηρεσίες πληροφοριών έδαφος της επικράτειάς του για το σκοπό αυτό, θα υπήρχε βεβαίως παραβίαση του κοινοτικού δικαίου. Διότι, τα κράτη μέλη υποχρεούνται, σύμφωνα με το άρθρο 10 της συνθήκης ΕΚ, να επιδεικνύουν κοινοτική πίστη, ιδίως να απέχουν από κάθε μέτρο που δύναται να θέσει σε κίνδυνο την πραγματοποίηση των σκοπών της Συνθήκης. Ακόμη και αν η αναχαίτιση τηλεπικοινωνιών δεν γίνεται προς όφελος της εγχώριας οικονομίας (γεγονός που επίσης θα εξομοιωνόταν με κρατική ενίσχυση, κατά παράβαση του άρθρου 87 της συνθήκης ΕΚ), αλλά προς όφελος τρίτων χωρών, μία τέτοια δραστηριότητα θα βρισκόταν σε πλήρη αντίθεση προς την βασική ιδέα της Συνθήκης της Ευρωπαϊκής Κοινότητας, που είναι η δημιουργία μιας κοινής αγοράς, καθώς θα συνεπαγόταν τη νόθευση του ανταγωνισμού.

Επίσης, μία τέτοια συμπεριφορά θα σήμαινε, κατά τη γνώμη του εισηγητή, παραβίαση της οδηγίας περί προστασίας προσωπικών δεδομένων στον τομέα των τηλεπικοινωνιών[99], καθώς το ζήτημα της εφαρμογής των οδηγιών πρέπει να επιλύεται σύμφωνα με λειτουργικά και όχι με οργανωτικά κριτήρια. Αυτό δεν προκύπτει μόνον από το κείμενο της διάταξης που ρυθμίζει το πεδίο εφαρμογής, αλλά και από το νόημα του νόμου. Αν οι υπηρεσίες πληροφοριών

---

[98] Στον τομέα της παρακολούθησης τηλεπικοινωνιών, τη στιγμή αυτή υπάρχουν στα πλαίσια της ΕΕ μόνον δύο νομοθετικές πράξεις, που δεν ρυθμίζουν το θέμα του παραδεκτού:

- η απόφαση του Συμβουλίου της 17ης Ιανουαρίου 1995 σχετικά με την νόμιμη παρακολούθηση των τηλεπικοινωνιών (Επίσημη Εφημερίδα αρ. C 329 από 4.11.1996), στο παράρτημα της οποίας περιέχονται οι τεχνικές προδιαγραφές για την υλοποίηση νόμιμων μέτρων παρακολούθησης σύγχρονων συστημάτων τηλεπικοινωνίας, και

- η πράξη του Συμβουλίου της 29ης Μαίου 2000 σχετικά με την κατάρτιση της σύμβασης –σύμφωνα με το άρθρο 34 της συνθήκης ΕΕ- σχετικά με τη δικαστική συνδρομή σε ποινικές υποθέσεις μεταξύ των κρατών μελών της Ευρωπαϊκής Ένωσης (Επίσημη Εφημερίδα 2000 C 197/1, άρθρο 17 f), στην οποία ρυθμίζονται οι προϋποθέσεις, κάτω από τις οποίες θα είναι δυνατή η δικαστική αρωγή σε ποινικές υποθέσεις σχετικά με την παρακολούθηση τηλεπικοινωνιών. Τα δικαιώματα αυτών που παρακολουθούνται δεν περιορίζονται καθ' οιονδήποτε τρόπο, καθώς το κράτος μέλος, στο οποίο βρίσκονται, μπορεί να αρνηθεί τη δικαστική συνδρομή κάθε φορά που αυτή δεν επιτρέπεται σύμφωνα με το εσωτερικό δίκαιο.

[99] Οδηγία 97/66 ΕΚ, Επίσημη Εφημερίδα 1998 L 24/1

χρησιμοποιούν τις δυνατότητές τους για οικονομική κατασκοπεία, η δραστηριότητά τους δεν εξυπηρετεί την ασφάλεια ή την ποινική δίωξη, ο σκοπός της όμως θα έχει αλλοιωθεί και συνεπώς δεν θα υπάγεται στο πεδίο εφαρμογής της οδηγίας. Η εν λόγω όμως οδηγία, στο άρθρο 5, υποχρεώνει τα κράτη μέλη να εξασφαλίζουν την εμπιστευτικότητα των επικοινωνιών, ιδίως να απαγορεύουν την παρακολούθηση, την παρακολούθηση και την αποθήκευση καθώς και κάθε άλλη μορφή αναχαίτισης ή παρακολούθησης των επικοινωνιών από άλλα πρόσωπα εκτός των χρηστών. Σύμφωνα με το άρθρο 14, εξαιρέσεις μπορούν να υπάρξουν μόνον όπου είναι απαραίτητες για την ασφάλεια και την άμυνα της χώρας ή για λόγους ποινικής δίωξης. Καθώς η οικονομική κατασκοπεία δεν νομιμοποιεί εξαιρέσεις, σε μία τέτοια περίπτωση θα υπήρχε παραβίαση του κοινοτικού δικαίου.

7.4. Συμπεράσματα

Βάσει των ανωτέρω, σύμφωνα με την παρούσα νομική κατάσταση, ένα σύστημα υπηρεσιών πληροφοριών του τύπου ECHELON δεν μπορεί να βρίσκεται σε αντίθεση με το ευρωπαϊκό δίκαιο, διότι δεν διαθέτει τα σημεία επαφής με το ευρωπαϊκό δίκαιο που θα ήταν απαραίτητα για να θεωρηθεί μη συμβατό. Αυτό ισχύει όμως μόνον εφόσον το σύστημα χρησιμοποιείται αποκλειστικά για την εξυπηρέτηση της κρατικής ασφάλειας. Αντιθέτως, αν το σύστημα απομακρυνθεί από το σκοπό του και χρησιμοποιηθεί για την ανταγωνιστική κατασκοπεία εις βάρος αλλοδαπών εταιριών, προκύπτει ζήτημα αντίθεσης προς το κοινοτικό δίκαιο. Σε περίπτωση που ένα κράτος μέλος συμμετείχε σε αυτό, θα παραβίαζε το κοινοτικό δίκαιο.

8. Η συμβατότητα της παρακολούθησης των επικοινωνιών από υπηρεσίες πληροφοριών με το θεμελιώδες δικαίωμα της προστασίας της ιδιωτικής ζωής του ατόμου

8.1. Η παρακολούθηση των επικοινωνιών ως παραβίαση του θεμελιώδους δικαιώματος της ιδιωτικής ζωής

Κάθε παρακολούθηση επικοινωνίας, ακόμη και η συγκέντρωση δεδομένων από υπηρεσίες πληροφοριών για το σκοπό αυτό[100] αποτελεί σοβαρή παρέμβαση στην ιδιωτική ζωή του ατόμου. Μόνο τα αστυνομικά κράτη επιτρέπουν απεριόριστη παρακολούθηση του ατόμου. Αντιθέτως, στα κράτη μέλη της ΕΕ, που είναι ώριμες δημοκρατίες, η ανάγκη του σεβασμού του ιδιωτικού βίου από τα κρατικά όργανα, και συνεπώς και από τις υπηρεσίες πληροφοριών, είναι αδιαμφισβήτητη και κατά κανόνα αποτυπώνεται και στα συντάγματα των κρατών μελών. Η ιδιωτική ζωή απολαμβάνει συνεπώς ιδιαίτερης προστασίας, ενώ οι παρεμβάσεις επιτρέπονται μόνον κατόπιν στάθμισης των εννόμων αγαθών και τηρούμενης της αρχής της αναλογικότητας.

Το πρόβλημα αυτό συνειδητοποιούν και οι χώρες του ECHELON. Όμως, οι προβλεπόμενες διατάξεις προστασίας αφορούν μόνο τον σεβασμό της ιδιωτικής ζωής των κατοίκων των χωρών αυτών, με αποτέλεσμα ο ευρωπαίος πολίτης κατά κανόνα να μην επωφελείται από αυτές. Έτσι για παράδειγμα, οι διατάξεις του αμερικανικού δικαίου που ρυθμίζουν τις προϋποθέσεις της ηλεκτρονικής παρακολούθησης δεν σταθμίζουν τα κρατικά συμφέροντα μιας εύρυθμης υπηρεσίας πληροφοριών με τα συμφέροντα της αποτελεσματικής εν γένει προστασίας των θεμελιωδών δικαιωμάτων, αλλά με την απαιτούμενη προστασία της ιδιωτικής ζωής των προσώπων που χαρακτηρίζονται "US-Persons".[101]

8.2. Η προστασία της ιδιωτικής ζωής δυνάμει διεθνών συμβάσεων

Ο σεβασμός της ιδιωτικής ζωής ως θεμελιώδες δικαίωμα περιλαμβάνεται σε πολλές διεθνείς συνθήκες.[102] Σε παγκόσμιο επίπεδο πρέπει να αναφερθεί ιδίως το "Διεθνές Σύμφωνο περί

---

[100] Γερμανικό Ομοσπονδιακό Συνταγματικό Δικαστήριο (BVerfG), 1 BvR 2226/94 από 14.7.1999, σημ. περ. 187 "Παρέμβαση αποτελεί [...] ήδη η συγκέντρωση καθεαυτή, εφόσον καθιστά δυνατή την διάθεση επικοινωνίας στην ομοσπονδιακή υπηρεσία πληροφοριών και αποτελεί την βάση της επακόλουθης συντέλεσης βάσει όρων αναζήτησης."

[101] Βλ. Σχετικά την έκθεση του αμερικανικού κογκρέσου από τέλη Φεβρουαρίου 2000 "Legal Standards for the Intelligence Community in Conducting Electronic Surveillance", http://www.fas.org/irp/nsa/standards.html, που παραπέμπει στον νόμο για την παρακολούθηση ξένων πληροφοριών (FISA), που δημοσιεύθηκε στον τίτλο 50 κεφάλαιο 36 U.S.C. § 1801 επ. και Exec. Order No. 12333, 3 C.F.R. 200 (1982), που δημοσιεύθηκε στον τίτλο 50, κεφάλαιο 15 U.S.C. § 401 επ., http://www4.law.cornell.edu/uscode/50/index.html.

[102] Άρθρο 12 Οικουμενική διακήρυξη των δικαιωμάτων του ανθρώπου. Άρθρο 17 του Συμφώνου του ΟΗΕ για τα ατομικά και πολιτικά δικαιώματα; Άρθρο 7 του Χάρτη της ΕΕ, άρθρο 8 ΕΣΔΑ; Σύσταση του Συμβουλίου ΟΟΣΑ σχετικά με κατευθυντήριες οδηγίες για την ασφάλεια συστημάτων πληροφοριών, που έγινε αποδεκτή στις 26./27.11.1993 C(92) 188/τελικό; Άρθρο 7 της Σύμβαση του Συμβουλίου της Ευρώπης σχετικά με την προστασία του ατόμου από την αυτόματη επεξεργασία δεδομένων. Βλ. σχετικά ; τη μελέτη που συντάχθηκε κατόπιν εντολής του STOA, Development of surveillance tehnology and risk of abuse of economic information; Vol 4/5: The legality of the interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law (Chris Elliot), october 1999, 2

ατομικών και πολιτικών δικαιωμάτων"[103], το οποίο ψηφίστηκε το 1966 στο πλαίσιο του ΟΗΕ και εγγυάται στο άρθρο 17 την προστασία της ιδιωτικής ζωής. Στις αποφάσεις της Επιτροπής Ανθρωπίνων Δικαιωμάτων, που συστάθηκε σύμφωνα με το άρθρο 41, έχουν υπαχθεί όλες οι χώρες του ECHELON στο μέτρο που πρόκειται για αγωγές άλλων χωρών. Ωστόσο το προαιρετικό πρωτόκολλο[104], που επεκτείνει την αρμοδιότητα της Επιτροπής Ανθρωπίνων Δικαιωμάτων και στις ατομικές προσφυγές, δεν υπεγράφη από τις ΗΠΑ, με αποτέλεσμα οι ιδιώτες να μην έχουν την δυνατότητα να προσφύγουν, σε περίπτωση παραβίασης του συμφώνου εκ μέρους των ΗΠΑ, ενώπιον της Επιτροπής Ανθρωπίνων Δικαιωμάτων.

Σε επίπεδο Ευρωπαϊκής Ένωσης, έγινε προσπάθεια να επιτευχθεί ευρωπαϊκή προστασία των θεμελιωδών δικαιωμάτων με την κατάρτιση ενός "Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ". Το άρθρο 7 του Χάρτη, που φέρει το τίτλο "Σεβασμός του ιδιωτικού και οικογενειακού βίου", αναφέρεται στο ρητό δικαίωμα για σεβασμό των επικοινωνιών.[105] Επίσης, στο άρθρο 8 κατοχυρώνεται το θεμελιώδες δικαίωμα της "προστασίας δεδομένων προσωπικού χαρακτήρα". Οι διατάξεις αυτές θα μπορούσαν να προστατεύσουν το άτομο στις περιπτώσεις κατά τις οποίες τα δεδομένα (αυτοματοποιημένα ή μη) υπόκεινται σε επεξεργασία, γεγονός που συμβαίνει κατά κανόνα στην παρακολούθηση και πάντα στις λοιπές μορφές αναχαίτισης.

Ο Χάρτης δεν έχει περιληφθεί μέχρι τώρα στη Συνθήκη. Για το λόγο αυτό αναπτύσσει δεσμευτική ισχύ μόνο για τα τρία όργανα τα οποία, με την "Πανηγυρική δήλωση" στο περιθώριο του Ευρωπαϊκού Συμβουλίου της Νίκαιας υπήχθησαν σ' αυτόν: Συμβούλιο, Επιτροπή και Ευρωπαϊκό Κοινοβούλιο. Αυτά τα όργανα, σύμφωνα με τα όσα γνωρίζει ο εισηγητής, δεν εμπλέκονται καθόλου σε δραστηριότητες μυστικών υπηρεσιών. Ακόμη και αν ο Χάρτης θα αποκτήσει την πλήρη ισχύ του μετά την συμπερίληψή του στη Συνθήκη, πρέπει να ληφθεί υπόψη το περιορισμένο πεδίο εφαρμογής του. Σύμφωνα με το άρθρο 51, ο Χάρτης ισχύει "… στα όργανα και τους οργανισμούς της Ένωσης … και στα κράτη μέλη, μόνο όταν εφαρμόζουν το δίκαιο της Ένωσης." Ο Χάρτης θα εφαρμοζόταν για το λόγο αυτό εν πάση περιπτώσει μέσω της απαγόρευσης αντίθετων προς τον ανταγωνισμό κρατικών ενισχύσεων (βλ. κεφάλαιο 7,7.3).

Το μοναδικό πράγματι αποτελεσματικό μέσο για την πλήρη προστασία της ιδιωτικής ζωής σε διεθνές επίπεδο είναι η Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου.

8.3. Οι ρυθμίσεις της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ)

8.3.1. Η σημασία της ΕΣΔΑ στην ΕΕ

Η προστασία των θεμελιωδών δικαιωμάτων, που παρέχει η ΕΣΔΑ, έχει σημασία στο μέτρο που η σύμβαση αυτή έχει επικυρωθεί από όλα τα κράτη μέλη της ΕΕ και συνεπώς αποτελεί ένα ενιαίο ευρωπαϊκό επίπεδο προστασίας. Τα κράτη μέλη της σύμβασης έχουν αναλάβει την διεθνούς δικαίου υποχρέωση, να εγγυώνται τα δικαιώματα που κατοχυρώνονται στην ΕΣΔΑ και

[103] Διεθνές σύμφωνο για τα ατομικά και πολιτικά δικαιώματα, που εγκρίθηκε από τη Γενική Συνέλευση των Ηνωμένων Εθνών στις 16.12.1996

[104] Προαιρετικό πρωτόκολλο στο διεθνές σύμφωνο για τα ατομικά και πολιτικά δικαιώματα που εγκρίθηκε από τη Γενική Συνέλευση των Ηνωμένων Εθνών στις 16.12.1966

[105] "Ο καθένας έχει δικαίωμα σεβασμού του ιδιωτικού και οικογενειακού βίου, της κατοικίας καθώς και της επικοινωνίας του"

έχουν υπαχθεί στην δικαιοδοσία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) στο Στρασβούργο. Οι εκάστοτε εθνικές κυβερνήσεις μπορούν συνεπώς να ελεγχθούν από το ΕΔΔΑ ως προς την τήρηση της ΕΣΔΑ και τα κράτη μέλη της σύμβασης είναι δυνατόν, σε περίπτωση παραβίασης ανθρωπίνων δικαιωμάτων, να καταδικασθούν και να υποχρεωθούν σε καταβολή αποζημίωσης. Πέραν τούτου, η ΕΣΔΑ απέκτησε σημασία επειδή το ΔΕΚ την επικαλέστηκε επανειλημμένως, μαζί με γενικές αρχές του δικαίου των κρατών μελών, στο πλαίσιο του ελέγχου νόμων, προκειμένου να λάβει τις αποφάσεις του. Περαιτέρω, με τη συνθήκη του Άμστερνταμ καθορίστηκε στο άρθρο 6 παρ. 2 της συνθήκης ΕΕ η υποχρέωση της ΕΕ για την τήρηση των θεμελιωδών δικαιωμάτων, όπως κατοχυρώνονται με την ΕΣΔΑ.

8.3.2. Η τοπική και προσωπική έκταση της προστασίας της ΕΣΔΑ

Τα δικαιώματα που κατοχυρώνονται με την ΕΣΔΑ αποτελούν γενικά ανθρώπινα δικαιώματα και συνεπώς δεν συνδέονται με συγκεκριμένη υπηκοότητα. Παρέχονται σε όλα τα πρόσωπα που υπάγονται στη δικαιοδοσία των κρατών της σύμβασης. Αυτό σημαίνει ότι τα ανθρώπινα δικαιώματα αναγνωρίζονται σε κάθε περίπτωση σε ολόκληρη την επικράτεια της χώρας και ότι οποιεσδήποτε τοπικές εξαιρέσεις αποτελούν παραβίαση της σύμβασης. Πέραν τούτου, ισχύουν όμως και εκτός της επικράτειας των κρατών της σύμβασης, εφόσον εκεί ασκείται κρατική εξουσία. Τα δικαιώματα που κατοχυρώνονται με την ΕΣΔΑ έναντι ενός κράτους μέλους της σύμβασης παρέχονται συνεπώς και σε πρόσωπα που βρίσκονται εκτός της επικράτειας, όταν ένα κράτος της σύμβασης παρεμβαίνει εκτός της επικράτειάς του στην ιδιωτική τους ζωή[106].

Το τελευταίο σημείο είναι ιδιαίτερα σημαντικό καθώς η προβληματική των θεμελιωδών δικαιωμάτων εμφανίζει την ιδιαιτερότητα στον τομέα της παρακολούθησης των τηλεπικοινωνιών, ότι το κράτος που είναι υπεύθυνο για την παρακολούθηση, ο παρακολουθούμενος και η πραγματική διαδικασία της παρακολούθησης είναι δυνατό να μην συμπίπτουν τοπικά. Αυτό ισχύει ιδίως για τις διεθνείς επικοινωνίες, ενδεχομένως όμως και για εθνικές, όταν η μετάδοση των πληροφοριών οδηγεί μέσω καλωδίων στην αλλοδαπή. Στην περίπτωση των υπηρεσιών πληροφοριών εξωτερικού, αυτό αποτελεί μάλιστα συνήθη πρακτική. Επίσης δεν μπορεί να αποκλειστεί το ενδεχόμενο, κάποιες πληροφορίες προερχόμενες από παρακολούθηση, τις οποίες απέκτησε μία υπηρεσία πληροφοριών, να διαβιβάζονται στη συνέχεια σε άλλες χώρες.

8.3.3. Το επιτρεπτό της παρακολούθησης των τηλεπικοινωνιών κατά το άρθρο 8 ΕΣΔΑ

Σύμφωνα με το άρθρο 8 παρ. 1 ΕΣΔΑ, "ο καθένας έχει δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής του ζωής, της κατοικίας και της αλληλογραφίας του". Η προστασία των τηλεφωνικών συνδιαλέξεων ή των τηλεπικοινωνιών δεν αναφέρεται ρητά, σύμφωνα όμως με τη νομολογία του ΕΔΔΑ εμπίπτουν στο πεδίο προστασίας του άρθρου 8 διαμέσου των όρων "ιδιωτική ζωή" και "αλληλογραφία".[107] Το πεδίο προστασίας του θεμελιώδους δικαιώματος εκτείνεται εν προκειμένω όχι μόνον στο περιεχόμενο της επικοινωνίας, αλλά και στην εγγραφή εξωτερικών δεδομένων της συνδιάλεξης. Αυτό σημαίνει, ότι ακόμη και αν η υπηρεσία

[106] βλ. σχετικά ΕΔΔΑ Λοϊζίδου / Τουρκίας, 23.3.1995, Z 62 με περαιτέρω αποδείξεις "...η έννοια της "δικαιοδοσίας" στην παρούσα διάταξη δεν περιορίζεται στην εθνική επικράτεια των συμβαλλομένων μερών [...] είναι δυνατόν να ανακύπτει ευθύνη λόγω πράξεων των αρχών τους, που τελέσθηκαν εντός ή εκτός των εθνικών ορίων, οι οποίες παράγουν αποτελέσματα εκτός της επικράτειάς τους" με παραπομπή στο ΕΔΔΑ, Drozd και Janousek, 26.6.1992, Z 91. Βλ. σχετικά αναλυτικά, The European Convention on Human Rights (1996), 21 επ.

[107] Βλ. σχετικά ΕΔΔΑ, Klass κλπ, 6.9.1978, Z 41.

πληροφοριών καταγράψει δεδομένα όπως είναι ο χρόνος και η διάρκεια της συνδιάλεξης καθώς και τους τηλεφωνικούς αριθμούς που επιλέγονται, αυτό αποτελεί επέμβαση στην ιδιωτική ζωή.[108]

Το θεμελιώδες δικαίωμα του άρθρου 8 της ΕΣΔΑ δεν παρέχεται απεριόριστα. Μπορεί να υπάρξουν επιτρεπτές παραβιάσεις του θεμελιώδους δικαιώματος σεβασμού της ιδιωτικής ζωής, εφόσον έχουν νομική βάση στο εγχώριο δίκαιο.[109] Το δίκαιο πρέπει να είναι προσιτό σε όλους και οι συνέπειές του πρέπει να είναι προβλέψιμες.[110]

Τα κράτη μέλη δεν έχουν απόλυτη διακριτική ευχέρεια κατά τις παρεμβάσεις αυτές. Το άρθρο 8 ΕΣΔΑ επιτρέπει παρεμβάσεις μόνον για την πραγματοποίηση των σκοπών που αναφέρονται στην παράγραφο 2 ήτοι κυρίως την εθνική ασφάλεια, τη δημόσια τάξη και ασφάλεια, την αποτροπή αξιόποινων πράξεων, αλλά και την οικονομική ευημερία της χώρας[111], γεγονός που δεν δικαιολογεί την οικονομική κατασκοπεία, καθώς επιτρέπονται μόνον παρεμβάσεις που "είναι αναγκαίες σε μία δημοκρατική κοινωνία". Για κάθε παρέμβαση πρέπει να επιλέγεται το καταλληλότερο για την επίτευξη του σκοπού μέσο, και επίσης πρέπει να υφίστανται επαρκείς εγγυήσεις για την αποτροπή ενδεχόμενης κατάχρησης.

8.3.4. Η σημασία του άρθρου 8 ΕΣΔΑ για την δραστηριότητα των υπηρεσιών πληροφοριών

Για τις υπηρεσίες πληροφοριών που επιθυμούν τον σεβασμό των θεμελιωδών δικαιωμάτων, οι γενικές αρχές που προαναφέρθηκαν σημαίνουν τα εξής: Όταν για τη διασφάλιση της εθνικής ασφάλειας κρίνεται αναγκαία η εξουσιοδότηση των υπηρεσιών πληροφοριών ώστε να αναχαιτίσουν το περιεχόμενο τηλεπικοινωνιών ή τουλάχιστο στοιχείων που αφορούν στη σύνδεση, αυτό πρέπει να αποτυπώνεται στο εσωτερικό δίκαιο και η ρύθμιση πρέπει να είναι δημοσίως προσβάσιμη. Οι συνέπειες αυτού πρέπει να είναι προβλέψιμες για τον καθένα, όμως οι ειδικές απαιτήσεις του τομέα των μυστικών υπηρεσιών πρέπει να λαμβάνονται σαφώς υπόψη. Έτσι το Δικαστήριο έκρινε σε μία απόφαση σχετικά με τη συμβατότητα μυστικών ελέγχων υπαλλήλων που εργάζονται σε τομείς που αφορούν στην εθνική ασφάλεια, ότι η αξίωση για προβλεψιμότητα στη συγκεκριμένη περίπτωση δεν μπορεί να είναι η ίδια όπως σε άλλους τομείς.[112] Όμως και εδώ το Δικαστήριο απαίτησε, να παρέχει το δίκαιο τουλάχιστον κάποιες πληροφορίες σχετικά με τις προϋποθέσεις και τους όρους, υπό τους οποίους η κρατική εξουσία

---

[108] Βλ. σχετικά ΕΔΔΑ, Malone, 2.8.1984, Z 83 επ; επίσης Davy, B/Davy/U, Aspekte staatlicher Informationssammlung und Art 8 MRK, JBl 1985, 656.

[109] Σύμφωνα με την νομολογία του ΕΔΔΑ (ιδίως Sunday Times, 26.4.1979, Z 46 ff, Silver κλπ, 25.3.1983, Z 85 επ) ο όρος "law" που αναφέρεται στο άρθρο 8 παρ. 2 δεν συμπεριλαμβάνει μόνον νόμους υπό τυπική έννοια, αλλά και νομικές διατάξεις ιεραρχικά κατώτερες του νόμου, ενδεχομένως μάλιστα και άγραφο δίκαιο. Προϋπόθεση είναι πάντως, ο υπαγόμενος στο δίκαιο να μπορεί να διακρίνει υπό ποιες προϋποθέσεις είναι δυνατή μία τέτοια επέμβαση. Βλ. σχετικά Wessley, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? OJZ 1999, 491 επ, 495

[110] Silver κλπ, 25.3.1983, Z 87 επ

[111] Η αιτιολογία της "οικονομική ευημερίας" έγινε δεκτή από το ΕΔΔΑ σε μία υπόθεση, σχετικά με την μετάδοση ιατρικών δεδομένων, που ήταν σημαντικά για την χορήγηση δημοσίων αντισταθμιστικών πληρωμών M.S./Schweden, 27.8.1997, Z 38; όπως επίσης σε μία υπόθεση σχετικά με την απέλαση από τις Κάτω Χώρες ενός προσώπου, το οποίο ενώ δεν υφίστατο πλέον λόγος παραμονής του στη χώρα, ζούσε από την κοινωνική πρόνοια. Ciliz/Niederlande, 11.7.2000, Z 65.

[112] ΕΔΔΑ, Leander, 26.3.1987, Z 51

επιτρέπεται να προβεί σε μυστικές και συνεπώς εν δυνάμει επικίνδυνες επεμβάσεις στην προσωπική ζωή του ατόμου.[113]

Για την σύμφωνη προς τα ανθρώπινα δικαιώματα δραστηριότητα των μυστικών υπηρεσιών πρέπει να ληφθεί εν προκειμένω υπόψη, ότι η εθνική ασφάλεια αποτελεί μεν λόγο που την δικαιολογεί, αλλά ο λόγος αυτός υπόκειται σύμφωνα με το άρθρο 8 παρ. 2 της ΕΣΔΑ στην αρχή της αναλογικότητας: ακόμη και η εθνική ασφάλεια δικαιολογεί παρεμβάσεις μόνον εκεί που αυτές είναι αναγκαίες σε μία δημοκρατική κοινωνία. Ως προς αυτό, το ΕΔΔΑ έχει κρίνει σαφώς ότι το συμφέρον του κράτους για προστασία της εθνικής του ασφάλειας πρέπει να σταθμίζεται, ως προς την βαρύτητα της παρέμβασης σε σύγκριση με το συμφέρον του ατόμου για σεβασμό της ιδιωτικής του ζωής.[114] Οι παρεμβάσεις δεν περιορίζονται βέβαια στις απολύτως απαραίτητες, αλλά δεν αρκεί να είναι απλώς χρήσιμες ή επιθυμητές[115]. Η άποψη ότι η παρακολούθηση κάθε τηλεπικοινωνίας είναι η καλύτερη προστασία από το οργανωμένο έγκλημα, θα προσέκρουσε στο άρθρο 8 ΕΣΔΑ ακόμη και αν κάτι τέτοιο προβλέπονταν στο εσωτερικό δίκαιο.

Επιπλέον πρέπει, λόγω του ιδιαίτερου χαρακτήρα της δραστηριότητας των υπηρεσιών πληροφοριών, που απαιτεί μυστικότητα και συνεπώς μία ειδική στάθμιση συμφερόντων, να προβλεφθούν ακόμη πιο ισχυρές δυνατότητες ελέγχου. Το Δικαστήριο επισήμανε ρητά, ότι ένα μυστικό σύστημα παρακολούθησης για την διασφάλιση της εθνικής ασφάλειας εγκυμονεί τον κίνδυνο υπονόμευσης ή κατάργησης της δημοκρατίας υπό την πρόφαση της προστασίας της, και ότι για το λόγο αυτό είναι αναγκαίες κατάλληλες και αποτελεσματικές εγγυήσεις κατά ενδεχόμενων καταχρήσεων.[116] Συνεπώς, η εκ του νόμου νομιμοποιημένη δραστηριότητα των υπηρεσιών πληροφοριών είναι σύμφωνη με τα θεμελιώδη δικαιώματα, μόνον όταν το συμβαλλόμενο κράτος της ΕΣΔΑ θεσπίζει επαρκή συστήματα ελέγχου και άλλες εγγυήσεις κατά των καταχρήσεων. Το Δικαστήριο τόνισε εν προκειμένω αναφερόμενο στη δραστηριότητα των μυστικών υπηρεσιών της Σουηδίας, ότι προσδίδει ιδιαίτερη σημασία στην παρουσία βουλευτών στο όργανο που ελέγχει την αστυνομία, καθώς και στην εποπτεία από τον υπουργό δικαιοσύνης, τον κοινοβουλευτικό Διαμεσολαβητή και την επιτροπή δικαιοσύνης της βουλής. Υπό το πρίσμα αυτό φαίνεται προβληματικό το γεγονός, ότι η Γαλλία, η Ελλάδα, η Ιρλανδία, το Λουξεμβούργο και η Ισπανία δεν διαθέτουν δικές τους κοινοβουλευτικές επιτροπές για τον έλεγχο των μυστικών υπηρεσιών[117] και ούτε γνωρίζουν κάποιο σύστημα ελέγχου, αντίστοιχο με αυτό του κοινοβουλευτικού Διαμεσολαβητή των σκανδιναβικών χωρών.[118] Γι αυτό ο εισηγητής χαιρετίζει τις προσπάθειες της επιτροπής άμυνας της γαλλικής εθνοσυνέλευσης για την ίδρυση μιας

[113] ΕΔΔΑ, Malone, 2.8.1984, Z 67

[114] ΕΔΔΑ, Leander, 26.3.1987, Z 59, Sunday Times, 26.4.1979, Z 46 επ

[115] ΕΔΔΑ, Silver κλπ, 24.10.1983, Z 97

[116] ΕΔΔΑ, Leander, 26.3.1987, Z 60.

[117] Ο εισηγητής γνωρίζει, ότι ούτε το Λουξεμβούργο ούτε η Ιρλανδία διαθέτουν υπηρεσία πληροφοριών εξωτερικού και ότι οι χώρες αυτές δεν δραστηριοποιούνται σε Sigint. Η αναγκαιότητα μιας ειδικής ελεγκτικής αρχής αναφέρεται εν προκειμένω μόνον στις δραστηριότητες των υπηρεσιών πληροφοριών στην ημεδαπή.

[118] Για την κατάσταση του ελέγχου των υπηρεσιών πληροφοριών στα κράτη μέλη βλ. κεφάλαιο 9.

επιτροπής ελέγχου,[119] πόσο μάλλον καθώς η Γαλλία διαθέτει, από τεχνικής και γεωγραφικής άποψης, σημαντικές δυνατότητες για υπηρεσίες πληροφοριών.

8.4. Η υποχρέωση επαγρύπνησης έναντι της δραστηριότητας ξένων υπηρεσιών πληροφοριών

8.4.1. Ανεπίτρεπτο της παράκαμψης του άρθρου 8 της ΕΣΔΑ με παρέμβαση ξένων υπηρεσιών πληροφοριών

Όπως αναφέρθηκε εκτενώς ανωτέρω, οι χώρες μέλη της σύμβασης πρέπει να πληρούν ένα σύνολο προϋποθέσεων, προκειμένου η δραστηριότητα των υπηρεσιών πληροφοριών τους να είναι σύμφωνη με το άρθρο 8 της ΕΣΔΑ. Είναι προφανές, ότι οι υπηρεσίες πληροφοριών δεν μπορούν να απαλλαγούν από τις υποχρεώσεις τους επικαλούμενος τη δραστηριότητα άλλων υπηρεσιών πληροφοριών, οι οποίες υπόκεινται σε λιγότερο αυστηρές διατάξεις. Στην αντίθετη περίπτωση θα στερούνταν ισχύος η αρχή της νομιμότητας μαζί με τις δύο συνιστώσες της προσβασιμότητας και της προβλεψιμότητας, και η νομολογία του ΕΔΔΑ θα αποδυναμωνόταν ως προς το περιεχόμενό της.

Αφενός, αυτό σημαίνει ότι η ανταλλαγή δεδομένων μεταξύ υπηρεσιών πληροφοριών επιτρέπεται μόνον υπό περιορισμούς. Μία υπηρεσία πληροφοριών μπορεί να αποκτήσει στοιχεία από μία άλλη, μόνον αν αυτά αποκτήθηκαν υπό τις προϋποθέσεις που προβλέπει το εσωτερικό δίκαιο της πρώτης. Το πεδίο δράσης που προβλέπεται από τον νόμο δεν μπορεί να διευρυνθεί βάσει συμφωνιών με άλλες υπηρεσίες. Έτσι, μία υπηρεσία πληροφοριών επιτρέπεται να εκτελεί εντολές μιας ξένης υπηρεσίας πληροφοριών σύμφωνα με οδηγίες της δεύτερης μόνον όταν είναι πεπεισμένη για τη συμφωνία με το δικό της εθνικό δίκαιο. Ακόμη και αν οι πληροφορίες προορίζονται για μία άλλη χώρα, αυτό δεν αλλάζει το γεγονός της καταπάτησης τους θεμελιώδους δικαιώματος λόγω της παρέμβασης.

Αφετέρου, τα κράτη μέλη της ΕΣΔΑ δεν δύνανται να επιτρέπουν τη δραστηριότητα ξένων υπηρεσιών πληροφοριών στην επικράτειά τους, αν υπάρχει υπόνοια ότι η δραστηριότητά τους δεν πληροί τις προϋποθέσεις της ΕΣΔΑ.[120]

8.4.2. Συνέπειες από την ανεχόμενη δραστηριότητα μη ευρωπαϊκών υπηρεσιών πληροφοριών στο έδαφος κρατών μελών της ΕΣΔΑ

8.4.2.1. Η σχετική νομολογία του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου

Με τη κύρωση της ΕΣΔΑ, τα κράτη μέλη ανέλαβαν την υποχρέωση να υπαγάγουν την άσκηση της κυριαρχίας τους σε έλεγχο ως προς την τήρηση των ανθρωπίνων δικαιωμάτων. Δεν μπορούν να ανταποκριθούν στην υποχρέωση αυτή παραιτούμενα από τα κυριαρχικά τους δικαιώματα. Τα κράτη παραμένουν υπεύθυνα για την περιοχή της επικράτειάς τους και συνεπώς ευθύνονται

[119] Βλ. σχετικά το σχέδιο νόμου "Proposition de loi tendant a la creation de delegations parlementaires pour le renseignement", ?αι την σχετική έκθεση του βουλευτή Arthur Paecht, N° 1951 Assmeblee nationale, 11. ?οινοβουλευτική περίοδος, καταχωρήθηκε στις 23. November 1999

[120] βλ. σχετικά και Yernault, "Echelon" et l'Europe. La protection de la vie privee face a l'espionnage des communications, Journal des tribunaux, Droit Europeen 2000, 187 ep.

έναντι των υποκείμενων στο ευρωπαϊκό δίκαιο ακόμη και αν η άσκηση της κυριαρχικής εξουσίας γίνεται από κάποιο άλλο κράτος, δια της δραστηριότητας υπηρεσιών πληροφοριών. Το ΕΔΔΑ δέχεται πλέον κατά πάγια νομολογία μία υποχρέωση των κρατών της σύμβασης προς λήψη θετικών μέτρων για την προστασία της ιδιωτικής ζωής, προκειμένου να μη παραβιαστεί το άρθρο 8 της ΕΣΔΑ από ιδιώτες (!), δηλαδή ακόμη και σε οριζόντιο επίπεδο, στο οποίο το άτομο δεν βρίσκεται αντιμέτωπο με την κρατική εξουσία, αλλά με ένα άλλο άτομο.[121] Αν το κράτος επιτρέπει σε μία ξένη υπηρεσία πληροφοριών να εργάζεται στο έδαφός του, η ανάγκη προστασίας είναι πολύ μεγαλύτερη, καθώς στην περίπτωση αυτή η κυριαρχική εξουσία ασκείται από μία άλλη αρχή. Εδώ φαίνεται λογικό να υποθέσει κανείς ότι το κράτος πρέπει να μεριμνά για τη συμφωνία της δραστηριότητας των μυστικών υπηρεσιών, που ασκείται στο έδαφός του, με τα ανθρώπινα δικαιώματα.

8.4.2.2. Συνέπειες για τους σταθμούς

Στο Bad Aibling της Γερμανίας, έχει παραχωρηθεί στις Ηνωμένες Πολιτείες της Αμερικής έδαφος για να χρησιμοποιηθεί αποκλειστικά για δορυφορική λήψη. Στο Menwith Hill της Μεγάλης Βρετανίας επιτρέπεται η κοινή χρήση έκτασης γης για τον ίδιο σκοπό. Σε περίπτωση που στους σταθμούς αυτούς μία αμερικανική υπηρεσία πληροφοριών υποκλέπτει μη στρατιωτικές πληροφορίες ιδιωτών ή επιχειρήσεων προερχόμενων από συμβαλλόμενο κράτος ΕΣΔΑ, ενεργοποιούνται οι υποχρεώσεις εποπτείας που προβλέπονται στην ΕΣΔΑ. Αυτό σημαίνει στην πράξη, ότι η Γερμανία και το Ηνωμένο Βασίλειο ως συμβαλλόμενες χώρες της ΕΣΔΑ είναι υποχρεωμένες να εξετάζουν τη συμφωνία της δραστηριότητας των αμερικανικών υπηρεσιών πληροφοριών με τα ανθρώπινα δικαιώματα. Αυτό ισχύει πολύ περισσότερο καθώς ήδη ορισμένοι εκπρόσωποι ΜΚΟ και του Τύπου έχουν εκφράσει επανειλημμένα τις ανησυχίες τους για τον τρόπο που ενεργεί η NSA.

8.4.2.3. Συνέπειες για υποκλοπές που γίνονται με ξένη εντολή

Σύμφωνα με τις υπάρχουσες πληροφορίες, στο Morwenstow της Μεγάλης Βρετανίας η GCHQ αναχαιτίζει σε συνεργασία με την NSA ιδιωτικές επικοινωνίες, οι οποίες παραδίδονται υπό τη μορφή μη επεξεργασμένου υλικού στις ΗΠΑ. Ακόμη και όταν πρόκειται για εργασίες κατ' εντολή τρίτων ισχύει η υποχρέωση του ελέγχου της εντολής ως προς τη συμφωνία της με τα ανθρώπινα δικαιώματα.

8.4.2.4. Υποχρέωση ιδιαίτερης μέριμνας όταν πρόκειται για τρίτες χώρες

Προκειμένου για συμβαλλόμενες χώρες της ΕΣΔΑ μπορεί κάθε πλευρά μπορεί να θεωρεί ότι η άλλη τηρεί πράγματι την ΕΣΔΑ. Αυτό ισχύει τουλάχιστο μέχρι να αποδειχτεί ότι μία χώρα της ΕΣΔΑ παραβιάζει συστηματικά ή χρόνια την ΕΣΔΑ. Σε ό,τι αφορά τις ΗΠΑ, πρόκειται για ένα κράτος που δεν έχει συμβληθεί με την ΕΣΔΑ και ούτε έχει υπαχθεί σε ένα ανάλογο σύστημα ελέγχου. Η δραστηριότητα των υπηρεσιών πληροφοριών του κράτους αυτού ρυθμίζεται με μεγάλη ακρίβεια σε ό,τι αφορά αμερικανούς πολίτες ή πρόσωπα που διαμένουν νόμιμα στις ΗΠΑ. Ως προς την δραστηριότητα της NSAστην αλλοδαπή εφαρμόζονται όμως άλλοι κανόνες, πολλοί από τους οποίους προφανώς είναι ταξινομημένοι και συνεπώς απόρρητοι. Πρόσθετες ανησυχίες δημιουργεί εν προκειμένω το γεγονός, ότι η αμερικανική υπηρεσία πληροφοριών υπόκειται μεν σε έλεγχο από τις επιτροπές του της Βουλής των Αντιπροσώπων και της Γερουσίας, αλλά οι επιτροπές δείχνουν ελάχιστο μόνον ενδιαφέρον για την δραστηριότητα της NSA στο εξωτερικό.

[121] ΕΔΔΑ, Abdulaziz, Cabales και Balkandali, 28.5.1985, Z 67; X u Y/Niederlande, 26.3.1985, Z 23; Gaskin vs Vereinigtes Konigreich 7.7.1989, Z 38; Powell και Rayner, 21.2.1990, Z 41

Για το λόγο αυτό φαίνεται σκόπιμο να ζητηθεί από τη Γερμανία και την Αγγλία να επανεξετάσουν τις υποχρεώσεις που απορρέουν από την ΕΣΔΑ και να εξαρτήσουν το επιτρεπτό της περαιτέρω δραστηριοποίησης της NSA το έδαφός τους από το αν αυτή βρίσκεται σε συμφωνία με την ΕΣΔΑ. Στο πλαίσιο αυτά πρέπει να ληφθούν υπόψη τρία βασικά σημεία.

1. Σύμφωνα με την ΕΣΔΑ, η παρέμβαση στην ιδιωτική ζωή επιτρέπεται μόνον όταν στηρίζεται σε νομοθετικές διατάξεις, οι οποίες είναι δημόσια προσβάσιμες και των οποίων οι συνέπειες είναι προβλέψιμες για τον καθένα. Η προϋπόθεση αυτή πληρούται μόνον στην περίπτωση που οι ΗΠΑ αποκαλύψουν στους κατοίκους της Ευρώπης τον τρόπο και τις προϋποθέσεις υπό τις οποίες διενεργούν αναγνώριση. Στο βαθμό που υπάρχουν σημεία που δεν συμφωνούν με την ΕΣΔΑ, οι ρυθμίσεις πρέπει να προσαρμοστούν στο ευρωπαϊκό επίπεδο προστασίας.

2. Σύμφωνα με την ΕΣΔΑ οι παρεμβάσεις δεν πρέπει να είναι δυσανάλογες, πρέπει δε να επιλεγεί το ηπιότερο μέσο. Για τον ευρωπαίο πολίτη, μία παρέμβαση που έχει ευρωπαϊκή προέλευση πρέπει να θεωρείται ως λιγότερο σημαντική σε σχέση με μία παρέμβαση που έχει αμερικανική προέλευση, καθώς μόνον στην πρώτη περίπτωση παρέχεται πρόσβαση στους εθνικούς βαθμούς δικαιοδοσίας.[122] Για το λόγο αυτό, οι παρεμβάσεις πρέπει να γίνονται, κατά το δυνατό, από τη Γερμανία ή τη Μεγάλη Βρετανία, και, κατά συνέπεια, αυτό πρέπει να συμβαίνει σε κάθε περίπτωση παρεμβάσεων που εξυπηρετούν σκοπούς ποινικής δίωξης. Η αμερικανική πλευρά προσπάθησε επανειλημμένα να δικαιολογήσει την παρακολούθηση τηλεπικοινωνιών επικαλούμενη τη διαφθορά και τη δωροδοκία στην Ευρώπη.[123] Ας επισημανθεί στις ΗΠΑ, ότι όλα τα κράτη της ΕΕ διαθέτουν εύρυθμα συστήματα ποινικού δικαίου. Σε περίπτωση αμφιβολίας, οι ΗΠΑ οφείλουν να αφήσουν την ποινική δίωξη στις φιλοξενούσες χώρες. Αν δεν υπάρχουν αμφιβολίες, η παρακολούθηση πρέπει να θεωρηθεί δυσανάλογη και συνεπώς αντίθετη προς τα ανθρώπινα δικαιώματα και για το λόγο αυτό ανεπίτρεπτη. Συνεπώς, συμφωνίες με την ΕΣΔΑ θα υπάρχει μόνον αν οι ΗΠΑ περιορίσουν τα δικά τους μέτρα παρακολούθησης σε αυτά που εξυπηρετούν την εθνική τους ασφάλεια και απέχουν από μέτρα παρακολούθησης για σκοπούς ποινικής δίωξης.

3. Όπως προαναφέρθηκε το ΕΔΔΑ απαιτεί στην νομολογία του για το σεβασμό των ανθρωπίνων δικαιωμάτων, να υπάρχουν επαρκή συστήματα ελέγχου και εγγυήσεις κατά των καταχρήσεων. Αυτό σημαίνει ότι η αμερικανική παρακολούθηση των τηλεπικοινωνιών από ευρωπαϊκό έδαφος είναι σύμφωνη με τα ανθρώπινα δικαιώματα μόνον αν οι ΗΠΑ δημιουργήσουν στις περιπτώσεις, στις οποίες αναχαιτίζουν από εκεί επικοινωνίες για σκοπούς της εθνικής τους ασφάλειας, αντίστοιχους αποτελεσματικούς ελέγχους ή αν η NSA υπαχθεί, ως προς την δραστηριότητά της επί ευρωπαϊκού εδάφους, στα ελεγκτικά όργανα της χώρας υποδοχής (δηλαδή σε αυτά της Γερμανίας ή της Μεγάλης Βρετανίας).

Μόνον αν πληρωθούν οι απαιτήσεις που αποτυπώνονται στα τρία αυτά σημεία θα μπορέσει να διασφαλιστεί η συμφωνία με την ΕΣΔΑ του τρόπου δράσης των ΗΠΑ κατά την αναχαίτιση τηλεπικοινωνίας και να διατηρηθεί το ενιαίο επίπεδο προστασίας που εγγυάται η ΕΣΔΑ στην Ευρώπη.

---

[122] Με τον τρόπο αυτό δημιουργείται και συμβατότητα προς το άρθρο 13 ΕΣΔΑ, το οποίο αναγνωρίζει στον παθόντα το δικαίωμα προσφυγής ενώπιον των εθνικών βαθμών δικαιοδοσίας.

[123] Woolsey (πρώην Διευθυντής της CIA), Why America Spies on its Allies, The Wall Street Journal Europe, 22.3.2000, 31

9. Προστατεύονται οι πολίτες της ΕΕ επαρκώς έναντι της δραστηριότητας των υπηρεσιών πληροφοριών;

9.1. Προστασία από τη δραστηριότητα των υπηρεσιών πληροφοριών: Καθήκον των εθνικών κοινοβουλίων

Επειδή η δραστηριότητα των υπηρεσιών πληροφοριών μπορεί μεν να αποτελέσει μελλοντικά στοιχείο της ΚΕΠΠΑ, όμως αυτή τη στιγμή δεν υπάρχουν ακόμη σχετικές ρυθμίσεις σε επίπεδο ΕΕ,[124] η διαμόρφωση της προστασίας έναντι της δραστηριότητας των υπηρεσιών πληροφοριών αποτελεί αρμοδιότητα αποκλειστικά των εσωτερικών έννομων τάξεων.

Τα εθνικά κοινοβούλια ασκούν εν προκειμένω μία διττή λειτουργία: Ως νομοθέτες, αποφασίζουν για την ύπαρξη και τις εξουσίες των υπηρεσιών πληροφοριών, καθώς και για τον έλεγχο της δραστηριότητας των υπηρεσιών αυτών. Όπως αναλυτικά αναφέρεται στο προηγούμενο κεφάλαιο, τα κοινοβούλια οφείλουν κατά την ρύθμιση του ζητήματος του αποδεκτού της παρακολούθησης των τηλεπικοινωνιών να σέβονται τους περιορισμούς του άρθρου 8 ΕΣΔΑ. Αυτό σημαίνει ότι οι σχετικές ρυθμίσεις πρέπει να είναι αναγκαίες και αναλογικές και οι συνέπειές τους πρέπει να είναι προβλέψιμες για τον καθένα. Επίσης, πρέπει να δημιουργούνται κατάλληλοι και αποτελεσματικοί μηχανισμοί ελέγχου των υπηρεσιών παρακολούθησης.

Πέραν αυτών, τα εθνικά κοινοβούλια των περισσοτέρων κρατών συνήθως έχουν και ενεργό ρόλο ως εποπτικές αρχές, καθώς ο έλεγχος της εκτελεστικής εξουσίας (και συνεπώς και των υπηρεσιών πληροφοριών) αποτελεί τη δεύτερη "κλασική" λειτουργία του κοινοβουλίου, μετά τη νομοθετική. Ο έλεγχος όμως, συντελείται στα κράτη μέλη της ΕΕ με πολύ διαφορετικούς τρόπους, συχνά δε συνυπάρχουν ταυτόχρονα κοινοβουλευτικά και εξωκοινοβουλευτικά όργανα.

9.2. Η εξουσία των εθνικών αρχών για την εφαρμογή μέτρων παρακολούθησης

Μέτρα παρακολούθησης από κρατικής πλευράς επιτρέπονται κατά κανόνα σε περιπτώσεις ποινικών διώξεων, για λόγους διασφάλισης της δημόσιας τάξης στο εσωτερικό, καθώς και για λόγους ασφάλειας της χώρας [125] (από εξωτερικούς κινδύνους).

Για σκοπούς ποινικών διώξεων, επιτρέπεται σε όλα τα κράτη μέλη η άρση του τηλεφωνικού απορρήτου, στο βαθμό που υπάρχουν αποχρώσες ενδείξεις για τη διάπραξη ενός (εκάστοτε ιδιαίτερα ενισχυμένου, δηλαδή περιβεβλημένου με υψηλότερο βαθμό απαξίας) ποινικού αδικήματος από συγκεκριμένο πρόσωπο. Λόγω της βαρύτητας της παρέμβασης, απαιτείται προς τούτο δικαστική άδεια,[126] ενώ υπάρχουν συγκεκριμένοι όροι σχετικά με την επιτρεπόμενη διάρκεια της παρακολούθησης, τον έλεγχό της και την διαγραφή των δεδομένων.

[124] Βλ. σχετικά κεφάλαιο 7

[125] Οι σκοποί αυτοί αναγνωρίζονται και από το άρθρο 8 παρ. 2 ΕΣΔΑ ως λόγοι που δικαιολογούν παρεμβάσεις στην ιδιωτική ζωή. Βλ. σχετικά παραπάνω 8.3.2.

[126] Διαφορετικά όμως το βρετανικό δίκαιο, το οποίο αναθέτει την απόφαση σχετικά με την άδεια στον Υπουργό Εσωτερικών (Νόμος για τη ρύθμιση των εξουσιών έρευνας του 2000, Ενότητα 5 παράγραφοι (1) και (3) (b)

Για τη διασφάλιση της δημόσιας ασφάλειας στο εσωτερικό της χώρας, η δυνατότητα συλλογής πληροφοριών εκ μέρους του κράτους εκτείνεται και πέραν της ατομικής έρευνας, σε περίπτωση ύπαρξης συγκεκριμένης υποψίας για τη διάπραξη ποινικού αδικήματος. Για τον έγκαιρο εντοπισμό εξτρεμιστικών ή ανατρεπτικών κινημάτων, τρομοκρατών ή οργανωμένου εγκλήματος, ο εθνικός νομοθέτης επιτρέπει την πρόσθετη συλλογή πληροφοριών σχετικά με συγκεκριμένα πρόσωπα ή ομάδες. Η συλλογή σχετικών δεδομένων καθώς και η ανάλυσή τους διενεργούνται εν προκειμένω από ειδικές υπηρεσίες πληροφοριών εσωτερικού.

Τέλος, ένα σημαντικό μέρος των μέτρων παρακολούθησης αποτελούν αυτά που εξυπηρετούν σκοπούς κρατικής ασφάλειας. Η επεξεργασία, αξιολόγηση και απεικόνιση σχετικών πληροφοριών που αφορούν σε εξωτερικούς κινδύνους, ανατίθεται κατά κανόνα σε κάποια υπηρεσία πληροφοριών εξωτερικού.[127] Ο στόχος της παρακολούθησης κατά κανόνα δεν είναι μεμονωμένα άτομα, αλλά συνήθως καλύπτονται συγκεκριμένες περιοχές ή συχνότητες. Ανάλογα με τα μέσα και τις έννομες εξουσίες που διαθέτει η εκάστοτε υπηρεσία πληροφοριών εξωτερικού, υπάρχει ένα ευρύ φάσμα μέτρων παρακολούθησης που ξεκινάει από την καθαρά στρατιωτική ραδιοαναγνώριση στην δεκαμετρική περιοχή και φτάνει μέχρι την παρακολούθηση κάθε είδους τηλεπικοινωνιακών επαφών στην αλλοδαπή. Σε μερικά κράτη μέλη, η παρακολούθηση τηλεπικοινωνιών για λόγους που αφορούν καθαρά τις υπηρεσίες πληροφοριών απαγορεύεται γενικά,[128] ενώ σε άλλα επιτρέπεται εν μέρει υπό την προϋπόθεση της έγκρισής της από μία ανεξάρτητη επιτροπή[129], κατόπιν υπουργικής απόφασης,[130] για κάποιους δε τρόπους επικοινωνίας και χωρίς κανέναν περιορισμό.[131] Οι σχετικά ευρείες εξουσίες κάποιων υπηρεσιών πληροφοριών εξωτερικού οφείλονται στο γεγονός ότι οι υπηρεσίες αυτές αποσκοπούν στην παρακολούθηση επικοινωνιών στο εξωτερικό και συνεπώς αφορούν μόνον σε ένα μικρό ποσοστό των πολιτών της εν λόγω χώρας, με συνέπεια να προκαλούνται λιγότερες ανησυχίες.

9.3. Ο έλεγχος των υπηρεσιών πληροφοριών

Ένας αποτελεσματικός και ενδελεχής έλεγχος είναι σημαντικός για το λόγο ότι αφενός μεν οι υπηρεσίες πληροφοριών εργάζονται μυστικά και η εργασία τους έχει μακροπρόθεσμο προσανατολισμό, δηλαδή το θιγόμενο άτομο συχνά δεν πληροφορείται την γενόμενη παρακολούθηση για μεγάλο χρονικό διάστημα ή (ανάλογα με την νομική κατάσταση) και ποτέ, και αφετέρου τα μέτρα παρακολούθησης αφορούν πολλές φορές μεγαλύτερες, μη σαφώς καθορισμένες ομάδες προσώπων, έτσι ώστε το κράτος να μπορεί να αποκτά πολύ γρήγορα έναν πολύ μεγάλο όγκο προσωπικών δεδομένων.

---

[127] Σχετικά με την δραστηριότητα των υπηρεσιών πληροφοριών εξωτερικού βλ. την διεξοδική παρουσίαση στο κεφάλαιο 2

[128] Έτσι στην Αυστρία και το Βέλγιο

[129] Έτσι στη Γερμανία, Νόμος για τον περιορισμό του απορρήτου της αλληλογραφίας και των τηλεπικοινωνιών (Gesetz zur Beschrankung des Brief-, Post-, und Fernmeldegeheimnisses) (Άρθρο σε συνάρτηση με το άρθρο 10 του γερμανικού Θεμελιώδους Νόμου). Σύμφωνα με το άρθρο 9, πρέπει να ειδοποιείται η Επιτροπή πριν από τη εκτέλεση, εκτός και αν γεννάται κίνδυνος από την καθυστέρηση.

[130] Έτσι στη Μεγάλη Βρετανία (Νόμος για τη ρύθμιση των εξουσιών έρευνας, Ενότητα 1) και την Γαλλία, σε ό,τι αφορά τις επικοινωνίες μέσω γραμμής (Άρθρα 3 και 4 του νόμου 91-646 της 10ης Ιουλίου 1991, για το απόρρητο των επικοινωνιών που μεταδίδονται μέσω τηλεπικοινωνιακών μέσων)

[131] Έτσι για τις επικοινωνίες μέσω γραμμής στην Γαλλία (Άρθρο 20 του νόμου 91-646 της 10ης Ιουλίου 1991, για το απόρρητο των επικοινωνιών που μεταδίδονται μέσω τηλεπικοινωνιακών μέσων)

Σε όλα τα όργανα ελέγχου, και ανεξάρτητα από τη μορφή τους, ανακύπτει βεβαίως το πρόβλημα ότι, λόγω του ειδικού χαρακτήρα των μυστικών υπηρεσιών, συχνά δεν μπορεί να διαπιστωθεί αν πραγματικά όλες οι πληροφορίες διαγράφονται ή αν παρακρατείται ένα μέρος από αυτές. Για το λόγο αυτό, οι κανόνες πρέπει να διαμορφώνονται με ακόμη μεγαλύτερη επιμέλεια. Καταρχήν μπορεί να υποτεθεί ότι υπάρχει ενδελεχής έλεγχος και συνεπώς εγγύηση της νομιμότητας των παρεμβάσεων, καθώς η απόφαση για την παρακολούθηση τηλεπικοινωνιών εμπίπτει στην αρμοδιότητα του ανώτατου επίπεδου της διοίκησης, απαιτείται προηγούμενη δικαστική αδεία και επιπλέον, η εφαρμογή των μέτρων ελέγχεται από ανεξάρτητο όργανο. Περαιτέρω, από άποψη δημοκρατίας και κράτους δικαίου, είναι επιθυμητό η εργασία των υπηρεσιών πληροφοριών να υπόκειται στο σύνολό της στον έλεγχο κάποιου κοινοβουλευτικού οργάνου, σύμφωνα με την αρχή της διάκρισης των εξουσιών.

Τα παραπάνω ισχύουν σε μεγάλο βαθμό στην Γερμανία, όπου τα μέτρα παρακολούθησης τηλεπικοινωνιών διατάσσονται από τον αρμόδιο ομοσπονδιακό υπουργό. Εκτός από την περίπτωση που μπορεί να γεννηθεί κίνδυνος από την καθυστέρηση, πρέπει να ειδοποιηθεί πριν από την εκτέλεση μία ανεξάρτητη επιτροπή ("G 10-Kommission"[132]), η οποία αποφασίζει για την αναγκαιότητα και το επιτρεπτό του μέτρου. Στις περιπτώσεις όπου η γερμανική υπηρεσία πληροφοριών εξωτερικού (BND) μπορεί να εξουσιοδοτηθεί προς παρακολούθηση μη ενσύρματης τηλεπικοινωνίας φιλτράροντας συγκεκριμένους όρους αναζήτησης, η επιτροπή αποφασίζει και για το επιτρεπτό των όρων αναζήτησης. Επιπλέον, η επιτροπή G-10 είναι επιφορτισμένη να ελέγχει την τήρηση της επιβαλλόμενης από τον νόμο ειδοποίησης των προσώπων στα οποία αφορά το μέτρο, καθώς και να ελέγχει την καταστροφή των δεδομένων που αποκτώνται κατά τον τρόπο αυτό από την BND.

Περαιτέρω, μία κοινοβουλευτική επιτροπή ελέγχου (PKGr)[133], που αποτελείται από 9 μέλη του ομοσπονδιακού κοινοβουλίου, εποπτεύει τη δραστηριότητα και των τριών γερμανικών υπηρεσιών πληροφοριών. Η PKGr έχει δικαίωμα γνώσης του φακέλου, ακρόασης συνεργατών των υπηρεσιών πληροφοριών καθώς και επίσκεψης των υπηρεσιών και πληροφόρησης. Οι τελευταίες δικαιούνται να της το αρνηθούν μόνο εάν αυτό επιβάλλεται για λόγους σχετικούς με την πρόσβαση σε πληροφορίες ή για λόγους που άπτονται της προστασίας της προσωπικότητας τρίτων, ή αν αφορά στον πυρήνα της ευθύνης της εκτελεστικής εξουσίας. Οι συνεδριάσεις της PKGr είναι μυστικές, ενώ τα μέλη της υποχρεούνται, ακόμη και μετά την αποχώρησή τους, σε εχεμύθεια. Στα μέσα και στο τέλος της εκλογικής περιόδου, η PKGr υποβάλλει στο γερμανικό ομοσπονδιακό κοινοβούλιο έκθεση σχετικά με την ελεγκτική της δραστηριότητα.

Όμως ένας τέτοιου είδους εμπεριστατωμένος, σχεδόν άνευ κενών έλεγχος των υπηρεσιών πληροφοριών αποτελεί στα κράτη μέλη την εξαίρεση.

Για παράδειγμα, στη Γαλλία[134], η λήψη μέτρων παρακολούθησης που απαιτούν τη λαθραία διασύνδεση με τα καλώδια, προϋποθέτει άδεια του υπουργού επικοινωνιών. Μόνον αυτά

[132] Σχετικά βλ. αναλυτικά: Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland, Stand 9.9.2000, έκδοση του Γερμανικού Κοινοβουλίου, Γραμματεία της Ελεγκτικής Επιτροπής του Κοινοβουλίου

[133] Νόμος σχετικά με τον έλεγχο της δραστηριότητας των υπηρεσιών πληροφοριών της Ομοσπονδίας [Gesetz uber die Kontrolle nachrichtendienstlicher Tatigkeit des Bundes (PKGrG)] της 17ης Ιουνίου 1999, BGBl I 1334, όπως ισχύει

[134] Νόμος 91-646 της 10ης Ιουλίου 1991, για το απόρρητο των επικοινωνιών που μεταδίδονται μέσω τηλεπικοινωνιακών μέσων

υπάγονται στην εποπτεία της ειδικά συσταθείσας επιτροπής (Εθνική επιτροπή ελέγχου των παρακολούθησης για λόγους ασφαλείας), που αποτελείται από έναν βουλευτή και έναν γερουσιαστή. Η έγκριση ενός μέτρου παρακολούθησης που ζητείται από κάποιον υπουργό ή από εκπρόσωπό του, κοινοποιείται στον πρόεδρο της επιτροπής, ο οποίος, στην περίπτωση αμφιβολιών ως προς τη νομιμότητα μπορεί να απασχολήσει σχετικά την επιτροπή, η οποία με τη σειρά της κάνει συστάσεις και ειδοποιεί, στην περίπτωση που υπάρχουν υπόνοιες για ποινικά κολάσιμες παρανομίες, τις εισαγγελικές αρχές. Τα μέτρα παρακολούθησης που έχουν ως σκοπό την υπεράσπιση εθνικών συμφερόντων και συμπεριλαμβάνουν την παρακολούθηση ραδιοεπικοινωνιών, δηλαδή και τις επικοινωνίες μέσω δορυφόρου, δεν υπόκεινται σε οποιουσδήποτε περιορισμούς και συνεπώς ούτε σε έλεγχο από κάποια επιτροπή.

Ούτε οι εργασίες των γαλλικών υπηρεσιών πληροφοριών υπόκεινται σε έλεγχο από κάποια ειδική κοινοβουλευτική επιτροπή ελέγχου, γίνονται όμως εργασίες προς την κατεύθυνση αυτή. Η επιτροπή άμυνας της Γαλλικής Εθνοσυνέλευσης έχει ήδη κάνει αποδεκτή μία σχετική πρόταση,[135] εκκρεμεί όμως ακόμη η συζήτηση στην ολομέλεια.

Στο Ηνωμένο Βασίλειο, κάθε παρακολούθηση επικοινωνίας σε βρετανικό έδαφος απαιτεί έγκριση σε υπουργικό επίπεδο (Υπουργός Εσωτερικών). Η διατύπωση του νόμου δεν καθιστά σαφές αν η άνευ συγκεκριμένου στόχου, ευρεία αναχαίτιση επικοινωνίας, η οποία ελέγχεται βάσει λέξεων κλειδιών, θα ενέπιπτε στον όρο "παρακολούθηση" (interception) που χρησιμοποιείται στο "Νόμο για τη ρύθμιση των εξουσιών έρευνας του 2000" (RIP 2000), αν η αποτίμηση δεν γινόταν επί βρετανικού εδάφους, αλλά η "πρώτη ύλη" διαβιβαζόταν ανεπεξέργαστη στην αλλοδαπή. Ο έλεγχος της τήρησης των διατάξεων της RIP 2000 γίνεται (εκ των υστέρων) από τους λεγόμενους επιτρόπους (Commissioners), πρώην ή εν ενεργεία ανώτερους δικαστικούς που είναι διορισμένοι από τον πρωθυπουργό. Ο αρμόδιος για μέτρα παρακολούθησης επίτροπος (επίτροπος παρακολούθησης) εποπτεύει την χορήγηση αδειών παρακολούθησης και την εξέταση προσφυγών που έχουν σχέση με μέτρα παρακολούθησης. Το δικαστήριο εξουσιών έρευνας, του οποίου προεδρεύει ανώτερος δικαστής, εξετάζει τις προσφυγές που σχετίζονται με μέτρα παρακολούθησης και τη σχετική δραστηριότητα των υπηρεσιών.

Ο κοινοβουλευτικός έλεγχος διενεργείται από την επιτροπή πληροφοριών και ασφάλειας,[136] η οποία εποπτεύει τη δραστηριότητα και των τριών πολιτικών υπηρεσιών πληροφοριών (MI5, MI6 και GCHQ). Στην επιτροπή αυτή έχει ανατεθεί ιδίως ο έλεγχος των δαπανών και της διοίκησης καθώς και ο έλεγχος του τρόπου δράσης της υπηρεσίας ασφαλείας, της υπηρεσίας πληροφοριών και της GCHQ. Η επιτροπή αποτελείται από 9 μέλη που προέρχονται από την Άνω και Κάτω Βουλή, μεταξύ των οποίων δεν επιτρέπεται να βρίσκεται κάποιος υπουργός. Σε αντίθεση με τις ελεγκτικές επιτροπές άλλων κρατών, οι οποίες κατά κανόνα εκλέγονται από το κοινοβούλιο ή διορίζονται από τον πρόεδρο του κοινοβουλίου, η επιτροπή αυτή διορίζεται από τον Πρωθυπουργό κατόπιν διαβουλεύσεων με τον αρχηγό της αντιπολίτευσης.

Ήδη από τα παραπάνω παραδείγματα καταδεικνύεται ότι το επίπεδο προστασίας διαφέρει σημαντικά από κράτος σε κράτος. Σε ό,τι αφορά στον κοινοβουλευτικό έλεγχο, ο εισηγητής

[135] βλ. σχετικά το νομοσχέδιο "Πρόταση νόμου σχετικά με τη δημιουργία κοινοβουλευτικών αντιπροσωπειών για τις πληροφορίες", και τη σχετική έκθεση του βουλευτή Arthur Paecht, N° 1951 Εθνοσυνέλευση, 11η κοινοβουλευτική περίοδος, καταχωρήθηκε στις 23 Νοεμβρίου 1999

[136] Νόμος του 1994 για τις υπηρεσίες πληροφοριών, Ενότητα 10

θέλει να επισημάνει ότι η ύπαρξη ειδικών επιτροπών, με αντικείμενο τον έλεγχο της παρακολούθησης που διενεργούν οι υπηρεσίες πληροφοριών, είναι ιδιαίτερα σημαντική. Και αυτό γιατί οι επιτροπές αυτές διαθέτουν, σε σχέση με τις εκτελεστικές επιτροπές, το πλεονέκτημα ότι απολαμβάνουν της υψηλότερης εμπιστοσύνης των υπηρεσιών πληροφοριών, καθώς τα μέλη τους υποχρεούνται σε εχεμύθεια και οι συνεδριάσεις διεξάγονται κεκλεισμένων των θυρών. Επιπλέον, εξοπλίζονται, προκειμένου για την εκπλήρωση των καθηκόντων τους, με ιδιαίτερα δικαιώματα, πράγμα απαραίτητο για την εποπτεία δραστηριοτήτων του τομέα των πληροφοριών.

Ευχάριστο είναι το γεγονός ότι η πλειοψηφία των κρατών μελών της ΕΕ έχουν συστήσει ειδικές κοινοβουλευτικές επιτροπές ελέγχου των υπηρεσιών πληροφοριών. Στο Βέλγιο[137], τη Δανία[138], τη Γερμανία[139], την Ιταλία[140], την Ολλανδία[141] και την Πορτογαλία[142] υπάρχουν κοινοβουλευτικές επιτροπές ελέγχου, οι οποίες είναι αρμόδιες για τον έλεγχο τόσο των στρατιωτικών όσο και των πολιτικών υπηρεσιών πληροφοριών. Στο Ηνωμένο Βασίλειο[143] η ειδική επιτροπή ελέγχου εποπτεύει μόνον τις (πάντως πολύ σημαντικότερες) πολιτικές υπηρεσίες πληροφοριών, ενώ η στρατιωτική υπηρεσία πληροφοριών εποπτεύεται από την κοινή επιτροπή άμυνας. Στην Αυστρία[144], οι δύο κλάδοι της υπηρεσίας πληροφοριών ελέγχονται από δύο διαφορετικές επιτροπές ελέγχου, οι οποίες όμως είναι εξοπλισμένες με τα ίδια δικαιώματα και έχουν την ίδια οργάνωση. Στη Φινλανδία[145] και τη Σουηδία[146] καθήκοντα κοινοβουλευτικού ελέγχου ασκούν οι Διαμεσολαβητές, οι οποίοι είναι ανεξάρτητοι και εκλέγονται από το κοινοβούλιο. Στη Γαλλία, την Ελλάδα, την Ιρλανδία, το Λουξεμβούργο και την Ισπανία δεν υπάρχουν ειδικές κοινοβουλευτικές επιτροπές, αλλά τα εποπτικά καθήκοντα ασκούνται στις

[137] Comité permanent de contrôle des services de renseignements et de sécurité, Comité permanent R, Loi du 18 juillet 1991 /IV, organique du contrôle des services de police et de renseignements.

[138] Udvalget vedrørende efterretningstjenesterne, Lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester, lov 378 af 6/7/88.

[139] Das parlamentarische Kontrollgremium (PKGr), Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG)vom 17. Juni 1999 BGBl I 1334 idgF.

[140] Comitato parlamentare, L. 24 ottobre 1977, n. 801, art. 11, Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato.

[141] Tweede-Kamercommissie voor de Inlichtingen- en Veiligheidsdiensten, 17. Reglement van orde van de Tweede Kamer der Staten-General, Art. 22.

[142] Conselho de Fiscalização dos Serviços de Informações (CFSI), Gesetz 30/84 vom 5. September 1984, geändert durch das Gesetz 4/95 vom 21. Februar 1995, das Gesetz 15/96 vom 30. April 1996 und das Gesetz 75-A/97 vom 22. Juli 1997.

[143] Intelligence and Security Committee (ISC), intelligence services act 1994, Section 10.

[144] Ständigen Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Maßnahmen zur Sicherung der militärischen Landesverteidigung und dem Ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit, Art 52a B-VG, §§ 32b ff Geschäftsordnungsgesetz 1975.

[145] Ombudsmann, gesetzliche Grundlage für die Kontrolle für die Polizei (SUPO): Poliisilaki 493/1995 §33 und Laki pakkokeinolain 5 a luvun muuttamisesta 366/1999 §15, für das Militär: Poliisilaki 493/1995 §33 und Laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995 §5.

[146] Rikspolisstyrelsens ledning, Förordning (1989:773) med instruktion för Rikspolisstyrelsen (Verordnung (1989:773) über die nationale Polizeibehörde).

χώρες αυτές από τις εκτελεστικές επιτροπές στα πλαίσια της εν γένει κοινοβουλευτικής δραστηριότητας.

9.4. Αξιολόγηση της θέσης του ευρωπαίου πολίτη

Η κατάσταση που επικρατεί στην Ευρώπη εμφανίζεται ελάχιστα ικανοποιητική για τον ευρωπαίο πολίτη. Οι εξουσίες των υπηρεσιών πληροφοριών στον τομέα της παρακολούθησης των τηλεπικοινωνιών διαφέρουν σημαντικά ως προς το εύρος τους, το ίδιο δε ισχύει και για τις επιτροπές ελέγχου. Δεν διαθέτουν όλες οι χώρες στις οποίες λειτουργούν υπηρεσίες πληροφοριών, ανεξάρτητες κοινοβουλευτικές επιτροπές ελέγχου που να είναι εξοπλισμένες με τα ανάλογα εποπτικά δικαιώματα. Απέχουμε πολύ από ένα ενιαίο επίπεδο προστασίας.

Αυτό, από ευρωπαϊκή σκοπιά, είναι ακόμη πιο λυπηρό, καθώς η κατάσταση αυτή δεν αφορά τόσο τους πολίτες των ίδιων των χωρών αυτών, οι οποίοι μπορούν να ασκήσουν επιρροή στο επίπεδο προστασίας επιδεικνύοντας ανάλογη εκλογική συμπεριφορά. Οι αρνητικές επιπτώσεις θίγουν κυρίως τους υπηκόους άλλων κρατών, καθώς η περιοχή δράσης των υπηρεσιών πληροφοριών εξωτερικού από τη φύση της στρέφεται προς την αλλοδαπή. Καθώς έναντι αλλοδαπών συστημάτων το άτομο είναι σχεδόν αβοήθητο, η ανάγκη προστασίας είναι εν προκειμένω ακόμη μεγαλύτερη. Δεν πρέπει επίσης να ξεχνάμε ότι, λόγω του ειδικού χαρακτήρα των υπηρεσιών πληροφοριών, κάποιοι πολίτες της ΕΕ μπορεί να θίγονται συγχρόνως από την δραστηριότητα περισσοτέρων υπηρεσιών πληροφοριών. Επιθυμητό είναι εδώ ένα ενιαίο επίπεδο προστασίας, το οποίο να ανταποκρίνεται στις δημοκρατικές αρχές. Σε σχέση με αυτό, θα έπρεπε να γίνουν και σκέψεις ως προς το κατά πόσο στον τομέα αυτό είναι δυνατό να εφαρμοστούν διατάξεις περί προστασίας δεδομένων.

Επιπλέον, το ζήτημα της προστασίας του ευρωπαίου πολίτη θα τεθεί σε τελείως νέα βάση όταν στα πλαίσια μιας κοινής πολιτικής ασφαλείας επιχειρηθεί η συνεργασία των υπηρεσιών πληροφοριών των κρατών μελών. Τότε, τα ευρωπαϊκά θεσμικά όργανα θα είναι αναγκασμένα να θεσπίσουν επαρκείς κανόνες προστασίας. Καθήκον του Ευρωπαϊκού Κοινοβουλίου, ως υπερασπιστή των αρχών του κράτους δικαίου, θα είναι να πιέσει ώστε να υπάρξει ένας ανάλογος έλεγχος από πλευράς του, ως δημοκρατικά νομιμοποιημένου οργάνου. Το Ευρωπαϊκό Κοινοβούλιο καλείται όμως εν προκειμένω και να δημιουργήσει τις κατάλληλες προϋποθέσεις, ώστε να μπορεί να διασφαλιστεί η εμπιστευτική μεταχείριση τέτοιου είδους ευαίσθητων δεδομένων όπως και άλλων μυστικών εγγράφων διαμέσου μιας επιτροπής ειδικά διαμορφωμένης, της οποίας τα μέλη θα υποχρεούνται να τηρούν εχεμύθεια. Μόνον εφόσον υπάρξουν αυτές οι προϋποθέσεις θα είναι ρεαλιστικό και, ενόψει μίας –απόλυτα αναγκαίας για την ύπαρξη μιας σοβαρής κοινής πολιτικής ασφάλειας- εύρυθμης συνεργασίας των υπηρεσιών πληροφοριών, υπεύθυνο να απαιτηθούν αυτά τα εποπτικά δικαιώματα.

10. Η προστασία από οικονομική κατασκοπεία

10.1. Η οικονομία ως στόχος κατασκοπείας

Στις οικονομικές επιχειρήσεις υπάρχουν, ως προς την εμπιστευτικότητα, τρία ήδη πληροφοριών. Πρόκειται, πρώτον, για πληροφορίες οι οποίες **διαδίδονται όσο το δυνατό ευρύτερα.** Σε αυτές ανήκουν οι ενημερωτικές πληροφορίες σχετικά με τα προϊόντα της επιχείρησης (π.χ. ιδιότητες των προϊόντων, τιμές κλπ.) καθώς και διαφημιστικές πληροφορίες, οι οποίες επηρεάζουν την εικόνα της επιχείρησης.

Δεύτερον, υπάρχουν πληροφορίες οι οποίες ούτε προστατεύονται ούτε διαδίδονται με ενεργό τρόπο, διότι δεν έχουν σχέση με την ανταγωνιστική θέση της επιχείρησης. Ως παραδείγματα αναφέρονται η ημερομηνία της εκδρομής του προσωπικού, ο κατάλογος των φαγητών στην καντίνα ή η μάρκα των συσκευών φαξ που χρησιμοποιούνται.

Τέλος, υπάρχουν πληροφορίες οι οποίες προστατεύονται ως **εμπιστευτικές.** Οι πληροφορίες αυτές προστατεύονται από τους ανταγωνιστές, αλλά και, στην περίπτωση που μια επιχείρηση δεν θέλει να τηρήσει τους νόμους, και από το κράτος (φορολογία, κανόνες εμπάργκο κλπ.). Στα πλαίσια αυτά υπάρχουν διάφοροι βαθμοί προστασίας που φθάνουν μέχρι την αυστηρή εμπιστευτικότητα, π.χ. όταν πρόκειται για τα αποτελέσματα ερευνών πριν από την κατοχύρωση δικαιωμάτων ευρεσιτεχνίας ή για την παραγωγή στρατιωτικού εξοπλισμού[147].

Η κατασκοπεία σχετίζεται στη δεδομένη περίπτωση με την απόκτηση πληροφοριών που τηρούνται από κάποια επιχείρηση ως εμπιστευτικές. Αν ο επιτιθέμενος είναι κάποια ανταγωνιστική επιχείρηση, κάνουμε λόγο για **ανταγωνιστική κατασκοπεία** (επίσης: εργοστασιακή κατασκοπεία, βιομηχανική κατασκοπεία). Αν ο επιτιθέμενος είναι μία κρατική υπηρεσία πληροφοριών, κάνουμε λόγο για **οικονομική κατασκοπεία.**

10.1.1. Οι στόχοι της κατασκοπείας αναλυτικά

Τα στρατηγικά δεδομένα, που έχουν σημασία για την κατασκοπεία που στρέφεται προς την οικονομία, μπορούν να ταξινομηθούν κατά κλάδους ή κατά επιχειρησιακούς τομείς.

10.1.1.1. Κλάδοι

Είναι αυτονόητο ότι πληροφορίες προερχόμενες από τους παρακάτω κλάδους είναι υψηλού ενδιαφέροντος: Βιοτεχνολογία, γενετική τεχνολογία, ιατρική τεχνολογία, τεχνολογία περιβάλλοντος, υπολογιστές υψηλής απόδοσης, λογισμικό, οπτοηλεκτρονική, τεχνολογία αισθητήρων και σημάτων, αποθήκη δεδομένων, κεραμική τεχνολογία, κράματα υψηλής απόδοσης, νανοτεχνολογία. Ο κατάλογος δεν είναι πλήρης και μεταβάλλεται άλλωστε συνεχώς, ανάλογα με τις τεχνολογικές εξελίξεις. Στους τομείς αυτούς, η κατασκοπεία συνίσταται κυρίως στην κλοπή ερευνητικών αποτελεσμάτων ή ειδικών τεχνικών παραγωγής.

[147] Informationen für geheimschutzbetreute Unternehmen, BMWI 1997

10.1.1.2. Επιχειρησιακοί τομείς

Οι στόχοι κατασκοπευτικής επίθεσης είναι λογικό να βρίσκονται στους τομείς της έρευνας και της ανάπτυξης, των αγορών, του προσωπικού, της παραγωγής, της διανομής, των πωλήσεων, του μάρκετινγκ, των γραμμών παραγωγής και των οικονομικών. Πολλές φορές, η σημασία και η αξία αυτών των δεδομένων υποτιμάται (βλ. κατωτέρω 10,1.4)

10.1.2. Ανταγωνιστική κατασκοπεία

Η στρατηγική θέση μιας επιχείρησης στην αγορά εξαρτάται από την κατάστασή της στους τομείς έρευνας και ανάπτυξης, παραγωγικών διαδικασιών, γραμμών παραγωγής, χρηματοδότησης, μάρκετινγκ, πωλήσεων, διανομής, αγορών και εργατικού δυναμικού[148]. Οι πληροφορίες σχετικά με αυτούς τους τομείς έχουν ιδιαίτερο ενδιαφέρον για κάθε συνανταγωνιστή στην αγορά, καθώς προσφέρουν στοιχεία για τα σχέδια και τις αδυναμίες και έτσι επιτρέπουν την λήψη στρατηγικών αντιμέτρων.

Ένα μέρος των πληροφοριών αυτών είναι δημόσια προσιτό. Υπάρχουν εξειδικευμένες εταιρίες συμβούλων, οι οποίες συντάσσουν, μέσα σε τελείως νόμιμα πλαίσια, αναλύσεις σχετικά με τον ανταγωνισμό. Μεταξύ τους συγκαταλέγονται και καθιερωμένες εταιρίες όπως η Roland& Berger στη Γερμανία. Στις ΗΠΑ, η συλλογή πληροφοριών για τον ανταγωνισμό (Competitive Intelligence) αποτελεί πλέον ένα από τα βασικά εργαλεία της διοίκησης επιχειρήσεων[149]. Μέσα από έναν μεγάλο αριθμό μεμονωμένων πληροφοριών, μία επαγγελματική ανάλυση μπορεί να δημιουργήσει μία σαφή εικόνα της κατάστασης.

Η μετάβαση από την νομιμότητα στην ποινικά κολάσιμη ανταγωνιστική κατασκοπεία εξαρτάται από τα μέσα που χρησιμοποιούνται για την απόκτηση των πληροφοριών. Μόνον αν τα χρησιμοποιούμενα μέσα είναι βάσει της εκάστοτε νομοθεσίας παράνομα θεωρείται αδίκημα η συλλογή των σχετικών πληροφοριών – η σύνταξη καθεαυτή των αναλύσεων δεν είναι ποινικά κολάσιμη. Οι πληροφορίες που είναι ιδιαίτερα σημαντικές για κάποιον ανταγωνιστή φυλάσσονται βέβαια και μπορούν να αποκτηθούν μόνον παράνομα. Οι τεχνικές που χρησιμοποιούνται εν προκειμένω δεν διαφέρουν σε τίποτε από τις συνήθεις μεθόδους της κατασκοπείας που περιγράφονται στο κεφάλαιο 2.

Δεν υπάρχουν ακριβή στοιχεία σχετικά με την έκταση της ανταγωνιστικής κατασκοπείας. Ο κρυφός αριθμός είναι, όπως και στην κλασσική κατασκοπεία, πολύ υψηλός. Τα δύο εμπλεκόμενα μέρη (δράστης και θύμα) δεν έχουν κανένα συμφέρον για δημοσιοποίηση. Για τις θιγόμενες εταιρίες, αυτό σημαίνει πάντοτε δημιουργία αρνητικής εικόνας, ενώ οι επιτιθέμενοι βεβαίως δεν έχουν επίσης κανένα συμφέρον για δημοσιοποίηση των δραστηριοτήτων τους. Για το λόγο αυτό μόνον λίγες υποθέσεις φθάνουν ενώπιον των δικαστηρίων.

Παρόλα αυτά, στον τύπο υπάρχουν συχνά άρθρα με θέμα την ανταγωνιστική κατασκοπεία. Ο εισηγητής συζήτησε επίσης το ζήτημα αυτό με μερικούς διευθυντές ασφάλειας μεγάλων γερμανικών επιχειρήσεων[150] και με διοικητικά στελέχη αμερικανικών και ευρωπαϊκών εταιριών. Συνοπτικά, διαπιστώνεται ότι συχνά αποκαλύπτονται δραστηριότητες ανταγωνιστικής κατασκοπίας, χωρίς αυτό να αποτελεί καθημερινή πραγματικότητα.

---

[148] M.F.Porter, Competitive Strategy

[149] Hummelt, Roman, Wirtschaftsspionage auf dem Datenhighway, Hanserverlag, München 1997

[150] Προστατεύονται ονόματα και λεπτομέρειες.

10.2. Η ζημία από οικονομική κατασκοπεία

Λόγω του υψηλού κρυφού αριθμού, το μέγεθος της ζημίας που προκαλείται από την ανταγωνιστική/οικονομική κατασκοπεία δεν μπορεί να υπολογιστεί επακριβώς. Σε αυτό προστίθεται το γεγονός ότι ένα μέρος των αναφερόμενων αριθμών είναι, από την φύση των συμφερόντων, υψηλοί. Οι εταιρίες ασφάλειας και οι υπηρεσίες αντικατασκοπίας έχουν ευνόητο συμφέρον να τοποθετούν τη ζημία στο ανώτατο άκρο της ρεαλιστική δυνατής κλίμακας. Παρόλα αυτά, οι αριθμοί δίνουν μία πρώτη εκτίμηση του σχετικού μεγέθους.

Ήδη το 1998, το Ινστιτούτο Max Planck εκτιμούσε το ύψος της ζημίας που προκαλείται στη Γερμανία από οικονομική κατασκοπεία σε τουλάχιστο 8 δισεκατομμύρια γερμανικά μάρκα[151]. Ο πρόεδρος του συνδέσμου των εταιριών συμβούλων ασφαλείας αναφέρει, επικαλούμενος ειδικούς, ένα ποσό ύψους 15 δισεκατομμυρίων γερμανικών μάρκων ανά έτος. Ο πρόεδρος του ευρωπαϊκού συνδέσμου των Hermann Lutz εκτιμά τη ζημία σε 20 δισεκατομμύρια γερμανικά μάρκα ετησίως. Το FBI[152] αναφέρει για τα έτη 1992/1993 ζημία 1,7 δισεκατομμυρίων δολαρίων, την οποία υφίσταται η αμερικανική οικονομία από ανταγωνιστική και οικονομική κατασκοπεία. Ο πρώην πρόεδρος της επιτροπής ελέγχου μυστικών υπηρεσιών της Βουλής των Αντιπροσώπων στις ΗΠΑ κάνει λόγο για ζημίες 100 δισεκατομμυρίων δολαρίων, λόγω διαφυγόντων παραγγελιών και πρόσθετων δαπανών για έρευνα και ανάπτυξη. Μεταξύ του 1990 και του 1996, το γεγονός αυτό οδήγησε κατά τα λεγόμενά του στην απώλεια 6 εκατομμυρίων θέσεων εργασίας.[153]

Ουσιαστικά δεν είναι αναγκαίο να γνωρίζει κανείς το ακριβές ύψος της ζημίας. Η υποχρέωση του κράτους να κινείται, με τη βοήθεια της αστυνομίας και των υπηρεσίας αντικατασκοπίας, κατά της ανταγωνιστικής και οικονομικής κατασκοπείας υφίσταται ανεξάρτητα από το ύψος της ζημίας που υφίσταται η εθνική οικονομία. Ούτε για τις αποφάσεις που λαμβάνονται στο πλαίσιο των επιχειρήσεων σχετικά με την προστασία των πληροφοριών και τα αντικατασκοπευτικά μέτρα αποτελούν χρήσιμη βάση οι αριθμοί για το συνολικό ύψος της ζημίας. Κάθε επιχείρηση πρέπει να υπολογίσει για τον εαυτό της την μέγιστη ζημία που δύναται να υποστεί από την παρακολούθηση πληροφοριών, να εκτιμήσει τις πιθανότητες επέλευσης και να συγκρίνει τα με τον τρόπο αυτό εξαχθέντα ποσά με το κόστος ασφάλειας. Το πραγματικό πρόβλημα δεν συνίσταται στην έλλειψη αριθμών σχετικά με το ακριβές ύψος της ζημίας. Πολύ περισσότερο συνίσταται στο ότι, εκτός από τις μεγάλες επιχειρήσεις, σχεδόν κανείς δεν προβαίνει σε τέτοιου είδους αναλύσεις κόστους/ οφέλους και για το λόγο αυτό, η ασφάλεια παραμελείται.

10.3. Ποιος κατασκοπεύει;

Οι κύριοι εντολείς κατασκοπείας εις βάρος επιχειρήσεων είναι, σύμφωνα με μία μελέτη της εταιρίας οικονομικών Ernest Young LLP[154] σε ποσοστό 39% ανταγωνιστές, σε ποσοστό 19% πελάτες, σε ποσοστό 9% προμηθευτές και σε ποσοστό 7% μυστικές υπηρεσίες. Η κατασκοπεία διενεργείται από συνεργάτες, των ιδιωτικών κατασκοπευτικών επιχειρήσεων, από πληρωμένους πληροφορικούς πειρατές και από επαγγελματίες των μυστικών υπηρεσιών.[155]

[151] IMPULSE,3/97, σ.13 επ.

[152] Congressional Statement, L.J.Freech, Director FBI, 9.5.1996

[153] Robert Lyle, Radio Liberty/Radio fre Europe, 10 Φεβρουαρίου 1999

[154] Computerzeitung, 30.11.1995, σ.2

[155] R.Hummelt, Spionage auf dem Datenhighway, München 1997, s. 49 ep.

10.3.1. Ιδιοι συνεργάτες (αδικήματα από κατόχους εμπιστευτικών πληροφοριών)

Η ερευνηθείσα βιβλιογραφία, οι σχετικές αναφορές ειδικών στην επιτροπή και οι συζητήσεις του εισηγητή με διευθυντές ασφαλείας και αντικατασκοπευτικές υπηρεσίες οδηγούν στο ίδιο συμπέρασμα: Ο μεγαλύτερος κίνδυνος για κατασκοπεία προέρχεται από απογοητευμένους και ανικανοποίητους συνεργάτες. Αυτοί έχουν, ως εργαζόμενοι στην επιχείρηση, άμεση πρόσβαση σε πληροφορίες, μπορούν να δελεαστούν με χρήματα και να κατασκοπεύσουν για λογαριασμό των εντολέων τους επιχειρηματικά μυστικά.

Μεγάλους κινδύνους εγκυμονεί η αλλαγή του εργοδότη. Σήμερα δεν χρειάζεται να φωτοτυπηθούν στοίβες χαρτιού, προκειμένου να μεταφερθούν πληροφορίες εκτός της επιχείρησης. Είναι δυνατό να αποθηκευτούν κρυφά σε δισκέτες και να συνοδεύσουν τον συνεργάτη κατά την αλλαγή της θέσης εργασίας στον νέο εργοδότη.

10.3.2. Ιδιωτικές εταιρίες κατασκοπείας

Ο αριθμός των εταιριών που ειδικεύονται στην κατασκοπεία δεδομένων αυξάνεται συνεχώς. Στις εταιρίες αυτές εργάζονται και πρώην συνεργάτες υπηρεσιών πληροφοριών. Οι εταιρίες αυτές λειτουργούν συχνά τόσο ως εταιρίες συμβούλων ασφαλείας όσο και ως γραφεία ιδιωτικών αστυνομικών, που προμηθεύουν πληροφορίες κατόπιν εντολής. Κατά κανόνα χρησιμοποιούνται σύννομες μέθοδοι, αν και υπάρχουν εταιρίες που χρησιμοποιούν παράνομες μεθόδους.

10.3.3. Πληροφορικοί πειρατές

Οι πληροφορικοί πειρατές είναι ειδικοί στους ηλεκτρονικούς υπολογιστές, οι οποίοι με τις γνώσεις τους μπορούν να αποκτήσουν έξωθεν πρόσβαση σε δίκτυα Η/Υ. Την εποχή που δημιουργούνταν ο κύκλος των πληροφορικών πειρατών, επρόκειτο για λάτρεις των υπολογιστών, οι οποίοι διασκέδαζαν παραβιάζοντας τα μέτρα ασφαλείας των συστημάτων υπολογιστών. Σήμερα, τόσο στις υπηρεσίες όσο και στην αγορά, υπάρχουν πληροφορικοί πειρατές που ενεργούν κατόπιν εντολής.

10.3.4. Υπηρεσίες πληροφοριών

Μετά το τέλος του ψυχρού πολέμου, τα καθήκοντα των υπηρεσιών πληροφοριών μετατοπίστηκαν. Νέους τομείς καθηκόντων τους αποτελούν το διεθνές οργανωμένο έγκλημα και αντικείμενα οικονομικής φύσης. (περισσότερα στο κεφάλαιο 10,10.5)

10.4. Ποιος αποτελεί αντικείμενο κατασκοπίας;

Σύμφωνα με στοιχεία αντικατασκοπευτικών υπηρεσιών και διευθυντών ασφαλείας μεγάλων επιχειρήσεων, στην οικονομική κατασκοπεία χρησιμοποιούνται όλες οι δοκιμασμένες μέθοδοι και τα εργαλεία των μυστικών υπηρεσιών (βλ. κεφάλαιο 2,2.). Οι επιχειρήσεις έχουν όμως πιο ανοιχτές δομές σε σχέση με στρατιωτικές υπηρεσίες και υπηρεσίες πληροφοριών ή κυβερνητικές αρχές. Για το λόγο αυτό, στην οικονομική κατασκοπεία προστίθενται οι παρακάτω κίνδυνοι:

- Η στρατολόγηση συνεργατών είναι πιο εύκολη, διότι οι δυνατότητες της ασφάλειας των επιχειρήσεων δεν μπορούν να συγκριθούν με αυτές των αντικατασκοπευτικών εταιριών
- Η κινητικότητα της θέσης εργασίας οδηγεί στο να μεταφέρονται σημαντικές πληροφορίες με φορητούς ηλεκτρονικούς υπολογιστές. Γι' αυτό, η κλοπή φορητών

ηλεκτρονικών υπολογιστών ή η κρυφή αντιγραφή του σκληρού δίσκου μετά από διάρρηξη δωματίων ξενοδοχείου ανήκουν στις βασικές τεχνικές της οικονομικής κατασκοπείας.

- Η διάρρηξη συστημάτων υπολογιστών επιτυγχάνεται ευκολότερα από ό,τι συμβαίνει στις ευαίσθητες σε θέματα ασφάλειας κρατικές υπηρεσίες, διότι, ιδίως στις μικρές και τις μεσαίες επιχειρήσεις, η συνείδηση και τα μέτρα ασφάλειας είναι πολύ λιγότερο αναπτυγμένα.

- Για τους ίδιους λόγους είναι ευκολότερη η επί τόπου παρακολούθηση (βλ. κεφάλαιο 3, 3.2)

Από την αξιολόγηση των πληροφοριών που συλλέχτηκαν σχετικά προκύπτει ότι η οικονομική κατασκοπεία κινείται κυρίως επί τόπου ή στην κινητή θέση εργασίας, διότι, εκτός ελαχίστων εξαιρέσεων, (βλ. κατωτέρω 10.6) οι ζητούμενες πληροφορίες δεν μπορούν να συλλεχθούν μέσω παρακολούθησης του διεθνούς τηλεπικοινωνιακού δικτύου.

10.5. Οικονομική κατασκοπεία από κράτη

10.5.1. Στρατηγική οικονομική κατασκοπεία από υπηρεσίες πληροφοριών

Μετά το τέλος του ψυχρού πολέμου ελευθερώθηκε μέρος της δυναμικότητας των μυστικών υπηρεσιών, το οποίο τώρα χρησιμοποιείται σε άλλους τομείς. Οι ΗΠΑ έχουν δηλώσει ανοιχτά ότι ένα μέρος της δραστηριότητας των μυστικών τους υπηρεσιών αφορά και στην οικονομία. Εδώ υπάγεται π.χ. ο έλεγχος της τήρησης οικονομικών κυρώσεων, ο έλεγχος της τήρησης των κανόνων για την προμήθεια όπλων και των λεγόμενων αγαθών διπλής χρήσης, οι εξελίξεις στις αγορές πρώτων υλών και τα δρώμενα στις διεθνείς χρηματαγορές. Κατά την πεποίθηση του εισηγητή, οι αμερικανικές υπηρεσίες δεν είναι οι μόνες που δραστηριοποιούνται στον τομέα αυτό, και για τον λόγο αυτό δεν ασκείται και μεγάλη κριτική.

10.5.2. Υπηρεσίες πληροφοριών ως πράκτορες ανταγωνιστικής κατασκοπείας

Κριτική διατυπώνεται στις περιπτώσεις όπου κρατικές υπηρεσίες πληροφοριών χρησιμοποιούνται για να επιτύχουν, για λογαριασμό επιχειρήσεων εγκατεστημένων στην επικράτεια της χώρας τους, πλεονεκτήματα στον διεθνή ανταγωνισμό. Εδώ διακρίνουμε δύο περιπτώσεις[156]:

10.5.2.1. Χώρες υψηλής τεχνολογίας

Οι υψηλά ανεπτυγμένες βιομηχανικές χώρες μπορούν κάλλιστα να επωφεληθούν από βιομηχανική κατασκοπεία. Με τη συλλογή πληροφοριών σχετικά με το βαθμό ανάπτυξης ενός κλάδου μπορεί να εφαρμοσθούν μέτρα που αφορούν στις συναλλαγές εξωτερικού ή μέτρα πολιτικής επιδοτήσεων, τα οποία είτε καθιστούν την βιομηχανία της χώρας περισσότερο ανταγωνιστική είτε εξοικονομούν επιδοτήσεις. Ένα άλλο κεντρικό σημείο μπορεί να έγκειται στην παροχή στοιχείων σχετικά με αναθέσεις υψηλής αξίας. (βλ. κατωτέρω 10.6).

10.5.2.2. Τεχνολογικά λιγότερο ανεπτυγμένες χώρες

Σε ένα μέρος των χωρών αυτών πρόκειται για την παροχή τεχνολογικής τεχνογνωσίας, προκειμένου να μπορέσουν να καλύψουν τα κενά της δικής τους βιομηχανίας δίχως

[156] Ιδιωτική δήλωση μιας αντικατασκοπευτικής υπηρεσίας προς τον εισηγητή, η πηγή προστατεύεται.

αναπτυξιακές δαπάνες και δαπάνες για δικαιώματα. Πέραν αυτού, πρόκειται για την προμήθεια βιομηχανικών σχεδίων και μεθόδων κατασκευής, προκειμένου να καταστούν, με τη διάθεση στην αγορά απομιμήσεων, οι οποίες έχουν φθηνότερο κόστος παραγωγής (μικρότερο μισθολογικό κόστος!) ανταγωνιστικές στην παγκόσμια αγορά. Είναι αποδεδειγμένο ότι στις ρωσικές υπηρεσίες έχουν ανατεθεί τα καθήκοντα αυτά. Ο ομοσπονδιακός νόμος αριθ. 5 της Ρωσικής Ομοσπονδίας σχετικά με την συλλογή πληροφοριών εξωτερικού, αναφέρει ρητά την προμήθεια οικονομικών, επιστημονικών και τεχνικών πληροφοριών ως καθήκον των υπηρεσιών πληροφοριών.
Σε μία άλλη μερίδα χωρών (π.χ. Ιράν, Ιράκ, Συρία, Λιβύη, Βόρεια Κορέα, Ινδία και Πακιστάν) πρόκειται για την προμήθεια πληροφοριών για τα εθνικά τους εξοπλιστικά προγράμματα, ιδίως στον τομέα των πυρηνικών και στον τομέα των βιολογικών και χημικών όπλων. Ένα άλλο μέρος της δραστηριότητας των υπηρεσιών των κρατών αυτών συνίσταται στη λειτουργία κεκαλυμμένων εταιριών με στόχο την αγορά αγαθών διπλής χρήσης χωρίς να κινούνται υποψίες.

10.6. Ενδείκνυται το ECHELON για βιομηχανική κατασκοπεία;

Από τον στρατηγικό έλεγχο των διεθνών τηλεπικοινωνιακών κινήσεων μόνον τυχαία μπορεί να προκύψουν πληροφορίες σημαντικές για την ανταγωνιστική κατασκοπεία. Πράγματι, τα ευαίσθητα δεδομένα της επιχείρησης κυρίως βρίσκονται μέσα στην ίδια την επιχείρηση, **έτσι ώστε η ανταγωνιστική κατασκοπεία να επιχειρείται κατά πρώτο λόγο δια της προσπάθειας να ληφθούν οι πληροφορίες από συνεργάτες** ή στρατευμένα πρόσωπα ή μέσω εισβολής στα εσωτερικά δίκτυα υπολογιστών. Μόνον αν κάποια ευαίσθητα στοιχεία καταλήξουν μέσω γραμμών ή ασύρματα (δορυφόρος) προς τα έξω, μπορεί να χρησιμοποιηθεί ένα σύστημα παρακολούθησης επικοινωνιών για σκοπούς ανταγωνιστικής κατασκοπείας. Αυτό ισχύει στις ακόλουθες τρεις περιπτώσεις:
- σε επιχειρήσεις, οι οποίες δραστηριοποιούνται σε 3 χρονικές ζώνες, έτσι ώστε τα ενδιάμεσα αποτελέσματα να αποστέλλονται από την Ευρώπη στην Αμερική και στη συνέχεια στην Ασία
- στην περίπτωση τηλεσυνδιασκέψεων σε πολυεθνικές εταιρίες, οι οποίες μεταδίδονται μέσω δορυφόρου ή καλωδίου.
- όταν γίνεται επί τόπου διαπραγμάτευση σημαντικών αναθέσεων (όπως συμβαίνει στην ανέγερση εγκαταστάσεων, στην κατασκευή τηλεπικοινωνιακής υποδομής, στην ανακατασκευή συστημάτων μεταφοράς κλπ), και πρέπει από το σημείο αυτό να γίνεται συνεννόηση με τις κεντρικές υπηρεσίες της εταιρίας**.**

Αν οι επιχειρήσεις δεν προστατεύουν στις παραπάνω περιπτώσεις τις επικοινωνίες τους, η παρακολούθηση αυτών των επικοινωνιών προσφέρει πολύτιμα δεδομένα στην ανταγωνιστική κατασκοπεία.

10.7. Δημοσιευθείσες περιπτώσεις

Υπάρχουν ορισμένες περιπτώσεις οικονομικής κατασκοπείας ή κατασκοπείας των ανταγωνιστών, οι οποίες περιγράφονται στον Τύπο ή σε σχετική βιβλιογραφία. Ένα μέρος αυτών των πηγών αξιολογήθηκε και συνοψίζεται στον κατωτέρω πίνακα. Αναφέρεται σε συντομία, ποιος συμμετείχε σ' αυτές, πότε προέκυψε η περίπτωση, γιατί επρόκειτο ακριβώς, ποιός ήταν ο στόχος και οι συνέπειες.
Αξιοσημείωτο είναι ότι εν μέρει για την μία και αυτή περίπτωση υπάρχουν πολύ διαφορετικές πληροφορίες. Ως παράδειγμα αναφέρεται η περίπτωση Enercon, στην οποία περιγράφεται ως "δράστης" η NSA ή το Υπουργείο Οικονομίας των ΗΠΑ ή οι ανταγωνιστές που έβγαλαν φωτογραφίες.

Περίπτωση	Ποιος	Πότε	Τι	Πως	Στόχος	Συνέπειες	Πηγή
Air France	DGSE	έως 1994	Συνομιλίες επιχειρηματιών που ταξίδευαν	Στα διαμερίσματα της 1ης θέσης της Air France ανακαλύφθηκαν κοριοί – Η αεροπορική εταιρία ζήτησε δημοσία συγνώμη	Κτήση πληροφοριών	Δεν αναφέρονται	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ του Arno Schütze, 1/
Airbus	NSA	1994	Πληροφορίες σχετικά με αγορές αεροπλάνων μεταξύ της Airbus και των σαουδαραβικών αερογραμμών	Παρακολούθηση Φαξ και τηλεφωνικών συνδιαλέξεων μεταξύ των διαπραγματευομένων	Διαβίβαση πληροφοριών στον αμερικανό ανταγωνιστή Boeing και Mc-Donnell-Douglas	Οι αμερικανοί συνήψαν την αγορά ύψους 6 δισεκατ. δολαρίων	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. Νοέμβριος 2000
Airbus	NSA	1994	Σύμβαση για 6 δισεκατ. δολάρια με τη Σαουδική Αραβία Ανακάλυψη δωροδοκίας της ευρωπαϊκής κοινοπραξίας Airbus.	Παρακολούθηση Φαξ και τηλεφωνικών συνδιαλέξεων μεταξύ της ευρωπαϊκής κοινοπραξίας Airbus και της σαουδαραβικής αεροπορικής εταιρίας/κυβέρνησης μέσω επικοινωνιακών δορυφόρων	Αποκάλυψη δωροδοκίας	Η McDonnel-Douglas, ο αμερικανός ανταγωνιστής της Airbus συνάπτει τη σύμβαση.	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, του Duncan Campbell
BASF	Διαχειριστής	Δεν αναφέρεται	Περιγραφή μεθόδου για την παραγωγή πρώτης ύλης κρέμας για το δέρμα της επιχείρησης BASF (Τμήμα καλλυντικών)	Δεν αναφέρεται	Καμία γιατί ματαιώθηκε	keine, weil aufgeflogen	„Nicht gerade zimperlich“, Wirtschaftswoche Nr.43 / 16. Οκτώβριος 1992
Ομοσπονδιακό Υπουργείο Οικονομίας της Γερμανίας	CIA	1997	Πληροφορίες για προϊόντα υψηλής τεχνολογίας στο Ομοσπονδιακό Υπουργείο Οικονομίας	Χρησιμοποίηση πράκτορα	Κτήση πληροφοριών	Αποκαλύπτεται ο πράκτορας κατά την απόπειρα και απελαύνεται	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ του Arno Schütze, 1/98
Ομοσπονδιακό Υπουργείο Οικονομίας της Γερμανίας	CIA	1997	Παρασκήνιο της δίκης Μύκονος στο Βερολίνο, πιστώσεις Hermes για εξαγωγές στο Ιράν, κατάλογος γερμανικών επιχειρήσεων που προμηθεύουν το Ιράν με προϊόντα υψηλής τεχνολογίας	Πράκτορας της CIA εμφανιζόμενος ως πρέσβης των ΗΠΑ πραγματοποιεί φιλικές συζητήσεις με τον προϊστάμενο της αρμόδιας υπηρεσίας για τον αραβικό χώρο (επίκεντρο Ιράν) στο Ομοσπονδιακό Υπουργείο Οικονομίας	Κτήση πληροφοριών	Δεν αναφέρονται Ο υπάλληλος στρέφεται στις γερμανικές Υπηρεσίες Ασφαλείας, οι οποίες επισημαίνουν στις αμερικανικές Υπηρεσίες ότι η επιχείρηση της CIA είναι ανεπιθύμητη. Ο πράκτορας της CIA κατόπιν αυτού "αποσύρεται".	„Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste“, Ομόσπονδη Υπηρεσία Προστασίας Συντάγματος Βάδης-Βυρτεμβέργης, Στουτγάρδη, κατάσταση : 1998
Dasa	Ρωσική Υπηρεσία Πληροφοριών	1996 – 1999	Πώληση και παράδοση εγγράφων σχετικών με τεχνολογία εξοπλισμού μιας επιχείρησης του Μονάχου στον τομέα της αμυντικής	2 εντεταλμένοι Γερμανοί	Απόκτηση πληροφοριών για κατευθυνόμενα βλήματα, οπλικά συστήματα (αντιαρματικά και αντιαεροπορικά)	Εφημερίδα Süddeutsche Zeitung / 30.05.2000: „(...) Προδοσία υπό στρατιωτικό πρίσμα "όχι ιδιαίτερα βαρεία". Αυτό ισχύει	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Βόννη, Απρίλιος 2001

			τεχνολογίας (σύμφωνα με την εφημερίδα Süddeutsche Zeitung / 30.05.2000: Όμιλος εξοπλισμών Dasa στο Ottobrunn)			και για την οικονομική ζημία, διαπίστωσε το δικαστήριο".	„Haftstrafe wegen Spionage für Russland“, SDZ / 30. Μαΐου 2000
Αποκλεισμός	Ομοσπονδιακή Υπηρεσία Πληροφοριών	κατά το 1990	Επανειλημμένη εξαγωγή προστατευόμενης από τον αποκλεισμό τεχνολογίας προς την Λιβύη (μεταξύ άλλων από Siemens)	Παρακολούθηση τηλεπικοινωνιών	Αποκάλυψη παράνομων μεταφορών όπλων και τεχνολογίας	Όχι ιδιαίτερες συνέπειες, δεν εμποδίζονται οι παραδόσεις	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 110

Περίπτωση	Ποιος	Πότε	Τι	Πως	Στόχος	Συνέπειες	Πηγή
Enercon	Ειδικός της αιολικής ενέργειας από το Oldenburg και γυναίκα υπάλληλος της Kenetech	Δεν αναφέρεται	Εγκατάσταση αιολικής ενέργειας της επιχείρησης Enercon του Auricher	Δεν αναφέρεται	Δεν αναφέρεται	Δεν αναφέρεται	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Βόννη, Απρίλιος 2001
Enercon	NSA	Δεν αναφέρεται	Ανεμοτροχός για την παραγωγή ρεύματος, που αναπτύχθηκε από τον μηχανικό Aloys Wobben στο Ostfriesen	Δεν αναφέρεται	Περαιτέρω παράδοση τεχνικών οδηγιών του Wobbens σε επιχείρηση των ΗΠΑ	Η επιχείρηση των ΗΠΑ καταθέτει αίτηση ευρεσιτεχνίας για τον ανεμοτροχό πριν τον Wobben· ο Wobben ενάγεται από αμερικανικό δικηγορικό γραφείο (παραβίαση δικαιώματος ευρεσιτεχνίας)	„Aktenkrieger“, SÜDDEUTSCHE ZEITUNG, 29 Μαρτίου 2001
Enercon	Αμερικανική επιχείρηση Kenetech Windpower Corp	1994	Σημαντικές λεπτομέρειες μίας εγκατάστασης αιολικής ενέργειας υψηλής τεχνολογίας (σύστημα εκκίνησης έως πλατίνες)	Φωτογραφίες	Επιτυχής διαδικασία ευρεσιτεχνίας στις ΗΠΑ	Η Enercon GmbH παγώνει σχέδια για επέκταση στην αμερικανική αγορά	„Sicherheit muss künftig zur Chefsache werden“, HB / 29. Αύγουστος 1996
Enercon	Μηχανικός του Oldenburg W. και η αμερικανική επιχείρηση Kenetech	Μάρτιος 1994	Ανεμογεννήτρια τύπου E-40 της Enercon	Ο μηχανικός W. παραδίδει περαιτέρω πορίσματα, η υπάλληλος της Kenetech φωτογραφίζει εγκαταστάσεις και ηλεκτρολογικές λεπτομέρειες	Kenetech: αναζητεί αποδείξεις για μεταγενέστερη (1995) αγωγή παραβίασης δικαιώματος ευρεσιτεχνίας κατά της Enercon Enercon: παράνομη κτήση πληροφοριών επιχειρηματικών μυστικών Δημοσιογράφος της τηλεόρασης πληροφορήθηκε από πρώην υπάλληλο της NSA ότι λεπτομερή στοιχεία της Enercon διαβιβάσθηκαν μέσω του Echelon από τους Αμερικανούς στην Kenetech..	Δεν αναφέρονται	„Klettern für die Konkurrenz“, SÜDDEUTSCHE ZEITUNG 13 Οκτωβρίου 2000
Enercon	Kenetech Windpower	Πριν το 1996	Στοιχεία για την εγκατάσταση αιολικής ενέργειας της Enercon	Μηχανικοί της Kenetech φωτογραφίζουν την εγκατάσταση	Αντιγραφή της κατασκευής της εγκατάστασης από την Kenetech	Η Enercon δικαιώνεται, υποβάλλεται μήνυση κατά των κατασκόπων· εκτίμηση ζημίας: πολλές εκατοντάδες	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ του Arno Schütze, 1/98

						εκατομμύρια μάρκα.	
Υπουργείο Εμπορίου της Ιαπωνίας	CIA	1996	Διαπραγματεύσεις για ποσοστώσεις εισαγωγών αμερικανικών αυτοκινήτων στην ιαπωνική αγορά	Πειρατεία στο σύστημα υπολογιστών του ιαπωνικού Υπουργείου Εμπορίου	Ο διαπραγματευτής των ΗΠΑ Mickey Kantor θα συμφωνήσει στη χαμηλότερη προσφορά	Ο Kantor αποδέχεται τη χαμηλότερη προσφορά	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ του Arno Schütze, 1/98
Ιαπωνικά αυτοκίνητα	Κυβέρνηση ΗΠΑ	Δεν αναφέρεται	Διαπραγματεύσεις για την εισαγωγή ιαπωνικών αυτοκινήτων πολυτελείας Πληροφορίες για προδιαγραφές εκπομπών ιαπωνικών αυτοκινήτων	COMINT, δεν περιγράφεται ακριβέστερα	Κτήση πληροφοριών	Δεν διατίθενται στοιχεία	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, του Duncan Campbell

Περίπτωση	Ποιος	Πότε	Τι	Πως	Στόχος	Συνέπειες	Πηγή
López	NSA	Δεν αναφέρεται	Τηλεδιάσκεψη της VW και του López	Παρακολούθηση από το Bad Aibling	Περαιτέρω παράδοση πληροφοριών στην General Motors και την Opel	Με ενέργειες παρακολούθησης η Εισαγγελία έλαβε "πολύ ακριβείς ενδείξεις" με τις έρευνες	Ο λοχαγός του Ομοσπονδιακού Στρατού Erich Schmidt-Eenboom, αναφέρει στο "Wenn Freunde spionieren“ www.zdf.msnbc.de/news/54637.asp?cp1=1
López	López και τρεις από τους υπαλλήλους του	1992 - 1993	Έγγραφα και στοιχεία από τους τομείς έρευνας, σχεδιασμού, παραγωγής και αγοράς (έγγραφα για εργοστάσιο στην Ισπανία, στοιχεία κόστους διαφόρων μοντέλων, μελέτες σχεδίων, στρατηγικές αγορών και οικονομιών)	Συλλογή υλικού	Χρησιμοποίηση των εγγράφων της General-Motors από την VW	Μετά από αντιπαράθεση στα ποινικά δικαστήρια, συμφωνούν οι όμιλοι εξώδικα. Ο López παραιτείται το 1996 από διευθυντής της VW. Η VW αποχωρίζεται επίσης το 1997 τρεις περαιτέρω συνεργάτες της της ομάδας του López, πληρώνει 100 εκατομμύρια δολάρια στην GM/Opel (αμοιβές δικηγόρων, όπως αναφέρεται) και αγοράζει επί 7 έτη ανταλλακτικά αξίας 1 δισ. δολαρίων από την GM/Opel	„Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste“, Ομόσπονδη Υπηρεσία Προστασίας του Συντάγματος της Βάδης-Βυρτεμβέργης, Στουτγάρδη, κατάσταση : 1998
López	NSA	1993	Βιντεοδιάσκεψη μεταξύ του José Ignacio López και του διευθυντή της VW Ferdinand Piëch	Απόσπασμα της βιντεοδιάσκεψης και περαιτέρω παράδοσή του στην General Motors (GM)	Προστασία των αμερικανικών επιχειρηματικών μυστικών της GM, που ήθελε να παραδώσει ο López στην VW (τιμοκατάλογοι, μυστικά σχέδια για νέο εργοστάσιο παραγωγής αυτοκινήτων και νέο μικρό αυτοκίνητο)	Ο López αποκαλύπτεται, η ποινική διαδικασία σταματά το 1998 έναντι πληρωμής χρηματικών ποινών. Όσον αφορά την NSA ουδέν	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. Νοέμβριος 2000 „Abgehört“, Berliner Zeitung, 22 Ιανουαρίου 1996 „Die Affäre López ist beendet“, Wirtschaftsspiegel, 28 Ιουλίου 1998 „Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ του Arno Schütze, 1/98
Los Alamos	Ισραήλ	1988	Δύο συνεργάτες του ερευνητικού προγράμματος στην ατομική ενέργεια του Ισραήλ διεισδύουν στον κεντρικό υπολογιστή του	Πληροφορική πειρατεία	Κτήση πληροφοριών για νέο αναφλεκτήρα πυρηνικών όπλων των ΗΠΑ	Όχι ιδιαίτερες συνέπειες, λόγω του ότι οι πειρατές πληροφορικής δραπετεύουν στο Ισραήλ, ένας συλλαμβάνεται προσωρινά,	"Maulwürfe in Nadelstreifen", Andreas Förster, σελ. 137

			εργαστηρίου πυρηνικών όπλων του Los Alamos			σχέση με μυστικές υπηρεσίες του Ισραήλ επισήμως δεν υπάρχει	
Λαθρεμπορία	Γερμανική Υπηρεσία Πληροφοριών	Δεκαετία του '70	Λαθρεμπορία εγκαταστάσεων υπολογιστών στην Λαοκρατική Δημοκρατία της Γερμανίας	Δεν αναφέρεται	αποκάλυψη μεταφοράς τεχνολογίας στο Ανατολικό Μπλοκ	Όχι ιδιαίτερες συνέπειες, οι παραδόσεις δεν εμποδίζονται	"Maulwürfe in Nadelstreifen", Andreas Förster, σελ. 113

Περίπτωση	Ποιος	Πότε	Τι	Πως	Στόχος	Συνέπειες	Πηγή
TGV	DGSE	1993	υπολογισμός κόστους της Siemens Ανάθεση για την παράδοση τρένων μεγάλης ταχύτητας στη Νότια Κορέα	Δεν αναφέρεται	Προσφορά χαμηλότερης τιμής	Ο κατασκευαστής ICE χάνει την ανάθεση προς όφελος της Alcatel-Alsthom	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ του Arno Schütze, 1/98
TGV	Άγνωστος	1993	Υπολογισμός κόστους της AEG και της Siemens όσον αφορά κρατική ανάθεση στη Νότια Κορέα για την παράδοση τρένων υψηλής ταχύτητας	Η Siemens ισχυρίζεται ότι οι τηλεφωνικές συνδέσεις και οι συνδέσεις φαξ στο υποκατάστημα της επιχείρησης στη Σεούλ παρακολουθούνται	Διαπραγματευτικό πλεονέκτημα για τον βρετανο-γαλλικό ανταγωνιστή GEC Alsthom	Οι αναθέτοντες αποφασίζουν υπέρ της GEC Alsthom, αν και η γερμανική προσφορά ήταν αρχικά καλύτερη	„Abgehört“, Berliner Zeitung, 22 Ιανουαρίου 1996
Thomson-Alcatel κατά Raytheon	CIA/ NSA	1994	Κατακύρωση μιας ανάθεσης δισεκατομμυρίων της Βραζιλίας για την εποπτεία δορυφόρων του Αμαζόνα στη γαλλική Thomson-Alcatel (1,4 δισ. δολάρια)	Παρακολούθηση των επικοινωνιών αυτού που κέρδισε το διαγωνισμό (Thomson-Alcatel, Γαλλία)	Αποκάλυψη διαφθοράς (πληρωμή χρημάτων για δωροδοκία)	Ο Κλίντον παραπονείται στην κυβέρνηση της Βραζιλίας· κατόπιν πιέσεων της αμερικανικής κυβέρνησης, νέα κατακύρωση της σύμβασης στην αμερικανική επιχείρηση "Raytheon"	"Maulwürfe in Nadelstreifen", Andreas Förster, σελ. 91
Thomson-Alcatel κατά Raytheon	Το Υπουργείο Οικονομίας των ΗΠΑ "προσπάθησε"	1994	Διαπραγματεύσεις για σχέδιο δισεκατομμυρίων για την παρακολούθηση με ραντάρ του τροπικού δάσους της Βραζιλίας	Δεν αναφέρεται	Ανάθεση σύμβασης	Οι γαλλικοί όμιλοι Thomson CSF και Alcatel χάνουν την ανάθεση προς όφελος της επιχείρησης των ΗΠΑ Raytheon	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. Νοέμβριος 2000
Thomson-Alcatel κατά Raytheon	NSA Department of Commerce	Department of Commerce	Διαπραγματεύσεις για έργο δισεκατομμυρίων (1.4 δισ. δολάρια) για παρακολούθηση του Αμαζόνα (SIVA) Αποκάλυψη δωροδοκίας της επιτροπής επιλογής της Βραζιλίας. Παρατήρηση του Campbell: η Rayethon εξοπλίζει σταθμό παρακολούθησης στο Sugar Grove	Παρακολούθηση της διαπραγμάτευσης μεταξύ Thomson-CSF και της Βραζιλίας και παράδοση των αποτελεσμάτων στη Raytheon Corp.	Αποκάλυψη δωροδοκίας Ανάθεση σύμβασης	Η Raytheon παίρνει τη σύμβαση	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, του Duncan Campbell http://www:rayethon:com/sivam/contract:html
Thyssen	BP	1990	Ανάθεση εκατομμυρίων για την εξόρυξη αερίου και πετρελαίου στη Βόρειο Θάλασσα	Παρακολούθηση των φαξ αυτού που κέρδισε το διαγωνισμό (Thyssen)	Αποκάλυψη διαφθοράς	Η BP ενάγει την Thyssen για αποζημίωση.	"Maulwürfe in Nadelstreifen", Andreas Förster, σελ. 92

VW	Άγνωστος	"Προηγούμενα έτη“	Δεν αναφέρεται	Μεταξύ άλλων με μηχανή λήψεως με υπέρυθρα που είχε ταφεί σε γαιόλοφο και διαβιβάζει εικόνες με ραδιοσήματα	Κτήση πληροφοριών για νέες εξελίξεις	Η V W αναφέρει μεγάλα διαφυγόντα κέρδη	„Sicherheit muss künftig zur Chefsache werden“, HB / 29. Αύγουστος 1996
VW	Άγνωστος	1996	Διαδρομή δοκιμής στο Ehra-Lessien της VW	Κρυμμένη μηχανή λήψεως	Πληροφορίες για νέα μοντέλα της VW	Δεν αναφέρεται	„Auf Schritt und Tritt“ Wirtschaftswoche Nr. 25, 11. Ιούνιος 1998

10.8. Προστασία από οικονομική κατασκοπεία

10.8.1. Έννομη προστασία

Στις έννομες τάξεις όλων των βιομηχανικών κρατών είναι αξιόποινη η κλοπή επιχειρηματικών μυστικών. Όπως σε όλες τις άλλες περιπτώσεις του ποινικού δικαίου, είναι διαφορετική η διαμόρφωση του εθνικού επιπέδου προστασίας. Κατά κανόνα όμως ισχύει ότι η ποινή υστερεί σαφώς έναντι αυτής που προβλέπεται για κατασκοπεία σε σχέση με τη στρατιωτική ασφάλεια. Σε πολλές περιπτώσεις απαγορεύεται η κατασκοπεία των ανταγωνιστών, όμως σε επιχειρήσεις στην ημεδαπή αλλά όχι σε επιχειρήσεις στην αλλοδαπή. Αυτό συμβαίνει και στις Ηνωμένες Πολιτείες της Αμερικής.

Οι σχετικοί νόμοι απαγορεύουν κατά βάση την κατασκοπευτική δραστηριότητα μεταξύ βιομηχανικών επιχειρήσεων. Είναι αμφίβολο εάν περιορίζουν και τη δραστηριότητα κρατικών υπηρεσιών πληροφοριών. Γιατί αυτές έχουν, βάσει των νόμων που τις συγκροτούν, την άδεια για την κλοπή πληροφοριών.

Μία οριακή περίπτωση προκύπτει όταν υπηρεσίες πληροφοριών διαθέτουν πληροφορίες που απέκτησαν με κατασκοπεία σε μεμονωμένες επιχειρήσεις. Κανονικά αυτό δεν καλύπτεται πλέον από τους νόμους που δίδουν στις υπηρεσίες πληροφοριών ιδιαίτερες αρμοδιότητες. Ιδίως, εντός της ΕΕ αυτό θα αποτελούσε παραβίαση της Συνθήκης ΕΟΚ (βλ. κεφάλαιο ...).

Ανεξαρτήτως αυτού, θα ήταν όμως στην πράξη ιδιαίτερα δυσχερές να υλοποιηθεί η επίκληση νομικής προστασίας από μία επιχείρηση με την προσφυγή σε δικαστήρια. Η παρακολούθηση δεν αφήνει ίχνη και δεν οδηγεί σε αποδείξεις που μπορούν να αξιολογηθούν από το δικαστήριο.

10.8.2. Λοιπά εμπόδια στην οικονομική κατασκοπεία

Το γεγονός ότι οι υπηρεσίες πληροφοριών στο πνεύμα της απόκτησης γενικών στρατηγικών πληροφοριών δραστηριοποιούνται και στον τομέα της οικονομίας γίνεται αποδεκτό μεταξύ κρατών. Η "συμφωνία κυρίων" όμως παραβιάζεται μαζικά κατά την κατασκοπεία ανταγωνιστών προς όφελος της οικείας βιομηχανίας. Εάν εν προκειμένω συλληφθεί αποδεδειγμένα ένα κράτος, τότε αυτό αποκτά πολιτικά προβλήματα σε μεγάλη έκταση. Αυτό ισχύει ακριβώς και για την παγκόσμια δύναμη, όπως οι ΗΠΑ, της οποίας η αξίωση για παγκόσμια πολιτική ηγεσία ζημιώθηκε δραματικά κατ' αυτό τον τρόπο. Μεσαίες δυνάμεις θα μπορούσαν να έχουν την πολυτέλεια να γελοιοποιηθούν, μία παγκόσμια δύναμη ποτέ.

Παράλληλα με τα πολιτικά προβλήματα τίθεται το πρακτικό ερώτημα, σε ποια μεμονωμένη επιχείρηση διατίθενται τα αποτελέσματα της κατασκοπείας ανταγωνιστών. Στον τομέα κατασκευής αεροπλάνων είναι εύκολη η απάντηση, λόγω του ότι εν προκειμένω, σε παγκόσμιο επίπεδο, υπάρχουν μόνο δύο προσφέροντες. Σε όλες τις άλλες περιπτώσεις είναι εκεί όπου υπάρχουν περισσότεροι προσφέροντες οι οποίοι, εκτός αυτού, δεν ανήκουν στο κράτος, ιδιαίτερα δυσχερές να προτιμηθεί ένας μεμονωμένος. Κατά τη διαβίβαση λεπτομερών πληροφοριών σχετικά με προσφορές συνυποψηφίων σε μεμονωμένες επιχειρήσεις όσον αφορά διεθνείς δημόσιους διαγωνισμούς, θα ήταν δυνατή μια παράδοση των πληροφοριών της κατασκοπείας σε όλους τους υποψήφιους της οικείας χώρας. Αυτό ισχύει ιδιαίτερα όταν για όλους τους εθνικούς υποψηφίους υπάρχει μία ισότιμα προσπελάσιμη δομή υποστήριξης της κυβέρνησης, όπως αυτό συμβαίνει στις ΗΠΑ με το αποκαλούμενο Adcocacy Center. Στην

περίπτωση κλοπής τεχνολογίας, η οποία αναγκαστικά θα πρέπει να καταλήξει σε μία αίτηση ευρεσιτεχνίας, δεν θα ήταν πλέον λογικά δυνατή μία ισότιμη μεταχείριση επιχειρήσεων.

Αυτό θα ήταν πάντως, ιδιαίτερα στο αμερικανικό πολιτικό σύστημα, ένα μεγάλο πρόβλημα. Οι αμερικανοί πολιτικοί εξαρτώνται, όσον αφορά τη χρηματοδότηση των εκλογικών τους αγώνων, ιδιαίτερα από δωρεές της βιομηχανίας στις εκλογικές τους περιφέρειες. Εάν η προτίμηση μεμονωμένων επιχειρήσεων από τις υπηρεσίες πληροφοριών δημοσιοποιείτο έστω και σε μία περίπτωση, θα υπήρχαν τεράστιες αποδοκιμασίες στο πολιτικό σύστημα. Όπως ανέφερε ο πρώην διευθυντής της CIA Woolsey σε μια συνομιλία με εκπροσώπους της επιτροπής: "In this case the hill (i..e the US-Congress) would go mad!". Και όντως έχει δίκιο!

10.9. ΗΠΑ και οικονομική κατασκοπεία

10.9.1. Η επίσημη θέση της αμερικανικής πλευράς όσον αφορά την οικονομική κατασκοπεία

Ο πρώην διευθυντής της CIA Woolsey και ο πρόεδρος της Επιτροπής Ελέγχου των Μυστικών Υπηρεσιών στο Σώμα των Αντιπροσώπων Porter Goss υποστήριξαν σε συνομιλίες συνοπτικά την ακόλουθη θέση:

1. Οι ΗΠΑ παρακολουθούν τις διεθνείς τηλεπικοινωνίες προκειμένου να λαμβάνουν γενικές πληροφορίες για οικονομικές εξελίξεις, παραδόσεις αγαθών διπλής χρήσεως και την τήρηση εμπορικών αποκλεισμών.

2. Οι ΗΠΑ παρακολουθούν ειδικά επικοινωνίες μεμονωμένων επιχειρήσεων σε σχέση με διαγωνισμούς για την ανάθεση συμβάσεων προκειμένου να εμποδίζουν στρεβλώσεις της αγοράς με δωροδοκίες εις βάρος επιχειρήσεων των ΗΠΑ.

Η δωροδοκία απαγορεύεται δια νόμου στις αμερικανικές επιχειρήσεις και οικονομικοί ελεγκτές υποχρεούνται να τις ανακοινώνουν, εφόσον συναντούν αριθμούς που αναφέρονται σε χρήματα δωροδοκιών. Εφόσον διαπιστωθεί κατά την παρακολούθηση επικοινωνιών δωροδοκία σε δημόσιες αναθέσεις, τότε θα παρενέβαινε ο Αμερικανός Πρεσβευτής στην κυβέρνηση του αντίστοιχου κράτους. Οι συνυποψήφιες αμερικανικές επιχειρήσεις δεν θα ενημερώνονταν αντιθέτως άμεσα.

10.9.2. Ο ρόλος του Advocacy Centers κατά την ενίσχυση των εξαγωγών των ΗΠΑ

10.9.2.1. Η αποστολή του Advocacy Centers

Το εγκατεστημένο στο Υπουργείο Εμπορίου των ΗΠΑ Adcocacy Center αποτελεί τον πυρήνα της από τον Πρόεδρο Κλίντον ακολουθηθείσας και από τον Μπους συνεχιζόμενης εθνικής στρατηγικής των εξαγωγών. Το Κέντρο, που ιδρύθηκε το 1993, βοήθησε έκτοτε εκατοντάδες αμερικανικές επιχειρήσεις να κερδίσουν διεθνείς διαγωνισμούς στο εξωτερικό. Το Κέντρο συγκεντρώνει τους σχετικούς πόρους της αμερικανικής κυβέρνησης από πραγματογνώμονες σε επί μέρους τομείς έως οικονομικούς ακολούθους των πρεσβειών μέχρι και τον Λευκό Οίκο.

10.9.2.2. Ο τρόπος εργασίας του Κέντρου

Στο ίδιο το Κέντρο εργάζεται μόνο ένα μικρό επιτελείο 12 ατόμων (κατάσταση 6.2.2001). Το Κέντρο χρησιμεύει στις επιχειρήσεις ως κεντρική υπηρεσία επαφής για τις διάφορες υπηρεσίες της αμερικανικής κυβέρνησης που ασχολούνται με την ενίσχυση των εξαγωγών. Εργάζεται για τις επιχειρήσεις χωρίς να κάνει διακρίσεις, υποστηρίζει όμως, σύμφωνα με σαφείς κανόνες, μόνο σχέδια προς όφελος του εθνικού συμφέροντος των ΗΠΑ. Έτσι πρέπει τα παραδιδόμενα προϊόντα να έχουν αξία που έχει κατά 50% παραχθεί στις ΗΠΑ.

10.9.2.3. Ανοικτά ζητήματα σε σχέση με το Κέντρο

Η αμερικανική κυβέρνηση δεν επέτρεψε τη σχεδιασμένη συνομιλία μεταξύ μελών της επιτροπής και του Κέντρου. Για το λόγο αυτό δεν μπόρεσαν να συζητηθούν δύο θέματα, τα οποία συνδέονται με αμφιβολίες:

α) η επιτροπή έχει στη διάθεσή της έγγραφα, τα οποία αποδεικνύουν συμμετοχή της CIA σε εργασίες του Κέντρου·

β) το Κέντρο αναφέρει στο πλαίσιο των πληροφοριών που διατίθενται στο Ιντερνέτ ότι συνενώνει τους πόρους 19 "U.S. government agencies". Σε άλλο σημείο όμως αναφέρονται ονομαστικά μόνο 14 agencies. Τίθεται το ερώτημα γιατί δεν δημοσιοποιούνται τα ονόματα 5 agencies.

10.10.Η ασφάλεια των δικτύων Η/Υ

Θα διατυπωθεί αργότερα.

10.11.Η υποτίμηση των κινδύνων

Θα διατυπωθεί αργότερα

10.11.1. Μεγάλες επιχειρήσεις

10.11.2. Μικρές και μεσαίες επιχειρήσεις

10.11.3. Ευρωπαϊκοί οργανισμοί

10.11.4. Οργανισμοί έρευνας

11. Αυτοπροστασία μέσω της κρυπτογράφησης

11.1. Σκοπός και λειτουργία της κρυπτογράφησης

11.1.1. Σκοπός της κρυπτογράφησης

Σε κάθε περίπτωση διαβίβασης πληροφοριών υπάρχει ο κίνδυνος να περιέλθουν οι εν λόγω πληροφορίες σε μη εξουσιοδοτημένα πρόσωπα. Προκειμένου να αποφευχθεί ο ανωτέρω κίνδυνος, πρέπει να διασφαλιστεί ότι το μήνυμα δεν μπορεί να αναγνωσθεί ή να υποκλαπεί, πρέπει δηλαδή να κρυπτογραφηθεί. Στο στρατιωτικό και το διπλωματικό τομέα χρησιμοποιούνταν, για το λόγο αυτό, ανέκαθεν κρυπτογραφικές τεχνικές.[157]

Τα τελευταία 20 χρόνια, η σημασία της κρυπτογράφησης ενισχύθηκε, καθώς αυξάνονται διαρκώς οι διεθνείς επικοινωνίες, τομέας όπου το κάθε κράτος δεν μπορεί πλέον να προστατεύσει το απόρρητο της αλληλογραφίας και των τηλεπικοινωνιών των πολιτών του. Επιπρόσθετα, στο βαθμό που έχει καταστεί τεχνικά ευκολότερο για τις υπηρεσίες του κάθε κράτους να παρακολουθούν και να καταγράφουν νόμιμα τις επικοινωνίες των πολιτών τους, οι πολίτες που ανησυχούν έχουν αυξημένες ανάγκες προστασίας. Η παρατηρούμενη αύξηση στις απόπειρες παράνομης πρόσβασης σε πληροφορίες και νόθευσής τους, τέλος, οδήγησε στη λήψη μέτρων προστασίας (π.χ. στον τραπεζικό τομέα).

Με την ανακάλυψη μεθόδων ηλεκτρικής και ηλεκτρονικής επικοινωνίας (τηλέγραφος, τηλέφωνο, ασύρματος, τηλέτυπο, τηλεομοιοτυπία και διαδίκτυο), η μετάδοση πληροφοριών κατέστη πολύ ευκολότερη και ασύγκριτα γρηγορότερη. Το μειονέκτημα ήταν, ότι δεν προσφέρονταν κανενός είδους **τεχνική** προστασία κατά της παρακολούθησης και της καταγραφής της επικοινωνίας, ενώ ο καθένας μπορούσε, εφόσον αποκτούσε πρόσβαση στον φορέα της, να παρέμβει στην επικοινωνία χρησιμοποιώντας μία ανάλογη συσκευή. Η παρακολούθηση, όταν συντελείται με επαγγελματικό τρόπο, αφήνει ελάχιστα ή και καθόλου ίχνη. Εξ αιτίας των ανωτέρω η κρυπτογράφηση απέκτησε πρωτοφανή αξία. Ο τραπεζικός τομέας πρωτοπόρησε κρυπτογραφώντας και προστατεύοντας έτσι συστηματικά τις επικοινωνίες που αφορούσαν στις ηλεκτρονικές χρηματικές συναλλαγές. Η αυξανόμενη διεθνοποίηση της οικονομίας οδήγησε στην, τουλάχιστον έως ένα βαθμό, υιοθέτηση μεθόδων προστασίας των επικοινωνιών μέσω της κρυπτογράφησης και από τους εμπλεκόμενους στο διεθνοποιημένο οικονομικό γίγνεσθαι. Η εξάπλωση της χρήσης του διαδικτύου ως μέσου επικοινωνίας σήμανε την αύξηση της ανάγκης προστασίας του απορρήτου των επικοινωνιών και των ιδιωτών, δεδομένου ότι η επικοινωνία μέσω διαδικτύου είναι εξαιρετικά ευάλωτη στις υποκλοπές.

Σε σχέση με την παρούσα έκθεση τίθεται συνεπώς το ερώτημα, εάν υπάρχει κάποια οικονομικά συμφέρουσα, νόμιμη, επαρκώς ασφαλής και εύκολη στη χρήση της μέθοδος κρυπτογράφησης των επικοινωνιών, η οποία να προσφέρεται ως μέθοδος αυτοπροστασίας από υποκλοπές.

[157] Οι σχετικές ενδείξεις φθάνουν μέχρι την αρχαιότητα, για παράδειγμα η χρήση της σκυτάλης από τους Σπαρτιάτες τον 5ο π.Χ. αιώνα.

11.1.2. Η λειτουργία της κρυπτογράφησης

Η βασική αρχή της κρυπτογράφησης έγκειται στο ότι ένα κανονικό κείμενο μετατρέπεται σε μυστικό, έτσι ώστε να αλλάζει το νόημά του ή να μην βγαίνει καθόλου νόημα. Από μυημένα πρόσωπα μπορεί όμως να μετατραπεί ξανά στο πρωτότυπο. Μία λογική διάταξη γραμμάτων μετατρέπεται π.χ. κατά την κρυπτογράφηση σε μία παράλογη, την οποία δεν κατανοεί κανείς.

Αυτό γίνεται σύμφωνα με κάποια συγκεκριμένη μέθοδο (αλγόριθμος της κρυπτογράφησης), η οποία βασίζεται στην αντιμετάθεση (transposition) ή/ και στην υποκατάσταση (substitution) γραμμάτων. **Η μέθοδος της κρυπτογράφησης** (αλγόριθμος) δεν τηρείται σήμερα μυστική. Αντιθέτως: πριν από λίγο καιρό διεξήχθη ένας παγκόσμιος διαγωνισμός για τις νέες παγκόσμιες προδιαγραφές κρυπτογράφησης για εφαρμογή στην οικονομία. Αυτό ισχύει και για την υλοποίηση ενός συγκεκριμένου αλγόριθμου κρυπτογράφησης ως υλισμικό σε μια συσκευή, π.χ. σε μία συσκευή κρυπτογραφημένης τηλεομοιοτυπίας.

Το **πραγματικά μυστικό** στοιχείο είναι το λεγόμενο **κλειδί**. Ο τρόπος λειτουργίας του μπορεί να εξηγηθεί με ένα παράδειγμα από έναν συγγενικό χώρο. Ο τρόπος λειτουργίας των κλειδαριών των θυρών είναι κατά κανόνα δημοσίως γνωστός, καθώς μάλιστα αποτελούν αντικείμενο πατέντας. Η προστασία κάθε μεμονωμένης πόρτας προκύπτει από το γεγονός, ότι για κάθε συγκεκριμένο τύπο κλειδαριάς μπορεί να υπάρχουν πολλά διαφορετικά κλειδιά. Το ίδιο συμβαίνει και στην κρυπτογράφηση πληροφοριών: Με μία **δημοσίως γνωστή μέθοδο** κρυπτογράφησης (αλγόριθμος) δύνανται, με τη χρήση πολλών διαφορετικών κλειδιών, που **τηρούνται μυστικά** από τους εμπλεκόμενους, να κρατηθούν μυστικές **πολλές** διαφορετικές πληροφορίες.

Για την επεξήγηση των παραπάνω χρησιμοποιηθέντων όρων, θα αναφέρουμε το παράδειγμα της λεγόμενης "καισαρικής κρυπτογράφησης". Ο ρωμαίος στρατηγός Καίσαρας κρυπτογραφούσε μηνύματα, αντικαθιστώντας απλά κάθε γράμμα με το γράμμα το οποίο βρισκόταν τρεις θέσεις πιο κάτω στη σειρά του αλφαβήτου, δηλαδή το Α με το D, το Β με το Ε κλπ. Με αυτό τον τρόπο, η λέξη **ECHELON** θα μετατρέπονταν σε **HFKHORQ.** Ο αλγόριθμος της κρυπτογράφησης συνίσταται λοιπόν στην **μετατόπιση γραμμάτων** εντός του αλφαβήτου, ενώ το συγκεκριμένο **κλειδί** είναι η οδηγία για μετατόπιση κατά **τρεις θέσεις του αλφαβήτου!** Τόσο η κρυπτογράφηση όσο και η αποκρυπτογράφηση γίνονται με τον ίδιο τρόπο: Με την μετατόπιση γραμμάτων κατά τρεις θέσεις. Πρόκειται συνεπώς για μία συμμετρική μέθοδο. Στις ημέρες μας, μία τέτοια μέθοδος δεν θα παρείχε προστασία ούτε για ένα δευτερόλεπτο!

Σε μία καλή κρυπτογράφηση, η μέθοδος μπορεί να είναι καθ' όλα γνωστή δημοσίως, και εντούτοις η κρυπτογράφηση να μπορεί να χαρακτηριστεί ασφαλής. Εν προκειμένω απαιτείται όμως, η ποικιλία των κλειδιών να είναι τόσο μεγάλη, ώστε μία ενδεχόμενη δοκιμή όλων των κλειδιών (η λεγόμενη **brute force attack**) να μην είναι δυνατή εντός εύλογου χρόνου, ακόμη και εάν χρησιμοποιηθούν υπολογιστές. Από την άλλη, η ποικιλία κλειδιών δεν αποτελεί αυτή καθεαυτή ένδειξη ασφάλειας όταν η μέθοδος της κρυπτογράφησης δημιουργεί ένα μυστικό κείμενο, το οποίο εμπεριέχει στοιχεία στα οποία θα μπορούσε να βασιστεί η αποκρυπτογράφησή του (π.χ. επανάληψη συγκεκριμένων γραμμάτων).[158] Υπό αμφότερα τα ανωτέρω πρίσματα, η καισαρική κρυπτογράφηση δεν αποτελεί ασφαλή μέθοδο κρυπτογράφησης. Στην απλή υποκατάσταση ένα κείμενο μπορεί να αποκωδικοποιηθεί γρήγορα λόγω της διαφορετικής

[158] Βλ. σχετικά και Leiberich, Vom diplomatischen Code zur Fallfürfunktion - Hundert Jahre Kryptographie in Deutschland, Spektrum der Wissenschaft, Juni 1999, 26 επ.

συχνότητας εμφάνισης των γραμμάτων σε μία γλώσσα, ενώ επιπλέον υπάρχουν μόνον 25 δυνατότητες μετατόπισης, δηλαδή 25 μόνον κλειδιά, καθώς το αλφάβητο αποτελείται από 26 μόνο γράμματα. Ο αντίπαλος μπορεί στην περίπτωση αυτή να ανακαλύψει πολύ γρήγορα το σωστό κλειδί και να αποκρυπτογραφήσει το κείμενο, δοκιμάζοντας απλώς διάφορες εναλλακτικές.

Παρακάτω θα αναφερθούμε στο ερώτημα, πως θα πρέπει να διαμορφώνεται ένα ασφαλές σύστημα.

11.2. Η ασφάλεια των συστημάτων κρυπτογράφησης

11.2.1. Γενικά για την έννοια της ασφάλειας κατά την κρυπτογράφηση

Όταν απαιτούμε από ένα σύστημα κρυπτογράφησης να είναι "ασφαλές", μπορεί να εννοούμε δύο διαφορετικά πράγματα. Κατά πρώτον, μπορεί να ζητούμε το σύστημα να είναι απόλυτα ασφαλές, δηλαδή να είναι αδύνατη η αποκρυπτογράφηση του μηνύματος δίχως γνώση του κλειδιού και ο αποκλεισμός αυτής της δυνατότητας να αποδεικνύεται μαθηματικά. Κατά δεύτερον, μπορεί κανείς να αρκεστεί στο ότι ο κωδικός δεν μπορεί, δεδομένων των υφιστάμενων τεχνολογικών περιορισμών, να παραβιαστεί και ότι συνεπώς παρέχεται ασφάλεια για ένα χρονικό διάστημα που υπερβαίνει κατά πολύ τον "κρίσιμο" χρόνο, κατά τον οποίο πρέπει να παραμείνει μυστικό το μήνυμα.

11.2.2. Απόλυτη ασφάλεια: το κλειδί μίας χρήσης (one-time pad)

Απόλυτα ασφαλή μέθοδο συνιστά μέχρι σήμερα μόνον το κλειδί μίας χρήσης (one-time pad). Το σύστημα αυτό αναπτύχθηκε περί τα τέλη του πρώτου παγκοσμίου πολέμου[159], χρησιμοποιήθηκε όμως αργότερα και για τον δίαυλο επικοινωνίας σε περίπτωση κρίσης μέσω τηλετύπου μεταξύ Μόσχας και Ουάσινγκτον. Η ιδέα συνίσταται στη χρήση ενός κλειδιού, το οποίο αποτελείται από τελείως τυχαία κατά σειρά τοποθετημένα γράμματα, όπου η σειρά δεν επαναλαμβάνεται. Ο αποστολέας και ο παραλήπτης κρυπτογραφούν το κείμενο βάσει αυτών των σειρών γραμμάτων και καταστρέφουν το κλειδί μετά την πρώτη χρήση του. Καθώς εντός του κλειδιού δεν υπάρχει κάποια εσωτερική τάξη, είναι αδύνατο να παραβιαστεί ο κωδικός. Αυτό μπορεί μάλιστα να αποδειχθεί και μαθηματικά.[160]

Το μειονέκτημα αυτής της μεθόδου έγκειται στο ότι δεν είναι εύκολο να παραχθούν μεγάλες ποσότητες τέτοιων κλειδιών,[161] και ότι η διανομή των κλειδιών με ασφαλή τρόπο είναι δύσκολη και μη πρακτική. Για το λόγο αυτό, η μέθοδος αυτή δεν χρησιμοποιείται στις κοινές εμπορικές συναλλαγές.

[159] Εισήχθη από τον Ταγματάρχη Joseph Mauborgne, διευθυντή του τμήματος κρυπτογραφικών ερευνών του αμερικανικού στρατού. Βλ. σχετικά Singh, Geheime Botschaften (1999), 151

[160] Βλ. σχετικά Singh, Geheime Botschaften (1999), 151 επ.

[161] Βλ. σχετικά Wobst, Abenteuer Kryptologie^2 (1998), 60.

11.2.3. Σχετική ασφάλεια ανάλογα με την τεχνολογική πρόοδο

11.2.3.1. Η χρήση συσκευών κρυπτογράφησης και αποκρυπτογράφησης

Ήδη πριν από την ανακάλυψη της μεθόδου του κλειδιού μίας χρήσης είχαν αναπτυχθεί κρυπτογραφικές μέθοδοι, οι οποίες παρείχαν τη δυνατότητα δημιουργίας μεγάλου αριθμού κλειδιών και παρήγαγαν μυστικά κείμενα, τα οποία περιείχαν όσο το δυνατό λιγότερη τακτικότητα στο κείμενο και συνεπώς δεν προσέφεραν σχεδόν καθόλου πρόσφορες βάσεις για κρυπτογραφική ανάλυση. Προκειμένου να διαμορφωθούν αρκετά γρήγορα οι μέθοδοι αυτές, ώστε να μπορούν να χρησιμοποιηθούν στην πράξη, σχεδιάστηκαν συσκευές κρυπτογράφησης και αποκρυπτογράφησης. Η εντυπωσιακότερη του είδους της ήταν μάλλον η ENIGMA[162], η οποία χρησιμοποιήθηκε κατά τον δεύτερο παγκόσμιο πόλεμο από τη Γερμανία. Η στρατιά των ειδικών αποκρυπτογράφησης, που εργάστηκε στο Bletchley Park της Αγγλίας, κατάφερε να σπάσει την κρυπτογράφηση της ENIGMA με τη βοήθεια ειδικών συσκευών, των λεγόμενων "βομβών". Τόσο η ENIGMA όσο και οι "βόμβες" ήταν μηχανικές συσκευές.

11.2.3.2. Η χρήση των υπολογιστών στην κρυπτογράφηση

Η ανακάλυψη του ηλεκτρονικού υπολογιστή υπήρξε επαναστατική για την επιστήμη της κρυπτογράφησης, καθώς η ταχύτητα υπολογισμών του επιτρέπει την χρήση ολοένα και πιο σύνθετων συστημάτων. Παρότι οι βασικές αρχές της κρυπτογράφησης δεν άλλαξαν από το γεγονός αυτό, προέκυψαν ορισμένες καινοτομίες. Πρώτον, διότι πολλαπλασιάστηκε ο βαθμός της δυνατής πολυπλοκότητας των συστημάτων κρυπτογράφησης, καθώς αυτή έπαψε να περιορίζεται από μηχανικούς παράγοντες και δεύτερον, διότι αυξήθηκε δραστικά η ταχύτητα της διαδικασίας κρυπτογράφησης.

Ο υπολογιστής επεξεργάζεται την πληροφορία ψηφιακά με δυαδικούς αριθμούς. Αυτό σημαίνει, ότι η πληροφορία εκφράζεται με τη σειρά δύο σημείων, ήτοι του 0 και του 1. Το 1 στη φυσική επιστήμη αντιστοιχεί στην ύπαρξη τάσης ηλεκτρισμού ή μαγνητισμού ("light on"), ενώ το Ο αντιστοιχεί στην έκλειψη της τάσης ή του μαγνητισμού ("light off"). Σχετικά έχει επικρατήσει η τυποποίηση σύμφωνα με το σύστημα ASCII[163], το οποίο απεικονίζει κάθε γράμμα δια ενός επταψήφιου συνδυασμού των Ο και 1[164]. Ως εκ τούτου, το κείμενο παίρνει τη μορφή μιας σειράς των αριθμών Ο και 1 και αντί γραμμάτων καταχωρίζονται αριθμοί.

Στο πλαίσιο αυτό δύνανται να τύχουν εφαρμογής τόσο η μέθοδος της transposition (αντιμετάθεσης) όσο και αυτή της substitution (υποκατάστασης). Υποκατάσταση μπορεί για παράδειγμα να λάβει χώρα με την πρόσθεση ενός κλειδιού υπό τη μορφή μιας τυχαίας σειράς αριθμών. Σύμφωνα με τους δυαδικούς μαθηματικούς κανόνες, το αποτέλεσμα της πρόσθεσης ίδιων αριθμών είναι το μηδέν (δηλ. 0+0=0 και 1+1=0), ενώ το αποτέλεσμα της πρόσθεσης δύο διαφορετικών αριθμών είναι το ένα (0+1=1). Η νέα κρυπτογραφημένη σειρά αριθμών που προκύπτει από την πρόσθεση είναι συνεπώς μία δυαδική σειρά, η οποία είτε μπορεί να τύχει

[162] Η μέθοδος Enigma αναπτύχθηκε από τον Arthur Scherbius και καταχωρήθηκε ως πατέντα το 1928. Προσομοίαζε κατά κάποιον τρόπο με γραφομηχανή, καθώς διέθετε πληκτρολόγιο, με το οποίο γράφονταν το κανονικό κείμενο. Διαμέσου ενός πίνακα βυσμάτων και ενός περιστρεφόμενου κυλίνδρου, το κείμενο κρυπτογραφούνταν σύμφωνα με κάποιες συγκεκριμένες προδιαγραφές, ενώ αποκωδικοποιούνταν με την ίδια συσκευή βάσει βιβλίων κωδίκων.

[163] American Standard Code for Information Interchange

[164] A = 1000001, B= 1000010, C= 1000011, D= 1000100, E = 1000101, κλπ

περαιτέρω επεξεργασίας είτε μπορεί να καταστεί, με την αφαίρεση του προστεθέντος κλειδιού, και πάλι αναγνώσιμη.

Με την χρήση των υπολογιστών μπορούν να δημιουργηθούν μυστικά κείμενα, με την εφαρμογή ισχυρών αλγόριθμων κρυπτογράφησης, τα οποία ουσιαστικά δεν προσφέρουν πλέον βάσεις αποκρυπτογράφησης. Η αποκρυπτογράφησή τους θα μπορούσε συνεπώς να επιχειρηθεί μόνον με την δοκιμή όλων των δυνατών κλειδιών. Όσο πιο μακροσκελές είναι το κλειδί, τόσο δυσκολότερη καθίσταται η αποκρυπτογράφηση εντός του υφιστάμενου χρονικού πλαισίου, ακόμη και αν χρησιμοποιηθούν υπολογιστές υψηλής απόδοσης. Υπάρχουν συνεπώς διαθέσιμες μέθοδοι, οι οποίες να μπορούν να θεωρηθούν ασφαλείς με βάση τα σημερινά τεχνολογικά δεδομένα.

11.2.4. Τυποποίηση και ηθελημένος περιορισμός της ασφάλειας

Λόγω της εξάπλωσης των ηλεκτρονικών υπολογιστών κατά τη δεκαετία του ’70, ανέκυψε μια κλιμακούμενη ανάγκη τυποποίησης των συστημάτων κρυπτογράφησης, διότι μόνον με τον τρόπο αυτό ήταν δυνατή για τις επιχειρήσεις η ασφαλής επικοινωνία με τους επαγγελματικούς τους συνεργάτες δίχως να απαιτούνται δυσανάλογες δαπάνες. Οι πρώτες προσπάθειες προς την κατεύθυνση αυτή έγιναν στις ΗΠΑ.
Μία ισχυρή κρυπτογράφηση μπορεί να χρησιμοποιηθεί και για αθέμιτους σκοπούς ή από κάποιο ενδεχόμενο στρατιωτικό αντίπαλο. Επίσης, μπορεί να δυσχεράνει ή να καταστήσει αδύνατη την ηλεκτρονική κατασκοπεία. Για το λόγο αυτό, η NSA άσκησε πιέσεις, ώστε να επιλεγεί ένα πρότυπο κρυπτογράφησης που παρείχε μεν επαρκή ασφάλεια για τα δεδομένα των επιχειρήσεων, αλλά το οποίο η ίδια μπορούσε, λόγω του ειδικού τεχνικού εξοπλισμού της, να αποκρυπτογραφήσει. Για το σκοπό αυτό περιορίστηκε το μήκος του κλειδιού σε 56-Bit. Έτσι περιορίζεται ο αριθμός των πιθανών κλειδιών σε 100 000 000 000 000 000[165]. Πράγματι, στις 23 Νοεμβρίου1976 έγινε επίσημα αποδεκτός υπό την ονομασία Data Encryption Standard (DES) ο λεγόμενος κωδικός Lucifer του Horst Feistel στην έκδοση των **56 bit,** που αποτέλεσε επί εικοσιπενταετία το επίσημο αμερικανικό πρότυπο κρυπτογράφησης.[166] Επίσης, το πρότυπο αυτό χρησιμοποιήθηκε και στον τραπεζικό τομέα στην Ευρώπη και την Ιαπωνία. Ο αλγόριθμος του DES, παρά τους αντίθετους ισχυρισμούς διάφορων ΜΜΕ, δεν έχει μέχρι σήμερα παραβιαστεί, υπάρχει όμως εν τω μεταξύ υλισμικό (hardware), το οποίο είναι αρκετά ισχυρό ώστε να δοκιμάσει όλα τα κλειδιά ("brute force attack"). Αντιθέτως, το Triple-DES, το οποίο έχει κλειδί 112 bit, εξακολουθεί να θεωρείται ασφαλές. Ο διάδοχος του DES, το AES (Advanced Encryption Standard), είναι μία ευρωπαϊκή δημιουργία[167], η οποία σχεδιάστηκε υπό την ονομασία Rijndael στο Leuven του Βελγίου. Είναι γρήγορη και θεωρείται ασφαλής, **καθώς εν προκειμένω αποφεύχθηκε ο περιορισμός του μήκους του κλειδιού**. Το γεγονός αυτό οφείλεται στην αλλαγή της αμερικανικής πολιτικής στον τομέα της κρυπτογραφίας (βλ. ανωτέρω 11,1.4).

Η τυποποίηση επέφερε μία σημαντική απλούστευση της κρυπτογράφησης για τις επιχειρήσεις. Παρέμεινε, ωστόσο, το πρόβλημα της διανομής των κλειδιών.

---

[165] Ο αριθμός αυτός αποτελείται σε δυαδική απεικόνιση από 56 μηδενικά και μονάδες. Βλ. σχετικά Singh, Geheime Botschaften (1999), 03

[166] Βλ. σχετικά Singh, Geheime Botschaften (1999), 302 επ

[167] Σχεδιάστηκε από δύο βέλγους κρυπτογράφους του Καθολικού Πανεπιστημίου του Leuven, τους Joan Daemen και Vincent Rijmen.

11.3. Το πρόβλημα της διανομής ή της παράδοσης των κλειδιών

11.3.1. Ασύμμετρη κρυπτογράφηση: η μέθοδος του δημοσίου κλειδιού (public-key)

Ένα σύστημα που λειτουργεί με κάποιο κλειδί, με το οποίο ταυτόχρονα κρυπτογραφείται και αποκρυπτογραφείται κάποιο κείμενο (συμμετρική κρυπτογράφηση), δύσκολα μόνο μπορεί να χρησιμοποιηθεί από **πολλούς,** οι οποίοι επικοινωνούν μεταξύ τους, διότι το κλειδί θα πρέπει να παραδοθεί σε καθέναν από αυτούς εκ των προτέρων, ενώ παράλληλα δεν θα πρέπει να μπορεί να το πληροφορηθεί κάποιος τρίτος. Αυτό είναι στην πράξη δυσχερές στο πλαίσιο των οικονομικών συναλλαγών, ενώ σε ό,τι αφορά στους ιδιώτες είναι δυνατό μόνο σε μεμονωμένες περιπτώσεις.

Μία λύση στο πρόβλημα αυτό προσφέρει η ασύμμετρη κρυπτογράφηση: για την κρυπτογράφηση και την αποκρυπτογράφηση δεν χρησιμοποιείται το ίδιο κλειδί. Η πληροφορία κρυπτογραφείται με ένα κλειδί, το οποίο είναι προσιτό στον καθένα και ονομάζεται **δημόσιο κλειδί**. Η μέθοδος λειτουργεί όμως σε μία μόνον κατεύθυνση, καθώς η αποκρυπτογράφηση της πληροφορίας δεν είναι δυνατή με τη χρήση του δημοσίου κλειδιού. Έτσι μπορεί ο καθένας που επιθυμεί να λάβει μία κρυπτογραφημένη πληροφορία, να αποστείλει στο πρόσωπο με το οποίο επικοινωνεί το δημόσιο κλειδί του για την κρυπτογράφηση της πληροφορίας, χωρίς να είναι αναγκασμένος να χρησιμοποιήσει κάποια ασφαλή μέθοδο αποστολής. Για την αποκρυπτογράφηση της πληροφορίας που θα ληφθεί χρησιμοποιείται ένα άλλο κλειδί, το **ιδιωτικό κλειδί**, το οποίο τηρείται απόρρητο και δεν αποστέλλεται.[168] Ο καταλληλότερος παραλληλισμός για την κατανόηση της μεθόδου είναι αυτός με το λουκέτο: ο καθένας μπορεί να κλείσει ένα λουκέτο και να κλειδώσει έτσι με ασφαλή τρόπο μία κασέλα, να ανοίξει όμως την κασέλα αυτή μπορεί μόνον όποιος κατέχει το σωστό κλειδί.[169] Το δημόσιο και το ιδιωτικό κλειδί σχετίζονται μεν μεταξύ τους, τα στοιχεία που περιέχονται στο δημόσιο κλειδί όμως δεν επαρκούν για να αποκαλυφθεί το ιδιωτικό.

Οι Ron Rivest, Adi Shamir και Leonard Adleman εφηύραν έναν τρόπο ασύμμετρης κρυπτογράφησης, τη μέθοδο RSA, που ονομάστηκε έτσι από τα αρχικά των επωνύμων τους. Σε μία λειτουργία μίας κατεύθυνσης (τη λεγόμενη λειτουργία της καταπακτής) χρησιμοποιείται ως συστατικό μέρος του δημοσίου κλειδιού το γινόμενο του πολλαπλασιασμού δύο πολύ μεγάλων πρώτων αριθμών. Με τον τρόπο αυτό κρυπτογραφείται το κανονικό κείμενο. Η αποκρυπτογράφηση είναι δυνατή μόνον σε όποιον γνωρίζει τις τιμές των δύο πρώτων αριθμών που χρησιμοποιήθηκαν. Δεν υπάρχει όμως καμία γνωστή μαθηματική μέθοδος μέσω της οποίας να μπορούν να υπολογιστούν βάσει του γινομένου οι τιμές των αρχικών πρώτων αριθμών. Μέχρι σήμερα, αυτό είναι δυνατό μόνο μέσω της συστηματικής δοκιμής. Για το λόγο αυτό, η μέθοδος αυτή είναι, με τα σημερινά επιστημονικά δεδομένα, ασφαλής, εφόσον επιλεγούν επαρκώς υψηλοί πρώτοι αριθμοί. Ο μοναδικός κίνδυνος έγκειται στο ότι θα μπορούσε κάποτε ένας λαμπρός μαθηματικός να ανακαλύψει έναν γρηγορότερο τρόπο διάσπασης του γινομένου σε συντελεστές. Μέχρι σήμερα όμως, αυτό δεν έχει επιτευχθεί, παρά τις σημαντικές

[168] Η ιδέα της ασύμμετρης κρυπτογράφησης υπό την μορφή της μεθόδου public-key προέρχεται από τους Whitfield Diffie και Martin Hellmann.

[169] Singh, Geheime Botschaften (1999), 327

προσπάθειες που έχουν καταβληθεί.[170] Πολλές φορές έχει υποστηριχτεί μάλιστα η άποψη, ότι το πρόβλημα είναι άλυτο, ισχυρισμός που όμως δεν έχει αποδειχθεί επαρκώς μέχρι σήμερα.[171]

Η κρυπτογράφηση τύπου public-key απαιτεί βέβαια, σε σύγκριση με τις συμμετρικές μεθόδους, πολύ περισσότερο χρόνο υπολογισμών του προσωπικού υπολογιστή, ή τη χρήση ισχυρών, υψηλών επιδόσεων υπολογιστών.

11.3.2. Κρυπτογράφηση public-key για ιδιώτες

Προκειμένου να καταστεί η μέθοδος public-key προσιτή στο κοινό, ο Phil Zimmerman είχε την ιδέα να συνδυάσει την από άποψη υπολογισμών πολύπλοκη μέθοδο public-key με μία ταχύτερη συμμετρική μέθοδο. Η πληροφορία μεταβιβαζόταν με μία συμμετρική μέθοδο, την μέθοδο IDEA που είχε σχεδιαστεί στην Ζυρίχη, ενώ το κλειδί για την κρυπτογράφηση μεταβιβαζόταν ταυτοχρόνως με την μέθοδο public-key. Ο Zimmermann ανέπτυξε ένα φιλικό προς το χρήστη πρόγραμμα υπό την ονομασία Pretty Good Privacy, το οποίο με το πάτημα ενός πλήκτρου (ή με ένα κλικ του ποντικιού) δημιουργούσε το απαραίτητο κλειδί και διενεργούσε την κρυπτογράφηση. Το πρόγραμμα διατέθηκε στο διαδίκτυο, από όπου μπορούσε ο καθένας να το φορτώσει στον υπολογιστή του. Το PGP αγοράστηκε τελικά από την αμερικανική εταιρία NAI, εξακολουθεί όμως να διατίθεται δωρεάν σε ιδιώτες.[172] Ο πηγαίος κώδικας των προηγούμενων εκδόσεων δημοσιεύτηκε, γεγονός που οδηγεί στο συμπέρασμα ότι δεν περιέχονται πίσω πόρτες. Ο πηγαίος κώδικας της νεότερης έκδοσης, PGP 7, η οποία χαρακτηρίζεται από μία εξαιρετικά φιλική προς το χρήστη γραφική επιφάνεια, δεν έχει δυστυχώς δημοσιευτεί.

Υπάρχει όμως άλλη μία εφαρμογή του Open PGP Standards: το GnuPG. Το GnuPG προσφέρει τις ίδιες μεθόδους κρυπτογράφησης όπως και το PGP και είναι επίσης συμβατό με το PGP. Πρόκειται όμως για ελεύθερο λογισμικό, του οποίου ο πηγαίος κώδικας είναι γνωστός και ο καθένας μπορεί να τον χρησιμοποιήσει και να τον μεταβιβάσει. Το γερμανικό ομοσπονδιακό υπουργείο οικονομίας και τεχνολογίας ενίσχυσε την μετατροπή του GnuPG σε Windows και την ανάπτυξη μιας επιφάνειας γραφικών, δυστυχώς όμως αυτά δεν έχουν μέχρι στιγμής ωριμάσει τελείως. Πάντως, σύμφωνα με τις πληροφορίες του εισηγητή, οι σχετικές εργασίες συνεχίζονται.

Περαιτέρω υπάρχουν και ανταγωνιστικά προς το OpenPGP πρότυπα, όπως για παράδειγμα το S/MIME, το οποίο υποστηρίζεται από πολλά προγράμματα ηλεκτρονικού ταχυδρομείου. Ο εισηγητής δεν διαθέτει όμως καμία πληροφόρηση σχετικά με την ελεύθερη εφαρμογή αυτού.

11.3.3. Μελλοντικές μέθοδοι

Τελείως νέα δεδομένα για την ασφαλή παράδοση του κλειδιού θα μπορούσαν να προκύψουν μελλοντικά από την κβαντική κρυπτογράφηση. Αυτή διασφαλίζει, ότι κάθε απόπειρα παρακολούθησης θα γίνεται αντιληπτή κατά την παράδοση του κλειδιού. Όταν αποστέλλονται πολωμένα φωτόνια, δεν μπορεί να πιστοποιηθεί η πόλωσή τους δίχως αυτή να μεταλλαχθεί. Με τον τρόπο αυτό θα μπορεί να διαπιστωθεί με βεβαιότητα ενδεχόμενη παρακολούθηση δεδομένων. Στην περίπτωση αυτή θα χρησιμοποιηθεί μόνο κάποιο κλειδί που δεν έχει

[170] Βλ. σχετικά Buchmann, Faktorisierung großer Zahlen, Spektrum der Wissenschft 2 1999, 6 επ

[171] Βλ. σχετικά Singh, Geheime Botschaften (1999), 335 επ

[172] Πληροφορίες για το λογισμικό θα βρείτε στη σελίδα www.pgpi.com

υποκλαπεί. Σε δοκιμές έχει επιτευχθεί ήδη μετάδοση δεδομένων δια 48 χλμ καλωδίου ινών υάλου, καθώς και εναέρια μετάδοση σε απόσταση 500 μ.[173]

11.4. Η ασφάλεια των προϊόντων κρυπτογράφησης

Στη συζήτηση σχετικά με την πραγματική ασφάλεια της κρυπτογράφησης ακούγεται συχνά η κατηγορία, ότι τα αμερικανικά προϊόντα εμπεριέχουν πίσω πόρτες. Πρωτοσέλιδα στα ΜΜΕ έχει κάνει π.χ. το Excel, για το οποίο υπάρχει ο ισχυρισμός, ότι στην ευρωπαϊκή έκδοση του προγράμματος το ήμισυ του κλειδιού βρίσκεται ανοιχτά τοποθετημένο στο Header του αρχείου. Την προσοχή του τύπου κίνησε και η Microsoft λόγω του γεγονότος, ότι ένας αμερικανός hacker βρήκε κρυμμένο στο πρόγραμμα μία πίσω πόρτα εισόδου και παρακολούθησης των κινήσεων του χρήστη από την NSA ("NSA-key"), πράγμα που η Microsoft αρνήθηκε βεβαίως κατηγορηματικά. Καθώς η Microsoft δεν έχει αποκαλύψει τον πηγαίο κώδικα του προγράμματός της, μπορούν να γίνουν μόνο εικασίες σχετικά. Για τις παλαιότερες εκδόσεις των PGP και GnuPG μπορεί πάντως με βεβαιότητα να αποκλειστεί η ύπαρξη μιας τέτοιας πίσω πόρτας, καθώς ο πηγαίος κώδικας των ανωτέρω προγραμμάτων βρίσκεται δημοσιευμένος.

11.5. Η κρυπτογράφηση σε σύγκρουση με κρατικά συμφέροντα

11.5.1. Προσπάθειες περιορισμού της κρυπτογράφησης

Πολλές χώρες απαγορεύουν καταρχήν τη χρήση λογισμικού κρυπτογράφησης ή κρυπτογραφικών συσκευών, επιτρέποντάς την κατ' εξαίρεση και εξαρτώντας την από τη λήψη σχετικής αδείας. Δεν πρόκειται εν προκειμένω μόνο για δικτατορίες όπως π.χ. η Κίνα, το Ιράν ή το Ιράκ. Ακόμη και δημοκρατικές χώρες έχουν περιορίσει νομοθετικά τη χρήση ή την πώληση προγραμμάτων ή συσκευών κρυπτογράφησης. Διατείνονται, ότι η επικοινωνία πρέπει μεν να προστατεύεται από την παρακολούθηση από μη εξουσιοδοτημένους ιδιώτες, ότι όμως το κράτος θα πρέπει να συνεχίσει να διατηρεί τη δυνατότητα νόμιμης παρακολούθησης των επικοινωνιών. Η απώλεια της τεχνικής υπεροχής των αρχών επιχειρήθηκε να αντιμετωπιστεί με νομοθετικές απαγορεύσεις. Έτσι η Γαλλία απαγόρευε μέχρι πρότινος γενικά την χρήση μεθόδων κρυπτογράφησης, επιτρέποντάς την κατ' εξαίρεση και εξαρτώντας την από τη λήψη ειδικής άδειας. Στη Γερμανία τέθηκε επίσης πριν από μερικά χρόνια το ζήτημα του περιορισμού της χρήσης μεθόδων κρυπτογράφησης και της υποχρέωσης γνωστοποίησης του κλειδιού. Οι ΗΠΑ περιόρισαν στο παρελθόν το επιτρεπτό μέγεθος του κλειδιού.

11.5.2. Η σημασία της ασφαλούς κρυπτογράφησης για το ηλεκτρονικό εμπόριο

Οι ανωτέρω προσπάθειες θα έπρεπε να έχουν αποτύχει οριστικά. Διότι το συμφέρον του κράτους, να έχει πρόσβαση στις επικοινωνίες και συνεπώς στα κανονικά κείμενα, δεν βρίσκεται μόνον αντιμέτωπο με το δικαίωμα στην προστασία της ιδιωτικής ζωής, αλλά και με χειροπιαστά οικονομικά συμφέροντα. Διότι το ηλεκτρονικό εμπόριο και οι ηλεκτρονικές τραπεζικές συναλλαγές απαιτούν μία ασφαλή επικοινωνία στο διαδίκτυο. Αν αυτή δεν μπορεί να διασφαλιστεί, οι τεχνικές αυτές είναι καταδικασμένες να αποτύχουν, διότι στην περίπτωση αυτή θα χανόταν η εμπιστοσύνη των πελατών. Αυτό εξηγεί τη στροφή στην αμερικανική ή την γαλλική πολιτική στον τομέα της κρυπτογράφησης.

[173] Σχετικά με τη κβαντική κρυπτογράφηση βλ. vgl Wobst, Abenteuer Kryptographie[2] (1998), 234 επ.

Στο σημείο αυτό πρέπει να παρατηρηθεί, ότι το ηλεκτρονικό εμπόριο έχει ανάγκη τις ασφαλείς μεθόδους κρυπτογράφησης για δύο λόγους: Όχι μόνο για λόγους κρυπτογράφησης πληροφοριών, αλλά και για να μπορεί να αποδειχθεί με βεβαιότητα η ταυτότητα του αντισυμβαλλομένου. Διότι η ηλεκτρονική υπογραφή μπορεί να χορηγηθεί με την ανάποδη εφαρμογή της μεθόδου public-key: Το ιδιωτικό κλειδί χρησιμοποιείται για την κρυπτογράφηση, ενώ το δημόσιο κλειδί χρησιμοποιείται για την αποκρυπτογράφηση. Αυτή η μορφή κρυπτογράφησης πιστοποιεί την προέλευση της υπογραφής. Με την χρήση του δημοσίου κλειδιού, ο καθένας μπορεί να βεβαιωθεί για την γνησιότητα της υπογραφής ενός προσώπου, χωρίς όμως να μπορεί να πλαστογραφήσει την ίδια την υπογραφή. Και αυτή η λειτουργία εμπεριέχεται στο PGP με φιλικό προς το χρήστη τρόπο.

11.5.3. Προβλήματα όσων ταξιδεύουν για επαγγελματικούς λόγους

Σε μερικές χώρες απαγορεύεται σε όσους βρίσκονται εκεί για επαγγελματικούς λόγους η χρήση προγραμμάτων κρυπτογράφησης με τους φορητούς υπολογιστές που μεταφέρουν. Αυτό ακυρώνει κάθε προστασία του απορρήτου της επικοινωνίας των προσώπων αυτών με την εταιρία τους, καθώς και κάθε προστασία των δεδομένων, που μεταφέρουν μαζί τους, από αθέμιτες παραβιάσεις.

11.6. Πρακτικά ερωτήματα για την κρυπτογράφηση

Αν θέλουμε να απαντήσουμε στο ερώτημα σχετικά με το σε ποιον και υπό ποιες συνθήκες συνίσταται η χρήση μεθόδων κρυπτογράφησης, θα πρέπει να διακρίνουμε μεταξύ ιδιωτών και επιχειρήσεων.

Σε ό,τι αφορά στους ιδιώτες, θα πρέπει να επισημανθεί ότι η προστασία των επικοινωνιών μέσω φαξ και τηλεφώνου μέσω της χρήσης σχετικών κρυπτογραφικών συσκευών δεν είναι πρακτικά εφικτή. Αυτό δεν οφείλεται μόνο στο υψηλό κόστος των σχετικών συσκευών, αλλά και στο γεγονός ότι η χρήση τους προϋποθέτει ότι ο συνομιλητής διαθέτει επίσης τέτοιου είδους συσκευές, γεγονός μάλλον σπάνιο.

Αντιθέτως, τα μηνύματα μέσω ηλεκτρονικού ταχυδρομείου (e-mails) μπορούν και πρέπει να κρυπτογραφούνται από τον καθένα. Στον συχνά προβαλλόμενο ισχυρισμό, ότι εφόσον δεν έχουμε μυστικά και έχουμε ανάγκη κρυπτογράφησης των επικοινωνιών μας, πρέπει να αντιλεχθεί, ότι ακόμη και τα γραπτά μηνύματα συνήθως δεν τα αποστέλλουμε γραμμένα επάνω σε καρτ-ποστάλ. Ένα μη κρυπτογραφημένο μήνυμα ηλεκτρονικού ταχυδρομείου δεν είναι παρά ένα γράμμα δίχως φάκελο. Η κρυπτογράφηση των μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι ασφαλής και σχετικά εύκολη, καθώς στο διαδίκτυο διατίθενται ήδη φιλικά προς τον χρήστη προγράμματα, όπως το PGP/GnuPG, τα οποία διατίθενται μάλιστα στους ιδιώτες δωρεάν. Δυστυχώς όμως η χρήση τους δεν είναι ακόμη αρκετά διαδεδομένη. Επιθυμητό θα ήταν να προηγηθεί το δημόσιο, δίνοντας το καλό παράδειγμα μέσω της χρήσης μεθόδων τυποποιημένης κρυπτογράφησης, προκειμένου να καταστεί περισσότερο προσιτή στο κοινό η έννοια της κρυπτογράφησης.

Σε ότι αφορά στις επιχειρήσεις, θα έπρεπε να προσέχουν ιδιαίτερα, ώστε οι ευαίσθητες πληροφορίες τους να μεταδίδονται μόνον με ασφαλείς τρόπους επικοινωνίας. Αυτό μολονότι φαίνεται αυτονόητο εφαρμόζεται μόνο από τις μεγάλες επιχειρήσεις. Στις μικρές και τις μεσαίες επιχειρήσεις, αντίθετα, διαβιβάζονται συχνά μέσω του ηλεκτρονικού ταχυδρομείου εσωτερικές πληροφορίες της εταιρίας σε μη κρυπτογραφημένη μορφή, καθώς οι άνθρωποί τους δεν έχουν

συνείδηση της σημασίας του ζητήματος. Ελπίζουμε, ότι οι βιομηχανικοί σύνδεσμοι και τα οικονομικά επιμελητήρια θα καταβάλλουν συστηματικές προσπάθειες ενημέρωσης των μελών τους. Βέβαια, η κρυπτογράφηση των μηνυμάτων ηλεκτρονικού ταχυδρομείου αποτελεί μια μόνο από τις πολλές παραμέτρους ασφαλείας, και κυρίως δεν ωφελεί σε τίποτα, όταν οι πληροφορίες έγιναν ήδη πριν από την κρυπτογράφηση προσιτές σε τρίτους. Αυτό σημαίνει, ότι πρέπει να ασφαλιστεί ολόκληρο το περιβάλλον εργασίας, δηλαδή να διασφαλιστεί η ασφάλεια των χώρων που χρησιμοποιούνται και να ελεγχθεί η φυσική πρόσβαση σε γραφεία και υπολογιστές. Πρέπει όμως να εμποδίζεται και η μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες διαμέσου δικτύου με την βοήθεια fire-walls. Ιδιαίτερους κινδύνους εγκυμονεί εν προκειμένω η σύνδεση του εσωτερικού δικτύου με το διαδίκτυο. Επίσης, για μεγαλύτερη ασφάλεια, θα πρέπει να χρησιμοποιούμε μόνον λειτουργικά συστήματα, των οποίων ο πηγαίος κώδικας έχει δημοσιευθεί και ελεγχθεί. Για τις εταιρίες ανακύπτουν συνεπώς πολλαπλά ζητήματα σχετικά με την ασφάλεια. Ήδη, στην αγορά υπάρχει ένας μεγάλος αριθμός εταιριών, οι οποίες προσφέρουν σε λογικές τιμές συμβουλές σε θέματα ασφαλείας και επιβλέπουν την υλοποίησή σχετικών προγραμμάτων. Ανάλογα με τη ζήτηση, η προσφορά αυξάνεται συνεχώς. Πέραν αυτού μένει όμως να ελπίσουμε, ότι οι βιομηχανικοί σύνδεσμοι και τα οικονομικά επιμελητήρια θα μεριμνήσουν για τα προβλήματα αυτά, ιδίως για να επισημάνουν στις μικρές επιχειρήσεις την προβληματική της ασφάλειας και να τις υποστηρίξουν στον σχεδιασμό και την υλοποίηση ολοκληρωμένων προγραμμάτων ασφάλειας.

12. Οι εξωτερικές σχέσεις της ΕΕ και η συλλογή πληροφοριών

12.1. Εισαγωγή

Η κοινή εξωτερική πολιτική και πολιτική ασφάλειας (ΚΕΠΠΑ) θεσπίστηκε, υπό τη στοιχειώδη μορφή της, με τη Συνθήκη του Μάαστριχτ το 1991, ως νέο μέσο άσκησης πολιτικής της Ευρωπαϊκής Ένωσης. Έξι χρόνια αργότερα, η Συνθήκη του Άμστερνταμ ενίσχυσε τη δομή της ΚΕΠΠΑ παρέχοντας τη δυνατότητα ανάπτυξης κοινών αμυντικών πρωτοβουλιών εντός της Ευρωπαϊκής Ένωσης, με παράλληλη διατήρηση των υφιστάμενων συμμαχιών. Βάσει της Συνθήκης του Άμστερνταμ και έχοντας κατά νου την εμπειρία του Κοσσυφοπεδίου, το Ευρωπαϊκό Συμβούλιο του Δεκεμβρίου 1999 στο Ελσίνκι δρομολόγησε την ευρωπαϊκή πρωτοβουλία για την ασφάλεια και την άμυνα. Η εν λόγω πρωτοβουλία στοχεύει στη σύσταση μίας πολυεθνικής δύναμης περίπου 50.000-60.000 στρατιωτών έως το δεύτερο εξάμηνο του 2003. Η ύπαρξη της πολυεθνικής αυτής δύναμης θα καταστήσει αναπόφευκτη την ανάπτυξη αυτόνομων δυνατοτήτων συλλογής πληροφοριών. Για τον σκοπό αυτό, η απλή ενσωμάτωση των υφιστάμενων δυνατοτήτων συλλογής πληροφοριών στο πλαίσιο της ΔΕΕ θα αποδεικνυόταν ανεπαρκής. Η περαιτέρω συνεργασία μεταξύ των υπηρεσιών πληροφοριών των κρατών μελών, πέραν των υφιστάμενων μορφών συνεργασίας, θεωρείται αναπόφευκτη.

Ωστόσο, η περαιτέρω ανάπτυξη της ΚΕΠΠΑ δεν είναι το μόνο στοιχείο που οδηγεί σε στενότερη συνεργασία μεταξύ των υπηρεσιών πληροφοριών της Ένωσης. Η περαιτέρω οικονομική ολοκλήρωση εντός της Ευρωπαϊκής Ένωσης θα καταστήσει επίσης αναγκαία την στενότερη συνεργασία στον τομέα της συλλογής πληροφοριών. Η ενιαία ευρωπαϊκή οικονομική πολιτική απαιτεί ενιαία αντίληψη της οικονομικής πραγματικότητας στον κόσμο, εκτός Ευρωπαϊκής Ένωσης. Η ενιαία θέση στις εμπορικές διαπραγματεύσεις στο πλαίσιο του ΠΟΕ ή με τρίτες χώρες απαιτεί κοινή προστασία της διαπραγματευτικής θέσης. Οι ισχυρές ευρωπαϊκές βιομηχανίες χρειάζονται κοινή προστασία κατά της οικονομικής κατασκοπείας από παράγοντες εκτός Ευρωπαϊκής Ένωσης.

Τέλος, πρέπει να τονιστεί ότι η περαιτέρω ανάπτυξη του δεύτερου πυλώνα της Ένωσης και των δραστηριοτήτων της τελευταίας στους τομείς της δικαιοσύνης και των εσωτερικών υποθέσεων θα οδηγήσει επίσης σε περαιτέρω συνεργασία μεταξύ των υπηρεσιών πληροφοριών. Ειδικότερα, οι κοινές προσπάθειες κατά της τρομοκρατίας, του λαθρεμπορίου όπλων, της εμπορίας ανθρώπων και της νομιμοποίησης των εσόδων από παράνομες δραστηριότητες είναι αδύνατο να υλοποιηθούν χωρίς εντατική συνεργασία μεταξύ των υπηρεσιών πληροφοριών.

12.2. Δυνατότητες συνεργασίας εντός της ΕΕ

12.2.1 Υφιστάμενη συνεργασία

Μολονότι οι υπηρεσίες πληροφοριών εμπιστεύονταν ανέκαθεν μόνο τις πληροφορίες που συνέλεγαν οι ίδιες, και επικρατούσε δυσπιστία μεταξύ των διαφόρων υπηρεσιών πληροφοριών της Ευρωπαϊκής Ένωσης, σήμερα η συνεργασία μεταξύ των εν λόγω υπηρεσιών αυξάνει βαθμιαία με τις επαφές που πραγματοποιούν στο πλαίσιο του ΝΑΤΟ, της ΔΕΕ και της

Ευρωπαϊκής Ένωσης. Εξάλλου, παρότι οι υπηρεσίες πληροφοριών στο πλαίσιο του NATO εξαρτώνται ακόμα σε μεγάλο βαθμό από τις σημαντικά πιο προηγμένες συνεισφορές των Ηνωμένων Πολιτειών της Αμερικής, η εγκαθίδρυση του δορυφορικού κέντρου της ΔΕΕ στο Torrejon (Ισπανία), καθώς και η ίδρυση μίας υπηρεσίας πληροφοριών στο επίπεδο της έδρας της ΔΕΕ, συνέβαλαν στην ανάπτυξη μίας περισσότερο αυτόνομης ευρωπαϊκής δράσης στον τομέα αυτό.

12.2.2. Πλεονεκτήματα της κοινής ευρωπαϊκής πολιτικής συλλογής πληροφοριών

Πέραν των τρεχουσών εξελίξεων, πρέπει να τονιστεί ότι η κοινή ευρωπαϊκή πολιτική συλλογής πληροφοριών εμφανίζει πραγματικά αντικειμενικά πλεονεκτήματα, τα οποία περιγράφονται κατωτέρω.

12.2.2.1. Επαγγελματικά πλεονεκτήματα

Καταρχάς, ο όγκος του υπάρχοντος απόρρητου και μη υλικού είναι υπερβολικά μεγάλος ώστε να μπορεί να συλλεχθεί, να αναλυθεί και να αξιολογηθεί από μία μόνο υπηρεσία ή στο πλαίσιο διμερούς συμφωνίας στη Δυτική Ευρώπη. Οι ανάγκες για υπηρεσίες πληροφοριών καλύπτουν από τις αμυντικές πληροφορίες και τις πληροφορίες για τις εθνικές και διεθνείς οικονομικές πολιτικές τρίτων κρατών μέχρι τις πληροφορίες για τη στήριξη των προσπαθειών κατά του οργανωμένου εγκλήματος και του λαθρεμπορίου ναρκωτικών. Ακόμα και αν η συνεργασία περιοριζόταν στο πιο βασικό επίπεδο, δηλαδή τη συλλογή πληροφοριών από ανοικτές πηγές (OSINT), τα αποτελέσματά της θα είχαν μεγάλη σημασία για τις πολιτικές της Ευρωπαϊκής Ένωσης.

12.2.2.2. Δημοσιονομικά πλεονεκτήματα

Κατά το πρόσφατο παρελθόν, τα κονδύλια για τη συλλογή πληροφοριών περικόπηκαν και, σε ορισμένες περιπτώσεις, εξακολουθούν να μειώνονται. Παράλληλα, όμως, αυξάνουν οι ανάγκες για ενημέρωση και, συνεπώς, για συλλογή πληροφοριών. Η μείωση των κονδυλίων καθιστά τη συνεργασία όχι μόνο δυνατή, αλλά και μακροπρόθεσμα επωφελή. Ειδικότερα, όσον αφορά την εγκαθίδρυση και τη συντήρηση τεχνικών εγκαταστάσεων, οι κοινές επιχειρήσεις παρουσιάζουν ενδιαφέρον όταν οι πόροι είναι περιορισμένοι, αλλά και στον τομέα της αξιολόγησης των συλλεγεισών πληροφοριών. Η περαιτέρω συνεργασία θα αυξήσει την αποτελεσματικότητα της συλλογής πληροφοριών.

12.2.2.3. Πολιτικά πλεονεκτήματα

Κατ' αρχήν, οι κυβερνήσεις χρησιμοποιούν τις συλλεγείσες πληροφορίες για την καλύτερη και καλύτερα στοιχειοθετημένη λήψη αποφάσεων. Η περαιτέρω πολιτική και οικονομική ολοκλήρωση σε επίπεδο Ευρωπαϊκής Ένωσης απαιτεί οι πληροφορίες να είναι διαθέσιμες σε ευρωπαϊκό επίπεδο και να βασίζονται σε περισσότερες από μία πηγές.

12.2.3. Συμπερασματικές παρατηρήσεις

Τα ανωτέρω αντικειμενικά πλεονεκτήματα απεικονίζουν απλώς την αυξανόμενη σημασία της συνεργασίας εντός της Ευρωπαϊκής Ένωσης. Στο παρελθόν, τα κράτη-έθνη διασφάλιζαν μόνα τους την εξωτερική ασφάλεια, την εσωτερική τάξη, την εθνική ευημερία και την πολιτιστική τους ταυτότητα. Σήμερα, σε πολλούς τομείς, η Ευρωπαϊκή Ένωση ετοιμάζεται να αναλάβει έναν ρόλο, ο οποίος είναι τουλάχιστον συμπληρωματικός του ρόλου του κράτους-έθνους. Δεν είναι

δυνατόν οι υπηρεσίες πληροφοριών να είναι ο τελευταίος και μοναδικός τομέας που θα παραμείνει ανεπηρέαστος από τη διαδικασία της ευρωπαϊκής ολοκλήρωσης.

12.3. Συνεργασία πέραν του επιπέδου της Ευρωπαϊκής Ενωσης

Μετά τον Β' Παγκόσμιο Πόλεμο, η συνεργασία στον τομέα της συλλογής πληροφοριών δεν αναπτύχθηκε πρώτα σε ευρωπαϊκό επίπεδο, αλλά κυρίως σε διατλαντικό επίπεδο. Όπως ήδη αναφέρθηκε, ιδιαίτερα στενές σχέσεις στον τομέα της συλλογής των πληροφοριών ανέπτυξαν το Ηνωμένο Βασίλειο και οι Ηνωμένες Πολιτείες της Αμερικής. Όμως, και στον τομέα της συλλογής αμυντικών πληροφοριών στο πλαίσιο του ΝΑΤΟ, και εκτός αυτού, οι Ηνωμένες Πολιτείες ήταν και παραμένουν απόλυτα κυρίαρχος εταίρος. Συνεπώς, το καίριο ερώτημα είναι κατά πόσο η ανάπτυξη ευρωπαϊκής συνεργασίας στον τομέα της συλλογής πληροφοριών μπορεί να διαταράξει σημαντικά τις σχέσεις της Ευρωπαϊκής Ένωσης με τις Ηνωμένες Πολιτείες ή, αντίθετα, να οδηγήσει στην ενίσχυσή τους. Πώς θα εξελιχθούν οι σχέσεις ΕΕ/ΗΠΑ με τη νέα κυβέρνηση Bush, και ειδικότερα πώς θα διατηρηθεί η ειδική σχέση μεταξύ Ηνωμένων Πολιτειών και Ηνωμένου Βασιλείου στο πλαίσιο αυτό;
Ορισμένοι πιστεύουν ότι δεν υπάρχει κατ' ανάγκη αντίθεση μεταξύ της ειδικής βρετανο-αμερικανικής σχέσης και της περαιτέρω ανάπτυξης της ΚΕΠΠΑ. Άλλοι πιστεύουν ότι πρόβλημα μπορεί να ανακύψει ιδίως στον τομέα της συλλογής πληροφοριών, φέρνοντας το Ηνωμένο Βασίλειο προ του διλήμματος να επιλέξει μεταξύ του ευρωπαϊκού και του διατλαντικού προσανατολισμού του. Οι στενές σχέσεις της Μεγάλης Βρετανίας με τις ΗΠΑ (και τα άλλα μέρη του συμφώνου UKUSA) είναι δυνατό να δυσχεράνει την ανταλλαγή πληροφοριών μεταξύ των λοιπών κρατών της ΕΕ – επειδή η Μεγάλη Βρετανία είναι δυνατόν να ενδιαφέρεται λιγότερο για την ανταλλαγή πληροφοριών με τους ευρωπαίους εταίρους της και επειδή η εμπιστοσύνη των εν λόγω εταίρων απέναντι στη Μεγάλη Βρετανία μπορεί να κλονιστεί. Ομοίως, εάν οι ΗΠΑ σχηματίσουν την πεποίθηση ότι η Μεγάλη Βρετανία έχει αναπτύξει ειδικούς δεσμούς με τους εταίρους της ΕΕ, και εάν κάτι τέτοιο αποτελέσει αντικείμενο ειδικής ευρωπαϊκής συμφωνίας, οι ΗΠΑ είναι δυνατόν να επιδείξουν απροθυμία όσον αφορά την ανταλλαγή πληροφοριών με το Ηνωμένο Βασίλειο. Κατά συνέπεια, η περαιτέρω συνεργασία σε επίπεδο ΕΕ στον τομέα της συλλογής πληροφοριών είναι δυνατόν να αποτελέσει σημαντική δοκιμασία όσον αφορά τις ευρωπαϊκές φιλοδοξίες του Ηνωμένου Βασιλείου, αλλά και τη δυνατότητα της ευρωπαϊκής ολοκλήρωσης.

Ωστόσο, υπό τις παρούσες συνθήκες, θεωρείται εξαιρετικά απίθανο η έστω και εξαιρετικά ταχεία πρόοδος στη συνεργασία μεταξύ των ευρωπαίων εταίρων να μπορέσει, βραχυπρόθεσμα ή ακόμα και μακροπρόθεσμα, να υποκαταστήσει το τεχνολογικό προβάδισμα των Ηνωμένων Πολιτειών. Η Ευρωπαϊκή Ένωση δεν είναι σε θέση να εγκαταστήσει ένα τελειοποιημένο δίκτυο δορυφόρων SIGINT, δορυφόρων απεικόνισης και επίγειων σταθμών. Η Ευρωπαϊκή Ένωση δεν είναι σε θέση να αναπτύξει βραχυπρόθεσμα το εξαιρετικά προηγμένο δίκτυο ηλεκτρονικών υπολογιστών που είναι αναγκαίο για τη διαλογή και την αξιολόγηση του συλλεχθέντος υλικού. Η Ευρωπαϊκή Ένωση δεν είναι έτοιμη να διαθέσει τα αναγκαία χρηματοοικονομικά μέσα ώστε να αποτελέσει πραγματική εναλλακτική λύση στις προσπάθειες συλλογής πληροφοριών των Ηνωμένων Πολιτειών. Συνεπώς, ακόμα και από τεχνολογική και δημοσιονομική άποψη, η Ευρωπαϊκή Ένωση έχει συμφέρον να διατηρήσει μία στενή σχέση με τις Ηνωμένες Πολιτείες στον τομέα της συλλογής πληροφοριών. Ωστόσο, και από πολιτική άποψη, είναι σημαντική η διατήρηση και, όπου κρίνεται απαραίτητο, η ενίσχυση των σχέσεων με τις Ηνωμένες Πολιτείες, ιδίως όσον αφορά τις κοινές προσπάθειες κατά του οργανωμένου εγκλήματος, της τρομοκρατίας, του λαθρεμπορίου ναρκωτικών και όπλων και της νομιμοποίησης των εσόδων από παράνομες δραστηριότητες. Οι κοινές επιχειρήσεις συλλογής πληροφοριών είναι αναγκαίες

για τη στήριξη των κοινών προσπαθειών. Οι κοινές ειρηνευτικές δράσεις, όπως αυτή που αναλήφθηκε στην πρώην Γιουγκοσλαβία, απαιτούν αυξημένη ευρωπαϊκή συνεισφορά σε όλους τους τομείς δράσης.

Παράλληλα, η διόγκωση της ευρωπαϊκής ευαισθητοποίησης πρέπει να συνοδεύεται από αύξηση των ευρωπαϊκών ευθυνών. Η Ευρωπαϊκή Ένωση πρέπει να επιτύχει μεγαλύτερη ισοτιμία ως εταίρος όχι μόνο στον οικονομικό τομέα, αλλά και στον τομέα της άμυνας και κατ' επέκταση στον τομέα της συλλογής πληροφοριών. Κατά συνέπεια, η ανάπτυξη περισσότερο αυτόνομων ευρωπαϊκών δυνατοτήτων συλλογής πληροφοριών δεν πρέπει να θεωρείται ότι απειλεί με αποδυνάμωση τις διατλαντικές σχέσεις, αλλά πρέπει να χρησιμοποιηθεί για την ενίσχυσή τους με την καθιέρωση της Ευρωπαϊκής Ένωσης ως περισσότερο ισότιμου και ικανού εταίρου. Ταυτόχρονα, η Ευρωπαϊκή Ένωση πρέπει να αναλάβει αυτόνομη πρωτοβουλία προστασίας της οικονομίας και της βιομηχανίας της κατά παράνομων και ανεπιθύμητων απειλών, όπως η οικονομική κατασκοπεία, η εγκληματικότητα στον κυβερνοχώρο και οι τρομοκρατικές επιθέσεις. Επίσης, η διατλαντική συνεννόηση είναι αναγκαία στον τομέα της βιομηχανικής κατασκοπείας. Η Ευρωπαϊκή Ένωση και οι Ηνωμένες Πολιτείες πρέπει να συμφωνήσουν ένα σύνολο κανόνων σχετικά με το τι επιτρέπεται και τι απαγορεύεται στον τομέα αυτό. Προκειμένου να ενισχυθεί η διατλαντική συνεργασία στον εν λόγω τομέα, μπορεί να αναληφθεί κοινή πρωτοβουλία σε επίπεδο ΠΟΕ, ώστε να χρησιμοποιηθούν οι μηχανισμοί του Οργανισμού για την προστασία της θεμιτής οικονομικής ανάπτυξης παγκοσμίως.

12.4. Τελικές παρατηρήσεις

Η περαιτέρω ανάπτυξη των κοινών δυνατοτήτων της Ευρωπαϊκής Ένωσης στον τομέα της συλλογής πληροφοριών πρέπει να θεωρείται αναγκαία και αναπόφευκτη, μεριμνώντας παράλληλα για τη διαφύλαξη του θεμελιώδους δικαιώματος της προστασίας της ιδιωτικής ζωής των πολιτών. Η συνεργασία με τρίτες χώρες, και ιδίως με τις Ηνωμένες Πολιτείες, πρέπει να διατηρηθεί και, κατά πάσα πιθανότητα, να ενισχυθεί. Αυτό δεν σημαίνει κατ' ανάγκη ότι οι ευρωπαϊκές δραστηριότητες SIGINT πρέπει να ενσωματωθούν αυτόματα σε ένα ανεξάρτητο σύστημα ECHELON της Ευρωπαϊκής Ένωσης ή ότι η τελευταία πρέπει να γίνει πλήρες μέλος του υφιστάμενου συμφώνου UKUSA. Ωστόσο, η ανάπτυξη ιδίας ευθύνης εκ μέρους της Ευρωπαϊκής Ένωσης στον τομέα της συλλογής πληροφοριών είναι ένα ζήτημα που πρέπει να εξεταστεί ενδελεχώς. Η ανάπτυξη ενός ολοκληρωμένου ευρωπαϊκού συστήματος συλλογής πληροφοριών απαιτεί, ταυτόχρονα, την ύπαρξη ενός συστήματος ευρωπαϊκού πολιτικού ελέγχου επί των δραστηριοτήτων των σχετικών υπηρεσιών. Θα πρέπει να ληφθούν αποφάσεις σχετικά με τα μέσα αξιολόγησης των πληροφοριών και λήψης των πολιτικών αποφάσεων που προκύπτουν από την ανάλυση εκθέσεων συλλογής πληροφοριών. Η απουσία ενός τέτοιου συστήματος πολιτικού ελέγχου, και κατά συνέπεια η έλλειψη πολιτικής ευαισθητοποίησης και ανάληψης ευθυνών σχετικά με τη διαδικασία συλλογής πληροφοριών, θα είχε καταστροφικές συνέπειες για τη διαδικασία της ευρωπαϊκής ολοκλήρωσης.

13. Συμπεράσματα και συστάσεις

13.1. Εισαγωγική παρατήρηση

Στο κεφάλαιο αυτό περιέχονται συνοπτικά κάποιες σκέψεις και κατατίθενται κάποια πιθανά συμπεράσματα. Δεν πρέπει να θεωρηθεί οριστικό. Ο εισηγητής θέλει πολύ περισσότερο να θέσει μία βάση εργασίας για την συζήτηση που θα διεξαχθεί στην επιτροπή. Στη συνέχεια, το κείμενο θα πρέπει να τροποποιηθεί άλλη μια φορά, προκειμένου να ενσωματωθούν στοιχεία της συζήτησης αυτής.

13.2. Συμπεράσματα

Ως προς την ύπαρξη ενός παγκοσμίου συστήματος παρακολούθησης της ιδιωτικής και οικονομικής επικοινωνίας (Σύστημα παρακολούθησης ECHELON)

Η ύπαρξη ενός ενεργούντος σε παγκόσμιο επίπεδο συστήματος παρακολούθησης των επικοινωνιών, το οποίο λειτουργεί με τη σύμμετρη συμμετοχή των ΗΠΑ, του Ηνωμένου Βασιλείου, του Καναδά, της Αυστραλίας και της Νέας Ζηλανδίας, στο πλαίσιο της συμφωνίας UKUSA, δεν είναι δυνατόν πλέον να αμφισβητηθεί. Βάσει των υφισταμένων ενδείξεων φαίνεται πιθανό ότι η μυστική ονομασία του είναι πραγματικά "ECHELON", το τελευταίο όμως είναι ωστόσο δευτερεύουσας σημασίας, Σημασία έχει ότι το σύστημα χρησιμεύει στην παρακολούθηση όχι στρατιωτικής, αλλά ιδιωτικής και οικονομικής επικοινωνίας
Η ανάλυση κατέδειξε ότι το μέγεθος αυτού του συστήματος σε κάθε περίπτωση δεν μπορεί να είναι τόσο εκτεταμένο όσο υποθέτουν εν μέρει τα μέσα ενημέρωσης

Ως προς τα όρια του συστήματος παρακολούθησης

Το σύστημα παρακολούθησης στηρίζεται στην παγκόσμια παρακολούθηση δορυφορικής επικοινωνίας, αλλά όμως η επικοινωνία σε περιοχές με υψηλή πυκνότητα επικοινωνίας μεταδίδεται μόνο σε πολύ μικρό τμήμα μέσω δορυφόρων. Αυτό σημαίνει ότι το μεγαλύτερο μέρος της επικοινωνίας δεν είναι δυνατόν να παρακολουθηθεί από επίγειους σταθμούς, αλλά μόνο με λαθροσύνδεση καλωδίων και αναχαίτιση ραδιοσημάτων. Οι έρευνες όμως κατέδειξαν ότι οι χώρες του ECHELON έχουν πρόσβαση σε ένα πολύ περιορισμένο τμήμα της καλωδιακής και ασύρματης επικοινωνίας και ότι λόγω του κόστους σε προσωπικό είναι δυνατόν να αξιολογηθεί μόνο περιορισμένο τμήμα της επικοινωνίας.

Ως προς την πιθανή ύπαρξη άλλων συστημάτων παρακολούθησης

Η παρακολούθηση επικοινωνίας αποτελεί ένα σύνηθες για τις μυστικές υπηρεσίες πληροφοριών μέσο κατασκοπείας και ένα τέτοιο σύστημα θα μπορούσε να χρησιμοποιηθεί και από άλλες χώρες, εφόσον αυτές διαθέτουν τα ανάλογα οικονομικά μέσα και τις γεωγραφικές προϋποθέσεις. Η Γαλλία, τουλάχιστον σε ό,τι αφορά στις γεωγραφικές προϋποθέσεις – λόγω των υπερποντίων εδαφών της – θα ήταν το μοναδικό κράτος μέλος της ΕΕ που θα ήταν σε θέση να εγκαταστήσει από μόνη της ένα παγκόσμιο σύστημα παρακολούθησης, και ότι πέραν αυτού υπάρχουν ενδείξεις ότι και η Ρωσία θα μπορούσε να χρησιμοποιήσει ένα τέτοιο σύστημα.

Ως προς την συμβατότητα με το δίκαιο της ΕΕ

Σε ό,τι αφορά στο ζήτημα της συμβατότητας ενός συστήματος τύπου ECHELON με το δίκαιο της ΕΕ, πρέπει να γίνει η εξής διάκριση: Αν το σύστημα χρησιμοποιείται μόνον για τους σκοπούς των υπηρεσιών πληροφοριών, δεν προκύπτει αντίθεση προς το δίκαιο της Ένωσης,

καθώς οι δραστηριότητες που βρίσκονται στην υπηρεσία της κρατικής ασφάλειας δεν καλύπτονται από τη συνθήκη ΕΚ, αλλά υπάγονται στον τίτλο V της συνθήκης ΕΕ (Κοινή Εξωτερική Πολιτική και Πολιτική Ασφαλείας), όπου όμως προς το παρόν δεν υπάρχουν σχετικές ρυθμίσεις και συνεπώς λείπουν τα σημεία επαφής. Αν όμως γίνεται κατάχρηση του συστήματος, το σύστημα βρίσκεται σε αντίθεση με την υποχρέωση πίστης των κρατών μελών και με την ιδέα της κοινής αγοράς που διέπεται από ελεύθερο ανταγωνισμό. Αν ένα κράτος μέλος συμμετέχει σε αυτό, παραβιάζει το κοινοτικό δίκαιο.

Ως προς την συμβατότητα με το θεμελιώδες δικαίωμα στην ιδιωτική ζωή (άρθρο 8 ΕΣΔΑ)

Κάθε παρακολούθηση επικοινωνίας συνιστά μία βαθιά επέμβαση στην ιδιωτική ζωή του ατόμου. Το άρθρο 8 ΕΣΔΑ, που προστατεύει την ιδιωτική ζωή, επιτρέπει παρεμβάσεις μόνον όταν πρόκειται για τη διασφάλιση της εθνικής ασφάλειας, εφόσον οι σχετικές ρυθμίσεις προβλέπονται από το εσωτερικό δίκαιο, είναι κοινώς προσιτές, και καθορίζουν υπό ποιες προϋποθέσεις και συνθήκες μπορεί το κράτος να προβαίνει σε επεμβάσεις. Οι επεμβάσεις πρέπει να είναι ανάλογες, για το λόγο δε αυτό πρέπει να διενεργείται μία στάθμιση συμφερόντων, καθώς δεν αρκεί το γεγονός ότι είναι απλά χρήσιμες ή επιθυμητές.

Ένα σύστημα των υπηρεσιών πληροφοριών, το οποίο θα παρακολουθούσε δίχως καμία διασφάλιση της τήρησης της αρχής της αναλογικότητας κάθε επικοινωνία, θα προσέκρουε στην ΕΣΔΑ. Κατά τον ίδιο τρόπο θα υπήρχε παραβίαση της ΕΣΔΑ, αν η ρύθμιση ήταν μεταγενέστερη της παρακολούθησης της επικοινωνίας, αν αυτή δεν είχε νομική βάση, αν δεν ήταν δημοσίως προσιτή ή αν ήταν διατυπωμένη κατά τέτοιον τρόπο, ώστε οι συνέπειές της να μην είναι προβλέψιμες για τον καθέναν. Λόγω του ότι οι ρυθμίσεις σύμφωνα με τις οποίες αμερικανικές υπηρεσίες πληροφοριών δραστηριοποιούνται στην αλλοδαπή είναι στο μεγαλύτερο μέρος τους απόρρητες, είναι αμφίβολη τουλάχιστον η προστασία της αρχής της αναλογικότητας. Υφίσταται όμως πράγματι παραβίαση των από το ΕΔΔΑ καθορισθεισών αρχών της πρόσβασης στο δίκαιο και της δυνατότητας πρόβλεψης των επιπτώσεών του. Ακόμη και αν οι ΗΠΑ δεν είναι συμβαλλόμενο κράτος στην ΕΣΔΑ πρέπει όμως τα κράτη μέλη να συμπεριφέρονται σύμφωνα με την ΕΣΔΑ. Δεν πρέπει να αθετούν τις υποχρεώσεις τους που απορρέουν από την ΕΣΔΑ αφήνοντας τις υπηρεσίες πληροφοριών άλλων κρατών οι οποίες υπόκεινται σε λιγότερο αυστηρές διατάξεις να δραστηριοποιούνται στην επικράτειά τους. Άλλως θα απογυμνωνόταν η αρχή της νομιμότητας με τις δύο συνιστώσες της πρόσβασης στο δίκαιο και της δυνατότητας πρόβλεψης των επιπτώσεών του και θα απεστερείτο η νομολογία του Δικαστηρίου των Ανθρωπίνων Δικαιωμάτων του περιεχομένου της.

Η συμβατότητα μιας νομοθετικά προβλεπόμενης δραστηριότητας των υπηρεσιών πληροφοριών με τα θεμελιώδη δικαιώματα προϋποθέτει επίσης, την ύπαρξη επαρκών συστημάτων ελέγχου, προκειμένου να δημιουργείται μία εξισορρόπηση του κινδύνου που συνεπάγεται η μυστική δράση ενός μέρους της διοίκησης. Ενόψει του γεγονότος ότι το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων εξήρε με σαφήνεια τη σημασία ενός αποτελεσματικού συστήματος ελέγχου του τομέα της δράσης των υπηρεσιών πληροφοριών, φαίνεται προβληματικό το ότι μερικές χώρες μέλη δεν διαθέτουν καθόλου κοινοβουλευτικά όργανα ελέγχου των μυστικών τους υπηρεσιών.

Ως προς το ερώτημα, αν οι πολίτες προστατεύονται επαρκώς από τις υπηρεσίες πληροφοριών

Καθώς η προστασία των πολιτών της ΕΕ εξαρτάται από την έννομη κατάσταση των επιμέρους κρατών μελών, η οποία όμως διαφέρει σημαντικά από κράτος σε κράτος, ενώ μάλιστα σε μερικά δεν υπάρχουν καθόλου κοινοβουλευτικά όργανα ελέγχου, μάλλον δεν μπορεί να γίνει λόγος για επαρκή προστασία. Οι ευρωπαίοι πολίτες έχουν θεμελιώδες συμφέρον όπως τα εθνικά τους κοινοβούλια διαθέτουν μία ρητά διαρθρωμένη ειδική επιτροπή ελέγχου, η οποία εποπτεύει και ελέγχει τις δραστηριότητες των υπηρεσιών πληροφοριών. Αλλά ακόμη και εκεί όπου υπάρχουν όργανα ελέγχου, υπάρχουν γι' αυτά μεγάλα κίνητρα, να ασχολούνται περισσότερο με τη

δραστηριότητα υπηρεσιών πληροφοριών της ημεδαπής παρά με αυτήν των υπηρεσιών πληροφοριών της αλλοδαπής, λόγω του ότι, κατά κανόνα, μόνο στην πρώτη περίπτωση θίγονται οι πολίτες της ίδιας της χώρας.
Στην περίπτωση συνεργασίας μεταξύ των υπηρεσιών πληροφοριών στο πλαίσιο της ΚΕΠΠΑ, τα όργανα καλούνται να θεσπίσουν επαρκείς διατάξεις προστασίας των ευρωπαίων πολιτών.

Ως προς την οικονομική κατασκοπεία

Ένα μέρος του τομέα καθηκόντων των υπηρεσιών πληροφοριών εξωτερικού είναι να ενδιαφέρονται για οικονομικά δεδομένα, όπως είναι οι εξελίξεις σε επιχειρησιακούς κλάδους, η εξέλιξη των αγορών πρώτων υλών, η τήρηση οικονομικών αποκλεισμών, η τήρηση των κανόνων παράδοσης για αγαθά διττής χρήσης κλπ. Για τους λόγους αυτούς, παρακολουθούνται συχνά ενεχόμενες επιχειρήσεις. Η κατάσταση γίνεται μη ανεκτή, όταν οι υπηρεσίες πληροφοριών χρησιμοποιούνται για οικονομική κατασκοπεία, κατασκοπεύοντας αλλοδαπές επιχειρήσεις, προκειμένου να παράσχουν σε ημεδαπές επιχειρήσεις ανταγωνιστικά πλεονεκτήματα. Το ενδεχόμενο να έχει χρησιμοποιηθεί το Παγκόσμιο Σύστημα Παρακολούθησης για τους σκοπούς αυτούς, υποστηρίχτηκε μεν πολλές φορές, δεν υπάρχει όμως κάποια αποδεδειγμένη περίπτωση.
Πράγματι, τα ευαίσθητα δεδομένα μιας επιχείρησης βρίσκονται κατά βάση μέσα στην ίδια την επιχείρηση, έτσι ώστε η ανταγωνιστική κατασκοπεία να επιχειρείται κατά πρώτο λόγο δια της προσπάθειας, να ληφθούν οι πληροφορίες από συνεργάτες ή ανασχεθέντα πρόσωπα ή μέσω εισβολής στα εσωτερικά δίκτυα υπολογιστών. Μόνον αν κάποια ευαίσθητα στοιχεία διαβιβαστούν ενσύρματα ή ασύρματα (δορυφόρος) προς τα έξω, μπορεί να χρησιμοποιηθεί ένα σύστημα παρακολούθησης των επικοινωνιών με σκοπό ανταγωνιστικής κατασκοπείας. Αυτό ισχύει συστηματικά στις ακόλουθες τρεις περιπτώσεις:
- σε επιχειρήσεις, οι οποίες λειτουργούν σε 3 χρονικές ζώνες, έτσι ώστε τα ενδιάμεσα αποτελέσματα να αποστέλλονται από την Ευρώπη στην Αμερική και στη συνέχεια στην Ασία
- στην περίπτωση τηλεσυνδιασκέψεων σε πολυεθνικές εταιρίες, οι οποίες μεταδίδονται μέσω δορυφόρου ή ενσύρματα.
- όταν γίνεται επί τόπου διαπραγμάτευση σημαντικών αναθέσεων (όπως συμβαίνει στην ανέγερση εγκαταστάσεων, στις τηλεπικοινωνιακές υποδομές, στην ανακατασκευή συστημάτων μεταφοράς κλπ), και πρέπει από το σημείο αυτό να γίνεται συνεννόηση με τις κεντρικές υπηρεσίες της εταιρίας**.**

Ως προς τις δυνατότητες αυτοπροστασίας

Οι επιχειρήσεις πρέπει να ασφαλίσουν ολόκληρο το περιβάλλον εργασίας καθώς και να διασφαλίσουν όλες τις οδούς επικοινωνίας, δια των οποίων μεταβιβάζονται ευαίσθητες πληροφορίες. Ακόμη και σε ιδιώτες πρέπει να συσταθεί επειγόντως να κρυπτογραφούν τα μηνύματα ηλεκτρονικού ταχυδρομείου τους, διότι ένα μη κρυπτογραφημένο μήνυμα είναι σαν ένα γράμμα χωρίς φάκελο. Στο διαδίκτυο υπάρχουν σχετικά φιλικά προς το χρήστη συστήματα, τα οποία διατίθενται μάλιστα δωρεάν για ιδιωτική χρήση.

Ως προς μία συνεργασία των υπηρεσιών πληροφοριών εντός της ΕΕ

Η ΕΕ έχει συμφωνήσει να συντονίσει τη συλλογή πληροφοριών των υπηρεσιών πληροφοριών στο πλαίσιο της ανάπτυξης μιας οικείας πολιτικής ασφάλειας και άμυνας, εν προκειμένω όμως να συνεχίσει τη συνεργασία με άλλους εταίρους σ' αυτούς τους τομείς. Μία συνεργασία των υπηρεσιών πληροφοριών στο εσωτερικό της ΕΕ φαίνεται επιθυμητή στο μέτρο, που αφενός μία κοινή πολιτική ασφαλείας δίχως την ενσωμάτωση των υπηρεσιών πληροφοριών θα ήταν παράλογη, αφετέρου θα συνδέονταν με αυτή πολυάριθμα πλεονεκτήματα από οικονομικής, επαγγελματικής και πολιτικής άποψης. Επίσης θα ταίριαζε περισσότερο στην ιδέα ενός ισότιμου

εταίρου των ΗΠΑ, και θα μπορούσε να συμπεριλάβει όλα τα κράτη μέλη σε ένα σύστημα, το οποίο θα δημιουργηθεί σε πλήρη αρμονία με την ΕΣΔΑ. Στην περίπτωση αυτή θα πρέπει να εξασφαλίζεται βέβαια ένας αντίστοιχος έλεγχος από το Ευρωπαϊκό Κοινοβούλιο. Το Ευρωπαϊκό Κοινοβούλιο πρόκειται να θεσπίσει ίδιες ρυθμίσεις σχετικά με την πρόσβαση σε εμπιστευτικές και ευαίσθητες πληροφορίες και έγγραφα.

13.3. Συστάσεις

όσον αφορά τη σύναψη και τροποποίηση διεθνών συνθηκών για την προστασία των πολιτών και επιχειρήσεων

1. καλείται ο Γενικός Γραμματέας του Συμβουλίου της Ευρώπης να υποβάλει στην Επιτροπή Υπουργών μία μελέτη, κατά πόσον είναι λογική η προσαρμογή της εις το άρθρο 8 της ΕΣΔΑ κατοχυρωμένης προστασίας της ιδιωτικής ζωής στις σύγχρονες μεθόδους επικοινωνίας και δυνατότητες παρακολούθησης σε ένα πρόσθετο πρωτόκολλο ή από κοινού με τη ρύθμιση της προστασίας δεδομένων στο πλαίσιο της αναθεώρησης της σύμβασης για την προστασία δεδομένων, υπό την προϋπόθεση ότι κατ' αυτό τον τρόπο δεν θα υπάρξει ούτε υποβάθμισή του από το Δικαστήριο αναπτυχθέντος επιπέδου νομικής προστασίας ούτε μείωση της για την προσαρμογή σε περαιτέρω εξελίξεις αναγκαίας ευελιξίας·

2. Τα κράτη μέλη καλούνται να δημιουργήσουν ένα ευρωπαϊκό πλαίσιο, προκειμένου να επανεξετάσουν τις νομοθετικές ρυθμίσεις για τη διασφάλιση του απορρήτου της αλληλογραφίας και τηλεπικοινωνίας, να συμφωνήσουν επιπλέον σε ένα κοινό κείμενο, το οποίο διασφαλίζει στο σύνολό της και εγγυάται πέραν αυτής την προστασία της ιδιωτικής ζωής, όπως αυτή ορίζεται στο άρθρο 7 του Ευρωπαϊκού Χάρτη των Θεμελιωδών Δικαιωμάτων, σε όλους τους ευρωπαίους πολίτες στην επικράτεια των κρατών μελών, ότι η δραστηριότητα των υπηρεσιών πληροφοριών πραγματοποιείται σύμφωνα με τα θεμελιώδη δικαιώματα, καθώς και ότι αντιστοιχεί στο κεφάλαιο 8 της έκθεσης, ιδίως στο 8.3.4 στις από το άρθρο 8 της ΕΣΔΑ απορρέουσες προϋποθέσεις·

3. καλούνται τα κράτη μέλη του Συμβουλίου της Ευρώπης να θεσπίσουν ένα πρόσθετο πρωτόκολλο το οποίο καθιστά δυνατή την προσχώρηση των Ευρωπαϊκών Κοινοτήτων στην ΕΣΔΑ, ή να προβληματισθούν σχετικά με άλλα μέτρα, τα οποία αποκλείουν συγκρούσεις της νομολογίας των Δικαστηρίων του Στρασβούργου και του Λουξεμβούργου·

4. ο Γενικός Γραμματέας του ΟΗΕ καλείται να αναθέσει στην αρμόδια επιτροπή την υποβολή προτάσεων, οι οποίες στοχεύουν στην προσαρμογή του άρθρου 17 του Διεθνούς Συμφώνου για τα Αστικά και Πολιτικά Δικαιώματα, το οποίο εγγυάται την προστασία της ιδιωτικής ζωής στις τεχνολογικές καινοτομίες·

5. καλούνται οι ΗΠΑ να υπογράψουν το Πρόσθετο Πρωτόκολλο του Διεθνούς Συμφώνου για τα Αστικά και Πολιτικά Δικαιώματα, προκειμένου να καταστούν δυνατές ατομικές προσφυγές κατά των ΗΠΑ λόγω της παραβίασής του, ενώπιον της Συμβατικής Επιτροπής Ανθρωπίνων Δικαιωμάτων· οι σχετικές αμερικανικές ΜΚΟ, ιδίως η ACLU (American Civil Liberties Union) και EPIC (Electronic Privacy Information Center) καλούνται να ασκήσουν αντίστοιχη πίεση στην αμερικανική κυβέρνηση·

όσον αφορά εθνικά νομοθετικά μέτρα για την προστασία πολιτών και επιχειρήσεων

6. τα κράτη μέλη καλούνται να επανεξετάσουν τη σχετική με τη δραστηριότητα των υπηρεσιών πληροφοριών νομοθεσία τους ως προς τη συμβατότητά της με τα θεμελιώδη

δικαιώματα·

7. τα κράτη μέλη καλούνται να επιδιώξουν ένα κοινό επίπεδο προστασίας από τη δραστηριότητα των υπηρεσιών πληροφοριών, το οποίο προσδιορίζεται από το ανώτατο επίπεδο που υπάρχει σε κάποιο κράτος μέλος, καθώς οι θιγόμενοι από τη δραστηριότητα μιας αλλοδαπής υπηρεσίας πληροφοριών πολίτες είναι κατά κανόνα πολίτες άλλων κρατών και κατά συνέπεια και άλλων κρατών μελών·

8. τα όργανα της ΕΕ καλούνται, στην περίπτωση συνεργασίας των υπηρεσιών πληροφοριών στο πλαίσιο της ΚΕΠΠΑ, να θεσπίσουν επαρκείς διατάξεις προστασίας των ευρωπαίων πολιτών· το Ευρωπαϊκό Κοινοβούλιο, το οποίο λογικά θα αποτελέσει το ελεγκτικό όργανο, πρέπει να θέσει τις απαραίτητες για την εποπτεία αυτού του ευαίσθητου τομέα προϋποθέσεις, προκειμένου να είναι ρεαλιστικό αλλά και υπεύθυνο να απαιτήσει τα αναγκαία ελεγκτικά δικαιώματα·

όσον αφορά ειδικά νομικά μέτρα για την καταπολέμηση της οικονομικής κατασκοπείας

9. τα κράτη μέλη καλούνται να αναλογισθούν σε ποιο βαθμό μπορούν να καταπολεμηθούν με ρυθμίσεις στο ευρωπαϊκό και διεθνές δίκαιο η οικονομική κατασκοπεία και η δωροδοκία για το σκοπό της αποκόμισης ανάθεσης συμβάσεων, ιδίως αν θα ήταν εφικτή μια ρύθμιση στα πλαίσια του Παγκόσμιο Οργανισμού Εμπορίου, η οποία λαμβάνει υπόψη της την στρεβλωτική για τον ανταγωνισμό επίπτωση μιας τέτοιας συμπεριφοράς, π.χ. ορίζοντας ότι τέτοιες συμβάσεις είναι άκυρες·

10. τα κράτη μέλη καλούνται να αναλάβουν σε μία κοινή ρητή δήλωση την υποχρέωση να μην διενεργούν οικονομική κατασκοπεία μεταξύ τους, και με τον τρόπο αυτό να σηματοδοτήσουν τη συμφωνία τους με το πνεύμα και τις διατάξεις της Συνθήκης ΕΚ·

όσον αφορά μέτρα εφαρμογής του δικαίου και ελέγχου της

11. τα εθνικά κοινοβούλια, τα οποία δεν διαθέτουν ίδια κοινοβουλευτικά όργανα ελέγχου για την εποπτεία των υπηρεσιών πληροφοριών, καλούνται να προβούν στη σύσταση τέτοιων οργάνων·

12. οι εθνικές επιτροπές ελέγχου των μυστικών υπηρεσιών καλούνται να αποδίδουν κατά την άσκηση των ελεγκτικών αρμοδιοτήτων που τους έχουν ανατεθεί μεγάλη σημασία στην προστασία της ιδιωτικής ζωής, ανεξαρτήτως του εάν πρόκειται για την παρακολούθηση των δικών τους πολιτών, άλλων πολιτών της ΕΕ ή πολιτών τρίτων χωρών·

13. καλούνται οι υπηρεσίες πληροφοριών των κρατών μελών να δέχονται δεδομένα από άλλες υπηρεσίες πληροφοριών μόνο όπου αυτές δύνανται να αποκτηθούν υπό τις προϋποθέσεις που προβλέπει το εσωτερικό δίκαιο της δικής τους χώρας, καθώς τα κράτη μέλη δεν μπορούν να αποφύγουν τις υποχρεώσεις τους προσφεύγοντας σε άλλες υπηρεσίες πληροφοριών·

14. καλούνται η Γερμανία και ην Αγγλία να εξαρτήσουν την περαιτέρω άδεια παρακολούθησης επικοινωνιών από υπηρεσίες πληροφοριών των ΗΠΑ στην επικράτειά τους, από το εάν οι δραστηριότητες αυτές συμβιβάζονται με την ΕΣΔΑ, δηλαδή ότι ανταποκρίνονται στην αρχή της αναλογικότητας, υπάρχει πρόσβαση στη νομική βάση και είναι δυνατόν να προβλεφθεί η επίπτωση για το μεμονωμένο άτομο, καθώς και ότι υπάρχει αντίστοιχος αποτελεσματικός έλεγχος, λόγω του ότι είναι υπεύθυνες για τη συμβατότητα με τα ανθρώπινα δικαιώματα της

επιτρεπόμενης ή απλώς ανεκτής δραστηριότητας των υπηρεσιών πληροφοριών στην επικράτειά τους·

όσον αφορά μέτρα ενίσχυσης της αυτοπροστασίας πολιτών και επιχειρήσεων

15. η Επιτροπή και τα κράτη μέλη καλούνται να αναπτύξουν προγράμματα με τα οποία θα ενισχύεται η συνειδητοποίηση πολιτών και επιχειρήσεων της προβληματικής σχετικά με την ασφάλεια και συγχρόνως θα προσφέρουν πρακτική βοήθεια για το σχεδιασμό και την υλοποίηση ολοκληρωμένων λύσεων προστασίας·

16. καλούνται η Επιτροπή και τα κράτη μέλη να επεξεργασθούν κατάλληλα μέτρα για την προώθηση, την ανάπτυξη και την κατασκευή ευρωπαϊκής τεχνολογίας και λογισμικού κρυπτογράφησης, και ιδίως να υποστηρίξουν προγράμματα που έχουν ως στόχο την ανάπτυξη φιλικού προς τον χρήστη λογισμικού κρυπτογράφησης, του οποίου ο πηγαίος κώδικας θα είναι προσιτός σε όλους·

17. καλούνται η Επιτροπή και τα κράτη μέλη να ενισχύσουν σχέδια λογισμικού, των οποίων ο πηγαίος κώδικας θα είναι προσιτός σε όλους, λόγω του ότι έτσι μόνο μπορεί να διασφαλισθεί ότι δεν έχουν ενσωματωθεί "κερκόπορτες" (αποκαλούμενο: "open-source Software")·

18. καλούνται τα ευρωπαϊκά όργανα καθώς και οι δημόσιες διοικήσεις των κρατών μελών να εφαρμόζουν συστηματικά την κρυπτογράφηση των μηνυμάτων ηλεκτρονικού ταχυδρομείου, προκειμένου η κρυπτογράφηση να καταστεί μακροπρόθεσμα η συνήθης πρακτική·

όσον αφορά άλλα μέτρα

19. καλούνται οι επιχειρήσεις να συνεργάζονται στενότερα με τις υπηρεσίες αντικατασκοπίας, ιδίως να γνωστοποιούν σε αυτές επιθετικές ενέργειες που προέρχονται από την αλλοδαπή και έχουν σκοπό την οικονομική κατασκοπεία προκειμένου να αυξήσουν την αποτελεσματικότητα των υπηρεσιών·

20. καλείται η Επιτροπή να υποβάλει πρόταση για τη σύσταση μιας ευρωπαϊκής συμβουλευτικής υπηρεσίας για ζητήματα ασφάλειας επιχειρηματικών πληροφοριών, η οποία παράλληλα με την αύξηση της συνειδητοποίησης του προβλήματος έχει ως αποστολή και την παροχή πρακτικής βοήθειας·

21. καλείται το Ευρωπαϊκό Κοινοβούλιο να οργανώσει ένα πέραν της Ευρώπης συνέδριο για την προστασία της ιδιωτικής ζωής από την παρακολούθηση των τηλεπικοινωνιών, προκειμένου να δημιουργηθεί ένα πλαίσιο για ΜΚΟ από την Ευρώπη, τις ΗΠΑ και άλλα κράτη, όπου θα μπορέσουν να συζητηθούν διασυνοριακές και διεθνείς πτυχές και θα συντονισθούν τομείς δραστηριότητας και συμπεριφορές.