



«Αθηνά»

ΕΛΛΗΝΙΚΟ ΚΕΝΤΡΟ ΕΛΕΓΧΟΥ ΟΠΛΩΝ

Σαλαμίνας 10, Θεσσαλονίκη 54625, Τηλ/Fax: 2310904794 / 6944165341, www.armscontrol.info

ΜΟΡΦΕΣ ΚΑΙ ΕΠΙΔΡΑΣΕΙΣ ΤΟΥ ΚΥΒΕΡΝΗΤΙΚΟΥ ΠΟΛΕΜΟΥ

Μανώλης Αστρεινίδης, Διεθνολόγος Ερευνητής του Ε.Κ.Ε.Ο. «Αθηνά»

Σαλαμίνας 10, Θεσσαλονίκη 54625, email: athena@armscontrol.info

Δευτέρα 20 Ιουνίου 2005

ΜΟΡΦΕΣ ΚΑΙ ΕΠΙΔΡΑΣΕΙΣ ΤΟΥ ΚΥΒΕΡΝΗΤΙΚΟΥ ΠΟΛΕΜΟΥ

ΚΥΒΕΡΝΗΤΙΚΟΣ ΠΟΛΕΜΟΣ

Εισαγωγή

Κάθε χώρα νομιμοποιείται να αμυνθεί με κάθε κατάλληλο μέσο. Η αμυντική βιομηχανία έχει εκτοξευθεί σε δυσθεώρητα ύψη παραγωγικότητας προκειμένου να ικανοποιήσει τις αυξανόμενες εξοπλιστικές ανάγκες και όπως φαίνεται δεν πρόκειται να σταματήσει την ανοδική της πορεία. Η συγκεκριμένη βιομηχανία καθοδηγείται από την καθημερινή εξέλιξη της τεχνολογίας προηγμένης άμυνας ή επίθεσης η οποία καθιστά όλα τα πρότερα επιτεύγματα παρωχημένα. Βεβαίως είναι ελάχιστες εκείνες οι χώρες των οποίων ο οικονομικός πλούτος τους επιτρέπει να βαδίζουν με τόσο γοργό ρυθμό σ' αυτή τη κούρσα. Ακόμα και οι πιο εύρωστες οικονομικά χώρες δεν είναι σε θέση να αναπτύξουν τόσο προηγμένες τεχνολογίες εξαιτίας του απαιτούμενου υψηλού κόστους αυτών των προγραμμάτων.

Κάθε συμβατικός στρατός χρειάζεται καλό εξοπλισμό και καλή οργάνωση. Ο εξοπλισμός φυσικά δε συνιστά τη μοναδική δαπάνη δεδομένου ότι η οργάνωση ενός στρατού είναι κατά πολύ σημαντικότερη. Με τον όρο «οργάνωση» χαρακτηρίζουμε την ορθολογική κατανομή των πληροφοριών σε ακριβή κλίμακα και χρονική στιγμή. Κάθε στρατός χρειάζεται δίκτυα πληροφοριών και τηλεπικοινωνιών, κάθε στρατός βασίζεται στον έλεγχο των χειρισμών των επιχειρήσεων και κάθε στρατός οφείλει να γνωρίζει τον εχθρό. Η εποχή της πληροφορίας δεν φαίνεται να λειτουργεί άψογα μόνο στον επιχειρηματικό κόσμο αλλά ακόμα και στο πεδίο της μάχης. Η διάδοση της πληροφορίας πρέπει να γίνεται ακόμα ταχύτερα, η παραμικρή κίνηση του εχθρού πρέπει να μεταδίδεται ακριβέστερα, οι στρατιώτες πρέπει να αναπτύσσονται με μεγαλύτερη ακρίβεια ενώ οι αποφάσεις πρέπει να βασίζονται σε ασφαλέστερες πληροφορίες. Αυτό



καταδεικνύει ότι οι στρατοί στηρίζονται όλο και περισσότερο στη πληροφορία αλλά ακόμα δυσκολεύονται να συνειδητοποιήσουν ότι η πληροφορία είναι ένα ανεκτίμητης αξίας αγαθό που πρέπει να διαφυλαχθεί. Όλες οι προσπάθειες μέχρι σήμερα για τη διαφύλαξη και προστασία των πληροφοριών επικεντρώνονταν στη διασφάλισή της όμως σήμερα με το διαδίκτυο και τη τηλεματική έχουν ανακύψει άλλοι κίνδυνοι που πρέπει να ληφθούν υπ' όψιν. Μια αδυναμία στην αναλυτική ασφάλεια δίνει τη δυνατότητα στον επιτιθέμενο να κάνει ό,τι είναι δυνατό με συμβατικά όπλα (καταστροφή υποδομής) όπως και με όπλα μαζικής καταστροφής (π.χ. διάλυση πυρηνικών αντιδραστήρων).

- **Ορισμός του Κυβερνητικού Πολέμου**

Ο κυβερνητικός πόλεμος είναι ένα νέο σχετικά όπλο με ποικίλες επιπτώσεις επί του στόχου. Δεν έχει κανένα περιορισμό στη χρήση του και είναι σε θέση να πετύχει τους περισσότερους από τους σκοπούς. Τα όπλα που χρησιμοποιούνται στο κυβερνητικό πόλεμο είναι συνήθως βασικά προγράμματα που αποσκοπούν στην άμυνα ή επίθεση εναντίον ενός στόχου. Τα περισσότερα απ' αυτά είναι ελεύθερα διαθέσιμα στο διαδίκτυο ωστόσο κάποια πιο περίπλοκα ή υπερσύγχρονα φυλάσσονται για ιδιωτική χρήση.

- **Ανίχνευση**

Τα συστήματα σ' αυτή τη κατηγορία έχουν σκοπό να ανιχνεύουν πιθανούς «εισβολείς» και να αναγνωρίζουν αυτό που πρόκειται να επιχειρήσουν όπως και να εντοπίζουν το πού βρίσκονται. Η ανίχνευση βασίζεται στην εξειδικευμένη γνώση ή σε συγκεκριμένες συμπεριφορές.

Σ' αυτή τη κατηγορία τα διαθέσιμα μέσα είναι:

1. συστήματα ανίχνευσης εισβολής
2. παρακολούθηση και επιτήρηση της ασφάλειας
3. ανάλυση του ελέγχου χειρισμών των επιχειρήσεων

- **Πρόληψη**

Το πρώτιστο ενδιαφέρον είναι το σταμάτημα του επιτιθέμενου ακόμα και αν η επίθεση δεν έχει εντοπιστεί ή αναγνωριστεί. Οι περισσότερες επιθέσεις είναι πολύ απλές και άμεσες.

Τα σημαντικότερα εργαλεία σ' αυτή τη κατηγορία είναι:

1. τοίχοι προστασίας
2. συστήματα πιστοποίησης
3. συστήματα εξουσιοδότησης

- **Επίθεση**

Εδώ τίθενται σε εφαρμογή όλα τα μέσα και τρόποι ώστε να εκμεταλλευτούν την αδυναμία και την όποια ευαισθησία του συστήματος προκειμένου να επιτύχουν το τελικό σκοπό που επιθυμεί ο επιτιθέμενος. Υπάρχουν πολλά μέσα δεδομένου ότι για κάθε αδυναμία ή ευαισθησία του συστήματος υπάρχουν περισσότερα από ένα μέσα. Αξίζει να σημειώσουμε τους ιούς του διαδικτύου οι οποίοι είναι αυτοματοποιημένα μέσα που εκμεταλλεύονται συγκεκριμένες αδυναμίες και αυτο-



αντιγράφονται από ένα σύστημα σε ένα άλλο. Μια άλλη ομάδα είναι οι Δούρειοι Ίπποι που εξαπολύονται στο σύστημα με σκοπό την απόκτηση πρόσβασης στο σύστημα αργότερα ή τη δημιουργία ενός μυστικού διαύλου για την απόκτηση σημαντικών πληροφοριών.

- **Μέσα εξαπάτησης**

Η εξαπάτηση του εχθρού είναι πολύ σημαντική σε περίπτωση αναγκαστικού περισπασμού προκειμένου να διεξαχθεί μια επίθεση ή για να επιβραδυνθεί ο χρόνος ανίχνευσής της. Εδώ παρατίθενται μερικές από τις υποκατηγορίες:

1. τροποποιητές ελέγχου χειρισμών των επιχειρήσεων
2. συστήματα κατανομής της επίθεσης
3. μέσα υποκλοπής

- **Στρατηγική και Τακτικές**

Ο διάσημος Βρετανός στρατηγικός αναλυτής B.H. Liddell-Hart προσέγγισε τη στρατηγική από δύο διαφορετικές προοπτικές. Έκανε τη διάκριση ανάμεσα στη μεγάλη στρατηγική και τη στρατιωτική στρατηγική. Η μεγάλη στρατηγική σύμφωνα με το B.H. Liddell-Hart εστιάζεται στην ικανότητα ενός έθνους να συντονίσει και να κατευθύνει όλα του τα μέσα προς την επίτευξη ενός πολιτικού στόχου.

Η στρατιωτική στρατηγική έχει σαφώς στενότερη έννοια και σχετίζεται με την εκτέλεση ενός σχεδίου μάχης ή τη προώθηση της στρατιωτικής δύναμης.

Στη κυβερνητική ασφάλεια δεν υπάρχει διαφορά μεταξύ στρατιωτικής και αστικής υποδομής δεδομένου ότι πολλοί στόχοι είναι μη στρατιωτικοί αλλά έμμεσα εμπλέκονται στη στρατιωτική υποδομή. Η διάλυση της οικονομίας ή η καταστροφή της εικόνας μιας δημόσιας υποδομής μπορεί να επιφέρουν πολύ μεγαλύτερες επιπτώσεις ως όπλα μαζικής καταστροφής και για το λόγο αυτό απαιτείται ο μη περιορισμός των τακτικών ή μιας στρατηγικής από οποιοδήποτε φραγμό, προκειμένου να επιτευχθεί μια παγκόσμια κατανόηση ως προς αυτό που οι επιτιθέμενοι μπορεί να κερδίσουν ή να χάσουν.

Οι στρατηγικές βασίζονται σε συγκεκριμένη συμπεριφορά που προσδιορίζει το δρώντα. Στη κυβερνητική ασφάλεια υπάρχουν 3 κύριοι τύποι συμπεριφοράς.

1. **Αντιδραστική συμπεριφορά**

Στη περίπτωση αυτή η στρατηγική βασίζεται στη δράση που μπορεί να γίνει αισθητή ή να αναφερθεί με οποιοδήποτε τρόπο. Αντιδρά σ' αυτή με τη κατάλληλη αντίδραση αυξάνοντας την επαγρύπνηση στην όποια αδυναμία. Αυτή η συμπεριφορά ενισχύει εκείνα τα σημεία στην άμυνα όπου έχει ήδη εξαπολυθεί επίθεση, κάτι που σημαίνει όμως ότι θα έχουν υπάρξει στο μεταξύ αρκετές επιτυχημένες διεισδύσεις. Αν και φαίνεται η μακράς διάρκειας και αντοχής υποδομή έχει φτάσει σε ένα σημείο όπου τα συστήματα είναι αρκετά ασφαλή, το γεγονός είναι ότι με την εισαγωγή νέων λογισμικών η/υ και επικαιροποιημένων δεδομένων έχουν ανοίξει νέες «τρύπες» στην ασφάλεια που ανά πάσα στιγμή μπορεί να προβληθούν.

Οι υποδομές με περιορισμένες δυνατότητες ασφάλειας χρησιμοποιούν πολύ συχνά αυτή τη συμπεριφορά για να επιτύχουν τη μέγιστη ασφάλεια. Αυτό σημαίνει ότι η υπεύθυνη ομάδα



ασφαλείας είτε δεν είναι πολύ έμπειρη είτε ότι δεν υπάρχουν αρκετά άτομα απασχολούμενα αποκλειστικά στη συντήρηση και διαχείριση τέτοιων συστημάτων. Από την αντίδραση σε μια διακοπή του συστήματος μπορεί να εξαχθούν κάποια συμπεράσματα σχετικά με τη στρατηγική της κυβερνητικής ασφάλειας. Αναλύοντας τις αδυναμίες ενός συστήματος είναι δυνατό να δούμε την ιστορία των επιθέσεων στην υποδομή του.

Υπάρχει επίσης ακόμα μια εναλλακτική στη συμπεριφορά αυτή, η οποία συνίσταται στη γνώση από τα λάθη των άλλων ωστόσο δεν είναι δυνατό πάντα οι λύσεις άλλων να χρησιμοποιούνται προκειμένου να αυξηθεί η ασφάλεια μια λίγο διαφορετικής υποδομής.

2. Σχεδιασμένη συμπεριφορά

Η σημασία του σχεδιασμού είναι ήδη γνωστή αλλά εξαιτίας της φύσης των τηλεπικοινωνιακών υποδομών δεν είναι πάντα εφαρμόσιμη. Μια τέτοια υποδομή δεν μπορεί να παραμένει αυστηρά στατική και να μην προσαρμόζεται στις ανάγκες του ιδιοκτήτη της. Καθώς στοχεύουν στο να προλαβαίνουν τις εξελίξεις στο τομέα των τηλεπικοινωνιών καθώς και να συναρμόζουν τις απαιτήσεις για λειτουργικότητα σε εξαιρετικά σύντομο χρονικό διάστημα δεν είναι εύκολο να κρατούν τα πάντα σχεδιασμένα και καλά καταγεγραμμένα. Παρόμοια και στο σχεδιασμό εθνικής ασφάλειας, όπου τα λεπτομερή σχέδια δεν λειτουργούν όπως αναμένεται καθώς καλύπτουν τεράστια οικονομικά, στρατιωτικά και άλλα συστήματα που μεταβάλλονται πολύ συχνά και δεν είναι καλά καταγεγραμμένα.

Μόνο στη καλύτερη περίπτωση με το κατάλληλο σχεδιασμό ασφαλείας καλά επεξεργασμένο και εφαρμοσμένο κατάλληλα μπορεί να επιτευχθεί ένα αξιοπρεπές επίπεδο ασφάλειας της άμυνας.

Στις πρώην κομμουνιστικές χώρες ο σχεδιασμός γινόταν σε κάθε τμήμα του κράτους ωστόσο αν και τα υπό επεξεργασία σενάρια ήταν πολλά, μια πλευρά δεν ήταν απόλυτα καλυμμένη και αυτή ήταν των ανθρώπινων πόρων. Εξαιτίας απρόσμενων αποκλίσεων στην ανθρώπινη συμπεριφορά ολόκληρο το σύστημα εν τέλει κατέρρευσε.

Η κυβερνητική ασφάλεια μπορεί να είναι πολύ καλά σχεδιασμένη αλλά το σχέδιο δεν καλύπτει όλα τα σενάρια και όταν δεν απασχολούνται ικανά και έμπειρα άτομα που να μπορούν να υιοθετήσουν την αντίδραση θα υπάρχει πάντα ο κίνδυνος της «εισβολής».

Εάν μια εταιρία στερείται έμπειρων ατόμων στη χρήση μέτρων αμυντικής ασφάλειας ή στη διασφάλιση των συστημάτων είναι πολύ πιθανό να ακολουθήσει η κατάλληλη αντίδραση μετά από μεγάλο χρονικό διάστημα έρευνας και κλιμάκωσης. Γνωρίζοντας τις διαδικασίες που χρησιμοποιούνται από άλλες εταιρίες ένας «εισβολέας» μπορεί να προβλέψει συγκεκριμένες συμπεριφορές που θα ακολουθηθούν και να προσαρμόσει την κυβερνητική επίθεση ώστε να προλάβει οποιαδήποτε αντίδραση. Ένας κίνδυνος που ενδέχεται να προκύψει είναι υποτιμηθεί η δυνατότητα ύπαρξης υπερσύγχρονου συστήματος ασφαλείας που θα ήταν δύσκολο να ξεπεραστεί. Αυτή η τάση κερδίζει έδαφος σε μεσαίες ή προοδευτικά εξελισσόμενες εταιρίες και αν εφαρμοζόταν σε εθνικό επίπεδο μπορεί να αποτελούσε πολύ αποτελεσματικό μέτρο.

3. Ενεργητική συμπεριφορά



Οι προηγούμενες συμπεριφορές προσπαθούν να καλύψουν γνωστούς κινδύνους και αδυναμίες αλλά τί συμβαίνει εάν υπάρχει κάτι νέο που δεν έχει αναφερθεί ή καταγραφεί; Σ' αυτή τη περίπτωση αυτή η επίθεση δεν μπορεί να ανιχνευθεί και θα χαρακτηριστεί ως ανωμαλία. Για την ανίχνευση και πρόληψη νέων άγνωστων επιθέσεων είναι απαραίτητο να είμαστε εξαιρετικά ευέλικτοι και οι πρώτοι που θα γνωρίζουμε τις αδυναμίες μας.

Μια στρατηγική ασφαλείας που επικεντρώνεται στην αναγνώριση των δικών της πιθανών αδυναμιών και που καλύπτει τις δικές της «τρύπες» βασίζεται αποκλειστικά στην ενεργητική συμπεριφορά.

Υπάρχουν πολλές λειτουργίες που εμπίπτουν στη κατηγορία της ενεργητικής συμπεριφοράς:

1. αναθεώρηση του κώδικα πηγών
2. επίσημη απόδειξη λειτουργικότητας
3. δοκιμασία αυτο-διείσδυσης
4. αυτο-προσαρμοζόμενα μέτρα ασφαλείας

Υπάρχουν ήδη κάποιες λύσεις ασφαλείας και προϊόντα στην αγορά αλλά δεν είναι πολύ αποτελεσματικά εξαιτίας της έλλειψης εμπειρων ατόμων να τα χρησιμοποιήσουν. Η επίσημη δοκιμασία λειτουργικότητας και η αναθεώρηση του κώδικα πηγών δεν γίνονται απαραίτητα με σκοπό τη διασφάλιση της ασφάλειας ενός τέτοιου συστήματος. Αρκετές χώρες ήδη έχουν αρχίσει να ερευνούν αυτό το τομέα και άρχισαν να προσαρμόζουν κάποια τμήματα των συστημάτων τους. Η Κίνα ήδη έχει επενδύσει μεγάλα κονδύλια στην οικοδόμηση μεγάλης και καλά εκπαιδευμένης δύναμης κυβερνητικής ασφάλειας ενώ οι ΗΠΑ έχουν κατασκευάσει εθνικά ερευνητικά κέντρα για την κυβερνητική ασφάλεια με σκοπό να συγκεντρώσουν τους ειδικούς επί της ασφαλείας και καταρτισμένους μηχανικούς ώστε να βελτιώσουν τα διάφορα τμήματα της εθνικής τους κυβερνητικής ασφάλειας.

Η ενεργητική συμπεριφορά απαιτεί εξαιρετικά καταρτισμένους επιστήμονες και πολύ σφιχτό σύστημα ασφαλείας και για το λόγο αυτό είναι σημαντικό να παραμένουν οι καταρτισμένοι επιστήμονες στη χώρα τους για να διασφαλίζουν την ασφάλειά της ή για να αναπτύξουν συστήματα ασφαλείας που θα το επιτυγχάνουν.

4.Στρατηγική εθνικής ασφάλειας

Αυτή είναι μια μάλλον ουτοπική προσέγγιση καθώς δεν είναι δυνατό να ενσωματώσει και να συγχρονίσει όλα τα τμήματα ενός έθνους σε μια και μόνο πρωτοβουλία κυβερνητικής άμυνας αλλά θα πρέπει να αποτελεί το τελικό στόχο κάθε πρωτοβουλίας κυβερνητικής ασφάλειας. Υπάρχει ένα επίπεδο γενικής ασφάλειας και πολιτικής ασφαλείας που εφαρμόζεται και εξακριβώνεται από εξουσιοδοτημένους εξειδικευμένους επιστήμονες. Το κέντρο του ηλεκτρονικού πολέμου είναι υπεύθυνο για το χειρισμό περιστατικών που αναφέρονται από κάθε φορέα εντός της χώρας.

Το εκπαιδευτικό σύστημα είναι ικανό να παράσχει επαρκή αριθμό επιστημόνων εξειδικευμένων στην ασφάλεια καθώς και δυνατότητες για την έρευνα ώστε να διασφαλιστεί η εφαρμογή της εθνικής στρατηγικής ασφάλειας σε κάθε σημαντική υποδομή.



Η επίθεση και προσβολή ενός τέτοιου συστήματος είναι εξαιρετικά δύσκολη και μπορεί να γίνει μόνο εκ των έσω κοντά στο στόχο προκειμένου να ελαχιστοποιηθεί η πιθανότητα ανίχνευσης ή πρόληψης. Τέτοιες επιθέσεις προϋποθέτουν και απαιτούν συνεργασία με τις τοπικές ειδικές δυνάμεις που θα βοηθήσουν την ομάδα της κυβερνητικής επίθεσης να φτάσει στο στόχο όσο πιο κοντά γίνεται και να αποκτήσει πρόσβαση στα δεδομένα της λειτουργικότητάς του.

- **Το ανθρώπινο δυναμικό**

Η ασφάλεια βασίζεται σε τρεις πυλώνες: τους ανθρώπους, τα συστήματα και τις διαδικασίες. Καθώς τα συστήματα και οι διαδικασίες αναπτύσσονται από τους ανθρώπους, οι άνθρωποι πόροι αποτελούν το κλειδί στην πρωτοβουλία άμυνας της κυβερνητικής ασφάλειας.

Ειδικοί

Ο πυρήνας της δύναμης της άμυνας της κυβερνητικής ασφάλειας είναι οι άνθρωποι με γνώσεις ασφαλείας. Αυτοί δεν είναι διαχειριστικά όργανα που είναι σε θέση να εγκαταστήσουν ένα τοίχο προστασίας αλλά σχεδιάζουν και αναπτύσσουν τοίχους προστασίας και άλλα μέτρα ασφαλείας.

Χωρίς αυτούς τους ανθρώπους μια χώρα ή μια εταιρία χρειάζεται να βασίζεται σε εξωτερική βοήθεια που μπορεί να είναι αποτελεσματική αλλά μπορεί και να μην είναι.

Η θέση του ειδικού στην ασφάλεια είναι παρόμοια με αυτή του πυρηνικού επιστήμονα που μπορεί να εφεύρει και να αναπτύξει θανατηφόρα όπλα για οποιοδήποτε κράτος που είναι διατεθειμένο να πληρώσει για την έρευνά του.

Κατασκοπεία

Σύμφωνα με τον Sun Tzu η πληροφορία σχετικά με τον εχθρό είναι το κλειδί για την επιτυχία στη μάχη ή στο πόλεμο γενικότερα. Η συλλογή πληροφοριών σχετικά με τα μέσα του εχθρού και τα συστήματα κυβερνητικής ασφάλειας είναι τόσο ανεκτίμητα όσο και η γνώση του τί είδους όπλα και στρατιώτες διαθέτει ο εχθρός. Ακόμα και σε επίπεδο εταιρίας είναι πολύ σημαντικό να γνωρίζει κανείς τί

είδους προβλήματα στα νέα μέσα ασφαλείας έχουν πρόσφατα ανακαλυφθεί. Επιπλέον η πληροφορία σχετικά με τους ειδικούς στην ασφάλεια μπορεί να είναι ανεκτίμητης αξίας σε περίπτωση κάλυψης των αναγκών.

Χάκερς

Η δύναμη της άμυνας είναι η μια πλευρά της κυβερνητικής ασφάλειας ωστόσο θεωρείται απαραίτητο να υπάρχουν δυνατότητες επίθεσης, Οι χάκερς είναι σημαντικοί για εκπαίδευση σεναρίων αλλά και για την αναγνώριση υφιστάμενων και νέων «τρυπών» στην ασφάλεια.

Πολύ συχνά οι πρώην χάκερς έχουν τη τάση να παίζουν ρόλο συμβουλευτικό ως προς την ασφάλεια αλλά η κύρια διαφορά μεταξύ ενός χάκερ και ενός ειδικού στην ασφάλεια είναι ότι ο χάκερ πρέπει να αναγνωρίσει μια τρύπα ενώ ο ειδικός στην ασφάλεια πρέπει να τις καλύψει όλες.

Προγραμματιστές συστημάτων



Όλη αυτή η γνώση των προϋποθέσεων για την ασφάλεια και των νέων «τρυπών» στην ασφάλεια πρέπει να υπάρχει κάποιος που να ολοκληρώνει και να τροποποιεί μια λύση ή και τα ίδια τα προγράμματα η/υ και τα φυσικά του εξαρτήματα.

Η γνώση ενός συστήματος αλλά και οι ικανότητες στο προγραμματισμό είναι απαραίτητα εφόδια για την ανάπτυξη της βιομηχανίας τηλεπικοινωνιών καθώς επίσης και για τη κυβερνητική ασφάλεια.

- **Άμυνα**

Τα συστήματα πληροφοριών πάσχουν από πολλές πιθανές αδυναμίες αλλά όσα προβλήματα κι αν έχουν, εάν δε λειτουργούν δημιουργείται σημαντικότερο πρόβλημα.

Από τη κλίμακα αυτού του προβλήματος προσδιορίζονται η σημασία ενός τέτοιου συστήματος και των απαραίτητων μέσων προστασίας του. Η ελαχιστοποίηση του κινδύνου ενός τέτοιου προβλήματος ή της κλίμακας του απαιτεί μέτρα ασφαλείας που να καλύπτουν όλες τις πιθανές αιτίες του προβλήματος. Στη περίπτωση αυτή οι ειδικοί στην ασφάλεια συνήθως διακρίνουν 3 κύριες κατηγορίες παρόλο που κάποια μέτρα ασφαλείας είναι σε μεγαλύτερο βαθμό από άλλα και δεν υφίσταται σαφής ορισμός για το ποια μέτρα ασφαλείας ανήκουν πού .

Φυσική ασφάλεια

Για χιλιάδες χρόνια οι άνθρωποι, τα αγαθά, οι πόλεις ή και τα κράτη προστατεύονταν με μέτρα φυσικής ασφαλείας από πέτρινα τείχη μέχρι πυρηνικά καταφύγια. Ανεξάρτητα όμως από πόσο έξυπνη ή καλή ήταν η άμυνα υπήρχαν πάντα τρόποι προσβολής της. Για το λόγο αυτό επιβάλλεται ο συνδυασμός όλων των κατηγοριών προκειμένου να προληφθεί το δυσάρεστο γεγονός της εισβολής.

Λογική ασφάλεια

Αυτό είναι το κύριο πεδίο μάχης της κυβερνητικής ασφαλείας όπου η ψηφιακή πληροφορία ανταλλάσσεται ή αποθηκεύεται. Όλα τα μέτρα ασφαλείας που λαμβάνονται από μη ανθρώπινα μηχανήματα ανήκει σ' αυτή την ομάδα.

Υπάρχουν πολλοί υπο-τομείς:

1. Κρυπτογράφηση
2. Ασφάλεια του δικτύου
3. Ασφάλεια του συστήματος
4. Ασφάλεια της εφαρμογής
5. Επιτήρηση-επαλήθευση της ασφαλείας

Οργανωτική ασφάλεια

Ακόμα κι αν η πληροφορία κρατείται επτασφράγιστη πίσω από ερμητικά κλειστές πόρτες υπάρχει κίνδυνος κάποιος να ανοίξει τη πόρτα στον εισβολέα και να τον αφήσει να τη κλέψει.



Για το λόγο αυτό υπάρχουν διαδικασίες ασφαλείας ώστε να διασφαλίζουν ότι στη περίπτωση αποτυχίας των άλλων μέτρων ασφαλείας οι άνθρωποι να γνωρίζουν τι να κάνουν και ακολουθώντας τις διαδικασίες να εξασφαλίζουν την ασφάλεια της πληροφορίας. Πολύ συχνά σε πειστικές καταστάσεις όπου υπάρχει έλλειψη εξειδίκευσης οι άνθρωποι κάνουν περισσότερα σφάλματα από ποτέ. Οι διαδικασίες υπάρχουν για να βοηθούν τους ανθρώπους πράττουν το σωστό. Ακόμα κι όταν δεν γνωρίζουν τι να κάνουν αυτές οι κατευθυντήριες γραμμές τους δείχνουν πώς να προλαβαίνουν το χειρότερο.

- **Επίθεση**

- **Σενάριο επίθεσης**

Η κυβερνητική επίθεση απαιτεί λεπτομερώς οργανωμένη δομή και ένα σχέδιο για να επιτύχει το προσδοκώμενο σκοπό. Ένα τέτοιο σχέδιο θα πρέπει να έχει τη παρακάτω διάρθρωση:

1. Γενική ανάλυση του στόχου
2. Επιλογή συγκεκριμένων σκοπών
3. Επιλογή των μελών της ομάδας, τα οποία να διαθέτουν ικανοποιητικά προσόντα
4. Λεπτομερής ανάλυση του στόχου
5. Σχεδιασμός της επίθεσης
6. Εκπαίδευση για την επίθεση
7. Εκτέλεση της επίθεσης
8. Παρατήρηση του στόχου για να βεβαιωθούμε ότι ο σκοπός έχει εκπληρωθεί

Σ' ένα πρώτο στάδιο οι αναλυτές συλλέγουν όσο το δυνατό περισσότερες πληροφορίες σχετικά με το στόχο χρησιμοποιώντας συνήθη μέσα (εφημερίδες, ιστοσελίδες κ.α). Αυτές οι πληροφορίες βοηθούν στην αναγνώριση:

1. της αποστολής του στόχου (ποιος είναι σκοπός ύπαρξης του συστήματος)
2. του περιεχομένου και της δομής των συστημάτων του στόχου (δομή δικτύου, γεωγραφική περιοχή, συνδεδεμένα εξωτερικά συστήματα, πελάτες κ.α.)
3. τις χρησιμοποιούμενες τεχνολογίες (συστήματα που χρησιμοποιούνται, εφαρμοσμένο λογισμικό και ηλεκτρονικά εξαρτήματα, αμυντικά μέτρα κ.α)
4. την ιστορία της εφαρμογής του συστήματος (χρόνοι ολοκλήρωσης του συστήματος, ημερομηνίες αναβάθμισης, προμηθευτές κ.α.)
5. τους ανθρώπινους πόρους (πόσοι άνθρωποι απασχολούνται, πόσο καλά εκπαιδευμένοι είναι, τί είδους πληροφορίες συλλέγουν, ποια είναι τα ενδιαφέροντά τους, κ.α)

Όλες οι παραπάνω πληροφορίες μπορούν να βοηθήσουν στην επιλογή του καλύτερου (ή του πιο αδύναμου) στόχου και την πιθανή πηγή επίθεσης καθώς φυσικά και το χρονικό πλαίσιο της δράσης.

Στη δεύτερη φάση θα μπορέσουν να αναγνωρίσουν όλα τα αδύνατα σημεία ή τα ενδιαφέροντα σημεία στα οποία πρέπει να εμβαθύνουν οι αναλυτές. Αυτοί οι στόχοι δεν είναι



απαραίτητο να είναι συγκεκριμένα συστήματα, μπορούν ακόμα να είναι πηγές πληροφοριών ή άτομα.

Στη τρίτη φάση η ομάδα θα πρέπει να συγκροτηθεί περιλαμβάνοντας ειδικούς σε κάθε τύπο συστήματος που χρησιμοποιεί ο στόχος. Επειδή δεν είναι πάντα δυνατή η συλλογή όλων των απαραίτητων πληροφοριών ώστε η ομάδα να επιλέξει τα αρχικά της μέλη, θα πρέπει κατ' αρχή να καλείται οποιοσδήποτε ειδικός θεωρείται απαραίτητος στην ανάλυση του στόχου ή γενικότερα στην επίθεση.

Στο τέταρτο σημείο οι αναλυτές θα πρέπει να συλλέξουν όλες τις απαραίτητες πληροφορίες σχετικά με το στόχο ώστε να δημιουργηθεί ένα συγκεκριμένο σχέδιο δράσης που θα επιτύχει τους συγκεκριμένους σκοπούς της δεύτερης φάσης. Σ' αυτό το σημείο αναγνωρίζεται η δομή του συγκεκριμένου στόχου και επιβεβαιώνεται η πληροφορία που συλλέχθηκε στη πρώτη φάση. Αυτό επιτυγχάνεται με αναλυτική και εξονυχιστική «ακτινογραφία» των συστημάτων του στόχου και με την αναγνώριση των επιχειρησιακών συστημάτων, των στοιχείων του δικτύου, καθώς και των υπηρεσιών αλλά και των σφαλμάτων που ενυπάρχουν σ' αυτές.

Στη πέμπτη φάση, οι παραπάνω πληροφορίες γίνονται αντικείμενο επεξεργασίας και αναγνωρίζονται συγκεκριμένες αδυναμίες που θα επέτρεπαν πιθανή «εισβολή». Δεν είναι φυσικά δυνατό να αναγνωρίζονται ως την απαραίτητη λεπτομέρεια αλλά με το συσχετισμό άλλων πληροφοριών μπορεί να καταστεί το σχέδιο της επίθεσης πιο συγκεκριμένο. Το σχέδιο μπορεί να περιέχει επιπλέον δοκιμασίες και εξονυχιστικές αναλύσεις δεδομένου ότι μπορεί να υπάρχουν άλλα συστήματα που δεν είναι αναγνωρίσιμα απ' έξω.

Η εκπαίδευση για την επίθεση στο έκτο σημείο είναι μια προετοιμασία που βελτιστοποιεί και δοκιμάζει τα κυβερνητικά όπλα καθώς και το σχέδιο επίθεσης σε παρόμοια συστήματα. Αυτό εξυπηρετεί στην ανάπτυξη συγκεκριμένου επιπέδου αυτοματισμού που επιταχύνει την επίθεση και ελαχιστοποιεί τη πιθανότητα της ανθρώπινης παρέμβασης.

Το σχέδιο της επίθεσης συνήθως είναι πολύ απλό:

1. χρήση μιας ανιχνευμένης αδυναμίας του συστήματος
2. απόκτηση του απαιτούμενου επιπέδου εξουσιοδότησης
3. επιτυχία του τελικού σκοπού
4. απομάκρυνση όλων των αποδεικτικών στοιχείων (εάν ο τελικός σκοπός ήταν διάφορος από τη καταστροφή του στόχου)

Η επαλήθευση της επίτευξης του τελικού σκοπού εξαρτάται από το περιεχόμενό του ωστόσο μπορεί να αποδειχθεί μέσω ανάλυσης της συλλεγμένης πληροφορίας ή ελέγχου των υπηρεσιών του στόχου οι οποίες θα πρέπει να έχουν διακοπεί ή μέσω ανάλυσης των πηγών της τοπικής ενημέρωσης (π.χ. εφημερίδες)

- **Εκπαίδευση**

Η δημιουργία κυβερνητικού στρατού από εθελοντές δεν μπορεί να συνιστά λύση για την εθνική ασφάλεια ακόμα κι αν αποτελείται από την ελίτ της ηλεκτρονικής ασφάλειας. Είναι περίπου το ίδιο σαν να επρόκειτο οι καλύτεροι αθλητές και κνηγοί να απαρτίσουν ένα στρατό.



Μπορεί να τρέχουν γρήγορα ή να σκοπεύουν άριστα αλλά δεν είναι δυνατό να επιτύχουν στον έλεγχο των χειρισμών των επιχειρήσεων ή στις τακτικές.

Προκειμένου να εκπαιδευτεί ένας κυβερνητικός στρατός υπάρχει ανάγκη από μια στημένη δομή που θα τους χρησιμοποιήσει αποτελεσματικά. Πρέπει επίσης να υπάρχουν διαδικασίες που θα βοηθούν στον αποτελεσματικό χειρισμό των καταστάσεων. Όλα αυτά πρέπει να έχουν οικοδομηθεί πριν αρχίσει οποιαδήποτε εκπαίδευση. Είναι ήδη σαφές ότι τα συνηθισμένα εγχειρίδια του στρατού δεν μπορούν να χρησιμοποιηθούν ώστε να φτιαχτούν οι κυβερνο-στρατιώτες δεδομένου ότι εδώ μετράει περισσότερο η ποιότητα και όχι η ποσότητα. Επίσης οι τακτικές πρέπει να χαραχθούν από το μηδέν προκειμένου να επιτευχθεί ο απαραίτητος τελικός σκοπός. Εδώ ο διαχωρισμός μεταξύ επιθετικής και αμυντικής εκπαίδευσης είναι πιο σαφής και ορατός από ό,τι στη πραγματική πολεμική εκπαίδευση.

Αμυντική εκπαίδευση

Η προστασία της υποδομής απαιτεί εκπαίδευση στις τεχνολογίες της ασφάλειας. Υπάρχουν πολλές εκπαιδύσεις για εξειδικευμένες τεχνολογίες αλλά προκειμένου να χρησιμοποιηθούν στο κυβερνητικό πόλεμο πρέπει να ενσωματωθούν όλες μαζί σε μία.

Για παράδειγμα, υπάρχει ένας πιθανός ανιχνευμένος στόχος και ένας αξιωματικός αποφασίζει ότι είναι αναγκαίο να προστατευτεί ο στόχος. Στη περίπτωση αυτή υπάρχει ένα γενικό σχέδιο που πρέπει να εκτελεστεί:

1. οι ελεγκτές και επιθεωρητές στέλνονται επί τόπου να ερευνήσουν τη τρέχουσα κατάσταση της ασφάλειας
2. κάθε εξειδικευμένος τομέας αξιολογείται και ο αξιωματικός αποφασίζει ποιος τομέας χρειάζεται βελτίωση και τι είδους ειδικό πρέπει να στελεχώσουν το τομέα
3. οι ειδικοί αρχίζουν τις βελτιώσεις στην οργανωτική ασφάλεια
4. αφού βελτιώσουν της πολιτική ασφάλειας, αρχίζει η βελτίωση των συστημάτων και δικτύων σε άλλους τομείς
5. η αναφορά περιστατικών συνδέεται με ένα κέντρο άμυνας επανδρωμένο με στελέχη ειδικά στη παρακολούθηση της ασφάλειας
6. Δίνεται ένα γενικό έγγραφο πληροφόρησης στο επιτελείο ασφάλειας του Στόχου
7. αφού αποκλιμακωθεί η παρακολούθηση της ασφάλειας επιστρέφεται μια αναφορά περιστατικών στη ομάδα ασφαλείας του στόχου

Αυτά όλα πρέπει να συμβούν σε ελάχιστο χρόνο καθώς οι κυβερνητικές επιθέσεις μπορούν να αρχίσουν αμέσως μετά τη προειδοποίηση. Επίσης ζωτικής σημασίας είναι η συνεργασία με την ομάδα ασφάλειας του στόχου εξαιτίας του ότι γνωρίζουν καλύτερα το σύστημά τους.

Οι ομάδες άμυνας πρέπει να είναι εκπαιδευμένες σε ποικίλες τεχνολογίες διαθέσιμες στην αγορά και να εφαρμόζουν τις δεξιότητές τους στα περισσότερα από τα συνήθη συστήματα που κυκλοφορούν στην αγορά.



Η εκπαίδευση σε εξειδικευμένες τεχνολογίες πρέπει να γίνεται από εξωτερικές εταιρίες που διαθέτουν τα μέσα και τις ικανότητες για κάτι τέτοιο ωστόσο η εκπαίδευση στις τακτικές θα πρέπει να γίνεται επιτόπια σε συνεργασία με ομάδες επιθετικού πολέμου.

Υπάρχουν τρεις τύποι εκπαίδευσης:

1. ενεργητική προάσπιση του στόχου
2. άμεση αντίδραση σε επίθεση και εξασφάλιση του στόχου
3. επιχειρηματολογία της ασφάλειας μετά από επίθεση και προστασία της υποδομής του στόχου ώστε να προληφθούν περαιτέρω επιθέσεις

Η εκπαίδευση τύπου 1 αρχίζει με την εγκατάσταση ενός συστήματος με εφαρμογή και προσδιορίζοντας μια λειτουργία για αυτό. Συνεχίζει με τη κατάστρωση λίστας ελέγχου της ασφάλειας προκειμένου να φτάσει το σύστημα και τα συστατικά του δικτύου σε ένα ασφαλώς σχηματισμένο επίπεδο. Στη συνέχεια υπάρχουν εγκατεστημένα ενεργητικά μέτρα ασφάλειας προκειμένου να προληφθεί η πλειοψηφία των συνήθων επιθέσεων. Μετά απ' αυτό το στάδιο υπάρχουν εγκατεστημένα παθητικά μέτρα ασφαλείας με σκοπό τη παρακολούθηση και έλεγχο του συστήματος καθώς και τη παροχή ικανοποιητικών δεδομένων ελέγχου με σκοπό την αναγνώριση του τί ακριβώς συνέβη.

Η εκπαίδευση τύπου 2 έχει πολλές ομοιότητες με τις στρατιωτικές ασκήσεις ετοιμότητας για την ασφάλεια. Μόλις ανακοινωθεί ο συναγερμός τα μέλη της ομάδας πρέπει να αποκτήσουν τον έλεγχο επί του συστήματος και να απομακρύνουν τους εισβολείς από το σύστημα. Αυτό μπορεί να επιτευχθεί σε συνεργασία με ομάδες επιθετικού πολέμου. Μόλις ανακοινωθεί ο συναγερμός πρέπει να εκτελεστεί η διαδικασία κλιμάκωσης και η οποία ενημερώνει το παγκόσμιο κέντρο ελέγχου ασφάλειας (GSC2) για κάποια επίθεση που γίνεται εκείνη τη στιγμή. Αφού αποκτηθεί ο πλήρης έλεγχος του συστήματος, η ομάδα πρέπει να ερευνήσει πώς οι εισβολείς επιτέθηκαν στο σύστημα και να το αναφέρει στο GSC2. Με τον τρόπο αυτό το σύστημα πληροφοριών προστατεύεται και οι «τρύπες» της ασφάλειας επισκευάζονται. Επίσης αυτή η διαδικασία πρέπει να αναφερθεί στο GSC2 προκειμένου να προστατέψει και άλλα παρόμοια συστήματα που μπορεί να αποτελέσουν πιθανούς στόχους.

Η εκπαίδευση τύπου 3 λαμβάνει χώρα σε συστήματα που ήδη έχουν υποστήριξη και έχουν αντιγραφεί. Ο κύριος σκοπός τους είναι να αναλύσουν τη κατάσταση του συστήματος και να αναπαραστήσουν τις δράσεις που έκαναν οι επιτιθέμενοι. Αυτό εξυπηρετεί στο να προστατευτεί το σύστημα καθώς και να δοθούν επιπλέον πληροφορίες στις ομάδες επιθετικού πολέμου για το πώς να διεξαγάγουν παρόμοιες επιθέσεις. Ένας άλλος τελικός σκοπός είναι η ανίχνευση αυτού που έχει αλλάξει στο σύστημα με σκοπό να προληφθεί περαιτέρω βλάβη ή απάτη.

- **Επιθετική εκπαίδευση**

Είναι δύσκολο να διδάσκεις κάτι όχι τόσο συγκεκριμένο που μεταβάλλεται από στιγμή σε στιγμή. Ο επιθετικός κυβερνητικός πόλεμος είναι μια δέσμη μέσων και τεχνολογιών που βασίζεται στις «τρύπες» της ασφάλειας σε διάφορα λογισμικά. Αυτές οι τρύπες επισκευάζονται πολύ γρήγορα και η εκπαίδευση του πώς να τις προσβάλλει κανείς, μετά πάροδο λίγων ημερών, γίνεται



παρωχημένη. Για το λόγο αυτό η επιθετική εκπαίδευση θα πρέπει να βασίζεται μάλλον στις γενικές τεχνολογίες παρά σε εξειδικευμένα μέσα.

Οι σκοποί της εκπαίδευσης είναι:

1. η ψυχολογική καταλληλότητα (εργασία υπό πίεση χρόνου)
2. τεχνολογική κατανόηση (γενικές αντιλήψεις των συστημάτων και των δικτύων)
3. κατανόηση των επιχειρησιακών διαδικασιών και των πολιτικών)
4. κατανόηση της λειτουργικότητας του κράτους, της κυβέρνησης και του στρατού (ροή πληροφοριών, δομή της διοίκησης)

Προκειμένου να επιτευχθούν αυτοί οι τελικοί σκοποί θα πρέπει να υπάρχει ένα σχέδιο εκπαίδευσης για ανταποκρίνεται στις ανάγκες του στρατού.

Ψυχολογική καταλληλότητα

Ο στρατιώτης για να πετύχει στο πεδίο της κυβερνητικής μάχης πρέπει να είναι ικανός να εργάζεται κάτω από πίεση και παίρνει τις σωστές αποφάσεις πολύ γρήγορα. Όπως ακριβώς στο συμβατικό πόλεμο, μια τρύπα ή ένα παράθυρο στην άμυνα του εχθρού ανοίγει για πολύ περιορισμένο χρόνο. Η ομάδα επίθεσης πρέπει να χρησιμοποιήσει αυτό το παράθυρο και κάθε δευτερόλεπτο μετράει στο να κερδίσει με καλή προετοιμασία και εκπαίδευση. Το στρες δεν είναι μόνο μια απλή παρενέργεια όταν εργάζεται κανείς υπό πίεση αλλά ακόμα και ένας σημαντικός παράγοντας επιτυχίας. Η εκπαίδευση θα πρέπει να γίνεται ακριβώς με τον ίδιο τρόπο όπως και στη συμβατική εκπαίδευση με την εκμάθηση διαδικασιών προκειμένου να ελαχιστοποιηθεί ο ενδιάμεσος χρόνος αντίδρασης.

Τεχνολογική κατανόηση

Στο συμβατικό πόλεμο είναι απαραίτητο να γνωρίζουμε πώς λειτουργούν τα όπλα ώστε να τα χρησιμοποιούμε κατάλληλα. Αυτή η ίδια αντίληψη είναι απαραίτητη στον κυβερνητικό πόλεμο. Το επίπεδο ακρίβειας πρέπει να είναι ικανοποιητικό ώστε να εγγυάται τη κατανόηση του τί ακριβώς συνέβη, συμβαίνει ή πρόκειται να συμβεί. Γνωρίζοντας τις τεχνολογίες ένας πολεμιστής του κυβερνητικού πολέμου είναι σε θέση να παίρνει αποφάσεις και να προβλέπει τις ενέργειες του εχθρού δεδομένου ότι οι ανθρώπινες αλληλεπιδράσεις είναι πολύ σπάνιες. Η κατανόηση της λειτουργίας του δικτύου και της λειτουργίας της τεχνολογίας των συστημάτων επ' ουδενί θα πρέπει να υποτιμάται και θα πρέπει να αποτελεί το κύριο σκοπό της εκπαίδευσης του κυβερνοπολεμιστή.

Επιχειρησιακές διαδικασίες και πολιτικές

Η τεχνολογική προστασία είναι πολύ περιορισμένη χάρις στην διαβλητότητα κάθε συστήματος. Τα προστατευτικά μέτρα δεν επηρεάζουν την αναγκαία λειτουργικότητα ενός συστήματος και για το λόγο αυτό δεν μπορεί να αποτελούν τη μοναδική άμυνα του στόχου. Μετά τη λογική ασφάλεια έπεται η οργανωτική ασφάλεια που συνίσταται από πολιτικές και διαδικασίες. Αυτές συνήθως αναπτύσσονται με σκοπό την ενίσχυση της άμυνας στο μέγιστο βαθμό. Εξαιτίας της ανθρώπινης φύσης δεν είναι τόσο γρήγορες και ακριβείς όσο τα τεχνολογικά μέσα ωστόσο δεν είναι καθόλου ορατές και δεν μπορούν εύκολα να προβλεφθούν. Γνωρίζοντας τη συνήθη



διαδικασία που ακολουθείται σε μια συγκεκριμένη βιομηχανία ένας κυβερνο-πολεμιστής είναι σε θέση να προβλέψει την ανθρώπινη αντίδραση και να εκτιμήσει τις ενέργειες που πρέπει να κάνει ή να υπολογίσει τον υπόλοιπο χρόνο μέχρι την επίτευξη του τελικού σκοπού.

Γενική λειτουργικότητα του στόχου

Μαθαίνοντας για τη λειτουργικότητα της αντεπίθεσης και τη δομή της, ο στρατιώτης του κυβερνητικού πολέμου μπορεί να επιλέξει τους σωστούς στόχους καθώς και να παίρνει γρήγορες αποφάσεις σχετικά με τις τακτικές που θα ακολουθήσει σε συγκεκριμένη επίθεση. Κάνοντας επίθεση σε σωστούς στόχους είναι δυνατό να επιτύχει το προσδοκώμενο αποτέλεσμα καθώς και να δημιουργήσει αρκετή σύγχυση και περισπασμό ώστε να ανοίξει ακόμα περισσότερο το παράθυρο της επίθεσης ή να αφήσει απαρατήρητο το σύστημα που ο ίδιος έχει προσβάλει. Αν και δεν είναι πολύ χρήσιμο στην εκτέλεση της κυβερνητικής επίθεσης ωστόσο είναι σίγουρα ανεκτίμητο στην επιλογή στόχων ή το σχεδιασμό τακτικών.

Συμπέρασμα

Η σημαντικότητα των συστημάτων πληροφοριών στο πόλεμο του σήμερα καταδεικνύει ότι η ασφάλεια των πληροφοριών αποτελεί ένα σπουδαίο παράγοντα για την επιτυχία μιας σύγκρουσης ή ακόμα κι ενός πολέμου. Ο κυβερνητικός πόλεμος γίνεται ολοένα και περισσότερο πιο ισχυρός στο σύγχρονο πεδίο της μάχης και επηρεάζει την εξέλιξη του στρατού σε πολλές χώρες καθώς και την ανάπτυξη των εξοπλιστικών τεχνολογιών. Η χρήση του δεν θα πρέπει να υποτιμάται καθώς είναι εξαιρετικά ευέλικτος και δύσκολα ανιχνεύσιμος. Το κόστος του επιτρέπει σε οποιαδήποτε χώρα να εκπαιδεύει ή να προσλαμβάνει μια ομάδα ικανή να σχηματίσει κάτι περισσότερο από ένα πλήρως καταρτισμένο στρατό. Η αποτελεσματική χρήση τέτοιων ομάδων μπορεί να χαρίσει την επικράτηση στο πεδίο της μάχης ή να πείσει τον εχθρό να υποχωρήσει, κλείνοντας τη διοικητική του υποδομή ή το δίκτυο επικοινωνίας. Η αξία του κυβερνητικού πολέμου αυξάνεται και με τη ψηφιοποίηση των τεχνολογιών του συμβατικού πολέμου καθώς επίσης και η χρήση περισσότερο περίπλοκων μηχανημάτων δημιουργεί κινδύνους και αδυναμίες που δίνουν τη δυνατότητα στις μονάδες κυβερνητικού πολέμου να προξενήσουν μεγαλύτερη βλάβη απ' ό,τι στο παρελθόν.

Η εποχή της πληροφορίας εκτοπίζει τις συμβατικές βιομηχανίες και καθώς οι ανάγκες για αυτοματισμό και ψηφιοποίηση αυξάνονται, τα κράτη συνειδητοποιούν την έλλειψη καταρτισμένων ανθρώπων ικανών να τις ελέγξουν. Οι κυβερνήσεις αντιλαμβάνονται ότι αυτό το πρόβλημα επιβραδύνει τους ρυθμούς της οικονομίας αλλά δεν συνειδητοποιούν ότι δημιουργεί επιπλέον κινδύνους και κενά στη στρατηγική εθνικής ασφάλειας. Το κλείσιμο των πυρηνικών εργαστηρίων μπορεί να καταστρέψει ολόκληρη την οικονομία σε ελάχιστο χρόνο, το άνοιγμα των υδάτινων φραγμάτων μπορεί να σκοτώσει χιλιάδες ανθρώπους ή η αποδέσμευση δηλητηριωδών χημικών μπορεί να καταστρέψει το οικοσύστημα μιας χώρας.

Οι μονάδες κυβερνητικού πολέμου έχουν μια σημαντική αποστολή, να διατηρήσουν τη βιωσιμότητα, την ευημερία και τη σταθερότητα μιας χώρας. Πρέπει να διασφαλίσουν την εθνική ασφάλεια και στη χειρότερη περίπτωση να βοηθήσουν στην ανάκαμψη από μια καταστροφή. Στο παρελθόν οι χώρες βασίζονταν στην ισχύ των συμβατικών στρατιωτικών μονάδων αλλά τώρα το



μέλλον μιας χώρας μπορεί να εξαρτάται από το πόσο καλά εκπαιδευμένες είναι οι μονάδες κυβερνητικού πολέμου και πόση πρακτική εφαρμογή διαθέτουν.

Ο εχθρός υπάρχει πάντα και γίνεται πιο ισχυρός κάθε λεπτό. Πρέπει να είμαστε σίγουροι ότι μπορούμε να τον αποτρέψουμε από τη καταστροφή των αξιών μας που με τόση δυσκολία έχουμε δημιουργήσει.