ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΔΙΕΘΝΩΝ ΚΑΙ ΕΥΡΩΠΑΪΚΩΝ ΣΠΟΥΔΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
BRICS: «ΟΙΚΟΝΟΜΙΑ – ΚΟΙΝΩΝΙΑ – ΕΞΩΤΕΡΙΚΗ ΠΟΛΙΤΙΚΗ»

Διπλωματική Εργασία

Η Πολιτική Ασφαλείας Της Κίνας Στον Κυβερνοχώρο

Μαρία Δημητρακοπούλου
(MBP/15005)

Επιβλέπων Καθηγητής : κ. Ανδρέας Λιαρόπουλος

Πειραιάς , 2018

Η Μαρία Δημητρακοπούλου βεβαιώνω ότι το έργο που εκπονήθηκε και παρουσιάζεται στην
υποβαλλόμενη διπλωματική εργασία είναι αποκλειστικά ατομικό δικό μου. Όποιες πληροφορίες και υλικό που περιέχονται έχουν αντληθεί από άλλες πηγές, έχουν καταλλήλως αναφερθεί στην παρούσα διπλωματική εργασία. Επιπλέον τελώ εν γνώσει ότι σε περίπτωση διαπίστωσης ότι δεν συντρέχουν όσα βεβαιώνονται από μέρους μου, μου αφαιρείται ανά πάσα στιγμή αμέσως ο τίτλος.

(υπογραφή)

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΙΚΟ ΣΗΜΕΙΩΜΑ

Με την ευρεία χρήση του Διαδικτύου την δεκαετία του 1990 άλλαξαν ριζικά οι ζωές των ανθρώπων. Ξαφνικά ανοίχτηκαν άπειρες δυνατότητες για τους πολίτες και το διαδίκτυο έγινε καθημερινό εργαλείο στα χέρια τους. Η εκμηδένιση των αποστάσεων, η ελεύθερη επικοινωνία και η αποθήκευση πληροφοριών σε τεράστιας χωρητικότητας βάσεις δεδομένων αποτελούν κάποιες από τις ενέργειες τις οποίες μπορούν να εκτελέσουν μέσω των ηλεκτρονικών υπολογιστών τόσο οι απλοί πολίτες , όσο και οι επιχειρήσεις και οι δημόσιοι και ιδιωτικοί φορείς. Με την αυξανόμενη χρήση του Διαδικτύου και την ανάπτυξη του ήρθε στην επιφάνεια και η έννοια του κυβερνοχώρου, του εικονικού δηλαδή περιβάλλοντος μέσα στο οποίο εκτελούνται όλες οι ενέργειες του Διαδικτύου. Χαρακτηριστικό του κυβερνοχώρου αποτελεί η έλλειψη συνόρων και η ανωνυμία που προστατεύει τους χρήστες , καθώς και η εύκολη πρόσβαση σε αυτόν. Η πρόσβαση είναι εφικτή σχεδόν από όλους, γεγονός που απέφερε συγκρούσεις και ανασφάλεια στα κράτη, τα οποία προσπαθούν να προσαρμοστούν στα καινούργια δεδομένα , σε διαφορετικού είδους απειλές , να προετοιμαστούν για νέα είδη επιθέσεων και πάνω από όλα για την αντιμετώπιση νέων αντιπάλων. Οι παραδοσιακές έννοιες της ισχύος και της κυριαρχίας μεταβάλλονται στον κυβερνοχώρο, με τα κράτη να προσπαθούν να επιβιώσουν στο καινούργιο περιβάλλον αναπροσαρμόζοντας τις στρατηγικές τους. Το γεγονός που αποτέλεσε ορόσημο για την υιοθέτηση τεχνολογιών που συνδέονταν με το Δίκτυο , ήταν ο πρώτος πόλεμος του Κόλπου το 1990. Πολλά κράτη , όπως και η Κίνα, αναγνώρισαν την νίκη των ΗΠΑ και των συμμάχων τους, αλλά περισσότερο συνειδητοποίησαν τα αποτελέσματα που μπορεί να επιφέρει ο συνδυασμός των ηλεκτρονικών μέσων με τα παραδοσιακά στρατιωτικά μέσα.

Η Κίνα πλέον χρησιμοποιεί ευρέως το Διαδίκτυο σε όλους τους τομείς , δίνοντας έμφαση στην ασφάλεια και στην σταθερότητα του καθεστώτος. Στόχος της είναι να αξιοποιήσει όσο το δυνατόν περισσότερο το Ίντερνετ προς όφελος της , και αυτό θα το επιτύχει μέσω μίας αποτελεσματικής στρατηγικής. Προωθεί την άριστη εκπαίδευση των στρατιωτικών δυνάμεων στις νέες τεχνολογίες του κυβερνοχώρου και είναι κατάλληλα εξοπλισμένη και προετοιμασμένη για έναν επικείμενο κυβερνοπόλεμο. Επιπροσθέτως , χρησιμοποιεί ευρέως την κατασκοπεία , με σκοπό είτε να αντιγράψει νέους τεχνολογικούς εξοπλισμούς, είτε να συλλέξει διπλωματικές πληροφορίες από ξένα κράτη. Κατασκοπεία χρησιμοποιεί και στον τομέα της οικονομίας ήδη από το 1986 με σκοπό να φτάσει σε ρυθμούς ανάπτυξης τα ανεπτυγμένα κράτη , υποκλέβοντας δεδομένα τα οποία έπειτα τα χρησιμοποιούσε για δικό της όφελος.

Οι στρατηγικές αυτές της Κίνας έχουν δημιουργήσει διαφορές και συγκρούσεις με άλλα κράτη, τα οποία είναι αντίθετα σε αυτές τις πρακτικές.

Στο πρώτο κεφάλαιο της διπλωματικής εργασίας δίνονται οι βασικοί ορισμοί του κυβερνοχώρου και του Διαδικτύου καθώς και ο προσδιορισμός των χαρακτηριστικών τους. Πέραν των ορισμών , γίνεται προσπάθεια κατανόησης της συμπεριφοράς των κρατών στο καινούργιο περιβάλλον και πως αυτό επηρέασε την στρατηγική τους.

Στο δεύτερο κεφάλαιο δίνεται βάση στην κυβερνοασφάλεια και στις επιθέσεις και απειλές που προκύπτουν στον κυβερνοχώρο. Αναλύονται τα κυριότερα είδη των κυβερνοεπιθέσεων , οι σκοποί τους καθώς και ποιοι μπορούν να αποτελέσουν του θύτες και τα θύματα. Παράλληλα , αναλύεται ο ορισμός του κυβερνοπολέμου , τα χαρακτηριστικά του και οι συνέπειες του.

Στο τρίτο και τελευταίο κεφάλαιο της εργασίας, αναλύεται η πολιτική της Κίνας και ο τρόπος που αντιλαμβάνεται η ίδια τον κυβερνοχώρο. Οι απειλές που αναδύονται ολοένα και περισσότερο στον κυβερνοχώρο δεν αφήνουν αδιάφορη την Κίνα , και αυτό αποτελεί τον λόγο που σε αυτό το κεφάλαιο θα δοθεί έμφαση στην στρατηγική της Κίνας στην κυβερνοασφάλεια, πως θα αντιδράσει σε έναν ενδεχόμενο κυβερνοπόλεμο , καθώς και μερικές από τις επιθέσεις που έχει διεξάγει σε άλλα κράτη. Τέλος, θα αναλυθούν οι σχέσεις της με δύο από τα κράτη που έχει τις περισσότερες συγκρούσεις στον κυβερνοχώρο και η καταπάτηση των ανθρωπίνων δικαιωμάτων στο εικονικό περιβάλλον.

ΚΕΦΑΛΑΙΟ 1. ΚΥΒΕΡΝΟΧΩΡΟΣ

1. Ορισμός

Ο κυβερνοχώρος και όροι όπως η κυβερνοασφάλεια και οι κυβερνοεπιθέσεις αναδύονται όλο και περισσότερο στην επιστήμη των διεθνών σχέσεων. Ο κυβερνοχώρος ως έννοια όπως αναφέρει το Υπουργείο Άμυνας των Ηνωμένων Πολιτειών περιγράφει «ένα παγκόσμιο πεδίο μέσα στο περιβάλλον πληροφορίας που αποτελείται από τα αλληλοεξαρτώμενα δίκτυα στις υποδομές της τεχνολογίας των πληροφοριών, συμπεριλαμβανομένου του Διαδικτύου (Ίντερνετ), τα δίκτυα τηλεπικοινωνιών, των ηλεκτρονικών υπολογιστών, και ενσωματωμένους επεξεργαστές και ελεγκτές».[1] Σε μία άλλη προσπάθεια ορισμού του κυβερνοχώρου το πανεπιστήμιο της Οξφόρδης στην ηλεκτρονική έκδοση του λεξικού που εκδίδει , ορίζει τον κυβερνοχώρο ως «Το πλασματικό περιβάλλον στο οποίο λαμβάνει χώρα η επικοινωνία μέσω δικτύων υπολογιστών».[2]

Η συζήτηση γύρω από το κυβερνοχώρο γίνεται όλο και πιο έντονη καθώς οι περισσότερες χώρες μεταφέρουν στο δίκτυο όλο και περισσότερα δεδομένα. Ο κυβερνοχώρος αποτελεί ένα χώρο άκρατα δημοκρατικό και παγκόσμιο που επιτρέπει σε κράτη , οργανισμούς , εταιρείες ακόμα και ιδιώτες να έχουν παγκόσμιο αντίκτυπο.[3]

Καθημερινές λειτουργίες και συναλλαγές των πολιτών καθώς και πιο περίπλοκα στρατηγικά σχέδια δημιουργούνται και φυλάσσονται στο δίκτυο. Τα τραπεζικά συστήματα των χωρών και οι συναλλαγές των πολιτών με αυτά, λειτουργίες των επιχειρήσεων, προσωπικά δεδομένα , προσχέδια προϊόντων υψηλής τεχνολογίας , πυρηνικά προγράμματα και διάφορες λειτουργίες πυρηνικών και στρατιωτικών προγραμμάτων ψηφιοποιούνται ολοένα και περισσότερο τόσο από τις ανεπτυγμένες όσο και από τις αναπτυσσόμενες χώρες.

Χαρακτηριστική για τη σημασία του κυβερνοχώρου είναι η περιγραφή του στο ενημερωτικό δελτίο του Λευκού Οίκου : «Η ψηφιακή υποδομή γίνεται όλο και περισσότερο η ραχοκοκαλιά των ευημερουσών οικονομιών, των έντονα ερευνητικών κοινοτήτων, των ισχυρών ενόπλων δυνάμεων, των κυβερνήσεων διαφάνειας και των ελεύθερων κοινωνιών…»[4]

---

[1] Joint Publication 1-02 , Department of Defense Dictionary of Military and Associated Terms ,8 November 2010 (As Amended Through 15 February 2016) p. 58 http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

[2] https://en.oxforddictionaries.com/definition/us/cyberspace

[3] Kenneth Lieberthal, Peter W. Singer , Cyberspace Security and U.S- China Relations, Brookings, Author's Note p. iv

[4] International strategy for cyberspace https://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf

2. Χαρακτηριστικά

i. Το Μέγεθος του κυβερνοχώρου

Όντας εικονικό περιβάλλον ο κυβερνοχώρος , ο υπολογισμός του μεγέθους του καθίσταται πάρα πολύ δύσκολος. Όπως αναφέρθηκε , ο κυβερνοχώρος δεν περιλαμβάνει μόνο το εικονικό κομμάτι όπως τα δίκτυα και το Ίντερνετ αλλά και τις υποδομές που αναφέρονται στον εξοπλισμό που χρειάζεται για να τεθεί σε λειτουργία. Επίσης , μεγάλη σημασία έχει η ανθρώπινη παρουσία η οποία θα κάνει χρήση του υλικού , θα φέρει στη ζωή το οικοσύστημα του κυβερνοχώρου και θα αλληλεπιδράσει μέσα σε αυτό. Ο κυβερνοχώρος διευρύνεται όταν προστεθούν περισσότεροι χρήστες σε αυτόν και όταν αυξήσουν την δραστηριότητα τους μέσα σε αυτόν. Σε έκθεση της η Διεθνής Ένωση Τηλεπικοινωνιών για το έτος 2015, αναφέρει πως μέχρι το τέλος του 2015, 32 δισεκατομμύρια άνθρωποι χρησιμοποιούν το Ίντερνετ παγκοσμίως, από τους οποίους τα δύο δισεκατομμύρια προέρχονται από τις αναπτυσσόμενες χώρες [5]. Στην αντίστοιχη έκθεση της για το 2016 αναφέρει πως μέχρι το τέλος του 2016, το 56% του παγκόσμιου πληθυσμού , δηλαδή 3,9 δισεκατομμύρια άνθρωποι δεν χρησιμοποιούν το Διαδίκτυο [6]. Βάσει των παραπάνω στοιχείων μπορεί να γίνει εύκολα κατανοητό πως ακόμα και αν παραπάνω από το μισό του παγκόσμιου πληθυσμού είτε δεν έχει πρόσβαση είτε δεν χρησιμοποιεί το Διαδίκτυο ο αριθμός των χρηστών παραμένει τεράστιος και έχει αυξητική τάση.

Αρκεί να ληφθεί υπόψιν ο αριθμός των ανθρώπων που χρησιμοποιούν ηλεκτρονικό ταχυδρομείο οι οποίοι σύμφωνα με τις εκτιμήσεις της εταιρίας Radicati Group INC το 2016, θα υπάρχουν πάνω από 2,6 δισεκατομμύρια χρήστες email σε όλο τον κόσμο, και μέχρι το τέλος του 2020 ο αριθμός των χρηστών του ηλεκτρονικού ταχυδρομείου θα ξεπεράσει τα 3 δισεκατομμύρια [7].

Αυξητική τάση έχει και ο αριθμός των ιστοσελίδων σε λειτουργία και των ενεργών domain [8] αφού το δεύτερο τρίμηνο του 2016 έκλεισε με περίπου 334.600.000 καταχωρίσεις domain name [9]. Από τις παραπάνω στατιστικές έρευνες γίνεται φανερό πως καθημερινά καταγράφονται δισεκατομμύρια αλληλεπιδράσεις στο Διαδίκτυο οι οποίες σημαίνουν ότι καθημερινά διακινούνται άπειρα ψηφιακά δεδομένα.

---

[5] International Telecommunications Union (ITU) Facts and Figures 2015 https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

[6] International Telecommunications Union (ITU) Facts and Figures 2016 http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf

[7] The Radicati Group, Inc. A Technology Market Research Firm Email Statistics Report, 2016-2020 p. 2

[8] Domain name είναι το ξεχωριστό για κάθε ιστότοπο όνομα, το οποίο κατοχυρώνεται επί πληρωμή και περιέχει λέξεις-κλειδιά που το καθιστούν πιο εύκολο στην αναζήτηση του από τους χρήστες.

[9] THE VERISIGN DOMAIN REPORT p.2 https://www.verisign.com/assets/domain-name-report-sept2016.pdf

Η αύξηση του μεγέθους του κυβερνοχώρου οφείλεται επίσης και στην εξέλιξη της ψηφιακής τεχνολογίας καθώς με την ανάπτυξη των εξοπλισμών και την ανακάλυψη νέων τεχνολογιών, αλλά και την εξέλιξη των Δικτύων και της ταχύτητας του Διαδικτύου [10], θα πολλαπλασιαστούν οι χρήστες και τα δεδομένα που ψηφιοποιούνται.

Συμπερασματικά το μέγεθος του κυβερνοχώρου δεν μπορεί να καθοριστεί με ακρίβεια διότι δεν μπορούν να μετρηθούν με ακρίβεια οι παράγοντες από τους οποίους εξαρτάται , εν τούτοις δεν μπορεί να παραβλεφθεί η συνεχής αύξηση της έκτασης του, δεδομένου ότι η διακίνηση δεδομένων και πληροφοριών αυξάνεται διαρκώς σε όλους τους τομείς της ανθρώπινης ζωής.

ii. Ανωνυμία

Ένα από τα βασικότερα χαρακτηριστικά του κυβερνοχώρου αποτελεί η ανωνυμία που προσφέρει το Διαδίκτυο στους χρήστες του. Ανωνυμία μπορεί να οριστεί όταν κάποιος δεν έχει όνομα ή χρησιμοποιεί ένα άγνωστο όνομα [11]. Η ταυτότητα των χρηστών του Διαδικτύου έχει διττό χαρακτήρα. Από την μία πλευρά, η ανωνυμία στοχεύει στην προστασία του χρήστη , και από την άλλη πίσω από αυτή παραμονεύουν κακόβουλες ενέργειες οι οποίες βλάπτουν τον χρήστη. Η θετική πλευρά της ανωνυμία έχει άμεση σχέση με την ιδιωτικότητα και την προστασία αυτής. Σύμφωνα με τον Clarke η ιδιωτικότητα χωρίζεται στην ιδωτικότητα της προσωπικής συμπεριφοράς, την ελευθερία δηλαδή έκφρασης απόψεων και αντιλήψεων όπως η θρησκεία και οι πολιτικές πεποιθήσεις , και την ιδιωτικότητα των προσωπικών δεδομένων [12]. Η ανωνυμία διασφαλίζει την ιδιωτικότητα ,την εμπιστευτικότητα και την ασφάλεια των ιδιωτών [13].

Στην αρνητική πλευρά της ανωνυμίας συγκαταλέγονται όλες οι αρνητικές ενέργειες των χρηστών όπως τα spam mails , η προπαγάνδα ή ακόμα και ο κυβερνοεπιθέσεις.

Ομάδες χρηστών όπως οι hackers , αλλά και επιχειρήσεις και κράτη χρησιμοποιούν την ανωνυμία για προσωπικό συμφέρον με αποτέλεσμα να βλάπτουν άλλους δρώντες.

---

[10] Η εξέλιξη της νανοτεχνολογίας και διάφορα project σε πειραματικό στάδιο όπως το Mega MIMO 2.0 του MIT και το Li-Fi του Harald Haas υπόσχονται την εκτόξευση της ταχύτητας του Ίντερνετ σε ποσοστό ως και 330% πιο γρήγορο απ' ότι σήμερα.

[11] . Kabay, M. E, PhD, CISSP Director of Education , Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy *Paper presented at the Annual Conference of the European Institute for Computer Anti-virus Research (EICAR),* Munich, Germany 16-8 March 1998 International Computer Security Association p .4

[12] Roger Clarke, What's 'Privacy'? Version of 7 August 2006 Prepared for a Workshop at the Australian Law Reform Commission ,July 2006

[13] Kabay ,M. E., PhD, CISSP Director of Education , Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy *Paper presented at the Annual Conference of the European Institute for Computer Anti-virus Research (EICAR),* Munich, Germany 16-8 March 1998 International Computer Security Association p .8

iii. Έλλειψη ορίων

Στον κυβερνοχώρο δεν υπάρχουν σύνορα όπως υπάρχουν στον πραγματικό κόσμο. Δεν υπάρχουν οι οριοθετήσεις των κρατών και είναι αδύνατο ο κυβερνοχώρος να χωριστεί και να κατανεμηθεί όπως το έδαφος , ο αέρας και τα ύδατα. Αυτή η έλλειψη συνόρων προκαλεί τον ανταγωνισμό των χρηστών , και ιδιαίτερα των χωρών , οι οποίες προσπαθούν να επιβάλλουν την κυριαρχία τους στον κυβερνοχώρο. Οι χώρες που οραματίζονται την οριοθέτηση και την κυριαρχία του κυβερνοχώρου , δεν υιοθετούν στρατηγικές που περιορίζονται μόνο εσωτερικά , αλλά αναπτύσσουν αρκετά αισιόδοξες , διεθνείς στρατηγικές , οι οποίες έρχονται σε σύγκρουση με τις στρατηγικές και τα συμφέροντα των υπολοίπων δρώντων [14] είτε πρόκειται για άλλες χώρες είτε για διεθνής οργανισμούς.

Τέλος, η μεγαλύτερη πρόκληση που αντιμετωπίζουν τα κράτη όσον αφορά την έλλειψη συνόρων είναι η ασφάλεια. Σένα κράτος με δεδομένη εδαφική έκταση είναι ευκολότερο να αντιμετωπιστούν οι κίνδυνοι και οι απειλές από οποιαδήποτε πηγή και αν προέρχονται. Στον χαοτικό όμως κόσμο του κυβερνοχώρου , η ανάγκη ανάπτυξης νέων στρατηγικών αντιμετώπισης αυξάνεται καθώς αυξάνεται και η ανάγκη συνεργασίας κρατών και οργανισμών.

3. Ίντερνετ

Το διαδίκτυο ή Ίντερνετ, είναι ένα «δίκτυο δικτύων», δηλαδή ένα παγκόσμιο δίκτυο στο οποίο συνδέονται εκατοντάδες χιλιάδες άλλα δίκτυα διαφόρων μεγεθών και οποίο επιτρέπει την ανταλλαγή δεδομένων μεταξύ οποιουδήποτε διασυνδεδεμένου (δικτυωμένου) ηλεκτρονικού υπολογιστή [15].

Ως γνωστόν , το Διαδίκτυο αποτελεί απόγονο του ARPANET. Αρχικά, στα μέσα της δεκαετίας του 1960 οι επιστήμονες Larry Roberts και J.C.R. Licklider δουλεύοντας πάνω σε προγράμματα έρευνας και ανάπτυξης της αρμόδιας υπηρεσίας του Πενταγώνου ARPA (Advanced Research Project Agency) , δημιούργησαν το δίκτυο ARPANET , το οποίο αποτελούνταν από 4 Η/Υ οι οποίοι βρίσκονταν στα πανεπιστήμια των Η.Π.Α. (UCLA, SRI,UCB και πανεπιστήμιο της Γιούτα). Μετ' έπειτα με την ανάπτυξη του δικτύου συνδέθηκαν υπολογιστές από το πανεπιστήμιο της Santa Monica , του Michigan και του Illinois.

[14] Ronald Deibert, Cyber security :The New Frontier , Great Decisions 2012 p. 51-52
[15] Χρήστος Βεράτης, ΚΕΔΙΣΑ , Κυβερνοχώρος-Κυβερνοεπιθέσεις- Κυβερνοάμυνα-Μέρος 1ο , Νοέμβριος 2015 http://kedisa.gr/kybernoxwros-kybernoepitheseis-kybe

Ακολούθησαν το MIT, το Harvard , το Carnegie – Mellon και το πανεπιστήμιο του Pittsburgh [16]. Ο αρχικός σκοπός του δικτύου ήταν η ανταλλαγή ιδεών και απόψεων της ακαδημαϊκής κοινότητας και η άμεση επικοινωνία τους. Στόχος του Πενταγώνου ήταν η απαρακώλυτη επικοινωνία ακόμα και αν η Σοβιετική Ένωση πραγματοποιούσε ένα πυρηνικό χτύπημα. Οι ερευνητές της εποχής δεν μπορούσαν να φανταστούν την έκταση που θα λάμβανε το δίκτυο που δημιούργησαν ώστε να βελτιώσουν και να δώσουν έμφαση στην ασφάλεια με αποτέλεσμα να δημιουργηθούν αρκετά σημεία τρωτότητας. Σύμφωνα με τους Clarke και Knake πέντε είναι τα κύρια τρωτά σημεία του Ίντερνετ [17]:

1) Το πρώτο τρωτό σημείο του Ίντερνετ σχετίζεται με τις ISPs (Ίντερνετ Service Providers) τις εταιρίες –μεσάζοντες που διανέμουν το Ίντερνετ τοπικά. Οι εταιρίες παροχής του Δικτύου χωρίζονται σε δύο κατηγορίες : Υπάρχουν οι εθνικές ISPs που κατέχουν χιλιάδες μίλια οπτικών ινών και συνδέουν τις μεγαλύτερες πόλεις της χώρας και προκειμένου να φτάσει το Ίντερνετ σε όλες τις περιοχές συνδέονται με μικρότερες τοπικές εταιρίες όπως είναι οι τηλεφωνικές εταιρίες. Σε αυτή την διαδικασία εντοπίζεται και η τρωτότητα , αφού η μεταφορά του δικτύου και η διανομή του από μικρότερες τοπικές εταιρίες αφήνει ένα κενό ασφαλείας το οποίο μπορούν να εκμεταλλευτούν άλλοι χρήστες του Ίντερνετ . Για παράδειγμα , μπορούν να αλλάξουν τις πληροφορίες του domain name ανακατευθύνοντας τους χρήστες σε άλλον ιστότοπο από αυτή που επέλεξαν με σκοπό την υποκλοπή στοιχείων.

2) Το δεύτερο σημείο σχετίζεται με το Border Gateway Protocol (BGP) [18]. Στην διαδρομή που διανύουν τα δεδομένα από τον Server μιας ιστοσελίδας μέχρι τον Η/Υ του χρήστη θα συναντήσουν αρκετές φορές BGP το οποίο καθορίζει την βραχύχρονη διαδρομή των δεδομένων. Η λειτουργά του BGP περιορίζεται στο να «δείχνει τον δρόμο» στα δεδομένα και όχι να ελέγχει την εγκυρότητα και ορθότητα τους. Αυτός είναι και ο λόγος που αποτελεί ευάλωτο πρωτόκολλο για κακόβουλες επιθέσεις.

3) Το τρίτο ευπρόσβλητο τμήμα του Διαδικτύου αφορά την κρυπτογράφηση των δεδομένων. Τα δεδομένα που διακινούνται στο Ίντερνετ δεν είναι κρυπτογραφημένα επιτρέποντας την πρόσβαση σε όλους τους χρήστες.

---

[16] John Naughton , A Brief History of the Future THE ORIGINS OF THE ΊNTEPNET , Phoenix Publications, 2000 p. 88-89

[17] Richard Clarke, Robert. Knake , War The Next Threat to National Security and What to Do About It , Harper Collins E-books ,p. 39-43

[18] Το Border Gateway Protocol (BGP) είναι ένα τυποποιημένο πρωτόκολλο εξωτερικής δρομολόγησης που επιτρέπει την δρομολόγηση πακέτων και την ανταλλαγή πληροφοριών προσβασιμότητας μεταξύ αυτόνομων συστημάτων στο διαδίκτυο. Το BGP ανήκει στην κατηγορία των πρωτοκόλλων διανύσματος μονοπατιού (Path Vector) και οι αποφάσεις δρομολόγησης βασίζονται στα διαθέσιμα μονοπάτια δρομολόγηση https://el.wikipedia.org/wiki/Border_Gateway_Protocol

Πλέον πολλές ιστοσελίδες χρησιμοποιούν κρυπτογραφημένα δεδομένα όταν γίνεται σύνδεση του χρήστη με σκοπό την προστασία των κωδικών του.

Εν τούτοις , εξαιτίας του μεγάλου κόστους , από τη στιγμή της σύνδεσης και μετά παύει η κρυπτογράφηση των δεδομένων και το δίκτυο γίνεται για κόμη μία φορά μη ασφαλές.

4) Το τέταρτο ευπαθές σημείο του Ίντερνετ αφορά το λογισμικό (software), με το οποίο λειτουργούν οι Η/Υ. Η δομή του λογισμικού είναι τέτοια , που δεν αναγνωρίζει από μόνο του τα κακόβουλα προγράμματα με αποτέλεσμα το βάρος της ασφάλειας να πέφτει όλο πάνω στον χρήστη. Σε περίπτωση που ο χρήστης υποπέσει στο σφάλμα να κατεβάσει ή να ανοίξει κάποιο αρχείο με κακόβουλο λογισμικό τότε υπάρχει ο κίνδυνος υποκλοπής στοιχείων, τραπεζικών λογαριασμών και απάτης.

5) Το πέμπτο και τελευταίο ευάλωτο σημείο του Διαδικτύου είναι η αποκέντρωση του ελέγχου. Επηρεασμένοι από τα ρεύματα της εποχής οι εμπνευστές του Διαδικτύου έδωσαν περισσότερη έμφαση στην μη ύπαρξης μιας αρχής παρά στην ασφάλεια.

Όπως αναφέρθηκε το Ίντερνετ αρχικά κατασκευάστηκε για την ανταλλαγή ιδεών και απόψεων των ακαδημαϊκών και όχι να χρησιμοποιείται από εκατομμύρια ανθρώπους σε όλο τον πλανήτη. Το ARPANET βασίστηκε σε 4 αρχές για την ομαλή λειτουργία των Η/Υ που είναι συνδεδεμένοι στο δίκτυο [19]:

1) Κάθε ξεχωριστό δίκτυο θα στέκεται από μόνο του και δεν θα χρειάζονται εσωτερικές αλλαγές προκειμένου να συνδεθεί στο Διαδίκτυο.
2) Εάν το πακέτο των απεσταλμένων δεδομένων δεν φτάσει σύντομα στον προορισμό του τότε θα αποστέλλεται πίσω στην πηγή.
3) Για την σύνδεση των δικτύων θα χρησιμοποιούνται πύλες (gates) και δρομολογητές (routers) τα οποία δεν θα συγκρατούν τα στοιχεία των δεδομένων που διακινούνται.
4) Δεν πρέπει να υπάρχει παγκόσμιος έλεγχος στο επιχειρησιακό επίπεδο.

Αυτές οι βασικές αρχές ισχύουν μέχρι και σήμερα .

4. Η ισχύς στον κυβερνοχώρο

Το πρόβλημα με τις έννοιες όπως η ισχύς και η κυριαρχία στο Διαδίκτυο είναι πως μεταβάλλονται καθώς στον κυβερνοχώρο δεν υπάρχει ένα βασικό στοιχείο : τα σύνορα. Η έλλειψη οριοθέτησης αλλάζει τον τρόπο με τον οποίο τα κράτη αντιλαμβάνονται αυτές τις έννοιες καθώς και τον τρόπο που τις επιδιώκουν.

[19] Richard Clarke, Robert. Knake , War The Next Threat to National Security and What to Do About It , Harper Collins E-books ,p. 43

Το πώς αντιλαμβάνεται την ισχύς ένα κράτος στον κυβερνοχώρο εξαρτάται από το πώς αντιλαμβάνονται τον ίδιο τον κυβερνοχώρο. Από την μία πλευρά αν θεωρηθεί ότι ο κυβερνοχώρος έχει τα χαρακτηριστικά ενός γεωγραφικού χώρου τότε του αποδίδονται πολλές από τις ιδιότητες ενός φυσικού χώρου με αποτέλεσμα να επηρεάζει τον τρόπο με τον οποίο τα κράτη επιδιώκουν τα συμφέροντα τους μέσα σε αυτόν. Από την άλλη πλευρά, αν τα κράτη επικεντρωθούν στην έλλειψη συνόρων που χαρακτηρίζει τον κυβερνοχώρο , στην ροή των δεδομένων και στις πηγές από τις οποίες διοχετεύονται οι πληροφορίες τότε αντιδρούν πολύ διαφορετικά απέναντι στον κυβερνοχώρο και την πολιτική που ακολουθούν.[20]

Είναι κατανοητό λοιπόν , πως ο κυβερνοχώρος χρησιμοποιείται ως μέσο επιρροής. Οι θεσμοί πολλάκις λειτουργούν ως εργαλείο στα χέρια των κρατών για την παραγωγή ισχύος. Παρόλ' αυτά, οι θεσμοί δεν είναι τα μόνα εργαλεία που χρησιμοποιούν τα κράτη αλλά οποιαδήποτε πηγή μπορούν να εκμεταλλευτούν με στόχο την επίτευξη των στρατηγικών τους στόχων.[21]

Εντούτοις, το στοιχείο που επηρεάζει περισσότερο την χάραξη πολιτικής στον κυβερνοχώρο είναι η σχέση του κράτους με τους άλλους παίκτες που δρουν στον κυβερνοχώρο. Τα κράτη παραμένουν ισχυροί παίκτες αλλά στο Δίκτυο καλούνται να ανταγωνιστούν με ένα μεγάλο εύρος οντοτήτων- μεγαλύτερο από αυτό του Διεθνούς Συστήματος- που καρπώνονται τις ευκαιρίες που προσφέρει ο κυβερνοχώρος για το δικό τους όφελος. Το πώς αντιλαμβάνονται τα κράτη τους άλλους παίκτες είναι ικανό να καθορίσει την στρατηγική της χώρας και να τα βοηθήσει να διακρίνουν τις απειλές. Η δυσκολία που πηγάζει από την δομή του κυβερνοχώρου είναι ότι στο διαδίκτυο δεν μπορεί να βρεθεί με απόλυτη σιγουριά η πηγή των απειλών.

Γι' αυτό το λόγο , τα κράτη με τα δεδομένα που τους δίνει η αρχιτεκτονική του κυβερνοχώρου προσπαθούν να ενισχύσουν την ισχύ τους και να επιδιώξουν όσο πιο αποτελεσματικά είναι δυνατό τα συμφέροντα τους.

5. Η κυριαρχία στον κυβερνοχώρο

Όπως αναφέρθηκε ένα από τα προβλήματα που προκύπτουν όσον αφορά τον κυβερνοχώρο είναι η οριοθέτηση. Είναι λογικό πως όταν δεν υπάρχει γεωγραφικός χώρος , δεν υπάρχουν σύνορα και κατ' επέκταση δεν υφίσταται εδαφική κυριαρχία [22].

[20] David Betz, Tim Stevens, cyberspace and the state toward a strategy for cyber-power ,iiss , November 2011, p.37-39

[21] Ibid p.46-47

[22] David Betz, Tim Stevens, cyberspace and the state toward a strategy for cyber-power ,iiss , November 2011, p. 58-60

Τα κράτη κάνουν προσπάθειες να μεταφέρουν την κυριαρχία τους στον κυβερνοχώρο , οι οποίες όμως είναι αναποτελεσματικές , καθώς ο αντίκτυπος που έχει ο κυβερνοχώρος στην κυριαρχία πηγάζει περισσότερο από την αλληλεξάρτηση των κρατών λόγω του διακρατικού του χαρακτήρα, της ροής των πληροφοριών και την έλλειψη συνόρων παρά από την γεωγραφική θέση.

Επί παραδείγματι, αν γίνει μια επίθεση από χάκερς οι σέρβερς μπορούν να τοποθετηθούν παντού ανεξαρτήτως της χώρας από την οποία προέρχονται οι επιτιθέμενοι καταργώντας την στενή έννοια της γεωγραφικής θέσης.

Γι αυτό το λόγο ο κυβερνοχώρος αποτελεί πηγή απειλών για την κυριαρχία των κρατών. Για την αντιμετώπιση αυτών των απειλών ,πολλά κράτη προσπαθούν να ελέγξουν τους πολίτες τους και την πρόσβαση αυτών σε πληροφορίες και περιεχόμενα που εν δυνάμει θα αποτελέσουν απειλή για την εσωτερική τάξη του κράτους.

Σύμφωνα με τους David Betz και Tim Stevens υπάρχουν 3 είδη ελέγχου:

Ο έλεγχος της πρώτης γενιάς περιλαμβάνει την πρόσβαση σε συγκεκριμένες πηγές και περιεχόμενο.

Στον έλεγχο δεύτερης γενιάς τα κράτη υιοθετούν μια πολύπλευρη νομική και τεχνική προσέγγιση ώστε να μπορούν να αρνούνται στους πολίτες τους την πρόσβαση σε διάφορες πηγές όποτε κρίνεται απαραίτητο.

Το τελευταίο είδος ελέγχου της τρίτης γενιάς αποτελείται από την χρήση εκστρατειών ενημέρωσης και προπαγάνδας , ελεύθερη παρακολούθηση και συλλογή δεδομένων που επιτρέπουν στα κράτη τον πλήρη έλεγχο των πολιτών τους. Συνήθως αυτό το είδος ελέγχου χρησιμοποιούν κράτη με αυταρχικά καθεστώτα όπως η Μέση Ανατολή , η Κίνα και η Κεντρική Ασία καθώς κυριαρχεί ο φόβος μιας εξέγερσης ή η δράση των ακτιβιστών [23].

Όσον αφορά τα Δυτικά κράτη , χρησιμοποιούν αυστηρότερα μέτρα και ελέγχους στο Διαδίκτυο – υιοθετώντας και μέτρα που εμπίπτουν στον έλεγχο τρίτης γενιάς- με την πρόφαση της τρομοκρατίας .

Συμπερασματικά, με την κυρίαρχη αντίληψη ότι εάν ένα κράτος δεν μπορεί να ελέγξει τι περνάει τα σύνορα του, δεν είναι ικανό να ελέγξει το εσωτερικό του, τα κράτη επιδιώκουν να επιβάλλουν την κυριαρχία τους στον κυβερνοχώρο ανταγωνιζόμενοι όλους τους υπόλοιπους παίκτες.

[23] David Betz, Tim Stevens, cyberspace and the state toward a strategy for cyber-power ,iiss , November 2011, p. 65-66.

ΚΕΦΑΛΑΙΟ 2. ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

1.ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ

i) Γενικά

Οι κυβερνοεπιθέσεις αποτελούν ένα νέο είδος πολέμου είτε αφορούν ιδιώτες είτε αφορούν κράτη. Πλέον , κάθε πολιτική ή στρατιωτική διαμάχη έχει μία 'κυβερνοδιάσταση' ,της οποίας το μέγεθος και ο αντίκτυπος είναι δύσκολο να προβλεφθούν [24] .Εξαιτίας της αρχιτεκτονικής του Διαδικτύου , οι επιτιθέμενοι ανάλογα με το επίπεδο ων γνώσεων τους μπορούν να εκμεταλλευτούν πολλές από τις αδυναμίες του για να βλάψουν τον στόχο τους. Τα είδη των κυβερνοεπιθέσεων ποικίλουν , όπως ποικίλουν οι επιτιθέμενοι, οι στόχοι και οι σκοποί αυτών. Παρακάτω θα αναλυθούν ποιοι μπορούν να αποτελέσουν τους επιτιθέμενους, τα κίνητρα πίσω από τις επιθέσεις αλλά και ποιοι μπορούν να στοχοποιηθούν.

ii) Επιτιθέμενοι

Αρχίζοντας από την ταυτότητα των επιτιθέμενων , είναι ευκολότερο να κατανοηθούν τα κίνητρα και οι στόχοι τους. Σύμφωνα με το Communications-Electronics Security Group της κυβέρνησης του Ηνωμένου Βασιλείου , επιτιθέμενους μπορούν να αποτελέσουν οι κυβερνοεγκληματίες που αναζητούν το κέρδος εξαπατώντας τους χρήστες , οι hackers που αποζητούν την ευχαρίστηση εξαπολύοντας επιθέσεις σε ξένους υπολογιστές, ξένες υπηρεσίες πληροφοριών που έχουν ως στόχο να αποκτήσουν πληροφορίες κυρίως στο στρατιωτικό και οικονομικό τομέα ,οι επιχειρήσεις οι οποίες αποζητούν να αποκτήσουν ανταγωνιστικό πλεονέκτημα έναντι των ανταγωνιστών τους και την τελευταία κατηγορία επιτιθέμενων απαρτίζουν οι hactivists οι οποίοι οδηγούνται κυρίως από πολιτικά κίνητρα και ιδεολογία [25] .

[24] Per Concordian , Volume 2, Number 2, Journal of European Security and Defense Issues ,The Marshall center , September 2011 ,p.24
http://www.marshallcenter.org/mcpublicweb/MCDocs/files/College/F_Publications/perConcordiam/pC_V2N2_en.pdf
[25] Communications-Electronics Security Group, National Technical Authority for Information Assurance, Common Cyber Attacks: Reducing The Impact , 2015, p.4
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf

Οι επιτιθέμενοι δύναται να χρησιμοποιήσουν εργαλεία που βρίσκονται ήδη διαθέσιμα στο Ίντερνετ και αποτελούν τεχνικές πιο απλές στην χρήση και την λειτουργία τους. Τα εργαλεία αυτά αρχικά κατασκευάστηκαν για να χρησιμοποιηθούν από τους τεχνικούς ασφαλείας και η κύρια λειτουργία τους είναι να ανιχνεύουν ευπάθειες και τρωτά σημεία στο λογισμικό συστημάτων και εφαρμογών . Αυτό αποτελεί και το σημείο που εκμεταλλεύονται οι επιτιθέμενοι χρησιμοποιώντας αυτά τα σημεία όχι όμως με σκοπό να τα διορθώσουν αλλά να τα ενισχύσουν και να αποκτήσουν πρόσβαση σε δεδομένα [26]. Οι πιο έμπειροι επιτιθέμενοι , χρησιμοποιούν εργαλεία και τεχνικές που αναπτύσσονται και χρησιμοποιούνται για συγκεκριμένους σκοπούς και γι' αυτό απαιτούν εξειδικευμένες γνώσεις. Η δυσκολία αντιμετώπισης αυτών των λογισμικών έγκειται στο γεγονός ότι επειδή αποτελούν εξ αρχής δημιουργήματα των επιτιθέμενων δεν είναι γνωστά από τις εταιρίες ανάπτυξης αντιικών προγραμμάτων με αποτέλεσμα να καθίσταται πιο εύκολο για τους επιτιθέμενους να μολύνουν διάφορους και περισσότερους υπολογιστές με το λογισμικό τους μέχρι την αντιμετώπισή τους.

Οι επιτιθέμενοι εκμεταλλεύονται κυρίως τα χαρακτηριστικά του κυβερνοχώρου και τις αδυναμίες του. Η ανωνυμία όπως και η ανεπαρκής ασφάλεια στο διαδίκτυο αποτελούν τις πρώτες ιδιότητες που επιτρέπουν στους επιτιθέμενους να επιτίθονται. Επίσης, διάφορα σφάλματα στον σχεδιασμό διαφόρων λογισμικών τους επιτρέπουν να εκμεταλλευτούν ευπάθειες που μπορεί να προκύπτουν από αυτά και να πραγματοποιούν τις επιθέσεις τους. Αντίθετα με τα σφάλματα που αποτελούν ακούσιες λειτουργίες σε ένα σύστημα , οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν προς όφελος τους και τα χαρακτηριστικά ενός λογισμικού τα οποία αρχικά είχαν δημιουργηθεί από τους κατασκευαστές για να βελτιώσουν την εμπειρία του χρήστη και την αντιμετώπιση των προβλημάτων που ίσως παρουσιαστούν. Ωστόσο , ακόμα και αν ένα σύστημα δεν διαθέτει τίποτα από τα παραπάνω που μπορεί να αποτελέσουν βοηθητικά εργαλεία για τον επιτιθέμενο , υπάρχει η περίπτωση του σφάλματος στο οποίο θα υποπέσει ο χρήστης. Ένα σύστημα ορθά σχεδιασμένο και εφαρμοσμένο προσεκτικά είναι ικανό να ελαχιστοποιήσει τις ευπάθειες που προκύπτουν από την έκθεση του στο Διαδίκτυο. Εντούτοις, ένας άπειρος χρήστης που δεν διαχειρίζεται σωστά το λογισμικό μπορεί να προκαλέσει σημεία τρωτότητας [27]. Γενικότερα , η συμπεριφορά του χρήστη διαδραματίζει μεγάλο ρόλο , αφού δύναται να αποτελέσουν πηγή ευπαθειών. Ακόμα κα έμπειροι χρήστες μπορεί να υποπέσουν σε καλοστημένες παγίδες δίνοντας προσωπικά δεδομένα ή κωδικούς σε hackers που θα τους χρησιμοποιήσουν για απάτες.

[26] Ibid p.4

[27] Communications-electronics security group, national technical authority for information assurance, common cyber attacks: reducing the impact , 2015, p.4 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf

iii) Είδη Κυβερνοεπιθέσεων

Συνήθως οι κυβερνοεπιθέσεις χωρίζονται σε 2 κατηγορίες . Από τη μια πλευρά υπάρχουν οι επιθέσεις που δεν έχουν συγκεκριμένο σκοπό αλλά στοχεύουν στο να μολυνθούν όσο το δυνατόν περισσότεροι χρήστες . Δεν ενδιαφέρονται για την ταυτότητα του χρήστη ούτε για οποιοδήποτε άλλο χαρακτηριστικό του αλλά μόνο για την εκμετάλλευση αυτού με σκοπό το οικονομικό όφελος. Τέτοιου είδους επιθέσεις αποτελούν το phising [28] , το waterholder [29] και το ransomware [30]. Από την άλλη πλευρά , οι στοχευμένες επιθέσεις έχουν συγκεκριμένο στόχο και διαφορετικό κίνητρα. Σε αυτού του είδους τις επιθέσεις περιλαμβάνονται το pear-phising [31] και η και η κατασκευή ενός botnet [32],προκειμένου να υπάρξει μια DDOS [33] επίθεση. Και στις δύο κατηγορίες μπορούν να συμπεριληφθούν όλοι οι τύποι των κακόβουλων λογισμικών όπως οι ιοί (viruses) , τα σκουλήκια (warms) , τα λογισμικά κατασκοπείας (spyware) και τα προγράμματα Trojan [34].

iv) Σκοποί των κυβερνοεπιθέσεων

Οι σκοποί των επιτιθέμενων είναι άρρηκτα συνδεδεμένοι με την ταυτότητα τους και τον στόχο τους. Η κατασκοπεία αποτελεί ένα βασικό σκοπό των επιτιθέμενων είτε ιδιωτών είτε κρατών. Καθημερινά, υποκλέπτονται τεράστιες ποσότητες δεδομένων από διάφορα δίκτυα. Η κατασκοπεία αποτελεί ένα από τους κύριους σκοπούς των επιτιθέμενων , κυρίως των Υπηρεσιών πληροφοριών των κρατών , καθώς μπορεί να παρέχει στο κράτος χρήσιμες πληροφορίες για άλλα κράτη τόσο στο στρατηγικό επίπεδο , όσο στο οικονομικό. Η κατασκοπεία χρησιμοποιείται επίσης , για την παρακολούθηση του στρατού των άλλων χωρών και τον τρόπο λειτουργίας και οργάνωσης αυτών. Άλλη χρήση της κατασκοπείας μπορεί να βρεθεί στον τεχνολογικό τομέα . Στην σημερινή εποχή , που χαρακτηρίζεται ως εποχή της τεχνολογίας είναι λογικό πως η τεχνολογική υπεροχή επιφέρει πολλαπλά οφέλη για επιχειρήσεις και κράτη. Όποτε η κλοπή τεχνολογικών επιτευγμάτων και πατεντών ή προσχεδίων αυτών αποτελεί συχνή πρακτική που εφαρμόζουν κυβερνήσεις και επιχειρήσεις .

[28] Στέλνονται e-mails σε ένα μεγάλο αριθμό χρηστών ζητώντας τους ευαίσθητα προσωπικά δεδομένα .
[29] Δημιουργείται ένα ψεύτικο site παρόμοιο με το αυθεντικό με σκοπό να εξαπατήσει τον χρήστη.
[30] Κρυπτογράφηση δεδομένων του χρήστη με σκοπό την απόσπαση χρηματικού ποσού για να αποκρυπτογραφηθούν
[31] Σαν το phising αλλα στην συγκεκριμένη περίπτωση τα mails στέλνονται σε συγκεκριμένο χρήστη
[32] Δίκτυο υπολογιστών το οποίο ελέγχεται εξ αποστάσεως
[33] Distributes Denial of Service- επίθεση άρνησης υπηρεσιών
[34] IT Governance Ltd. , How cyber criminals work
https://www.itgovernance.co.uk/what-is-cybersecurity

Η κλοπή και η αντιγραφή αυτών μπορεί να επιφέρει καινούργια δυναμική στην λειτουργία και οργάνωση ενός κράτους , όπως και στρατιωτική υπεροχή , όσον αφορά τα κράτη, ενώ σε μία επιχείρηση μπορεί να επιφέρει ανταγωνιστικό πλεονέκτημα έναντι των ανταγωνιστών της , με αποτέλεσμα το κέρδος και την επιβίωση της επιχείρησης στην αγορά. Η προπαγάνδα αποτελεί έναν ακόμη από τους σκοπούς των κυβερνοεπιθέσεων. Προερχόμενη συνήθως από άλλες χώρες ή από εσωτερικούς αντιπάλους της κυβέρνησης, έχει ως σκοπό την διάδοση ψευδών ή μη πληροφοριών με σκοπό την χειραγώγηση του κοινού. Επιπροσθέτως , οι επιτιθέμενοι συχνά τροποποιούν τα δεδομένα των στόχων τους για να τους παραπλανήσουν. Αυτή η πρακτική μπορεί να έχει ως αποτέλεσμα είτε την προπαγάνδα , είτε την δυσλειτουργία των συστημάτων στα οποία βασίζονται οι υπηρεσίες ενός κράτους ή μιας επιχείρησης. Στην πιο ακραία μορφή της αυτή η μέθοδος μπορεί να χρησιμοποιηθεί για να στρεβλώσει τα δεδομένα σε εξελιγμένα όπλα.

Τέλος, πολλοί επιτιθέμενοι , στοχεύουν στον να αποκτήσουν τον έλεγχο των υποδομών. Το δίκτυο ηλεκτροδότησης ή άλλες παρόμοιες υποδομές διακοπούν οι διαστρεβλωθούν δύναται να επιφέρουν μεγάλες καταστροφές τόσο στον εξοπλισμό όσο και στο λογισμικό[35] .

2. Κυβερνοασφάλεια

Η στρατηγική , η πολιτική και οι πρακτικές που χρησιμοποιούνται στις δραστηριότητες που λαμβάνουν χώρα στον κυβερνοχώρο και στοχεύουν στην μείωση των απειλών και ευπαθειών, στην αποτροπή κακόβουλων δράσεων και στην αντιμετώπιση διάφορων περιστατικών αποτελούν την κυβερνοασφάλεια [36]. Στην κυβερνοασφάλεια εκτός από την προστασία των δραστηριοτήτων των χρηστών του Ίντερνετ , περιλαμβάνεται επίσης η προστασία των υποδομών όπως οι Η/Υ , οι servers , τα κινητά τηλέφωνα και οποιαδήποτε άλλη συσκευή μπορεί να συνδεθεί στο Δίκτυο [37].

Η κυβερνοασφάλεια αποτελεί πλέον μια από τις βασικές προτεραιότητες των κρατών. Σύμφωνα με το περιοδικό Forbes μέχρι το έτος 2020 θα είναι συνδεδεμένες στο Διαδίκτυο πάνω από διακόσα εκατομμύρια συσκευές παγκοσμίως. Οι συσκευές αυτές θα ανήκουν τόσο σε ιδιώτες όσο και σε κρατικούς φορείς : Η/Υ του δημοσίου τομέα, οπλικά συστήματα , λογισμικά τραπεζών είναι μερικές από τις συσκευές των κρατών ενώ αντίστοιχα για τους ιδιώτες οικιακοί υπολογιστές, αυτοκίνητα, έξυπνα σπίτια ακόμα και τα chips των κατοικίδιων [38].

[35] Per Concordian , Volume 2, Number 2 - Sep 22nd 2011 ,Journal of European Security and Defense Issues ,The Marshall center p.25-26
http://www.marshallcenter.org/mcpublicweb/MCDocs/files/College/F_Publications/perConcordiam/pC_V2N2_en.pdf

[36] National Initiative For Cybersecurity Careers And Studies-Glossary

[37] What is Cyber-Security?, Kaspersky lab
https://usa.kaspersky.com/resource-center/definitions/what-is-cyber-security

[38] Cesar Cerrudo, Why Cybersecurity Should Be The Biggest Concern Of 2017-Forbes Technology Council

Με καινούργιες απειλές να αναδύονται όλο και περισσότερο στον κυβερνοχώρο , τα κράτη προσπαθούν να ισορροπήσουν ανάμεσα σε μία αποτελεσματική στρατηγική κυβερνοασφάλειας , η οποία ταυτόχρονα θα σέβεται την ιδιωτικότητα , τα δικαιώματα και τις ελευθερίες των πολιτών [39].

Η ανάπτυξη του κυβερνοχώρου και των δικτύων ωθεί τις χώρες στον ανταγωνισμό , όχι μόνο στον τομέα της ανάπτυξης προηγμένων λογισμικών αλλά και στην δημιουργία και απόκτηση τεχνολογικών εξοπλισμών.

3. Κυβερνοπόλεμος

Ο κυβερνοπόλεμος έχει καταστεί ο πέμπτος τομέας πολέμου μετά την ξηρά , τον αέρα, την θάλασσα και το διάστημα. [40] Ως κυβερνοπόλεμος ορίζεται η χρήση της τεχνολογίας των ηλεκτρονικών μέσων με στόχο την διακοπή των δραστηριοτήτων ενός κράτους , ειδικά η σκόπιμη επίθεση σε συστήματα πληροφόρησης για στρατηγικούς ή στρατιωτικούς σκοπούς.[41] Στον συμβατικό πόλεμο οι κυβερνήσεις έχουν σχεδόν μονοπώλιο στην χρήση βίας, ενώ στον κυβερνοπόλεμο μπορούν να συμμετέχουν και μη κρατικοί δρώντες. Κυβερνοπόλεμο δεν αποτελούν οι πρακτικές κατασκοπείας και υποκλοπής αλλά αναφέρεται συνήθως σε επιθέσεις σε σημαντικές για το κράτος υποδομές.

Ο κυβερνοπόλεμος θεωρείται ως η απόλυτη μορφή πολέμου. Το κόστος διεξαγωγής του κυβερνοπολέμου είναι πολύ χαμηλότερο από τον συμβατικό. Στον συμβατικό πόλεμο οι κυβερνήσεις δαπανούν πολλούς από τους κρατικούς πόρους σε μετακινήσεις , οπλικά συστήματα και συντήρησης των στρατιωτών. Αντίθετα , στον διαδικτυακό πόλεμο το κόστος εισόδου είναι μηδαμινό , δεν υπάρχουν αποστάσεις και η απόκτηση εξοπλισμού είναι αρκετά φθηνότερη. [42]Επιπροσθέτως, στον κυβερνοχώρο δεν υπάρχει ο κίνδυνος απώλειας ανθρώπινων ζωών και μπορεί να κερδηθεί σχεδόν στιγμιαία. [43] Εξαιτίας του αρχικού σχεδιασμού του κυβερνοχώρου , δεν δόθηκε ιδιαίτερη σημασία στην ασφάλεια , [44] αλλά στην ευκολία του χρήστη,

---

https://www.forbes.com/sites/forbestechcouncil/2017/01/17/why-cybersecurity-should-be-the-biggest-concern-of-2017/#5fadb47a5218

[39] Center for Strategic and International Studies, Cybersecurity https://www.csis.org/topics/cybersecurity-and-technology/cybersecurity

[40] War in the fifth domain, The Economist , http://www.economist.com/node/16478792

[41] https://en.oxforddictionaries.com/definition/cyberwar

[42] Joseph Nye,Cyber Power ,Belfer Center for Science and International Affairs Harvard Kennedy School, 2010 p.3-4

[43]Myriam Dunn Cavelty, As likely as a visit from E.T, 07.01.2011 http://www.theeuropean-magazine.com/133-cavelty/134-cyberwar-and-cyberfear

[44] Joseph Nye,Cyber Power ,Belfer Center for Science and International Affairs Harvard Kennedy School, 2010 p.5

βοηθώντας να κρύβεται ευκολότερα ο επιτιθέμενος πίσω από την ανωνυμία και να είναι προστατευμένος σε περίπτωση εκδίκησης.[45]

Σύμφωνα με τους Clarke και Knake ο κυβερνοπόλεμος μπορεί να καταστρέψει μια ολόκληρη χώρα μέσα σε δεκαπέντε λεπτά , εξουδετερώνοντας όλες τις κρίσιμες υποδομές της, όπως τα οπλικά συστήματα , τις εγκαταστάσεις ενέργειας , την εναέρια κυκλοφορία, τα μέσα μαζικής μεταφοράς , το τραπεζικό της σύστημα και το ηλεκτρικό δίκτυο.[46]

Δεν είναι λίγοι που πιστεύουν πως η έννοια του κυβερνοπολέμου δεν υφίσταται καθώς δεν έχει κανένα κοινό σημείο με τον συμβατικό πόλεμο , ο οποίος επιφέρει βία, καταστροφή , εξαθλίωση και ανθρώπινες απώλειες. Ο κυβερνοπόλεμος δεν μπορεί να επιφέρει τέτοιες τραγικές συνέπειες. Ως εκ τούτου θεωρούν πως με τον κυβερνοπόλεμο όπως και με τα πυρηνικά όπλα , τα κράτη δεν σκοπεύουν να εξαπολύσουν άμεσα μια επίθεση αν αυτή δεν εξυπηρετεί τα συμφέροντα τους και αν το κόστος δεν είναι μικρότερο από το όφελος.[47]

[45] Myriam Dunn Cavelty, As likely as a visit from E.T, 07.01.2011
http://www.theeuropean-magazine.com/133-cavelty/134-cyberwar-and-cyberfear

[46] Richard Clarke, Robert Knake, Cyber War The Next Threat to National Security and What to Do About It, Harper Collins E-books, 2010, p.32

[47] Ibid, p.37

ΚΕΦΑΛΑΙΟ 3. ΚΙΝΑ

1. Υπηρεσίες Πληροφοριών και κατασκοπεία στον Κυβερνοχώρο

i) Στρατός

Για την Κίνα η έννοια των μυστικών υπηρεσιών (intelligence) είναι ριζωμένη στην κουλτούρα της , καθώς εμφανίστηκε πολλά χρόνια πριν στην 'Τέχνη του πολέμου' του Sun Tzu.[48] Ότι η κλασική στρατηγική σκέψη όντως διαμορφώνει την προσέγγιση της Κίνας στην κατασκοπεία φαίνεται στο γεγονός πως όπως στο έργο του Sun Tzu και σε άλλων στοχαστών έτσι και ο PLA δίνει περισσότερη σημασία στην πληροφόρηση στο πεδίο της μάχης , επιδιώκοντας μια γρήγορη νίκη με ελάχιστο κόστος. Η Κίνα έχει στραφεί στα μαθήματα του παρελθόντος , διότι από τον πόλεμο του Βιετνάμ δεν έχει εμπλακεί σε καμία διαμάχη και αυτό αποτελεί αιτία έλλειψης εμπειριών ώστε να διαμορφώσει ένα νέο δικό της δόγμα.[49]

Συνεχίζοντας λοιπόν την παράδοση, το 1983 η Κίνα ιδρύει το Υπουργείο Δημόσιας ασφαλείας , το οποίο λειτούργησε και ως υπηρεσία για την διατήρηση της εσωτερικής ασφάλειας , και ως όργανο συλλογής πληροφοριών από το εξωτερικό με σκοπό πάντα την διασφάλιση της εσωτερικής σταθερότητας . [50] Εκτός από το υπουργείο ασφάλειας , ο κύριος φορέας που είναι υπεύθυνος και διεξάγει κατασκοπεία είναι ο στρατός (PLA) . Το Επιτελείο Γενικών Καθηκόντων (General Staff Department) του PLA κατέχει τεράστιες υποδομές παρακολούθησης που στοχεύουν σε ξένες διπλωματικές επικοινωνίες, στρατιωτικές δραστηριότητες, οικονομικούς φορείς, δημόσια εκπαιδευτικά ιδρύματα και ιδιώτες που αποτελούν πρόσωπα ενδιαφέροντος. Τα δύο κύρια τμήματα του PLA που ασχολούνται με την κατασκοπεία είναι το Δεύτερο Τμήμα (Second Department) και τι Τρίτο Τμήμα (Third Department).[51]

Η κινεζική κατασκοπεία από τότε μέχρι σήμερα έχει συγκεκριμένους στόχους . Πρώτον , η κατασκοπεία και οι μυστικές υπηρεσίες στην Κίνα είναι σημαντικές για την αντιμετώπιση των 'τριών κακών'.

---

[48] Nigel Inkster, Chinese Intelligence in the Cyber Age , Survival: Global Politics and Strategy p. 48

[49] Jacqueline Deal ,China and Cyber security , Information Warfare Doctrine ,Chinese Information War: Historical Analogies and Conceptual Debates, Foreign Policy Research Institute and Long Range Strategy Group p.18-19

[50] Nigel Inkster, Chinese Intelligence in the Cyber Age , Survival: Global Politics and Strategy p. 48

[51] Mark Stokes, China and Cyber security, People's Liberation Army Infrastructure for Cyber Reconnaissance Project 2049 p. 22

Οι τρείς κακές δυνάμεις περιλαμβάνουν την απόσχιση, την τρομοκρατία και τον θρησκευτικό εξτρεμισμό. Δεύτερον , η Κίνα προσπαθεί να αποκτήσει πνευματική ιδιοκτησία από τις χώρες τις Δύσης και κυρίως από τις ΗΠΑ και κυρίως στον στρατιωτικό τομέα , υποκλέβοντας πληροφορίες και σχέδια όπλων υψηλής τεχνολογίας. Ο τρίτος στόχος της Κίνας αφορά τον οικονομικό τομέα και συγκεκριμένα τις ξένες επιχειρήσεις που ανταγωνίζονται τις κινεζικές.[52]

Το Τρίτο τμήμα του Γενικού Επιτελείου Στρατού είναι υπεύθυνο για την παρακολούθηση των τηλεπικοινωνιών των ξένων στρατών και την παραγωγή νέων πληροφοριών από τις πληροφορίες που συγκεντρώθηκαν. Η Κίνα διατηρεί το πιο εκτεταμένο δίκτυο SIGINT(Signal Intelligence) ανάμεσα στις χώρες της Ασίας και του Ειρηνικού. Οι εγκαταστάσεις περιλαμβάνουν αρκετές δεκάδες σταθμούς εδάφους , πλοία, φορτηγά και αερομεταφερόμενα συστήματα [53] . Ο διευθυντής του Τρίτου τμήματος δίνει αναφορά στην Κεντρική Στρατιωτική Υπηρεσία μέσω του αρχηγού του Γενικού Επιτελείου.[54]

Όσον αφορά το Δεύτερο Τμήμα του PLA είναι υπεύθυνο για τη συλλογή στρατιωτικών πληροφοριών. Οι δραστηριότητες του περιλαμβάνουν στρατιωτικές αποστολές σε κινεζικές πρεσβείες στο εξωτερικό και ειδικούς πράκτορες σε ξένες χώρες για την συλλογή πληροφοριών. Παρόλο που παραδοσιακά το Δεύτερο τμήμα είναι υπεύθυνο για την στρατιωτική πληροφόρηση , αρχίζει σταδιακά να επικεντρώνεται στην επιστημονική και τεχνολογική κατασκοπεία στον στρατιωτικό τομέα , συλλέγοντας επιστημονικές και τεχνολογικές πληροφορίες από την Δύση. [55]

Χάρις αυτών των δύο τμημάτων η Κίνα διαθέτει μια μεγάλη εξειδικευμένη κοινότητα κατασκοπείας στον κυβερνοχώρο η οποία έχει επιδείξει ευρέως την δυνατότητα να διεισδύσει με ευκολία σε διάφορους φορείς.[56]

ii) Οικονομία

Η Κίνα χρησιμοποιεί την κατασκοπεία για να μπορέσει να ανταγωνιστεί τους κύριους οικονομικούς της και στρατιωτικούς της αντιπάλους. Αν και χρησιμοποιεί την κατασκοπεία

[52] Nigel Inkster, China and Cyber security , Chinese Intelligence Operations and Transnational Consequences International Institute for Strategic Studies p. 25

[53] https://www.globalsecurity.org/intell/world/china/pla-dept_3.htm

[54] Mark Stokes, China and Cyber security, People's Liberation Army Infrastructure for Cyber Reconnaissance Project 2049 p. 22

[55] FAS (Federation of American Scientists), Second [Intelligence] Department https://fas.org/irp/world/china/pla/dept_2.htm

[56] USA Government Publishing Office, Annual Report , Chapter 2 , Section 3: Chinese Intelligence Services And Espionage Threats To The United State https://www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%202%2C%20Section%203%20-%20China%27s%20Intelligence%20Services%20and%20Espionage%20Threats%20to%20the%20United%20States.pdf

εκτενέστερα στον στρατιωτικό τομέα έχουν παρατηρηθεί φαινόμενα κατασκοπείας και με οικονομικά κίνητρα.

Το πρόγραμμα κατασκοπείας της Κίνας ξεκίνησε με το οικονομικό της άνοιγμα προς την Δύση την δεκαετία του 1980 και αργότερα μεταφέρθηκε και στον κυβερνοχώρο. Το 1986 ο Deng Xiaoping ίδρυσε το πρόγραμμα 863 , το οποίο αποτελούσε μία ακαδημία επιστημών και τεχνολογιών με αποστολή το κλείσιμο του επιστημονικού χάσματος μεταξύ Κίνας και των ανεπτυγμένων οικονομιών σε πολύ σύντομο χρονικό διάστημα. Το πρόγραμμα 863 λάμβανε χρηματοδότηση τόσο για την έρευνα και την ανάπτυξη όσο και για την απόκτηση προηγμένων τεχνολογιών από άλλες χώρες νόμιμα ή παράνομα. Επίσης, ήταν σύνηθες η ΛΔΚ να χρησιμοποιεί τους πολίτες της που ζούσαν ή σπούδαζαν στο εξωτερικό για να συλλέγουν εμπορικά μυστικά. [57]

Σήμερα, εκτός από τα κρατικά όργανα που χρησιμοποιούν την κυβερνοκατασκοπεία, η Κίνα έχει υιοθετήσει μια πολιτική που ενθαρρύνει ή τουλάχιστον ανέχεται την διεξαγωγή κατασκοπείας εκ μέρους κινεζικών εταιριών.[58] Στο ερώτημα γιατί η Κίνα χρησιμοποιεί την κατασκοπεία η απάντηση είναι απλή : πρώτον, δεν υπάρχουν ιδιαίτερα εμπόδια που θα την αποτρέψουν από την κατασκοπεία και έπειτα, η Κίνα διαθέτει υψηλής ποιότητας ανθρώπινο δυναμικό στον τομέα των πληροφοριών και της επικοινωνίας που της επιτρέπει να ασκεί κατασκοπεία.[59]

Για τις εταιρίες η οικονομική κατασκοπεία αποτελεί μια μορφή εξαπάτησης ή κλοπής εμπορικών μυστικών από μια άλλη εταιρία προκειμένου να παραλείψει το στάδιο της έρευνας και ανάπτυξης και να έχει απευθείας κέρδη ενισχύοντας παράλληλα την οικονομία της χώρας στην οποία εδρεύει και δραστηριοποιείται. [60]

Η Κίνα αποτελεί μια αναπτυσσόμενη χώρα με αναδυόμενη οικονομία και είναι φυσικό η κυβερνοκατασκοπεία να αποτελεί ορθολογική συμπεριφορά καθώς της προσφέρει ένα επίπεδο ασφάλειας σε ένα ανασφαλές οικονομικό περιβάλλον.

2. ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Η Κίνα συμπεριλαμβάνεται στις χώρες όπου το Ίντερνετ εγκαταστάθηκε το 1994, δηλαδή πολύ αργότερα από την δημιουργία του και την ευρεία χρήση του από τις ΗΠΑ και τον Δυτικό κόσμο.

[57]Melanie Reid, A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat? , University of Miami Law School Institutional Repository , 5-1-2016 p788-789

[58] Tyler Moore ,Bobby B., China and Cyber Security , The Economics of Information Security: Western Lessons for China? , Lyle School of Engineering, Southern Methodist University p. 13

[59] Dr. Paul Cornish , Professor of International Security, Chinese Cyber Espionage: Confrontation or Co-operation? , University of Bath , April 2012 p. 9

[60] Melanie Reid, A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat? , University of Miami Law School Institutional Repository , 5-1-2016 p 761

Το γεγονός αυτό προκαλεί ανησυχία και ανασφάλεια στην Κίνα , με την μεγαλύτερη ανησυχία της να πηγάζει από την κατάσταση στην βιομηχανία της διαδικτυακής ασφάλειας , η οποία κυριαρχείται από εταιρίες των ΗΠΑ και της ΕΕ.

Η στάση της Κίνας είναι έντονα σκεπτική έναντι εταιριών όπως η INTEL και η WINDOWS καθώς δεν εμπιστεύονται τις δικλείδες ασφαλείας που παρέχουν , και προωθεί την δημιουργία εγκαταστάσεων έρευνας και ανάπτυξης μέσα στις οποίες η Κίνα προσπαθεί να αναπτύξει την δική της πνευματική ιδιοκτησία. [61] Ωστόσο , ακόμη δεν είναι σε θέση να παράγει από την αρχή τέτοιου είδους τεχνολογία με αποτέλεσμα να προωθεί και να ενθαρρύνει ενέργειες για την απόκτηση ξένης τεχνολογίας , την οποία θα τροποποιήσει ελαφριά και θα την οικειοποιηθεί με σκοπό την απόκτηση πνευματικών δικαιωμάτων πάνω σε αυτή.

Το νομοθετικό πλαίσιο της Κίνας αναφορικά με την κυβερνοασφάλεια βασίζεται στο Golden Shield project και κυρίως στην λογική του Great Firewall. Ωστόσο η κυβέρνηση θεώρησε πως η ήδη υπάρχων νομοθεσία δεν αρκεί ώστε να περιορίσει τις κυβερνοεπιθέσεις και τα κρούσματα κυβερνοαπειλών. Από το 2010 η Κίνα επικεντρώνει τις προσπάθειες της στον έλεγχο της πρόσβασης στο διαδίκτυο και της ροής των πληροφοριών. Πιο δραστικά μέτρα εισήγαγε τον Ιούλιο του 2015, με μια σειρά νόμων που αφορούσαν μεγαλύτερους και συχνότερους ελέγχους στα ιδιωτικά δεδομένα. Στα μέσα του 2016 ψηφίστηκε νέα νομοθεσία για τον έλεγχο των δεδομένων στο διαδίκτυο.

Η λογική πίσω από τον καινούργιο νόμο και η άποψη της κυβέρνησης γύρω από την κυβερνοασφάλεια συνοψίζεται στην φράση ότι στο κινεζικό έδαφος το διαδίκτυο είναι υπό την κυριαρχία της Κίνας.[62]

Από την μία πλευρά, ο νόμος του 2016 αποτελεί μια προσπάθεια της Κίνα να ευθυγραμμιστεί με τις παγκόσμιες νόρμες και πρακτικές για την ασφάλεια στον κυβερνοχώρο. Σε σχέση με τις χώρες της Ευρώπης και τις ΗΠΑ , οι κινεζικοί νόμοι δεν έχουν επίσημες απαιτήσεις για την διασφάλιση των δεδομένων , οι οποίες θα συμβάλλουν στην προστασία του δικτύου από το κυβερνοέγκλημα.

Από την άλλη πλευρά, οι εταιρίες εκφράζουν τις ανησυχίες τους για τον καινούργιο νόμο , καθώς απαιτεί συνεργασία με κινέζους αξιωματούχους και την πρόσβαση αυτών σε δεδομένα κατόπιν αιτήματος. Επίσης, στο άρθρο 37 του νόμου αναφέρεται ότι οι φορείς εκμετάλλευσης των δικτύων θα πρέπει να αποθηκεύουν τα δεδομένα τους εντός της ηπειρωτικής Κίνας και επιπλέον τα δεδομένα που αφορούν κινέζους πολίτες και συλλέγονται εντός την Κίνας πρέπει να

[61] Richard Suttmeier, China and Cyber Security , Information Security and the Dynamics of Innovation ,Department of Political Science, University of Oregon p. 12

[62] Jack Wagner, The Diplomat , China's Cyber security Law: What You Need to Know , June 01, 2017https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

φυλάσσονται σε εγχώριους servers και απαγορεύεται η μεταφορά τους στο εξωτερικό χωρίς άδεια. [63] Ωστόσο, οι εταιρίες δεν γνωρίζουν ακόμα όλες τις πτυχές του νομοσχεδίου.[64]

Η Κίνα προσπαθεί να υποβάλλει τις ξένες επιχειρήσεις σε ένα καθεστώς που ισχύει ήδη για τις εγχώριες. Όλες οι κινεζικές επιχειρήσεις έχουν τους servers τους στο Πεκίνο ώστε οι κινεζικές αρχές να έχουν άμεση πρόσβαση στα δεδομένα τους. [65] Το καθεστώς αυτό δημιουργεί περισσότερα εμπόδια και προβληματισμούς στις ξένες εταιρίες καθώς δεν είναι πάντα πρόθυμες να δώσουν τα δεδομένα τους , σκεπτόμενες την αύξηση του κινδύνου απώλειας τους ή ακόμα και παραποίησης τους. Επίσης, θα υπάρξει και οικονομικό κόστος καθώς η συμμόρφωση στον καινούργιο νόμο απαιτεί είτε την επένδυση σε νέους διακομιστές στην Κίνα είτε στην πρόσληψη τοπικού παρόχου διακομιστών , οι οποίοι έχουν ήδη δαπανήσει δισεκατομμύρια για την ίδρυση εγχώριων κέντρων δεδομένων.[66]

Ωστόσο , ακόμα και αν οι ξένες επιχειρήσεις λάβουν όλα τα απαραίτητα μέτρα για να συμμορφωθούν με το νέο νόμο , ο ίδιος ο νόμος δεν αποσαφηνίζει πως θα μπορέσουν οι εταιρίες να αποδείξουν την συμμόρφωση τους.

Όπως φαίνετε , ακόμα και αν οι ξένες εταιρίες έχουν συνηθίσει τους αυστηρούς ελέγχους του Great Firewall, η καινούργια νομοθεσία θα επιφέρει μόνο σύγχυση στις εταιρίες και ικανοποίηση στην κινεζική κυβέρνηση.

3. ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ

Το δίκτυο της Κίνας αντιμετωπίζει μια ποικιλία κινδύνων που απορρέουν από την ιδιοσυγκρασία της , όπως τα διογκωμένα επίπεδα του εγχώριου κυβερνοεγκλήματος , την έντονη εξάρτηση από το δυτικό λογισμικό και τα άνισα καθεστώτα.

Ο βασικός τομέας στον οποίο η κυβέρνηση της Κίνας καλείται να αντιμετωπίσει μια πληθώρα απειλών είναι ο οικονομικός. Οι κινέζοι netizens υποφέρουν από μια ποικιλία απειλών ασφαλείας που στοχεύουν στα οικονομικά τους οφέλη πραγματικά ή εικονικά.

---

[63] Jack Wagner, The Diplomat , China's Cyber security Law: What You Need to Know , June 01, 2017
https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

[64] Wee Sui-Lee, China's New Cyber security Law Leaves Foreign Firms Guessing, The New York Times, May 31, 2017
https://www.nytimes.com/2017/05/31/business/china-cybersecurity-law.html

[65] Michael Anti: Behind the Great Firewall of China, TED Talks
https://www.youtube.com/watch?v=yrcaHGqTqHk

[66] Jack Wagner, China's Cyber security Law: What You Need to Know, The Diplomat , June 01, 2017
https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

Πίσω από αυτές τις διαδικτυακές απειλές κρύβεται μια περίπλοκη υπόγεια εγκληματική οικονομία που υποστηρίζεται από πάρα πολλές διαφορετικές τεχνικές . Αναλύοντας την εγκληματική οικονομία , σημειώνονται τέσσερις αλυσίδες αξίας :

Η πρώτη αναφέρεται στην κλοπή πραγματικών περιουσιακών στοιχείων , στην αφαίρεση δηλαδή χρηματικών ποσών από λογαριασμούς τραπέζης ή πιστωτικές κάρτες .

Η δεύτερη αφορά την διαδικτυακή κλοπή εικονικών αγαθών . Οι ενέργειες αυτές περιλαμβάνουν εικονικές συναλλαγές και εξοπλισμό από κλεμμένους λογαριασμούς διαδικτυακών παιχνιδιών τα οποία έπειτα πωλούνται νε αντάλλαγμα αληθινά χρήματα.

Η τρίτη περιλαμβάνει διαδικτυακούς πόρους και κατάχρηση υπηρεσιών . Συγκεκριμένα αφορά τη αρπαγή διαδικτυακών πόρων , παραβιάζοντας servers και έξυπνες συσκευές όπως τα κινητά τηλέφωνα με απώτερο σκοπό το κέρδος.

Η τέταρτη περιλαμβάνει την πώληση βλαβερών λογισμικών όπως οι ιοί Trojan Horses και εργαλείων επίθεσης στους κυβερνοεγκληματίες καθώς και παροχή εξειδικευμένης εκπαίδευσης σε καινούργιους hackers.

Από τις παραπάνω ενέργειες εκτιμάται ότι η συνολική ζημία στην κινέζικη οικονομία ξεπέρασε τα 5, 36 δισεκατομμύρια RMB . [67]Η κινέζικη οικονομία ζημιώνεται σημαντικά από την παραοικονομία στο διαδίκτυο και δίνει την αφορμή στην κυβέρνηση για αυστηρότερα μέτρα , σφίγγοντας τον κλοιό γύρω από τους πολίτες αυξάνοντας την παρακολούθηση και την κατασκοπεία.

Η εκτίναξη του κυβερνοεγκλήματος στην Κίνα προκλήθηκε κυρίως από την ραγδαία αύξηση της ανεργίας . Η αυξανόμενη ανεργία οδήγησε σε έναν μεγάλο αριθμό άνεργων νέων με άρτια εκπαίδευση και εξειδίκευση ιδιαίτερα στο τομέα της τεχνολογίας, οι οποίοι βρήκαν οικονομική διέξοδο στο κυβερνοέγκλημα. Εκτός από την εκπαίδευση που κατέχουν οι νέοι κυβερνοεγκληματίες είναι και καλά εξοπλισμένοι, με καινούργιες τεχνολογίες. Το γεγονός αυτό αποτελεί απόρροια της επιθυμίας της Κίνας να γίνει μια παγκόσμια υπερδύναμη η οποία θα είναι ικανή να ανταγωνίζεται την Δύση στον τομέα της τεχνολογίας. Ένας τρόπος για να το επιτύχει αυτό ήταν να ενθαρρύνει πολλές επιχειρήσεις και ιδιώτες να αποκτήσουν τις πιο καινούργιες και εξελιγμένες τεχνολογίες .[68]

---

[67] Zhuge Jianwei, Investigating the Chinese Underground Economy of Information Security
Network Research Center, Tsinghua University, and CCERT Team, CERNET Network Center
Gu Lion, TrendMicro Company,Duan Haixin, Network Research Center, Tsinghua University, and CCERT Team, CERNET Network Center, China and Cybersecurity: Political, Economic, and Strategic Dimensions, *Report from Workshops held at the University of California, San Diego April 2012 p.10*

[68] Marin Ivezic, Cybercrime in China:a Growing Threat for the Chinese Economy
https://medium.com/@marinivezic/cybercrime-in-china-a-growing-threat-for-the-chinese-economy-e44a213dcb99

Εκτός από τον οικονομικό τομέα, στο εσωτερικό της η Κίνα καλείται να αντιμετωπίσει και τις επιθέσεις των ακτιβιστών hacker .

Το φαινόμενο του hactivism αποτελεί έναν από τους μεγαλύτερους φόβους της κυβέρνησης καθώς αποτελούν απειλή για την σταθερότητα του καθεστώτος. Οι ακτιβιστές κινέζοι netizens μπορούν να τοποθετηθούν σε δύο κατηγορίες. Η πρώτη αποτελείται από τους hackers που αντιτίθενται στις πρακτικές και την πολιτική της κυβέρνησης και αντιδρούν με επιθέσεις κατά των κυβερνητικών αρχών και φορέων.

Ωστόσο, μεγαλύτερη απειλή για την κυβέρνηση αποτελεί η δεύτερη κατηγορία , που αποτελείται από τους εθνικιστές hackers. Η ανικανότητα της Κίνας να ελέγξει και να απαντήσει σε επιθέσεις που δέχεται από ξένα κράτη ελλοχεύει κινδύνους για την ίδια την χώρα που προέρχονται από του κινέζους εθνικιστές. Αν το κράτος δεν υιοθετήσει μια τόσο εθνικιστική στάση όσο αυτή των hackers ,τότε οι τελευταίοι μπορεί να στραφούν εναντίων της ηγεσίας της ίδιας τους της χώρας , εξαπολύοντας επιθέσεις ως μέσω έκφρασης της δυσαρέσκειας τους.[69] Αυτή η πρακτική βάζει σε κίνδυνο τις σχέσεις της Κίνας με τις άλλες χώρες.

Επιπροσθέτως , πολλά συμβατικά εγκλήματα έχουν μεταφερθεί στο διαδίκτυο. Σε αυτά συμπεριλαμβάνονται οι ηλεκτρονικές απάτες, κυρίως οικονομικές, τα τυχερά παιχνίδια και η πορνογραφία. Τα τυχερά παιχνίδια είτε συμβατικά είτε ηλεκτρονικά απαγορεύονται στην ηπειρωτική Κίνα , αλλά εξαιτίας των ιδιαιτεροτήτων του Ίντερνετ είναι πιο δύσκολο να περιοριστεί μιας και οι ιστοσελίδες είναι νόμιμα εγκατεστημένες σε άλλες χώρες όπου τα τυχερά παιχνίδια δεν αποτελούν παράβαση του νόμου. Οι κινέζοι πολίτες , συνήθως όταν παίζουν online χρησιμοποιούν πιστωτικές κάρτες , με αποτέλεσμα να πέφτουν συχνά θύματα απάτης και υποκλοπής τραπεζικών στοιχείων.

Τέλος, ένα από τα σοβαρότερα κυβερνοεγκλήματα , η πορνογραφία , ταλανίζει όλες τις χώρες και όχι μόνο την Κίνα , η οποία προσπαθεί να την αντιμετωπίσει και να την περιορίσει.

4.ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ

Η ανάπτυξη της κινεζικής στρατηγικής στον κυβερνοχώρο μπορεί να ανιχνευθεί στις αρχές της δεκαετίας του 1990. Μετά την ολοκλήρωση του Πρώτου πολέμου του Κόλπου το 1991 , η κινεζική κυβέρνηση και ο στρατός άρχισαν να μελετούν τον στρατό των Η.Π.Α διότι , οι Η.Π.Α και οι σύμμαχοι τους οργάνωσαν στρατιωτικές επιχειρήσεις συντονισμένες από ηλεκτρονικά μέσα για να νικήσουν τον Ιρακινό Στρατό.

[69] *Jeffrey Kwong, Department of Political Science, UC San Diego*,State Use of Nationalist Cyber Attacks as Credible Signals in Crisis Bargaining China and Cybersecurity: Political, Economic, and Strategic Dimensions, *Report from Workshops held at the University of California, San Diego ,April 2012 p. 32.*

Τότε , όλες οι χώρες ,όπως και η Κίνα θεώρησαν την νίκη των Η.Π.Α , η οποία συνδύαζε τις τεχνολογίες πληροφορίας και τη συμβατική ισχύ , ως επανάσταση στις στρατιωτικές υποθέσεις. Από τότε, το Πεκίνο έχει δημιουργήσει και υλοποιήσει μια πολύπλευρη στρατηγική , ενσωματώνοντας τις ξένες , εγχώριες, στρατιωτικές και οικονομικές πολιτικές, προκειμένου να επιτευχθούν οι εθνικοί στόχοι. [70]

Η Κίνα δανείζεται πολλά στοιχεία από την Τέχνη του πολέμου του Sun Tzu και την ιστορία της , παρόλ ' αυτά οι δύο πρώην συνταγματάρχες του PLA Wang Xiangsui και Qiao Liang εισάγουν μια καινούργια στρατηγική , απορρίπτοντας την ήδη υπάρχουσα η οποία ακολουθείται από τα περισσότερα κράτη. Υποστηρίζουν πως δεν πρέπει μια χώρα να πολεμά έναν πόλεμο με τα όπλα που έχει δημιουργήσει κάποιος άλλος, εν αντιθέσει είναι προτιμότερο να δημιουργεί όπλα που θα ταιριάζουν στον πόλεμο και μετά να χαράσσει την στρατηγική του.[71]

Τα τελευταία χρόνια η κυβέρνηση εργάζεται επιμελώς για να διατηρήσει την άνοδο της στην παγκόσμια γεωπολιτική τάξη. Γεγονότα όπως η πρώτη επανδρωμένη διαστημική πτήση της Κίνας και οι Ολυμπιακοί αγώνες του 2008 , αποτελούν μερικά από τα επιτεύγματα της χώρας που επιβεβαιώνουν την διαρκή προσπάθεια της. [72] Η Κίνα επιδιώκει να διατηρήσει την εσωτερική και περιφερειακή της σταθερότητα ενώ ταυτόχρονα αναπτύσσει την οικονομική , στρατιωτική , επιστημονική ,τεχνολογική και ήπια ισχύ της. Επίσης , επιζητά την ισορροπία μεταξύ της οικονομικής και στρατιωτικής ανάπτυξης γιατί πιστεύει ότι είναι αλληλένδετα.[73]

Υπεύθυνο για τις επιθέσεις σε ηλεκτρονικούς υπολογιστές και δίκτυα και για τον κυβερνοπόλεμο είναι το Τέταρτο τμήμα του Γενικού Επιτελείου Στρατού της Κίνας.[74] Οι επιθέσεις στον κυβερνοχώρο αποτελούν σημαντικό κομμάτι της πολιτικής της Κίνας , καθώς τις θεωρεί συνιστώσες μιας ολοκληρωμένης στρατηγικής για να νικήσει μια τεχνολογικά και αριθμητικά ανώτερη εχθρική στρατιωτική δύναμη.[75]

---

[70] Charles Billo,Welton Chang,Cyber Warfare An Analysis Of The Means And Motivations Of Selected Nation States, Institute For Security Technology Studies At Dartmouth College, November 2004 Revised December 2004, p.28
http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf

[71] Qiao Liang , Wang Xiangsui, Unrestricted Warfare, Beijing: PLA Literature and Arts Publishing House, February 1999 p.21

[72] Charles Billo,Welton Chang,Cyber Warfare An Analysis Of The Means And Motivations Of Selected Nation States, Institute For Security Technology Studies At Dartmouth College, November 2004 Revised December 2004, p.26
http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf

[73] Jason Fritz, How China Will Use Cyber Warfare To Leapfrog In Military Competitiveness, Culture Mandala, Vol. 8, No. 1, October 2008 p.38

[74] Desmond Ball,China's Cyber Warfare Capabilities, ANU Research Publications, 2011 p.38

[75] Charles Billo,Welton Chang,Cyber Warfare An Analysis Of The Means And Motivations Of Selected Nation States, Institute For Security Technology Studies At Dartmouth College, November 2004 Revised December 2004, p.26
http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf

Για αυτό το λόγο το κινέζικο στρατιωτικό δόγμα εστιάζει στον εκσυγχρονισμό. Σύμφωνα με την Λευκή Βίβλο της Κίνας για την εθνική άμυνα , πρέπει να δοθεί έμφαση στην πληροφόρηση του στρατού και στην ικανότητα του να μπορεί να χειρίζεται ανεπτυγμένες τεχνολογίες.[76] Η αναβάθμιση και η εκπαίδευση του στρατού στα ηλεκτρονικά μέσα περιλαμβάνει αυξημένη εκπαίδευση των στρατιωτών στον κυβερνοπόλεμο , την αναδιοργάνωση των στρατιωτικών κλάδων και του συστήματος διακίνησης. Ο PLA στοχεύει στην βελτίωση του δικτύου πληροφοριών ώστε να εξυπηρετεί την στρατιωτική εκπαίδευση και έχει κατασκευάσει περισσότερα εικονικά εργαστήρια , ψηφιακές βιβλιοθήκες και ψηφιακά πανεπιστημιακά μαθήματα για την παροχή εξ ' αποστάσεως εκπαίδευσης και κατάρτισης.

Τα ίδια τα πανεπιστήμια έχουν ενσωματώσει στα προγράμματα σπουδών τους, μαθήματα με αντικείμενο τις κυβερνοεπιθέσεις , την άμυνα, τις μεθόδους των hackers και τον σχεδιασμό και την εφαρμογή ιών. [77]

Αν και η Κίνα διατηρεί απόλυτη μυστικότητα γύρω από τις στρατιωτικές της ενέργειες και τις υπηρεσίες μυστικών υπηρεσιών της , είναι γνωστό πως ο PLA διενεργεί συχνά στρατιωτικές ασκήσεις , οι οποίες συμπεριλαμβάνουν και το ενδεχόμενο ενός κυβερνοπολέμου, με την πρώτη άσκηση να διεξάγεται μόλις το 1997.

Με τα χρόνια , ο κινεζικός στρατός αναπτύσσεται όχι μόνο προς την κατανόηση του στον κυβερνοχώρο και την ικανότητα του σε αυτόν αλλά και στην ανάπτυξη τεχνολογιών σχετικών με τον κυβερνοπόλεμο.

Εκτός από την εκπαίδευση και τον εκσυγχρονισμό , ο PLA προχώρησε και στην στρατολόγηση πολιτών. Για την κινεζική κυβέρνηση οποιοσδήποτε πολίτης μπορεί να χειριστεί υπολογιστή , μπορεί δυνητικά να βοηθήσει στις στρατιωτικές επιχειρήσεις. Στις εγκαταστάσεις του PLA φυλάσσεται αποθεματικός εξοπλισμός ο οποίος θα χρησιμοποιηθεί από κινέζους netizens . Σταδιακά ο PLA θα δημιουργήσει έναν τεράστιο ηλεκτρονικό στρατό χωρίς να δαπανήσει σχεδόν καθόλου χρήματα.[78] Για τους κινέζους netizens δημιουργήθηκε ο πόλεμος – βελονισμός , η παράλυση δηλαδή του εχθρού, όταν γίνεται επίθεση και στοχεύει το αδύναμο σημείο του.

Ο κυβερνοπόλεμος για το Πεκίνο αποτελεί ένα πιθανό σενάριο και γα αυτό εναποθέτει πολλούς πόρους και προσπάθεια στην ανάπτυξη στρατηγικών που θα την ωφελήσουν και θα την καταστήσουν ικανή να αντιμετωπίσει οποιοδήποτε αντίπαλο ανεξαρτήτως ισχύς.

---

[76] Jason Fritz, How China Will Use Cyber Warfare To Leapfrog In Military Competitiveness, Culture Mandala, Vol. 8, No. 1, October 2008 p.42

[77] Ibid p.43

[78] Charles Billo,Welton Chang,Cyber Warfare An Analysis Of The Means And Motivations Of Selected Nation States, Institute For Security Technology Studies At Dartmouth College, November 2004 Revised December 2004, p.32-33
http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf

Για την Κίνα μια αποτελεσματική στρατηγική κυβερνοπολέμου θα μπορούσε να επαναπροσδιορίσει το διεθνές σύστημα και την ισορροπία δυνάμεων. [79]

5. ΣΧΕΣΕΙΣ ΜΕ ΑΛΛΑ ΚΡΑΤΗ

i. ΣΧΕΣΕΙΣ ΜΕ ΤΑΙΒΑΝ

Οι πολιτικές διαφορές των δύο περιοχών δεν θα μπορούσαν να μην μεταφερθούν και στον κυβερνοχώρο. Σε σύγκριση με τις υπόλοιπες χώρες της Ασίας και της περιοχής του Ειρηνικού , η Κίνα και η Ταιβάν είναι εκείνες που δέχονται τις περισσότερες επιθέσεις με κακόβουλα λογισμικά, με την Κίνα να δέχεται τις περισσότερες από την Ταιβάν και αντίστοιχα η Ταιβάν από την Κίνα.[80] Έξαρση επιθέσεων παρατηρείται όταν υπάρχουν εντάσεις στο πολιτικό σκηνικό των δύο περιοχών. Για παράδειγμα , το 1999 ο τότε πρόεδρος της Ταιβάν Teng-hui Lee δήλωσε στο γερμανικό κανάλι Deutche Welle ότι οι σχέσεις μεταξύ Κίνας κα Ταιβάν αποτελούσαν σχέσεις κράτους προς κράτος ή τουλάχιστον ενός ιδιαίτερου κράτους προς κράτος . οι εθνικιστές κινέζοι hackers αντιλήφθηκαν αυτή την δήωση του προέδρου Lee ως μία διακήρυξη ανεξαρτησίας από την Ταιβάν και θέλησαν να εκφράσουν τν αντίδραση και τον θυμό τους μέσω ποικίλων επιθέσεων. Εξαπέλυσαν επιθέσεις σε κρατικές ιστοσελίδες της Ταιβάν , αντικαθιστώντας τες με εικόνες της κινεζικής σημαίας και με πολιτικά συνθήματα που εναντιώνονταν στην ανεξαρτησία της περιοχής. Παρόμοια περιστατικά επιθέσεων δεν αποτελούν εξαίρεση και είναι ικανά να περιγράψουν ακριβώς την ιδιαιτερότητα στις σχέσεις των δύο πλευρών . [81]

Εν τούτοις , οι επιθέσεις δεν προέρχονται μόνο από ακτιβιστές και εθνικιστές οι οποίοι χρησιμοποιούν τον κυβερνοχώρο ως μέσο έκφρασης δυσαρέσκειας αλλά και από κυβερνητικούς φορείς. Η Ταιβάν έχει πολλάκις κατηγορήσει ευθέως την Κίνα για επιθέσεις εναντίον της. Οι περισσότερες από αυτές τις κατηγορίες αφορούν κυρίως την υποκλοπή δεδομένων , τα οποία η Κίνα θα μπορούσε να χρησιμοποιήσει στις μεταξύ τους διαπραγματεύσεις. [82]

Επίσης, σύμφωνα με τον Simon Chang , υπουργό Επιστημών και Τεχνολογίας της Ταιβάν το 2014, η Κίνα χρησιμοποιεί την Ταιβάν ως πεδίο δοκιμών για να πειραματιστεί με καινούργιες τεχνολογίες hacking . [83]

---

[79] Ibid p.25-26
http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf

[80] *Yao-chung Chang,* Cyber Conflict Between Taiwan and China, Strategic Insights • Spring 2011 Volume 10, Issue 1 p.26

[81] *Ibid* p.28

[82] Shannon Tiezzi, Taiwan Complains of 'Severe' Cyber Attacks From China, The Diplomat, August 15, 2014
https://thediplomat.com/2014/08/taiwan-complains-of-severe-cyber-attacks-from-china/

[83] Taipei Times, Cyberattacks from China persist: science minister, Aug 14, 2014

Οι επιθέσεις της Κίνας προς την Ταιβάν δεν εστιάζουν τόσο στον οικονομικό τομέα αλλά στον διπλωματικό και στον στρατιωτικό. Η Κίνα θέλει να επιβεβαιώσει την πολιτική και στρατιωτική της υπεροχή έναντι της Ταιβάν , με την υποκλοπή σημαντικών πληροφοριών και επιθέσεις επίδειξης ισχύος, τόσο στο δίκτυο όσο και στις υποδομές της Ταιβάν.

Επίσημη συνεργασία μεταξύ των δύο δεν υπάρχει . Ωστόσο υπάρχουν ανεπίσημες σχέσεις συνεργασίας μεταξύ των αστυνομιών για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο. Η συνεργασία αυτή έχει ως βάση τις δύο συμφωνίες που έχουν υπογράψει τα δύο μέρη. Η πρώτη είναι η Kimmen Agreement που αφορά τον επαναπατρισμό των διαφόρων κακοποιών και , πιο γενικά αναφέρεται σε ένα πλαίσιο συνεργασίας σε περιπτώσεις εγκληματικών ενεργειών.[84]

Η δεύτερη ονομάζεται Agreement on cross-strait mutual assistance in crime matters , η οποία αναφέρεται και πάλι σε ένα ευρύτερο πλαίσιο συνεργασίας σε περιπτώσεις εγκληματικών ενεργειών . [85] Παρόλ' αυτά σε αυτές τις συμφωνίες δεν αναφέρεται ρητά η συνεργασία σε θέματα κυβερνοεγκλημάτων και η συνεργασία των αστυνομικών αρχών περιορίζεται κυρίως στις οικονομικές απάτες. Η κινεζική κυβέρνηση βοηθά και υποστηρίζει πολλούς απο τους hackers να προβούν σε συγκεκριμένες ενέργειες , αν και εφόσον αυτές εξυπηρετούν τα κρατικά συμφέροντα και το γεγονός αυτό την καθιστά απρόθυμη να συνεργαστεί με την Ταιβάν. Η συνεργασία προωθείται από τις κινεζικές αρχές χωρίς εμπόδια όταν οι hackers δρουν μεμονωμένα και δεν εμπλέκονται με την κυβέρνηση ή όταν δεν εξυπηρετούνται τα εθνικά συμφέροντα.

Η Κίνα με την Ταιβάν χαρακτηρίζονται από έναν χρόνιο ανταγωνισμό ο οποίος αντικατοπτρίζεται και στον κυβερνοχώρο με αμοιβαίες κυβερνοεπιθέσεις , οι οποίες στοχεύουν στην αποδυνάμωση του αντιπάλου και την υπεροχή έναντι αυτού.

ii. ΣΧΕΣΕΙΣ ΜΕ ΗΠΑ

Ο μεγαλύτερος ανταγωνιστής της Κίνας είναι οι ΗΠΑ. Οι ΗΠΑ υποστηρίζουν πως οι περισσότερες επιθέσεις που δέχονται προέρχονται από την Κίνα και βλέπουν την άνοδο της Κίνας ως μία δυνητική απειλή και η Κίνα προσπαθεί με κάθε τρόπο να φτάσει τις ΗΠΑ στους τομείς της τεχνολογίας, της οικονομίας, και του στρατού. Στον κυβερνοχώρο η κατάσταση γίνεται ακόμα πιο περίπλοκη , καθώς οι δύο χώρες έχουν τελείως διαφορετική αντίληψη για τον ίδιο τον κυβερνοχώρο και την λειτουργία αυτού. [86] Αν συγκρίνουμε την Κίνα με τις ΗΠΑ θα βρούμε

---

http://www.taipeitimes.com/News/taiwan/archives/2014/08/14/2003597396

[84] *Yao-chung Chang*, Cyber Conflict Between Taiwan and China, Strategic Insights • Spring 2011 Volume 10, Issue 1 p.28

[85] Chiang, Ping-Kung,Chen Yunlin, The third round of Chiang- Cheng Talks http://ws.mac.gov.tw/001/Upload/OldFile/public/MMO/MAC/crossstraitagreementscc3_ag1.pdf

[86] Kenneth Lieberthal, Peter W. Singer, Cybersecurity and U.S.-China Relations, February 2012 p.3

διαφορές στην συμπεριφορά αναφορικά με την ιδιοκτησία, τον έλεγχο και την ροή των πληροφοριών. Αυτές οι διαφορές προφανώς είναι μία μίξη της φύσης του πολιτικού συστήματος , της οικονομίας , του επιπέδου της οικονομικής ανάπτυξης και των ιστορικών γεγονότων.[87]

Διαφορές εντοπίζονται και στον τομέα της ασφάλειας του κυβερνοχώρου με την Κίνα να επενδύει τόσο στην άμυνα όσο και στην επίθεση , καθώς θεωρεί πως είναι πιο πιθανό να νικήσει έναν αντίπαλο σε έναν κυβερνοπόλεμο παρά σε έναν συμβατικό. Με αυτή την φιλοσοφία ο κινεζικός στρατός έχει προχωρήσει σε αναβάθμιση όλων των στρατιωτικών τεχνολογικών εγκαταστάσεων και στην εκπαίδευση των στρατιωτών πάνω στα σύγχρονα τεχνολογικά μέσα.

Η Κίνα διαθέτει πολλά εντυπωσιακά αμυντικά συστήματα , με το πιο αξιοσημείωτο να είναι η ικανότητα που έχει αναπτύξει , να μπορεί να απομονώνει ολόκληρο το δίκτυο της ηπειρωτικής χώρας από τον παγκόσμιο ιστό.

Οι πύλες από τις οποίες κυκλοφορούν όλες οι εισερχόμενες και εξερχόμενες πληροφορίες , μπορούν , εφόσον απαιτείται, να κλείσουν , απομονώνοντας το δίκτυο της ηπειρωτικής χώρας. Με την ενέργεια αυτή το Πεκίνο αποκτά ένα από τα μεγαλύτερα πλεονεκτήματα , σε ένα επικείμενο κυβερνοπόλεμο, διότι περιορίζει σημαντικά την πρόσβαση του αντιπάλου και υποβαθμίζει την αποτελεσματικότητα των επιθέσεων. [88]Η ικανότητα αυτή προέρχεται από τις πολιτικές της Κίνα και το Great Firewall με το οποίο φιλτράρονται όλες οι πληροφορίες που εισέρχονται και εξέρχονται από την χώρα.

Εν αντιθέσει, ο κυβερνοχώρος των ΗΠΑ διέπεται από την ιδέα της ελεύθερης διακίνησης πληροφοριών , που αποτελεί και τον λόγο της μη ανεπτυγμένης κυβερνοάμυνας. Σημαντικό ρόλο σε αυτό παίζουν και οι ιδιωτικές εταιρίες , που είναι υπεύθυνες για την λειτουργία του Ίντερνετ , οι οποίες δεν έχουν επενδύσει στην δημιουργία μιας ισχυρής κυβερνοάμυνας. Επίσης, Τρωτό σημείο των ΗΠΑ αποτελεί ο μεγάλος βαθμός εξάρτησης που έχει από τα δίκτυα, σε αντίθεση με την Κίνα , η οποία έχει μικρότερο βαθμό εξάρτησης και σε περίπτωση κυβερνοπολέμου είναι ικανή να προστατέψει τις κρίσιμες υποδομές της, για τις οποίες έχει εξασφαλίσει την λειτουργία τους με backup servers.[89]

Μεγάλο αγκάθι στις σχέσεις των δύο χωρών αποτελεί η κατασκοπεία. Η Κίνα θεωρεί πως η κατασκοπεία αποτελεί φυσιολογική πρακτική των ορθολογικών κρατών , καθώς τα δεδομένα κυκλοφορούν ελεύθερα στον κυβερνοχώρο και άρα μπορούν να χρησιμοποιηθούν.

---

[87] Richard Suttmeier, Information Security and the Dynamics of Innovation,
China and Cybersecurity: Political, Economic, and Strategic Dimensions,
Report from Workshops held at the University of California, San Diego April 2012 p.12

[88] George Patterson Manson, 'Cyberwar: The United States and China Prepare For the Next Generation of Conflict', Comparative Strategy, Jul 2014 p. 124

[89] Ibid p 126

Οι δύο κύριοι τομείς στους οποίους η ίνα ασκεί κατασκοπεία ίναι ο οικονομικός και ο στρατιωτικός. Αμερικάνικες εταιρίες υποστηρίζουν πως η κατασκοπεία έχει μεγάλες συνέπειες τόσο στις ίδιες όσο και στην αμερικάνικη οικονομία. Στον στρατιωτικό τομέα η κατασκοπεία θεωρείται πιο αποδεκτή και από τα δύο κράτη. Ο πρώην πρόεδρος των ΗΠΑ , Barack Obama σε συνέντευξη του είχε δηλώσει πως όλες οι χώρες ασχολούνται με την συλλογή πληροφοριών.
Υπάρχει, όμως, μεγάλη διαφορά αν η Κίνα προσπαθεί να ανακαλύψει τα θέματα που συζητάει στην συνάντηση του με τους Ιάπωνες και αν ένας hacker που συνδέεται με την κινεζική κυβέρνηση ή στρατό να επιτεθεί στα συστήματα της Apple για να αποκτήσει τα σχέδια για το τελευταίο της προϊόν. Το τελευταίο είναι κλοπή.[90]
Η στάση της Κίνας έγινε πι ο σκληρή μετά τις αποκαλύψεις του Snowden ότι οι ΗΠΑ κατασκόπευαν Σουηδικές Τράπεζες , κινεζικές εταιρίες τηλεπικοινωνιών και την βραζιλιάνικη εταιρία ενέργειας Petrobras. Οι ΗΠΑ επιμένουν πως ήταν καθαρά για λόγους ασφαλείας και προστασίας των πολιτών. Από την άλλη πλευρά η Κίνα τονίζει την αδικία που επικρατεί στον κυβερνοχώρο, υπογραμμίζοντας πως οι ΗΠΑ έχουν προνομιακή θέση στον κυβερνοχώρο εξαιτίας του πρωταρχικού τους ρόλου στην δημιουργία και ανάπτυξη του. Τονίζουν πως από τους δεκατρείς κύριους διακομιστές που είναι ζωτικής σημασίας για την λειτουργία του Ίντερνετ ως σύνολο, οι δέκα βρίσκονται στις ΗΠΑ και οι υπόλοιποι τρεις σε χώρες που αποτελούν συμμάχους τους , όπως η Ιαπωνία , η Ολλανδία και η Σουηδία.[91]

Η Κίνα δεν αποτελεί την μοναδική χώρα που ενστερνίζεται αυτή την άποψη. Η Ρωσία όπως και πολλά αναπτυσσόμενα κράτη υποστηρίζουν πως το σύστημα μεροληπτεί προς τις ΗΠΑ και τα εμπορικά και πολιτικά της συμφέροντα, ενώ εκείνα εκφράζουν την προτίμηση τους σε ένα πολυπολικό σύστημα με κέντρο τον ΟΗΕ και την Διεθνή Ένωση Τηλεπικοινωνιών.[92]
Οι σχέσεις των δύο χωρών θα μπορούσαν να καλυτερεύσουν αν υπήρχε μια αμοιβαία κατανόηση και εμπιστοσύνη. Θα πρέπει οι δύο χώρες να αποδεχτούν τις διαφορές τους, να συζητήσουν τα προβλήματα που αντιμετωπίζουν , χωρίς να θίξουν θέματα που περιέχουν πολιτικά στοιχεία ευαίσθητα για την κάθε χώρα και να μετατρέψουν τον ανταγωνισμό σε συνεργασία, έχοντας ως βασικό στόχο μόνο το κοινό όφελος.[93]

[90] Adam Segal, Cyberspace: The New Strategic Realm in US–China Relations, Strategic Analysis , 2014 , p.578-579.
[91] Kenneth Lieberthal, Peter W. Singer, Cybersecurity and U.S.-China Relations, February 2012 p.4-5
[92] Adam M. Segal (2014) Cyberspace: The New Strategic Realm in US–China Relations, Strategic Analysis p.580
[93] Kenneth Lieberthal, Peter W. Singer, Cybersecurity and U.S.-China Relations, February 2012 p.23-24

6. ΟΙ ΜΕΓΑΛΥΤΕΡΕΣ ΕΠΙΘΕΣΕΙΣ ΤΗΣ ΚΙΝΑΣ

Οι επιθέσεις της Κίνας συνήθως δεν στοχεύουν σε κρίσιμες υποδομές , αλλά αποτελούν επιθέσεις κυβερνοκατασκοπείας και αποκτήσεις πληροφοριών. Τα τελευταία χρόνια έχει εξαπολύσει εκατοντάδες επιθέσεις με διαφορετικούς στόχους και σκοπούς. Τον Μάρτιο του 2009 αποκαλύφθηκε μια τεράστια επιχείρηση κατασκοπείας, στην οποία δόθηκε το κωδικό όνομα GhostNet. Μετά από έρευνα δέκα μηνών από το κέντρο διεθνών σπουδών Munk του Τορόντο , αποκαλύφθηκε ότι το δίκτυο GhostNet όχι μόνο αναζητούσε πληροφορίες μέσω mail , αλλά περιελάμβανε κακόβουλο λογισμικό ,το οποίο μπορούσε να προκαλέσει στους μολυσμένους υπολογιστές ενεργοποίηση της κάμερας και των μικροφώνων, μετατρέποντάς τους σε συσκευές μαγνητοσκόπησης και καταγραφής οποιωνδήποτε συνομιλιών εντός της εμβέλειας τους.[94]

Η επίθεση υπέκλεψε δεδομένα από υπουργεία και πρεσβείες σε εκατόν τρεις χώρες, αλλά ο κυριότερος στόχος της ήταν το γραφείο του Δαλάι Λάμα στην Ινδία. Το γραφείο του Δαλάι Λάμα αποτελούν τον κόμβο του θιβετιανού κινήματος και είναι υπεύθυνα για τις στρατηγικές επικοινωνίες με παγκόσμιους ηγέτες και άλλους φορείς , και από το 2002 είναι υπεύθυνα και για τον συντονισμό των διαπραγματεύσεων με την Κίνα. [95]

Σύμφωνα με την έρευνα του Munk τα συστήματα κατασκοπείας του GhostNet ελέγχονταν σχεδόν αποκλειστικά από ηλεκτρονικούς υπολογιστές με έδρα την Κίνα [96], δεν είναι απολύτως σίγουρο πως η επίθεση προήλθε από την Κίνα και αν η κινεζική κυβέρνηση κρύβεται πίσω από αυτή. [97]

Το δίκτυο κατασκοπείας GhostNet θεωρείται από τις πιο σημαντικές επιθέσεις καθώς μόλυνε πολλούς υπολογιστές για αρκετό καρό, χωρίς να έχει γίνει αντιληπτό ούτε από τους χρήστες , ούτε επίσης από εξειδικευμένα προγράμματα anti-virus.

Η δεύτερη μεγαλύτερη επίθεση για την οποία έχει κατηγορηθεί η Κίνα είναι στην εταιρία Google. Τον Ιανουάριο του 2010 σε ανακοίνωση της η εταιρία παραδέχτηκε ότι δέχτηκε επίθεση από την Κίνα στα μέσα του Δεκεμβρίου του 2009 , και απέσπασαν πληροφορίες από τους ηλεκτρονικούς υπολογιστές της εταιρίας καθώς και πηγαίο κώδικα.[98]

Σύμφωνα με την Google εκτός από τον κώδικα, οι hackers είχαν πρόσβαση στους λογαριασμούς Gmail ακτιβιστών για τα ανθρώπινα δικαιώματα και επίσης μπόρεσαν να διεισδύσουν στα δίκτυα τριάντα τριών ακόμα επιχειρήσεων και να τους υποκλέψουν δεδομένα.

---

[94] Malcolm Moore, China's global cyber-espionage network GhostNet penetrates 103 countries , The Telegraph, Mar 2009

[95] The SecDev Group Tracking GhostNet: Investigating a Cyber Espionage Network, Mar 28, 2009 https://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

[96] Koelmeyer, Paul, Ghostnet – A Discussion Of Cyber Espionage, May 2009 p.22

[97] Malcolm Moore, China's global cyber-espionage network GhostNet penetrates 103 countries , The Telegraph, Mar 2009

[98] Timothy Thomas, Google Confronts China's "Three Warfares", 2010 p. 101

Όπως στις περισσότερες επιθέσεις στον κυβερνοχώρο , η πηγή της επίθεσης δεν μπορεί να επιβεβαιωθεί με σιγουριά, με αποτέλεσμα να μην μπορούν να προσάψουν άμεσες κατηγορίες στην κυβέρνηση της Κίνας για την εμπλοκή της σε αυτή την επίθεση. Η Google δεν απέκλισε το γεγονός ότι η επίθεση μπορεί να ήταν χορηγούμενη από το κράτος.[99] Εν τούτοις, οι Η/Υ από τους οποίους έγιναν κάποιες από τις επιθέσεις εντοπίστηκαν σε δύο εκπαιδευτικά ιδρύματα της Κίνας , στο Πανεπιστήμιο Jiaotong στην Σαγκάη και στην επαγγελματική σχολή Lanxiang. Πρέπει να σημειωθεί πως το Jiaotong αποτελεί ένα από τα εκπαιδευτικά ιδρύματα που επιδοτήθηκαν από το πρόγραμμα 863 , το οποίο στόχευε στην έρευνα και την ανάπτυξη ακόμα και με αθέμιτα μέσα. Καθηγητές του πανεπιστημίου δεν απέκλειαν να είναι κάποιος μέσα από το πανεπιστήμιο υπεύθυνος για τις επιθέσεις και πως διεξάγεται έρευνα για να διαλεύκανση της υπόθεσης.[100] Αντιθέτως, ο εκπρόσωπος των εξωτερικών υποθέσεων της Κίνας , Hong Lee, είχε δηλώσει πως η κινεζική κυβέρνηση είναι αντίθετη σε τέτοιες πρακτικές και αυτοί που τις εφαρμόζουν θα τιμωρούνται σύμφωνα με τον νόμο. Επιπροσθέτως, τόνισε πως η ίδια η Κίνα είναι θύμα κυβερνοεπιθέσεων και οι υποθετικές κατηγορίες εναντίων της είναι κατασκευασμένες και κρύβουν άλλα κίνητρα.[101]

Η Google δεν έμεινε άπραγη μετά από αυτή την επίθεση. Μετά από λίγο καιρό έκανε άρση της λογοκρισίας και του φιλτραρίσματος των πληροφοριών , με αποτέλεσμα η Κίνα να την κατηγορεί για παραβίαση των νόμων του κράτους.[102]

Το αξιοσημείωτο στην επίθεση αυτή είναι ότι η Google αποτέλεσε την πρώτη εταιρία που παραδέχτηκε δημοσίως ότι δέχτηκε κυβερνοεπίθεση. Πολλές εταιρίες δεν παραδέχονται ότι τα συστήματα ασφαλείας τους έχουν τρωτά σημεία και μπορούν να παραβιαστούν και να παρακαμφθούν ,διότι φοβούνται πως θα φανούν ευάλωτες και θα χαθεί η εμπιστοσύνη που έχει το κοινό σε αυτές. Η δήλωση της Google ενθάρρυνε πολλές εταιρίες να παραδεχτούν ότι έχουν πέσει θύματα κυβερνοεπιθέσεων και να μπορέσουν να διορθώσουν τις αδυναμίες τους.

7. ΑΝΘΡΩΠΙΝΑ ΔΙΚΑΙΩΜΑΤΑ

Οι πολίτες της Κίνας πιστεύουν πως το Ίντερνετ δεν αποτελεί μονάχα ένα μέσο διασκέδασης και ψυχαγωγίας, αλλά το μόνο μέσο που τους επιτρέπει να δημοσιοποιούν αδικίες που έχουν υποστεί

[99] Charles Arthur, Google phishing: Chinese Gmail attack raises cyberwar tensions, The Guardian, June 2011
[100] Timothy Thomas, Google Confronts China's "Three Warfares", 2010 p. 104

[101] Christopher Williams, Peter Foster ,Google Gmail cyber attack: 'Chinese spies had months of access , The Telegraph, June 2011.
[102] Timothy Thomas, Google Confronts China's "Three Warfares", 2010 p. 103

από τις αρχές και να αισθάνονται ότι ακούγονται οι φωνές τους. [103]Σε μια πιο γενική βάση, το Ίντερνετ αποτελεί τον χώρο όπου αναζητούν την διαφάνεια ή την λογοδοσία από το κράτος χωρίς να κινδυνεύουν άμεσα. Η κυβέρνηση τα προηγούμενα χρόνια έδειχνε μια πρωτόγνωρη ανοχή σε αυτή την στάση των πολιτών , αφού ως ένα βαθμό αποτελούσε ένα τρόπο αποκλιμάκωσης των εντάσεων διαφόρων περιστατικών ανάμεσα στους πολίτες και στις αρχές. Εντούτοις , τα τελευταία χρόνια η Κίνα αρχίζει να δημιουργεί ένα ολοένα και πιο ασφυκτικό κλοιό νόμων και μέτρων στον κυβερνοχώρο με απώτερο σκοπό την προστασία της 'κυριαρχίας του Ίντερνετ'.[104]
Τα μέτρα αυτά απειλούν όλο και περισσότερο τα θεμελιώδη δικαιώματα των πολιτών με το κυριότερο να είναι η ελευθερία του λόγου. Εκτός από την αυστηρή λογοκρισία που δέχονται οι πολίτες, η κυβέρνηση ζητά από τις εταιρίες και τους παρόχους εφαρμογών και ιστοσελίδων ,
να κρατούν προσωπικά αρχεία των χρηστών για εξήντα ημέρες , και να διαγράφουν όσα σχόλια δεν εγκρίνονται από την κυβέρνηση.
Επίσης , η κυβέρνηση απαιτεί από το προσωπικό των ιστοσελίδων να παρακολουθούν τα σχόλια και το περιεχόμενο που ανεβάζουν οι χρήστες όλο το εικοσιτετράωρο. Η κυβέρνηση της Κίνας , επιπροσθέτως, διέταξε όλα τα μέσα μαζικής ενημέρωσης να μην προωθούν τον δυτικό τρόπο ζωής, ιδιαίτερα όταν προβάλλονται ψυχαγωγικές εκπομπές.[105]

Το πρόβλημα για την κυβέρνηση της Κίνας γίνεται εντονότερο καθώς οι αντιδράσεις των πολιτών αυξάνονται. Οι καινούργιες μεταρρυθμίσεις που έγιναν από το China Netcasting Services Association (CNSA) τον Ιούνιο του 2017 , οι οποίες αφορούσαν την αναμετάδοση οπτικοακουστικού περιεχομένου στο διαδίκτυο [106], έγιναν γρήγορα αντιληπτές από τους πολίτες της Κίνας, οι οποίοι έσπευσαν να προστατεύσουν τα δικαιώματα τους. Οι συγκεκριμένες μεταρρυθμίσεις δεν έθιγαν μόνο σε πιο γενική βάση τα δικαιώματα των πολιτών ,αλλά πιο συγκεκριμένα έθιγαν τα δικαιώματα και συγκεκριμένων ομάδων όπως των LGTB και των γυναικών. [107]
Η κυβέρνηση της Κίνας προσπαθώντας να περιορίσει αυτές τις αντιδράσεις και να επιβάλλει τον κρατικό έλεγχο δημιούργησε από το 2014, ένα διαδικτυακό κοινωνικό σύστημα επιβράβευσης ,οι οποίες θα παρακολουθούνται και θα βαθμολογούνται είτε θετικά είτε αρνητικά.
Στο συγκεκριμένο σύστημα θα βαθμολογούνται όλες οι συμπεριφορές και οι ενέργειες των πολιτών και θα προκύπτει ένας μέσος όρος βάσει συγκεκριμένων κανόνων που θέτει η

[103] Tania Branigan, How China's internet generation broke the silence, The guardian
https://www.theguardian.com/world/2010/mar/24/china-internet-generation-censorship
[104] Bethany Allen-Ebrahimian, The 'Chilling Effect' of China's New Cybersecurity Regime, Foreign Policy
http://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/
[105] Kenneth Roth, China Events of 2016,Human Rights Watch
https://www.hrw.org/world-report/2017/country-chapters/china-and-tibet
[106] http://www.xinhuanet.com/zgjx/2017-07/01/c_136409024.htm
[107] Cheng Li,Xinyue Zhang, Online regulations and LGBT rights: A test for China's legal system, Brookings
https://www.brookings.edu/opinions/online-regulations-and-lgbt-rights-a-test-for-chinas-legal-system/

κυβέρνηση. Αυτός ο μέσος όρος θα αποτελεί την βαθμολογία των πολιτών και θα καθορίζει για όλους τους πολίτες αν είναι έμπιστοι . Ωστόσο , δεν πρόκειται για ένα απλό σύστημα βαθμολόγησης, καθώς το σκορ θα είναι δημόσιο και θα συγκρίνεται με αυτό των άλλων πολιτών και θα αποτελεί ένα δείκτη αξιοπιστίας ο οποίος θα καθορίζει αν τα παιδιά ενός πολίτη θα γίνουν δεκτά στο σχολείο ή αν ο πολίτης θα προσληφθεί σε μια θέση εργασίας. Σύμφωνα με την κινεζική κυβέρνηση , σκοπός του συστήματος είναι η ενίσχυση της εμπιστοσύνης και το χτίσιμο μιας εθνικής ειλικρίνειας . Προς το παρόν η συμμετοχή στο σύστημα βαθμολόγησης δεν είναι υποχρεωτική για τους πολίτες . Στο σύστημα θα ενταχθούν και οι επιχειρήσεις εκτός από τους ιδιώτες και θα γίνει υποχρεωτικό μέχρι το 2020.[108]

[108] Rachel Botsman , Big data meets Big Brother, Wired
http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

ΚΕΦΑΛΑΙΟ 4. ΣΥΜΠΕΡΑΣΜΑΤΑ

Όπως είναι αντιληπτό , ο κυβερνοχώρος χρησιμοποιείται όλο και περισσότερο από όλες τις χώρες. Εκτός από τις κυβερνήσεις που στις αρχές της δεκαετίας του 1990 αντιλήφθηκαν τον κυβερνοχώρο ως κομμάτι της στρατηγικής τους , τα δίκτυα παίζουν πολύ σημαντικό ρόλο και στην ζωή των πολιτών. Η σύνδεση των Η/Υ σε διάφορους τομείς της ανθρώπινης ζωής (οικονομία, τραπεζικό σύστημα, παιδεία, επικοινωνίες, στρατός)έχει φέρει ριζικές αλλαγές, βοηθώντας στον αυτοματισμό των διαδικασιών , την εκμηδένιση των αποστάσεων και την αύξηση του κέρδους. Τα κράτη έχουν πλέον μεγάλη εξάρτηση από το δίκτυο καθώς έχουν συνδέσει με αυτό όλες τις κρίσιμες υποδομές τους. Επίσης , δίνουν μεγαλύτερη έμφαση στον στρατιωτικό τομέα , αφού ο κυβερνοχώρος επέφερε μεγάλες αλλαγές στις στρατηγικές των χωρών και τον εξοπλισμό τους, αυξάνοντας την ακρίβεια και την αποτελεσματικότητα , μειώνοντας το κόστος.

Ο κυβερνοχώρος αποτελεί ένα πεδίο όπου τα κράτη επιθυμούν να εισέλθουν και να επιβάλλουν την ισχύ τους, όπως θα έκαναν και στον φυσικό χώρο. Τα ιδιαίτερα χαρακτηριστικά του κυβερνοχώρου δεν τους επιτρέπουν ωστόσο να το πράξουν αυτό με τις παραδοσιακές πρακτικές. Οι κυβερνήσεις θα πρέπει να προσαρμόσουν τις πολιτικές τους σε ένα περιβάλλον όπου δεν υπάρχουν σύνορα, οπότε δεν είναι εύκολο να ασκήσουν κυριαρχία και να επιβάλλουν νόμους, το μέγεθος του δεν μπορεί να μετρηθεί και υπάρχουν άπειροι χρήστες που με τα χρόνια αυξάνονται και προστατεύονται από την ανωνυμία που τους προσφέρει το Διαδίκτυο. Το διαδίκτυο αν και δημιουργήθηκε για ακαδημαϊκούς σκοπούς δεν αργήσει να χρησιμοποιηθεί από τον στρατό και έπειτα επεκτάθηκε και στους υπόλοιπους τομείς. Το τίμημα για την ευρεία χρήση του ήταν τα χαμηλά επίπεδα ασφαλείας . Επειδή οι αρχικές του χρήσεις διέφεραν σε μεγάλο βαθμό από τις σημερινές δεν δόθηκε μεγάλη σημασία στην ασφάλεια , καθώς οι χώροι από τους οποίους χρησιμοποιούνταν όπως τα πανεπιστήμια θεωρούνταν ασφαλείς , και δεύτερον οι δημιουργοί του έδωσαν μεγαλύτερο βάρος στην εύκολη πρόσβαση και την ευκολία του χρήστη.

Από την ευρεία χρήση του Διαδικτύου προκλήθηκαν και άλλα τρωτά σημεία, τα οποία προσπαθούν να εκμεταλλευτούν ομάδες χρηστών με κυριότερο στόχο το κέρδος. Τέτοιες ομάδες χρηστών έχουν συνήθως τρεις στόχους: ο πρώτος είναι το οικονομικό όφελος, μέσω της εξαπάτησης του χρήστη και αποσπώντας του χρηματικά ποσά, ο δεύτερος αφορά την προσωπική ευχαρίστηση και ικανοποίηση κα ο τρίτος είναι η έκφραση πολιτικών ιδεών από τους ακτιβιστές. Οι επιτιθέμενοι συνήθως έχουν συγκεκριμένους στόχους και συγκεκριμένα μέσα.

Τα είδη των κυβερνοεπιθέσεων ποικίλουν ανάλογα με τους επιτιθέμενους, με τους στόχους τους και τις προθέσεις τους. Η άμυνα σε αυτές τις επιθέσεις αποτελεί μία από τις βασικές

προτεραιότητες των κρατών . Χωρίς να θίξουν την ιδιωτικότητα και τα δικαιώματα των πολιτών τους , τα κράτη καλούνται να αναπτύξουν αποτελεσματικές πολιτικές κυβερνοασφάλειας.

Όσον αφορά την Κίνα, από τότε που το Διαδίκτυο εγκαταστάθηκε στην χώρα , προσπαθεί με κάθε μέσο να κλείσει την ψαλίδα που έχει δημιουργηθεί με τις ανεπτυγμένες χώρες, στον οικονομικό, στρατιωτικό και τεχνολογικό τομέα. Για να το επιτύχει αυτό έχει αναπτύξει σε μεγάλο βαθμό την κατασκοπεία στον κυβερνοχώρο. Στον στρατιωτικό τομέα, ο κινεζικός στρατός διαθέτει τεράστιες εγκαταστάσεις παρακολούθησης, εξοπλισμένες με τις πιο σύγχρονες τεχνολογίες , και πλέον εκτός από στρατιωτικές και διπλωματικές πληροφορίες, έχει επικεντρωθεί και στην συλλογή πληροφοριών που αφορούν την επιστήμη και την τεχνολογία. Στον οικονομικό τομέα, Η Κίνα χρησιμοποιεί την κατασκοπεία με σκοπό την ενίσχυση και ανάπτυξη της οικονομίας της. Η κυβέρνηση δεν είναι η μόνη που ασκεί οικονομική κατασκοπεία αφού προτρέπει ή τουλάχιστον δεν εμποδίζει και ιδιωτικές επιχειρήσεις να πράξουν το ίδιο, ώστε να αποκτήσουν ανταγωνιστικό πλεονέκτημα έναντι των ανταγωνιστών τους.

Σημαντικό κομμάτι για την Κίνα αποτελεί ο τομέας της κυβερνοασφάλειας. Μία χώρα με την δυναμική της Κίνας καλείται να αντιμετωπίσει μία πληθώρα απειλών , οι οποίες προέρχονται τόσο από το εσωτερικό της όσο και από το εξωτερικό της. Οι εσωτερικές απειλές που αντιμετωπίζει, αφορούν συνήθως κυβερνοεγκλήματα οικονομικής φύσης , καθώς οι πολίτες της πέφτουν συχνά θύματα απάτης. Εντούτοις, μεγαλύτερη απειλή για την χώρα αποτελούν οι επιθέσεις από hackers ακτιβιστές και εθνικιστές οι οποίοι δηλώνουν την δυσαρέσκεια τους για τις αποφάσεις της κυβέρνησης. Η κινεζική κυβέρνηση επιζητά την σταθερότητα στο εσωτερικό της και στο καθεστώς , με αποτέλεσμα να ελέγχει με ακραία μέτρα την ροή των πληροφοριών. Ανέπτυξε το Great Firewall, το οποίο εμπνεύστηκε από το Σινικό Τείχος οποίο προστάτευε την χώρα από τις εξωτερικές απειλές. Το Great Firewall φιλτράρει όλες τις πληροφορίες που κυκλοφορούν στο δίκτυο της Κίνας και λογοκρίνει όποιες δεν είναι κατάλληλες σύμφωνα με το καθεστώς. Επιπροσθέτως, κρατάει έξω από τα όρια της Κίνας τις ιστοσελίδες και τις εφαρμογές των δυτικών εταιριών , αφήνοντας κυρίως τις κινεζικές.

Το Πεκίνο θεωρεί την ασφάλεια ζωτικής σημασίας για το κράτος και της δίνει ιδιαίτερη βαρύτητα. Αποτελεί από τις λίγες χώρες που έχει αναπτύξει αποτελεσματικές στρατηγικές κυβερνοπολέμου και είναι ικανή να νικήσει μια αντίπαλη χώρα που σε έναν συμβατικό πόλεμο δεν θα μπορούσε. Η ικανότητα αυτή της Κίνας βασίζεται στην εκπαίδευση του στρατού πάνω στα τεχνολογικά μέσα, αλλά και στο μικρό ποσοστό εξάρτησης που έχουν οι βασικές τις υποδομές από το δίκτυο. Επίσης, στηρίζεται στην στρατολόγηση εκπαιδευμένων πολιτών , οι οποίοι θα αποτελέσουν ένα άρτιο δυναμικό σε περίπτωση κυβερνοπολέμου.

Όλες οι παραπάνω πρακτικές που αναφέρθηκαν δημιουργούν εντάσεις ανάμεσα στην Κίνα και σε άλλες χώρες, οι οποίες δεν συμφωνούν με αυτές. Η κατάσταση με την Ταιβάν είναι ήδη τεταμένη λόγω των πολιτικών διαφορών που έχουν οι δύο χώρες , οι οποίες αντικατοπτρίζονται και στον κυβερνοχώρο. Η Ταιβάν έχει κατηγορήσει πολλές φορές ευθέως την Κίνα για επιθέσεις, οι οποίες δεν έχουν οικονομικά κίνητρα αλλά κυρίως διπλωματικά. Παρόλ' αυτά , υπάρχουν τομείς στους οποίους οι δύο χώρες συνεργάζονται, προωθώντας το κοινό συμφέρον, ιδιαίτερα στα θέματα που αφορούν την καταπολέμηση του κυβερνοεγκλήματος.

Οι σχέσεις της Κίνας με τις ΗΠΑ είναι πιο περίπλοκες. Η Κίνα ως χώρα μέλος των BRICS υποστηρίζει την πολυπολικότητα του συστήματος, και απορρίπτει την συγκέντρωση ισχύς σε μία μόνο χώρα. Ενοχλείται και θεωρεί αδικία το γεγονός ότι ελέγχουν το Διαδίκτυο αμερικάνικες ιδιωτικές εταιρίες, και επιθυμεί να έχουν μερίδιο σε αυτό και οι υπόλοιπες χώρες. Από την άλλη πλευρά, ΟΙ ΗΠΑ θεωρούν απαράδεκτες τις πολιτικές της Κίνας και την κατηγορούν για καταπάτηση των ανθρωπίνων δικαιωμάτων και ανεξέλεγκτη κατασκοπεία που καταλήγει σε κλοπή. Ο ανταγωνισμός των δύο χωρών προκύπτει περισσότερο από τις διαφορές που έχουν στο καθεστώς διακυβέρνησης, στο επίπεδο της οικονομίας και της τεχνολογίας καθώς και στην διαφορετική αντίληψη του κυβερνοχώρου. Συνεργασία ανάμεσα στις δύο χώρες θα μπορούσε να υπάρξει μόνο αν επικεντρωθούν στα κοινά τους συμφέροντα, αφήνοντας πίσω τις πολιτικές διαφορές τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ξενόγλωσση Βιβλιογραφία

Adam Segal, Cyber Attacks Blurring Borders Between War and Peace, Brink News , June 2016
http://www.brinknews.com/cyber-attacks-blurring-borders-between-war-and-peace/

Adam Segal, Cyberspace: The New Strategic Realm in US–China Relations, Strategic Analysis,2014

Adam Segal, What's the Future of Chinese Hacking?, July 2016
https://motherboard.vice.com/en_us/article/ezpa5w/future-of-chinese-hacking

Andrew Liaropoulos, GREAT POWER POLITICS IN CYBERSPACE: U.S. AND CHINA ARE DRAWING THE LINES BETWEEN CONFRONTATION AND COOPERATION , PANORAMA of global security environment , 2013

Andrew Liaropoulos, Reconceptualising Cyber Security: Safeguarding Human Rights in the Era of Cyber Surveillance, International Journal of Cyber Warfare and Terrorism
Volume 6 - Issue 2 , April-June 2016

Arthur Charles, Google phishing: Chinese Gmail attack raises cyberwar tensions, the Guardian , June 2011 https://www.theguardian.com/technology/2011/jun/01/google-hacking-chinese-attack-gmail

Bethany Allen-Ebrahimian, The 'Chilling Effect' of China's New Cybersecurity Regime, Foreign Policy
http://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/

Center for Strategic and International Studies, Cybersecurity
https://www.csis.org/topics/cybersecurity-and-technology/cybersecurity

Cesar Cerrudo , Why Cybersecurity Should Be The Biggest Concern Of 2017-Forbes Technology Council
https://www.forbes.com/sites/forbestechcouncil/2017/01/17/why-cybersecurity-should-be-the-biggest-concern-of-2017/#5fadb47a5218

Charles Arthur , Google phishing: Chinese Gmail attack raises cyberwar tensions, The Guardian, June 2011

Charles Billo,Welton Chang,Cyber Warfare An Analysis Of The Means And Motivations Of Selected Nation States, Institute For Security Technology Studies At Dartmouth College, November 2004 Revised December 2004
http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf

Cheng Li,Xinyue Zhang, Online regulations and LGBT rights: A test for China's legal system, Brookings
https://www.brookings.edu/opinions/online-regulations-and-lgbt-rights-a-test-for-chinas-legal-system/

China and Cybersecurity:Political, Economic and Strategic Dimensions
Report from Workshops held at the University of California, San Diego April 2012
Christopher Williams ,Peter Foster,Google Gmail cyber attack: 'Chinese spies had months of access , The Telegraph, June 2011

Christopher Williams,Google Gmail cyber attack: 'Chinese spies had months of access' , The Telegraph, June 2011 http://www.telegraph.co.uk/technology/google/8553131/Google-Gmail-cyber-attack-Chinese-spies-had-months-of-access.html

David Betz, Tim Stevens, cyberspace and the state toward a strategy for cyber-power ,iiss , November 2011

Desmond Ball, China's Cyber Warfare Capabilities , ANU Research Publications,2011

Eric Jardine,Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime , Centre for International Governance Innovation ,Chatham House, 2015

FAS (Federation of American Scientists), Second [Intelligence] Department
https://fas.org/irp/world/china/pla/dept_2.htm

Front Matter, Journal of Information Policy 6 ,2016, I-Iv.
http://www.jstor.org/stable/10.5325/jinfopoli.6.2016.fm.

George Patterson Manson, 'Cyberwar: The United States and China Prepare For the Next Generation of Conflict', Comparative Strategy, 2011

Gerald O'Hara,Cyber-Espionage: A Growing Threat to the American Economy
http://commlaw.cua.edu/res/docs/articles/v19/19-1/11-v19-1-O-Hara-Final.pdf

Gu, Lion ,The Mobile Cybercriminal Underground Market in China, Trend Micro Research Paper

International Telecommunications Union (ITU) Facts and Figures 2015 https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

International Telecommunications Union (ITU) Facts and Figures 2016 http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf

IT Governance Ltd. , How cyber criminals work

Jack Wagner,The Diplomat,China's Cyber security Law: What You Need to Know ,2017
https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

Jacqueline Deal,China and Cyber security , Information Warfare Doctrine ,Chinese Information War: Historical Analogies and Conceptual Debates, Foreign Policy Research Institute and Long Range Strategy Group

James Mulvenon,Andrew Yang,The People's Liberation Army As Organization, Reference volume 1.0 , the RAND https://www.rand.org/content/dam/rand/pubs/conf_proceedings/2008/CF182part1.pdf

Jason Fritz,How China Will Use Cyber Warfare To Leapfrog In Military Competitiveness, Culture Mandala, Vol. 8, No. 1, October 2008

Jeffrey Kwong,Department of Political Science, UC San Diego,State Use of Nationalist Cyber Attacks as Credible Signals in Crisis Bargaining China and Cybersecurity: Political, Economic, and Strategic Dimensions, Report from Workshops held at the University of California, San Diego ,April 2012

John Naughton,A Brief History of the Future: T H E ORIGIN S O F TH E INTERNE T , Phoenix Publications , 2000

Joint Publication 1-02 , Department of Defense Dictionary of Military and Associated Terms ,8 November 2010 (As Amended Through 15 February 2016)

Joseph Nye,Cyber Power ,Belfer Center for Science and International Affairs
Harvard Kennedy School, 2010

Kenneth Lieberthal,Peter W. SingerCybersecurity and U.S.-China Relations, February 2012
https://www.brookings.edu/wp-content/uploads/2016/06/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf

Kenneth Roth, China Events of 2016,Human Rights Watch
https://www.hrw.org/world-report/2017/country-chapters/china-and-tibet

Lai Xuejia ,Dawu Gu ,Bo Jin,Yongquan Wang, Hui Li,Forensics in Telecommunications, Information and Multimedia ,Third International ICST Conference,e-Forensics 2010, Shanghai, China, November 11-12, 2010,Revised Selected Papers

M. E. Kabay, Anonymity and Pseudonymity in Cyberspace: Deindividuation, Incivility and Lawlessness Versus Freedom and Privacy Paper presented at the Annual Conference of the European Institute for Computer Anti-virus Research (EICAR), Munich, Germany 16-8 March 1998 ,International Computer Security Association

Magnus Hjortdal,China's Use of Cyber Warfare:
Espionage Meets Strategic Deterrence, CHINA-SEC, Centre for Military Studies, University of Copenhagen, Journal of Strategic Security,Volume IV Issue 2 2011

Malcolm Moore,China's global cyber-espionage network GhostNet penetrates 103 countries , The Telegraph, March 2009

MANDIANT, Exposing One of China's Cyberc Espionage Units,APT1
Marin Ivezic,Cybercrime in China—a Growing Threat for the Chinese Economy
https://medium.com/@marinivezic/cybercrime-in-china-a-growing-threat-for-the-chinese-economy-e44a213dcb99

Mark Stokes,China and Cyber security, People's Liberation Army Infrastructure for Cyber Reconnaissance Project 2049

Melanie Reid,A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing With This Global Threat? , University of Miami Law School Institutional Repository,2016

Miguel Alberto Gomez,AWAKEN THE CYBER DRAGON: CHINA'S CYBER STRATEGY AND ITS IMPACT ON ASEAN
https://www.academia.edu/3082490/Awaken_The_Cyber_Dragon_Chinas_Cyber_Strategy_and_Its_Impact_on_ASEAN

Mike McConnell,Michael Chertoff,William Lynn,China's Cyber Thievery is a National Policy and Must be Challenged, The Wall Street Journal, January 2012,
http://docs.house.gov/meetings/IF/IF00/20130521/100883/HHRG-113-IF00-20130521-SD006.pdf

Myriam Dunn Cavelty , As likely as a visit from E.T, The European Magazine, January,2011
http://www.theeuropean-magazine.com/133-cavelty/134-cyberwar-and-cyberfear

National Initiative For Cybersecurity Careers And Studies-Glossary

Nicholas Thomas,'Cyber Security in East Asia: Governing Anarchy',Asian Security,2009

Nigel Inkster,Chinese Intelligence in the Cyber Age, Survival: Global Politics and Strategy,2013

Oxford Dictionaires , Cyberwar, https://en.oxforddictionaries.com/definition/cyberwar

Paul Adams, Geographical Review, 2010

Paul Cornish, Chinese Cyber Espionage: Confrontation or Co-operation?, Cityforum Discussion Paper, April 2012

Paul Koelmeyer, Paul, Ghostnet – A Discussion Of Cyber Espionage, May 2009

Ping-Kung Chiang, Chen Yunlin, The third round of Chiang- Cheng Talks
http://ws.mac.gov.tw/001/Upload/OldFile/public/MMO/MAC/crossstraitagreementscc3_ag1.pdf

Qiao Liang,Wang Xiangsui,Unrestricted Warfare,PLA Literature and Arts Publishing House, Beijing,February 1999
Rachel Botsman , Big data meets Big Brother, Wired
http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion
Richard Clarke, Robert Knake, Cyber War The Next Threat to National Security and What to Do About It, Harper Collins E-books, 2010,
http://indianstrategicknowledgeonline.com/web/Cyber%20War%20-

%20The%20Next%20Threat%20to%20National%20Security%20and%20What%20to%20Do%20About%20It%20(Richard%20A%20Clarke)%20(2010).pdf

Richard Suttmeier,Professor Emeritus, China and Cyber Security , Information Security and the Dynamics of Innovation ,Department of Political Science, University of Oregon

Rob Knake,Adam Segal, How the Next U.S. President Can Contain China in Cyberspace ,Columbia University, January 2017 https://jia.sipa.columbia.edu/how-next-us-president-can-contain-china-cyberspace

Roger Clarke ,What's 'Privacy'?August 2006

Ronald Deibert Cyber security :The New Frontier , Great Decisions 2012

Scott Warren Harold, Martin C. Libicki, Astrid Stuth Cevallos, Getting to Yes with China in Cyberspace, RAND Corporation, 2016
https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf

Shannon Tiezzi,Taiwan Complains of 'Severe' Cyber Attacks From China, The Diplomat,2014
https://thediplomat.com/2014/08/taiwan-complains-of-severe-cyber-attacks-from-china/

Shirley Hung,, The Chinese Ίντερνετ: Control Through the Layers, October 30, 2012

Shu-ling, Ko Ma praises 1990 Kinmen Agreement, Taipei Times , September 2010
http://www.taipeitimes.com/News/taiwan/archives/2010/09/12/2003482689
Tania Branigan, How China's internet generation broke the silence, The guardian
https://www.theguardian.com/world/2010/mar/24/china-internet-generation-censorship

ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

Χαράλαμπος Γκιώνης,Κυβερνοχώρος - Κυβερνοάμυνα: Χαρακτηριστικά - Στόχοι, On Alert, Οκτώβριος 2013 http://www.onalert.gr/stories/kybernoxwros-kybernoamyna-xarakthristika-stoxoi/29371

Χρήστος Βεράτης, ΚΕΔΙΣΑ , Κυβερνοχώρος-Κυβερνοεπιθέσεις- Κυβερνοάμυνα-Μέρος 1ο & 2ο , ΚΕΔΙΣΑ ,2015 http://kedisa.gr/kybernoxwros-kybernoepitheseis-kybe

ΒΙΝΤΕΟ

Michael Anti, Behind the Great Firewall of China
https://www.youtube.com/watch?v=yrcaHGqTqHk

Jesse Hurley, Cyber security , TEDxReno
https://www.youtube.com/watch?v=tKAzA82Xf-4

Xiao Qiang , From 'fart people' to citizens on China's Ίντερνετ , TEDxLiberdade
https://www.youtube.com/watch?v=hx28EUiKEUc

ΠΑΡΑΡΤΗΜΑ

Συντομεύσεις & επεξηγήσεις χρήσιμων όρων

Επεξηγήσεις χρήσιμων όρων

Border Gateway Protocol (BGP):Ένα τυποποιημένο πρωτόκολλο εξωτερικής δρομολόγησης που επιτρέπει την δρομολόγηση πακέτων και την ανταλλαγή πληροφοριών προσβασιμότητας μεταξύ αυτόνομων συστημάτων στο διαδίκτυο. Το BGP ανήκει στην κατηγορία των πρωτοκόλλων διανύσματος μονοπατιού (Path Vector) και οι αποφάσεις δρομολόγησης βασίζονται στα διαθέσιμα μονοπάτια δρομολόγηση

Botnet :Δίκτυο υπολογιστών το οποίο ελέγχεται εξ αποστάσεως

Domain name:Το ξεχωριστό για κάθε ιστότοπο όνομα, το οποίο κατοχυρώνεται επί πληρωμή και περιέχει λέξεις-κλειδιά που το καθιστούν πιο εύκολο στην αναζήτηση του από τους χρήστες

Golden Shield Project:Το ευρύτερο κινεζικό κυβερνητικό σχέδιο λογοκρισίας και παρακολούθησης Διαδικτύου

Great Firewall: Συμπεριλαμβάνεται στο Golden Shield Project και πρόκειται για μία σειρά νόμων και μέτρων για την παρακολούθηση του Διαδικτύου

Hacker/s:Ένα άτομο που χρησιμοποιεί υπολογιστές, δικτύωση ή άλλες δεξιότητες για να ξεπεράσει ένα τεχνικό πρόβλημα. Ο όρος χάκερ μπορεί να αναφέρεται σε οποιονδήποτε διαθέτει τεχνικές δεξιότητες, αλλά συχνά αναφέρεται σε άτομο που χρησιμοποιεί τις ικανότητές του για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε συστήματα ή δίκτυα για να διαπράξει εγκλήματα

Hactivists/hactivism: Είναι η πρόσβαση ενός χάκερ σε μια ιστοσελίδα ή δίκτυο υπολογιστών σε μια προσπάθεια να μεταφέρει ένα κοινωνικό ή πολιτικό μήνυμα. Το πρόσωπο που εκτελεί την πράξη του hacktivism είναι γνωστό ως hacktivist

Netizens: Χρήστης του Διαδικτύου

Pear-phising: Σαν το phising αλλά στην συγκεκριμένη περίπτωση τα mails στέλνονται σε συγκεκριμένο χρήστη

Phising: Στέλνονται e-mails σε ένα μεγάλο αριθμό χρηστών ζητώντας τους ευαίσθητα προσωπικά δεδομένα

Ransomware: Κρυπτογράφηση δεδομένων του χρήστη με σκοπό την απόσπαση χρηματικού ποσού για να αποκρυπτογραφηθούν

Spam mails: Ανεπιθύμητη αλληλογραφία

Trojan Horses:Ένα είδος κακόβουλου λογισμικού που συχνά συγκαλύπτεται ως νόμιμο λογισμικό.

Waterholder: Δημιουργείται ένα ψεύτικο site παρόμοιο με το αυθεντικό με σκοπό να εξαπατήσει τον χρήστη.

Συντομεύσεις

DDOS: Distributes Denial of Service- επίθεση άρνησης υπηρεσιών. Μια επίθεση DDoS περιλαμβάνει πολλαπλές συνδεδεμένες διαδικτυακές συσκευές, γνωστές ως botnet, οι οποίες χρησιμοποιούνται για να συντρίψουν έναν ιστότοπο .

ISP (Internet Service Provider):Οργανισμοί ή εταιρίες που παρέχουν υπηρεσίες Διαδικτύου

PLA: People's Liberation Army :Ο Στρατός της Λαικής Δημοκρατίας Κίνας

Η /Υ: Ηλεκτρονικός Υπολογιστής

ΛΔΚ: Λαική Δημοκρατία της Κίνας