

e-πολεμος

Τα όπλα του μέλλοντος είναι (κατ' αρχήν) αναίμακτα

Με τις "χειρουργικές επεμβάσεις" της εκδίκησης να βρίσκονται σε εξέλιξη τη στιγμή που γράφονται οι γραμμές αυτές, η ζωή προσγειώνει και τους τελευταίους ρομαντικούς στη νέα πραγματικότητα του πολιτισμού της επόμενης μέρας. Παρά τη διαφορετική άποψη των μέσων μαζικής ενημέρωσης, η φιλοσοφική συζήτηση σχετικά με τα χαρακτηριστικά του πολιτισμού αυτού είναι ιδιαίτερα επίκαιρη, άσχετα με το αν, το πού και το πώς διεξάγεται. Σε τεχνικό επίπεδο ο πολιτισμός αυτός δεν θα χαρακτηρίζεται μόνο από τα σύγχρονα όπλα μαζικής καταστροφής. Τα τελευταία, μάλιστα, λίγο έλειπε να ξεχαστούν πίσω από τις οθόνες του Internet και των εφαρμογών ηλεκτρονικού εμπορίου.

Οπλα και τεχνολογία

Χρειάστηκε λίγη αρρωστημένη φαντασία και πολύ μίσος, για να καταλάβει όλος ο κόσμος ότι η κατοχή όπλων προηγμένης τεχνολογίας δεν είναι απαραίτητη για την επίτευξη πληγμάτων με χιλιάδες νεκρούς. Χρειάζεται απλή λογική για να γίνει αντιληπτό ότι η χρήση τέτοιων όπλων δεν μπορεί να αποτρέψει μελλοντικά πλήγματα, παρόμοια με αυτό της 11ης Σεπτεμβρίου, τουλάχιστον όχι ενόσω η κοινωνική οργάνωση είναι τέτοια όπως τη γνωρίζουμε σήμερα. Ακόμη και αν "αύριο", όλα τα όπλα μαζικής καταστροφής πετιόντουσαν στη θάλασσα, κάποια απειλή θα εξακολουθούσε να κρέμεται πάνω από τα κεφάλια των πολιτισμένων και μη, "πιστών" τε και "απίστων".

Η απλή λογική και όχι οι δήθεν σύνθετες αναλύσεις που εκπορεύονται από έναν πολιτισμό που θεωρεί έχει την καθολική καταστροφή "αναπόφευκτη", υπαγορεύει επίσης τη θέση ότι **οι "κακοί", όπως και αν τους ορίζουμε, θα υπάρχουν όσο υπάρχουν οι αιτίες που τους γεννούν και όχι όσο δεν χρησιμοποιούνται αυτά που οι "καλοί" αντιλαμβάνονται ως μέσα καταστροφής τους**, τα οποία μάλιστα "εξαγιάζονται" εκ του σκοπού τους. Αυτή η θέση ισχύει προς όλες τις πλευρές, όποιοι και αν είναι οι "καλοί" και οι "κακοί", "εμείς" και οι "άλλοι" και καλό θα ήταν να στρέψει τη σκέψη αυτών στο όνομα των οποίων γίνονται όλα, σε άλλες κατευθύνσεις. Σε κάθε περίπτωση, **τόσο τα όπλα που κατασκευάστηκαν σαν όπλα, όσο και αυτά που χρησιμοποιούνται σαν τέτοια, είναι επιτεύγματα υψηλής τεχνολογίας**. Ακόμη και πριν τα Γεγονότα, κανείς δε διαφωνούσε με το χαρακτηρισμό της τεχνολογίας ως μέσο για την εγκαθίδρυση (ή την επιβολή, διαλέξτε) μιας παγκόσμιας ευημερίας, όπως την αντιλαμβάνεται ο (τέως;) δυτικός κόσμος.

Οι εφαρμογές που βρίσκουν οι τεχνολογίες της πληροφορικής και των τηλεπικοινωνιών αποτελούσαν και αποτελούν την αιχμή του δόρατος για την επίτευξη αυτής της νέας κατάστασης. Το ηλεκτρονικό εμπόριο σε μια παγκόσμια αγορά, η ασύρματη επικοινωνία πολλών μερών με εικόνα και ήχο, οι εφαρμογές στην ιατρική, την εργασία, την εκπαίδευση και την ψυχαγωγία, καθώς και η λειτουργία των μελλοντικών φορέων οργάνωσης της εξουσίας, είναι μερικά από τα πεδία εφαρμογής τεχνολογιών που σήμερα σχετίζονται με το Internet και αναγνωρίζονται ως ιδιαίτερα κρίσιμης σημασίας. Ως τέτοιες, μπορούν να χρησιμοποιηθούν για καλό αλλά και για κακό. Ίσως όχι με τον αριθμό των άμεσων ανθρωπίνων θυμάτων που είχε η χρήση της τεχνολογίας του αεροπλάνου, αλλά σίγουρα με σημαντικές συνέπειες πολύ μεγαλύτερης εμβέλειας κατ' αρχήν στον οικονομικό τομέα και ακολούθως παντού.

Η σημασία των τεχνολογιών αυτών ήταν λίγο ως πολύ γνωστή και μπορούσε κανείς να αναγνωρίσει έναν υποβόσκοντα ανταγωνισμό σχετικά με την πρωτοκαθεδρία, κατά

ορισμένους κυριαρχία, στο τεχνολογικό πεδίο. Ο εν λόγω ανταγωνισμός αποτελούσε (και αποτελεί) περισσότερο εσωτερική διαμάχη και λιγότερο εκδήλωση εχθρικής δραστηριότητας. Συναντούσε δε δυσκολίες εγγενείς στο Internet και συγκεκριμένα στα δύο βασικότερα χαρακτηριστικά του: στην έλλειψη ασφάλειας και στην έλλειψη δυνατότητας κεντρικής διοίκησής του.

Ετσι, το Internet αναπτύχθηκε μεν ακολουθώντας εκρηκτικούς ρυθμούς, αλλά αφήνοντας πολλά ουσιώδη ζητήματα ασφάλειας και διοίκησης, στα οποία δεν μπορούσε να επιτευχθεί συμφωνία, να εκκρεμούν. Οι εκκρεμότητες αυτές έχουν ως επακόλουθο την καθυστέρηση της δημιουργίας μιας καθολικά αποδεκτής υποδομής για τις ηλεκτρονικές συναλλαγές. Συνδυάζοντας τις εν λόγω εκκρεμότητες με ενυπάρχουσες αντιθέσεις στο οικονομικό πεδίο, στα πλαίσια πάντα του συστήματος, αλλά και με την αδράνεια και την απροθυμία των λιανικών αγορών να αποδεχτούν σε αυτή τη φάση το Internet ως μέσο συναλλαγών και οικονομικής δραστηριοποίησης, μπορεί κανείς να έχει ένα μέρος των αιτιών της κρίσης των "dot-com".

Μέχρι το σημείο αυτό μπορούμε να μιλάμε για εσωτερικές ζυμώσεις στα πλαίσια μιας αναπτυξιακής διαδικασίας με κανόνες και όρια που γενικά όλοι αποδέχονται. Τυχόν ακραία φαινόμενα εκδήλωσης επιθετικής συμπεριφοράς μέσω ή πάνω στο Internet είτε είναι ελεγχόμενα προκειμένου να δημιουργηθούν συνθήκες για συγκεκριμένες εξελίξεις, είτε είναι από περιστατικά περιορισμένης εμβέλειας, έως ρομαντικά συμβάντα.

Εδώ είναι που τα γεγονότα της 11ης Σεπτεμβρίου οδηγούν τη σκέψη μας σε άλλες κατευθύνσεις και επιταχύνουν άλλες εξελίξεις. Τι θα γίνει αν το Internet χρησιμοποιηθεί ως μέσο για την εκδήλωση "κυβερνο-τρομοκρατίας"; Ποιες θα είναι οι επιπτώσεις δικτυακών επιθέσεων σε χρηματοπιστωτικούς οργανισμούς; Πόσο σημαντικές επιπτώσεις θα έχει η κατάρριψη των θεμελίων ή έστω των μηχανισμών του οικονομικού οικοδομήματος; Υπάρχει "ηλεκτρονική τρομοκρατία" και πώς μπορεί να εκδηλώνεται;

ε-πόλεμος

ε-πόλεμος, λοιπόν, και μάλιστα το τελευταίο διάστημα είναι πολλοί αυτοί που μιλούν σχετικά με το θέμα και φιλοξενούν ρεπορτάζ στις τηλεοπτικές, ηλεκτρονικές και έντυπες σελίδες τους. Ηλεκτρονικές επιθέσεις στο πεντάγωνο που καταλήγουν στην ενεργοποίηση του (συνδεδεμένου στο Internet!!!) συστήματος πυρόσβεσης, απώλεια μυστικών από παραβίαση συστημάτων υπηρεσιών ασφαλείας, διακόρευση τραπεζικών συστημάτων, hackers, ιοί και άλλα δαιμόνια. Θα αποφύγουμε προς το παρόν τον πειρασμό να χαρακτηρίσουμε τα ρεπορτάζ, τις έρευνες και τις δηλώσεις των (κατ' ανάγκην) ειδικών, για να ασχοληθούμε με τα πραγματικά "μέτωπα του πολέμου", τα οποία όντως υπάρχουν και δεν πολεμούν σε αυτά μόνο οι ...ταλιμπάν.

Μέτωπο πρώτο. Οι παροχείς τηλεπικοινωνιακών υπηρεσιών και οι ISPs. Με την απελευθέρωση των τηλεπικοινωνιών, η οποία μάλιστα στην Ευρώπη έγινε με σημαντική καθυστέρηση, οι τηλεπικοινωνιακοί φορείς είναι ιδιωτικές εταιρίες. Σαν τέτοιες, αναπτύσσουν υποδομή η οποία χρησιμοποιείται για επικοινωνίες δεδομένων και για υποδομή πρόσβασης και ραχοκοκαλιάς (backbone) του σημερινού και μελλοντικού Internet. Πάνω από αυτή, άλλες ιδιωτικές εταιρίες προσφέρουν υπηρεσίες προστιθέμενης αξίας πρόσβασης στο Internet. Η γιγάντωση τόσο των τηλεπικοινωνιακών εταιριών όσο και των ISPs, τις καθιστά στρατηγικούς στόχους, τόσο για εξαγορά στα πλαίσια του χρηματιστηριακού συστήματος, όσο και για παραβίαση του δικτύου τους.

Και στις δύο περιπτώσεις, τα πράγματα είναι επικίνδυνα. Όπως "κανείς" δεν μπορεί να απαγορεύσει σε κάποιον παρανοϊκό να εξαγοράσει μια αεροπορική εταιρία και στη

συνέχεια να ανατινάξει όλα τα αεροπλάνα εν πτήξει, έτσι και "κανείς" δεν μπορεί να απαγορεύσει σε μια τηλεπικοινωνιακή εταιρία καθόλα "εντάξει", να προσφέρει υπηρεσίες σε εκατομμύρια χρήστες οι οποίοι συνδέονται με εκατοντάδες πιστωτικά ιδρύματα. Ακόμη και όταν όλα γίνονται στα πλαίσια της νομιμότητας, η εγγύηση για την ακεραιότητα των επικοινωνιών είναι μάλλον μη ακράδαντη, όπως εξάλλου πάντα είναι όταν δεν μπορεί να εκδηλωθεί ουσιαστικός κοινωνικός έλεγχος. Τα δε αποτελέσματα κάποιας δράσης αντίστοιχης με το σενάριο της αεροπορικής εταιρίας που αναφέραμε ή με τα γεγονότα της 11ης Σεπτεμβρίου, αφήνονται ως (εύκολη) άσκηση επιστημονικής φαντασίας.

Μέτωπο δεύτερο. Η πιστοποίηση ταυτότητας ατόμων και φορέων και οι αρχές πιστοποίησης (certification authorities). Ένα από τα σημαντικότερα προβλήματα του ψηφιακού πολιτισμού είναι το πρόβλημα της ταυτότητας. Η σημερινή κατάσταση επιτρέπει στον καθένα να δηλώνει στο Δίκτυο οποιαδήποτε ταυτότητα νομίζει. Οι συναλλαγές που πραγματοποιούνται είναι όλες επισφαλείς, γεγονός που δηλώνεται ρητά και κατηγορηματικά στους εκάστοτε όρους χρήσης ("disclaimers").

Η πηλαστοπροσωπία στο Internet είναι απλούστατη υπόθεση και γενικά η θεμιτή ή αθέμιτη δραστηριότητα ενός χρήστη του Internet δεν μπορεί να συνδεθεί περάν πάσης αμφιβολίας με κάποιο υπαρκτό φυσικό πρόσωπο. Η υπογραφή, λοιπόν σε ηλεκτρονικές ταυτότητες οι φορείς που την βάζουν και ο έλεγχος της κίνησης των χρηστών που τις φέρουν, αποτελεί ένα άλλο μέτωπο του ηλεκτρονικού πολέμου, το οποίο αφορά θεμελιώδεις μονάδες συνοχής του κοινωνικού ιστού. Όσοι έχουν απορίες σχετικά με τα παραπάνω, παραπέμπονται στην παραγωγή του Hollywood με τίτλο "The Net" (1996).

Μέτωπο τρίτο. Τεχνολογίες κρυπτογράφησης και εφαρμογές τους στις επικοινωνίες και το ηλεκτρονικό εμπόριο. Η απόσταση από ένα δίκτυο προσβάσιμο και παρατηρήσιμο από "καλούς" και "κακούς" (όπως είναι σήμερα το Internet) σε ένα ασφαλές δίκτυο όπου κανείς δεν μπορεί να δει στοιχεία που δεν τον αφορούν, ορίζεται από την τεχνολογία της κρυπτογραφίας και τις τεχνικές συμβάσεις (πρωτόκολλα) στις οποίες αυτή ενσωματώνεται και διαμέσω των οποίων διακινείται κεφαλαιώδες περιεχόμενο επικοινωνιών και ηλεκτρονικών συναλλαγών. Οποιος την ελέγχει, μπορεί να ελέγχει και το περιεχόμενο που διακινείται και μπορεί να μεταφέρει το δικό του περιεχόμενο με ασφάλεια, ενώ παρακολουθεί και δύναται να μεταβάλει αυτό των άλλων, δυνατότητα επιθυμητή από όλες τις πλευρές καλών, υπόπτων και κακών.

Όσοι απορούσαν σχετικά, μπορούν σήμερα να αντιληφθούν για ποιο λόγο οι ΗΠΑ θεωρούν την κρυπτογραφία από τις σημαντικότερες μη-εξαγώγιμες τεχνολογίες και του αποδίδουν κεφαλαιώδη σημασία. Μάλιστα, οι οικονομικές απώλειες από την επιβράδυνση των ρυθμών ανάπτυξης του ηλεκτρονικού εμπορίου που οφείλεται στη μη προτυποποίηση των ηλεκτρονικών συναλλαγών (οι οποίες εξακολουθούν να εκτελούνται στη συντριπτική πλειοψηφία τους με SSL) δεν μπορούν να αποτελέσουν κινητήρια δύναμη ώθησης κάποιας εξέλιξης, χωρίς οι ΗΠΑ να διασφαλίζουν την κυριαρχία τους. Η κυριαρχία, ή τουλάχιστον κάποιο "fair play", είναι επιθυμητή και από άλλες πλευρές στη δική μας άκρη του ατλαντικού, οι οποίες ενίοτε εμφανίζονται με τη μορφή της ενωμένης Ευρώπης και ενίοτε όχι.

Υπάρχουν και άλλες περιοχές οι οποίες μπορούν να χαρακτηριστούν ως μέτωπα ηλεκτρονικού πολέμου. Θεωρούμε, ωστόσο, **ότι οι τρεις θεμελιώδεις διαστάσεις που ορίζουν μέτωπα ηλεκτρονικού πολέμου είναι η υποδομή τηλεπικοινωνιών, η διαχείριση δικτυακής ταυτότητας, και η τεχνολογία κρυπτογράφησης.** Αποσπασματικά και φαινομενικά ασύνδετα τεχνικά γεγονότα μπορούν να συνδυαστούν και να αναγνωριστούν ως "ύποπτα" στον τομέα της καταγραφής δραστηριότητας χρηστών διασυνδεδεμένων

συστημάτων. Τέτοια είναι το licencing λογισμικού μέσω δικτύου, και το Pentium serial number, οι πολλοί και διάφοροι "messenger", οι (ακούσιες;) τρύπες ασφαλείας δημοφιλών προγραμμάτων επικοινωνίας, κ.ά. Σε κάποιες περιπτώσεις (π.χ. licencing), υπάρχει τυπικά ευσταθές έρεισμα και μπορεί να υπάρξει και τεκμηριωμένος αντίλογος, σε άλλες, όμως (τρύπες ασφάλειας, messengers, ενεργοποίηση ή όχι του Pentium S/N) υπάρχουν μόνο δηλώσεις και ενδείξεις.

ε-χθροπραξίες

Εχοντας αναφερθεί στα μέτωπα του πολέμου, μπορούμε να αναφερθούμε και σε αυτές καθεαυτές τις "ε-χροπραξίες" που λαμβάνουν χώρα εκεί. Η κατάσταση είναι πολύ σύνθετη, όπως είναι σε όλες τις περιπτώσεις πολέμων. Η αυθόρμητη αντίδραση, η σχεδιασμένη επίθεση, ο ανταρτοπόλεμος, η προπαγάνδα, η δράση των κατασκόπων, και γενικά όλα όσα γνωρίζουμε από την καταγεγραμμένη πλην όμως όχι διδασκόμενη ιστορία των πολέμων, υπάρχουν και στις δικτυακές εχθροπραξίες.

Οι hackers και οι ιοί εμφανίζονται ως απειλή και (μόνο) σε ένα βαθμό πράγματι είναι. Τα αποτελέσματα των "επιθέσεων" τους συχνά λαμβάνουν εντυπωσιακή δημοσιότητα, χωρίς το ίδιο να συμβαίνει με τον προβληματισμό σε σχέση με το εύφορο τεχνικό έδαφος για την εκδήλωση τέτοιων φαινομένων. Το κοινό δεν είναι σε θέση να αντιληφθεί ότι τα πράγματα θα μπορούσαν να μην είναι έτσι, διότι, πολύ απλά, έχει γαλουχηθεί να είναι μόνο καταναλωτής και όχι κριτής της τεχνολογίας. Ετσι, δεν απορεί, πολύ περισσότερο δεν υποψιάζεται πώς είναι δυνατόν και αν είναι τυχαίο τα λειτουργικά συστήματα και οι εφαρμογές να έχουν τόσες πολλές "τρύπες ασφαλείας" που επιτρέπουν τέτοιας έκτασης δράση στους (πραγματικούς και όχι) "κακούς".

Οδηγείται, όμως, στην διαπίστωση της ανάγκης ότι χρειάζεται κάποιου τύπου "προστασία" και μάλιστα από προστάτες που είναι αυτονόητοι και δεν υπόκεινται σε επιλογή, διαπίστωση η οποία γίνεται αγανάκτηση όταν κανείς πέσει θύμα κάποιας ηλεκτρονικής εχθροπραξίας. Ετσι, η αντικοινωνική συμπεριφορά η οποία εκφράζεται σε όρους νέας τεχνολογίας και δεν αποτελεί αιτία, αλλά εκδήλωση της κρίσης του σύγχρονου πολιτισμού, μετατρέπεται σε δικαιολογία για την αποδοχή μιας ανάγκης προστασίας η ικανοποίηση της οποίας ενδέχεται και να επιφέρει άλλα αποτελέσματα.

Μεταφέροντας όλα τα παραπάνω από τα πεδία της οικονομικής δραστηριότητας και των προσωπικών επικοινωνιών, στα πεδία της ενημέρωσης, των διακρατικών επικοινωνιών, των αμυντικών (;) υποδομών, και της κλασσικής και πάντα υπάρχουσας κατασκοπείας, και αντιλαμβανόμενοι την έκταση και κατ' επέκταση τη δύναμη που διακυβεύεται, έχουμε μια εικόνα της κατάστασης.

Ο e-πολεμος ίσως είναι αναίμακτος, όμως έχει πολύ σημαντικότερα αποτελέσματα από την οικοπεδοποίηση που δεν ωφελεί και κανέναν. Όσο για την οικοπεδοποίηση και την επικαιρότητά της τα τελευταία χρόνια και ιδιαίτερα μετά από την κατάρρευση του αντίπαλου δέους, κάποιοι λένε ότι θα ολοκληρωθεί όταν ...καταναλωθούν οι βόμβες. Οι επόμενες βόμβες θα είναι ψηφιακές και θα εκρήγνυνται χωρίς την παρουσία τηλεοπτικών ανταποκριτών, αυτό δε που μας φοβίζει περισσότερο είναι ότι μπορεί να μην τις αντιλαμβάνεται κανείς, ούτε αυτοί οι οποίοι τις υποδέχονται...

Β.Βεσκούκης