Ο ΥΒΡΙΔΙΚΟΣ ΠΟΛΕΜΟΣ ΤΟΥ ISIS

Του Ιωάννη Μπαλτζώη*

Ο Υβριδικός Πόλεμος αν και ο όρος αυτός είναι σχετικά νέος, το φαινόμενο είναι τόσο παλιό, όσο και ο Δούρειος Ίππος. Αναφορές υβριδικού πολέμου, έστω και σε νηπιακή μορφή, συναντάμε και **στον Πελοποννησιακό πόλεμο του Θουκυδίδη, αλλά και στην Τέχνη του Πολέμου του Σουν Τσου**. Έτσι θα λέγαμε ότι ο υβριδικός πόλεμος και η υβριδική απειλή (hybrid threat), συνοδεύουν την ανθρωπότητα σε όλη την ιστορική πορεία της και σε άμεση συνάρτηση με τον πόλεμο.

Ως υβριδικός πόλεμος ορίζεται σύμφωνα με τον R. Aron (1966) ότι είναι η χρήση συμβατικών μη συμβατικών, τακτικών- άτακτων, φανερών -συγκεκαλυμμένων μέσων και η εκμετάλλευση όλων των διαστάσεων του πολέμου, σε όλο το μήκος και το πλάτος του, για να καταπολεμηθεί η ανωτερότητα των συμβατικών όπλων, μεθόδων και τακτικών στο πεδίο μάχης. Οι υβριδικές απειλές εκμεταλλεύονται όλο το φάσμα του σύγχρονου πολέμου, δεν περιορίζονται μόνο στα συμβατικά μέσα και άρα στο συμβατικό πεδίο μάχης. Με την χρήση ασυμμετριών, οι υβριδικές απειλές εκμεταλλεύονται τις αδυναμίες του αντιπάλου, περιπλέκοντας με αυτόν τον τρόπο το πεδίο της μάχης. Σύμφωνα με τον σχετικό ορισμό της ΕΕ, **Υβριδική επιχείρηση είναι «συνδυασμός καταναγκαστικής και ανατρεπτικής δραστηριότητας, συμβατικών και μη συμβατικών μεθόδων (π.χ. διπλωματικές, στρατιωτικές, οικονομικές, τεχνολογικές μέθοδοι) που χρησιμοποιούνται με συντονισμένο τρόπο από κρατικούς ή μη κρατικούς παράγοντες για την επίτευξη ειδικών στόχων, παραμένοντας ωστόσο κάτω από το κατώφλι, δηλαδή το όριο, της επίσημης κήρυξης**

πολέμου». Ο αντίστοιχος ορισμός που έχει δώσει το ΝΑΤΟ ορίζει ως υβριδική απειλή **«την προερχόμενη από υπάρχοντα ή μελλοντικό αντίπαλο (κρατικό, μη κρατικό, τρομοκράτες κλπ.) με τη δυνατότητα επίδειξης ή ταυτόχρονης χρήσης συμβατικών και μη συμβατικών μεθόδων για την επίτευξη των στόχων του**»

ISIS. Περίπτωση Μελέτης.

Η απειλή που έθετε το ISIS μέχρι την ήττα του στην Συρία, ήταν πολύ σοβαρή από ποτέ για δύο λόγους: Πρώτον, για την ικανότητά του να διεξάγει ασύμμετρο πόλεμο και, δεύτερον, η ικανότητά του να στρατολογεί ξένους μαχητές και μάλιστα και τα δύο στο αποκορύφωμά τους. Έτσι το μοντέλο του Ισλαμικού Κράτους είναι σημαντικό για ανάλυση , μελέτη και λήψη ανάλογων μέτρων, καθόσον διαπιστώνουμε ότι ο υβριδικός πόλεμος σήμερα είναι ακόμη ισχυρότερος και πιο επικίνδυνος, οπότε αξίζει να μελετήσουμε ως Key Study το μοντέλο ISIS.

Το ISIS , αν και μη κρατικός φορέας, παρουσίασε μια σχεδόν απαράμιλλη ικανότητα για χρήση και λήψη πληροφοριών και αποτελεσματικού ψυχολογικού πολέμου. Το ISIS ήταν ιδιαίτερα έμπειρο στη χρήση των δικτύων των «social media» και ιδιαίτερα το «YouTube», το «Twitter» και το «blog posts», για το σχεδιασμό, την πρόσληψη, την συγκέντρωση χρημάτων, το μάρκετινγκ, κλπ. **Εγκέφαλος αυτού του συστήματος υπό τον Abu Bakr Al-Baghdadi ήταν ο Haji Bakr (Samir Abd Mohamed Al-Khlifawi), πρώην συνταγματάρχης της Αεροπορίας και διευθυντής Πληροφοριών του Σαντάμ Χουσείν.**

<u>EMNI. Η Τρομερή Υπηρεσία Πληροφοριών του ΙΚ.</u>

Μια εξαιρετική και αποκαλυπτική μελέτη δημοσιεύτηκε στην πρώτη έκδοση του διεθνούς επιστημονικού περιοδικού «Perspectives on Terrorism» (Απόψεις Τρομοκρατίας) το έτος 2017 . Αναφέρεται στην άγνωστη μέχρι τότε υπηρεσία πληροφοριών του ΙΚ, γνωστή στα αραβικά ως EMNI , όπου εκτός από εκπληκτικές πληροφορίες για την υπηρεσία αυτή μας παρέχει τα πάντα για την εσωτερική λειτουργία του ΙΚ από τη γέννηση του μέχρι και σήμερα και πως η EMNI είχε βοηθήσει σε αυτό.

Η προέλευση της ΕΜΝΙ αποκαλύφθηκε από σύμπτωση με την ανεύρεση το 2014 εγγράφων, που ανήκαν στον Haji Bakr (Χάτζι Μπακρ), ενός πρώην σμηνάρχου της υπηρεσίας πληροφοριών του Santam Hussein, ο οποίος ήταν ο αρχιτέκτονας και δημιουργός της ΕΜΝΙ. Είχε προηγουμένως φυλακιστεί στις φυλακές Abu Ghraib και στη Βάση Buka, μαζί με τον ηγέτη του ΙΚ Abu Bakr al Baghdadi, όπου εκεί γνωρίστηκαν. Μαζί του και άλλοι πικραμένοι πρώην εθνικιστές αξιωματικοί πληροφοριών του Ιράκ. Ο Bakr σκοτώθηκε τον Ιανουάριο του 2014. Η Υπηρεσία Πληροφοριών της οργάνωσης, ΕΜΝΙ εισχωρούσε αθόρυβα σε μία περιοχή που ο ISIS ήθελε να καταλάβει και συγκέντρωνε πληροφορίες για τις στρατιωτικές και πολιτικές αρχές της περιοχής που είχε στοχεύσει η οργάνωση. Την κατάλληλη στιγμή οι πράκτορες της τρομοκρατικής οργάνωσης που ήταν ήδη μέσα στην περιοχή, υπονόμευαν την τοπική ηγεσία. Έτσι όταν εισέβαλε ο κύριος όγκος των τζιχαντιστών, η κατάρρευσή της ήταν θέμα λίγων ωρών. Τα κεντρικά της ΕΜΝΙ βρίσκονταν στη Συριακή πόλη Αλ-Μπαμπ. Στην ΕΜΝΙ εργαζόταν πολύ μεγάλος αριθμός Μπααθιστών Αξκων, που υπηρετούσαν στις υπηρεσίες πληροφοριών του Σαντάμ Χουσείν.

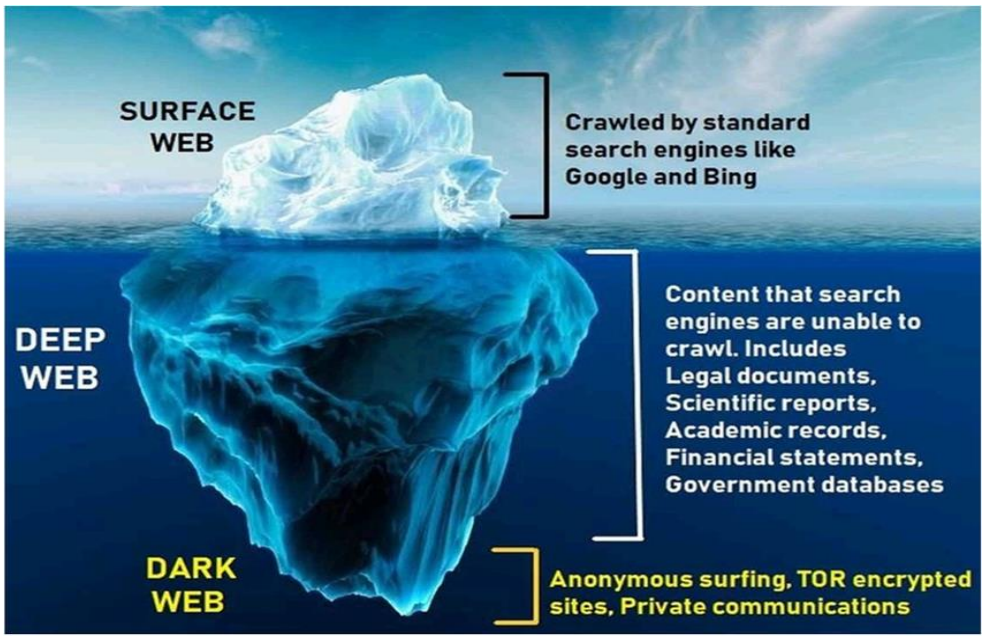
Μέσα Κοινωνικής Δικτύωσης (ΜΚΔ)- Ο Παγκόσμιος Ιστός WWW

Ζούμε σήμερα στην εποχή της «δικτατορίας» των μέσων κοινωνικής δικτύωσης, τα λεγόμενα NEW MEDIA που είναι πανίσχυρα όπλα επιρροής, προπαγάνδας, επικοινωνίας, παραπλάνησης κλπ. Πρόκειται για το «Facebook, το Twitter, το Flickr, το YOUTUBE, το Istangram» κ.α, τα οποία έχουν ξεπεράσει τα μέχρι τώρα παντοδύναμα ΜΜΕ. Είναι σημαντικότατα «εργαλεία» στην διάθεση των πάντων με πολλαπλασιαστικό δίκτυο επικοινωνίας και που χρησιμοποιούνται από οργανώσεις, κρατικές οντότητες, υπηρεσίες, εταιρίες , οργανισμούς και άτομα για διάχυση μηνυμάτων, προώθηση πληροφοριών, απόκτηση δυνατοτήτων μεγαλύτερου ακροατηρίου . Μέσω αυτών μπορείς επίσης να ενημερώσεις, να αποκαλύψεις, να παραπλανήσεις, να αποκρύψεις, να κατευθύνεις να προωθήσεις ιδέες, πράγματα και καταστάσεις και να κινηθείς σε εντελώς διαφορετικά πλαίσια από τα μέχρι τώρα δεδομένα.

Με σχετικά εύκολα πληροφοριακά συστήματα, οι διάφορες οργανώσεις, μπορούν να προκαλέσουν τεράστια ζημιά σε θέματα

οικονομικά, στρατιωτικά, εθνικής ασφάλειας, να προκαλέσουν πανικό, μαζική φοβία, υστερία, πλήγματα στις προσπάθειες ενημέρωσης και αντίδρασης της κοινής γνώμης κα. Μέσω αυτών διεξάγονται σύγχρονες ψυχολογικές και πληροφορικές επιχειρήσεις, ενώ πέραν των παρακρατικών – βίαιων και τρομοκρατικών οργανώσεων,

Ο Παγκόσμιος Ιστός, το γνωστό σε όλους μας www (world-wide web) είναι το Ίντερνετ, το Διαδίκτυο, Η βασική ιδέα του www είναι ο συνδυασμός της τεχνικής των δικτύων υπολογιστών με το υπερ-κείμενο (hypertext), σε ένα δυναμικό και ευκολόχρηστο σύστημα πληροφοριών. Για να καταλάβουμε καλύτερα πως γίνεται η χρήση του διαδικτύου θα αναφερθούμε στην δομή του. Στα παγόβουνα, το 91% του όγκου τους βρίσκεται κάτω από το νερό. Κάτι αντίστοιχο ισχύει και όσον αφορά το ίντερνετ. Το διαδίκτυο , World Wide Web (WWW) χωρίζεται σε τρία μέρη.



Το Surface Web (Επιφανειακός Ιστός), είναι ο παραδοσιακός παγκόσμιος ιστός που όλοι γνωρίζουμε. Περιέχει λίγο-πολύ όλες τις ιστοσελίδες που επισκεπτόμαστε και που χρησιμοποιούμε στις καθημερινές μας επαφές, με εφαρμογές όπως, **Google, Twitter, Facebook, Yahoo, In, Gmail, YouTube, Wikipedia, PCsteps, κλπ , το οποίο όμως είναι το 10% του χρησιμοποιούμενου διαδικτύου**. Κάποιες άλλες ονομασίες που χρησιμοποιούνται για αυτό το επίπεδο του διαδικτύου είναι Common Web, Clearnet, Visible Web, ή Lightnet. Ο επιφανειακός ιστός παρέχει σχετικά χαμηλή ανωνυμία και οι

περισσότεροι ιστότοποι ταυτοποιούν τους χρήστες τους μέσω της διεύθυνσης IP τους.

Το Deep Web (Βαθύς Ιστός) είναι το κομμάτι του διαδικτύου το οποίο δεν ευρετηριοποιείται από τις γνωστές μηχανές αναζήτησης. Τα προσωπικά μας email δεν εμφανίζονται στις μηχανές αναζήτησης, ειδάλλως ο καθένας θα είχε πρόσβαση με μια απλή αναζήτηση στο Google. **Άρα, ο προσωπικός μας λογαριασμός email ανήκει πρακτικά στο Deep Web**. Το ίδιο ισχύει για το προσωπικό μας e-banking, τις ρυθμίσεις του λογαριασμού μας στα social media, το διαχειριστικό περιβάλλον αν έχουμε ένα δική μας ιστοσελίδα κλπ. Εκτός από τους προσωπικούς μας λογαριασμούς, στο Deep Web **ανήκουν και σελίδες στις οποίες έχουμε πρόσβαση μόνο με κάποιον σύνδεσμο. Για παράδειγμα, ένα βίντεο στο YouTube που έχει οριστεί ως "Μη καταχωρισμένο".** Όποιος έχει τον σύνδεσμο του βίντεο μπορεί να το δει κανονικά, ακόμα και αν δεν έχει λογαριασμό στο YouTube. Εξετάζοντας το περιεχόμενο του Deep Web, θα διαπιστώσουμε πως αυτό είναι που περιέχει στην πραγματικότητα όλο το διαδίκτυο. Το μέγεθός του, σύμφωνα με μελέτες, είναι 400 έως 550 φορές μεγαλύτερο από αυτό του Surface Web.

Το Dark Web (Σκοτεινός Ιστός), που θα το συναντήσουμε επίσης ως **Charter Web ή Darknet**, είναι ένα πολύ μικρό υποσύνολο του Deep Web. Το «Dark Web» δεν αποτελεί ένα τόπο, αλλά περισσότερο μια μέθοδο που στοχεύει σε υψηλό επίπεδο διαδικτυακής ανωνυμίας. Αναφέρεται σε ιστοσελίδες που καλύπτουν τις διευθύνσεις IP των διακομιστών, κάνοντας αδύνατο να βρεθεί η ταυτότητα ή η τοποθεσία των χρηστών. Είναι δηλαδή αποτελεσματικά αόρατες. Στο βασικό στάδιο, η ασφάλεια στο «Dark Web» διέπεται από την εμπιστοσύνη και τη σχέση οικοδόμησης που δημιουργεί ο χρήστης σταδιακά. Για παράδειγμα, η είσοδος του χρήστη σε μια ιστοσελίδα «hacking» γίνεται μόνο μέσω πρόσκλησης και ο προσκεκλημένος έχει συστηθεί από άτομο το οποίο είναι ήδη μέλος της κοινότητας. **Το ΙΚ το χρησιμοποιεί στον δυτικό κόσμο για τις επαφές του με συνεργάτες, μοναχικούς λύκους κλπ .** Ο λεγόμενος Σκοτεινός Ιστός είναι το περιεχόμενο του παγκόσμιου ιστού που περιέχει τα Darknet. **Ένα Darknet είναι οποιοδήποτε δίκτυο στον παγκόσμιο ιστό, στο οποίο μπορούμε να έχουμε πρόσβαση με ειδικό λογισμικό,**

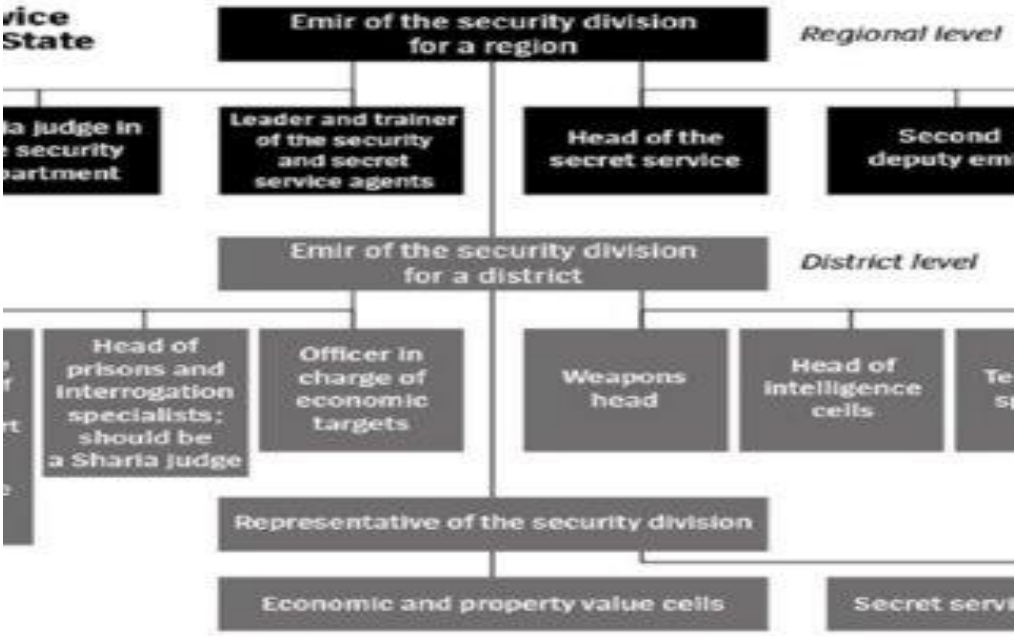
ειδικές ρυθμίσεις και διαπιστευτήρια, ή συγκεκριμένα πρωτόκολλα. Δύο χαρακτηριστικά παραδείγματα Darknet είναι τα δίκτυα peer-to-peer και δίκτυα ειδικά για αυξημένη ανωνυμία, όπως το Tor. Εξαιτίας του πολυεπίπεδου συστήματος κρυπτογράφησης του Dark Web, οι ταυτότητες και οι τοποθεσίες των χρηστών του παραμένουν κρυφές, και ο εντοπισμός τους είναι εξαιρετικά δύσκολος από τις αρχές. Κάποιοι άλλοι, εκμεταλλευόμενοι αυτή την "προστασία", χρησιμοποιούν τον Σκοτεινό Ιστό για κάθε είδους παράνομη δραστηριότητα. Το «Dark Web» σε συνδυασμό με τους «μοναχικούς λύκους» (Lone wolves) αποτελεί έναν επικίνδυνο συνδυασμό για την ειρήνη και τη σταθερότητα της ευρωπαϊκής ηπείρου.

Η Παρακολούθηση και η Χρήση του Διαδικτύου

Το ΙΚ δεν βασίζονταν σε οποιαδήποτε υψηλού επιπέδου τεχνική παρακολούθησης της χρήσης του διαδικτύου, αλλά αντίθετα τοποθετούσε στελέχη του στα «ταχυδρομεία» για να ακούνε και να βλέπουν τι επικοινωνίες γίνονται. Δηλαδή εδώ γίνεται ευρεία και αριστοτεχνική χρήση της αρχαιότερης μεθόδου συλλογής πληροφοριών, του ανθρώπινου παράγοντα, της γνωστής μεθόδου HUMINT (Human Intelligence Η Χισμπάχ, ή αστυνομία του ΙΚ, συχνά σταματούσε όσους είναι στις περιοχές του ΙΚ και έκανε σποραδικούς ελέγχους στις συσκευές κινητής τηλεφωνίας των πολιτών και των ίδιων των μαχητών τους. .

Τα μέλη της ΕΜΝΙ δεν χρησιμοποιούν e-mail ή τηλέφωνα που μπορούν να εντοπιστούν από ξένες υπηρεσίες πληροφοριών. Προτιμούσαν την επικοινωνία πρόσωπο με πρόσωπο. Αυτό είναι δύσκολο, ωστόσο, ειδικά στις περιπτώσεις όπου η ΕΜΝΙ χρειαζόταν να επικοινωνήσει με ξένους μαχητές που είχαν στρατολογηθεί και επιχειρούν εκτός Συρίας και Ιράκ. Αν και τα απλά μέλη του ΙΚ συχνά χρησιμοποιούσαν τηλεφωνικές επικοινωνίες μέσω κρυπτογραφημένων εφαρμογών μέσων κοινωνικής δικτύωσης όπως το Telegram και το Whats App, η ΕΜΝΙ απόφευγε τη χρήση τους. **Τα στελέχη της ΕΜΝΙ βασίζονταν σε προκαθορισμένες επικοινωνίες μέσω βιντεοπαιχνιδιών, κάνοντας χρήση βιντεοκλήσεων ή λειτουργίες συνομιλιών μέσα στο παιχνίδι. Η επικοινωνία μέσα από πλατφόρμες παιχνιδιών είναι εφευρετική, καθώς κρύβονται και αναμιγνύονται ανάμεσα από εκατοντάδες ανθρώπους που παίζουν, συζητούν, και επικοινωνούν κάθε**

στιγμή στο παιχνίδι. Επιπρόσθετα, χρησιμοποιούσαν VPN (Εικονικά Ιδιωτικά Δίκτυα: μία τεχνολογία που εγκαθιστά μία κρυπτογραφημένη σύνδεση επάνω από ένα λιγότερο ασφαλή δίκτυο για απόκρυψη της ταυτότητας, των πακέτων δεδομένων και της επικοινωνίας) για να κρύψουν της διευθύνσεις IP από όπου συνδέονται.



ng of Haji Bakr's Islamic State organigram.

Η ΕΜΝΙ έδινε στους νέους που στρατολογούσε στην Ευρώπη λογισμικό όπως το «CCleaner», ένα πρόγραμμα που διαγράφει το ιστορικό επισκέψεων του χρήστη. Επίσης τους ζητούνταν να χρησιμοποιούν διάφορα προγράμματα κρυπτογράφησης και καθοδηγούνταν να ανεβάζουν κρυπτογραφημένα μηνύματα σε ανενεργούς λογαριασμούς email σε ένα τουρκικό εξυπηρετητή για αποφυγή εντοπισμού. Σήμερα είναι γνωστό ότι η ΕΜΝΙ είχε εκπαιδεύσει τους δράστες όλων των επιθέσεων στην Ευρώπη, τα τελευταία χρόνια πριν διαταχθούν να εκτελέσουν την τρομοκρατική ενέργεια.

Τρόποι Χρήσης των ΜΚΔ από το Ισλαμικό Κράτος.

Το Ισλαμικό Κράτος και οι μεγάλες τρομοκρατικές οργανώσεις, όπως η Αλ Κάιντα, η Αλ Νούσρα και οι θυγατρικές της, η Χαγιάτ Ταχράτ Αλ Σιαμ κλπ. χρησιμοποιούν ευρέως τα ανωτέρω ΜΚΔ ως πλατφόρμες προπαγάνδας, προώθησης

ιδεολογικών θέσεων και τάσεων, ενημέρωσης των ομοϊδεατών για τακτικές ενέργειες της οργάνωσης σε διάφορα επίπεδα, για παρατεταμένες ψυχολογικές επιχειρήσεις, με πραγματικά εντυπωσιακούς ρυθμούς.

Αν και έχουν ληφθεί και καθημερινά λαμβάνονται μέτρα εναντίον του κυβερνοτζιχαντισμού, μέσω DENIAL OF SERVICE (άρνηση υπηρεσίας) , κλείσιμο επικίνδυνου περιεχομένου ιστοσελίδων, εν τούτοις διεξάγεται ένας αμείλικτος πόλεμος που απαιτεί να επιστρατευτούν όλοι με όλα τα μέσα γιατί οι καταστάσεις είναι πολύπλοκες και ο αγώνας επίπονος και χωρίς πάντοτε να φέρνει τα επιθυμητά αποτελέσματα. Όποιος έχει ένα σύγχρονο έξυπνο κινητό τηλέφωνο (Smart Phone), μπορεί να προωθήσει πολύ άνετα ριζοσπαστικά μηνύματα

Σύμφωνα με άρθρο του Spiegel, ευρωπαϊκές εταιρίες δίνουν (ακόμη και σήμερα) τη δυνατότητα σε πολλές ακραίες οργανώσεις να έχουν πρόσβαση σε πλατφόρμες για να συνεχίζουν την προπαγάνδα τους και η απορία είναι γιατί δεν μπορεί να αντιμετωπιστεί. Η τεχνολογία που χρειάζεται για να έχει κανείς διαδικτυακή πρόσβαση σε Ιράκ ή Συρία, ήταν δυνατόν να αγοραστεί στην επαρχία Χατάι, στην Τουρκία κοντά στα συριακά σύνορα. Ο συνολικός εξοπλισμός φτάνει περίπου 500 δολάρια στη Συρία.

Μέσα και Μέθοδοι Στρατολόγησης.

Μέχρι το 2017 το ISIS είχε αναρτήσει πάνω από 1000 βίντεο, μεταξύ των οποίων και γνωστών ιεροκηρύκων του, οι οποίοι προπαγανδίζουν την ουτοπική και μυθική UMMAH και ακόμη και τώρα μέσω του κυβερνοτζιχάντ προωθεί και την ONLINE UMMAH, με στόχο τις ευάλωτες Μουσουλμανικές κοινότητες της Δύσης.Στοχεύουν σε τρωτούς νεανικούς κύκλους που δεν βλέπουν φως στα προσεχή στάδια της ζωής τους.

Προώθηση της μηνιαίας και πολύ προσεγμένης περιοδικής έκδοσης DABIQ, η οποία περιλαμβάνει στην ύλη της πολλά στοιχεία, που απαιτούν προσεκτική ανάλυση και εμβάθυνση από πλευράς Δυτικών αναλυτών και Ισλαμολόγων. Μέσω του κυβερνοχώρου το ISIS προωθούσε μηνύματα σε ενδιάμεσους, οι οποίοι έχουνε το δικό τους ακροατήριο, οπότε όλα τα μηνύματα τους φθάνουν σε τεράστιο αριθμό.

Το ISIS, είχε προχωρήσει στην σύσταση Υπουργείων, βιλαετιών και υπηρεσιών . Μεταξύ αυτών, εκτός της ΕΜΝΙ ήταν το λεγόμενο **Υπουργείο Ενίσχυσης του Ισλαμικού ρεύματος,** που είχε και την ευθύνη των κυβερνοεπιχειρήσεων.

Το Ισλαμικό Κράτος χρησιμοποιούσε «ελεύθερους συνεργάτες» μέσω των οποίων επιδίωκε τη δημιουργία επαφών και σχέσεων με Δυτικούς υποστηρικτές**. Οι συνομιλίες γίνονταν μέσω ειδικής πλατφόρμας όπως το «Telegram» και το «Surespot**».

Τα διεθνή ΜΜΕ στην υπηρεσία του Cyber Jihad.

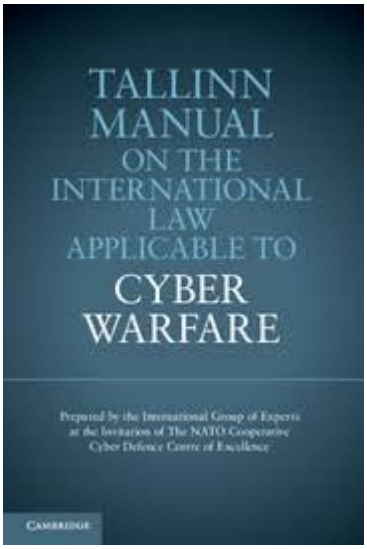
Τα διεθνή ΜΜΕ, σε όλες τις μορφές των βοηθούν στην ισλαμιστική και εξτρεμιστική προπαγάνδα του Ι.Κ., όσο και άλλων εξτρεμιστικών οργανώσεων, εκούσια αλλά και ακούσια. Ακούσια όταν αναφέρουν «ανθρωπιστικά γεγονότα», που συγκινούν τον άνθρωπο, επιλεγμένα όμως από την τζιχαντιστική ομάδα «κινηματογραφικής παραγωγής» θεαμάτων, με θέμα τον ανθρώπινο ΄πόνο και τα θύματα του πολέμου, που πάντα συγκινεί.

Θα αναφέρουμε μια πολύ χαρακτηριστική περίπτωση. Είναι η περίπτωση της απελευθέρωσης της ιστορικής πόλης Χαλέπι (Aleppo) από τον Συριακό Αραβικό στρατό και την εκδίωξη των εξτρεμιστών τζιχαντιστών . Στο Χαλέπι, όπως και σε πολλές εμπόλεμες περιοχές της Συρίας, δρούσε μία από τις πολλές ανθρωπιστικές οργανώσεις, **που έφερε το όνομα «Λευκά Κράνη»**, η οποία ήταν εξειδικευμένη σε διασώσεις εγκλωβισμένων ατόμων σε ερείπια κτιρίων. Τα «Λευκά Κράνη» εκτός από διασώστες ήταν και «πρωταγωνιστές» σε πολλά βίντεο με «διασώσεις» αμάχων στο Χαλέπι, σχεδόν όλες κατασκευασμένες, στον βωμό της εξυπηρέτησης της τζιχαντιστικής προπαγάνδας, αφού τελικά αποδείχθηκε ότι ήταν το καλύτερο μέρος της τζιχαντιστικής προπαγάνδας, κάτι που βλέπουμε και στους πολέμους που διεξάγονται σήμερα στην Ουκρανία και στην Γάζα. Οπότε σχεδίαζαν και υλοποιούσαν εικονικές διασώσεις για τον επηρεασμό της Δυτικής κοινής γνώμης, όταν οι εξελίξεις δεν ήταν ευνοϊκές για το Ι.Κ., με σκοπό την επίτευξη προσωρινής εκεχειρίας, για ανασύνταξη των τζιχαντιστών και τον ανεφοδιασμό των σε όπλα, πυρομαχικά και μαχητές, ώστε να αποφευχθεί η κατάληψη του Χαλεπίου από τις Συριακές δυνάμεις . Και φυσικά τα διεθνή και εγχώρια ΜΜΕ μας

μεταδίδουν μόνο αυτά που θέλουν να μας επηρεάσουν και προς μια πλευρά μόνο. Έτσι τότε είδαμε «νεκρά παιδάκια» μέσα στα αίματα, που μετά ήταν ζωντανά και χαμογελαστά, σε άλλες αποκαλυπτικές φωτό. Σε άλλη περίπτωση ένα κοριτσάκι «σώζεται» τρεις φορές, από βομβαρδισμένα κτίρια από τους διασώστες των «Λευκών Κρανών», αφού φαίνεται το ίδιο κοριτσάκι να διασώζεται σε τρία διαφορετικά χρονικά βίντεο. Και δεν ακούσαμε ποτέ επίσης για τους ομαδικούς τάφους που ανακαλύφθηκαν μετά στο απελευθερωμένο Χαλέπι, η την σφαγή 100 Σύριων στρατιωτών αιχμαλώτων, ηλικίας 18-25 ετών , πριν εγκαταλείψουν τις συνοικίες που κρατούσαν και τις παραδώσουν στον Συριακό στρατό. Το παράδειγμα του Χαλεπίου είναι χαρακτηριστικό του τρόπου δράσης και προπαγάνδας των τζιχαντιστών.

Τρόποι Αντιμετώπισης. Το εγχειρίδιο του Ταλλίν.

Το Άρθρο 51 του Καταστατικού Χάρτη του ΟΗΕ , ορίζει πως «Καμιά διάταξη αυτού του Χάρτη δε θα εμποδίσει το φυσικό δικαίωμα της ατομικής ή συλλογικής άμυνας, σε περίπτωση που ένα Μέλος των Ηνωμένων Εθνών δέχεται ένοπλη επίθεση, ως την στιγμή, που το Συμβούλιο Ασφαλείας θα πάρει τα αναγκαία μέτρα για να διατηρήσει την διεθνή ειρήνη και ασφάλεια». Μέχρι σήμερα δεν έχει καθοριστεί με σαφήνεια η έννοια της κυβερνοεπίθεσης, ούτε έχει επέλθει πλήρης διακρατική συμφωνία για το αν τελικά αυτή μπορεί να θεωρηθεί ή να εξομοιωθεί ως ένοπλη επίθεση. Το ΝΑΤΟ για την αντιμετώπιση της υβριδικής αυτής απειλής, με ειδική επιτροπή που συνέστησε, δημιούργησε το λεγόμενο «Εγχειρίδιο του Τάλλιν» (The Tallin Manual), όπου συμφώνησαν (εκτός των άλλων) ομόφωνα, πως οι υφιστάμενες κανόνες δικαίου, οι οποίοι ρυθμίζουν το “Jus ad Bellum”, αλλά και το “Jus in Bello” ισχύουν και για τις επιχειρήσεις στον κυβερνοχώρο.



Επίλογος.

Τα μέτωπα πλέον των πολέμων δεν είναι γραμμικά, ούτε ευκρινή. Είναι παράλληλα και σε άλλους χώρους όπου διεξάγονται δαιδαλώδεις ψυχολογικές, πληροφορικές και επιχειρήσεις επιρροής με βασικό χώρο το διαδίκτυο. Σε αυτό τον χώρο οι τρομοκράτες όλων των αποχρώσεων και ιδεολογιών, έχουνε προνομιακή θέση και προπαγανδίζουν, εκφοβίζουν, στρατολογούν στελέχη και προετοιμάζουν τις επόμενες πολύνεκρες τρομοκρατικές τους επιθέσεις. Και αυτός ο πόλεμος είναι επίσης πολύ δύσκολος και θα απαιτηθεί χρόνος από την Δύση να επικρατήσει. Κάποιοι μιλάνε για πόλεμο που μπορεί να κρατήσει 20-30 χρόνια. Έτσι θα λέγαμε ότι είναι όσο ποτέ άλλοτε απαραίτητη μια Στρατηγική Επικοινωνίας σε μεσαίο επίπεδο για να αντιληφθεί ο μέσος πολίτης της κάθε χώρας την φύση και το μέγεθος των κυβερνοαπειλών.

Το Ινστιτούτο Διεθνών Μελετών (CESIS) της Ρώμης δημοσίευσε το 2019 εκτενή έρευνα ειδικά αφιερωμένη στην ψηφιακή δραστηριότητα της ISIS . Σύμφωνα με το CESIS, το μέσο κοινωνικής δικτύωσης που χρησιμοποιήθηκε πιο συχνά είναι το Telegram. Σύμφωνα με έρευνα που έκανε πριν μερικά χρόνια το πανεπιστήμιο George Washington, υπάρχουν στο μέσο αυτό περίπου 600 κανάλια που διακινούν περιεχόμενα του Ισλαμικού Κράτους, με αυξανόμενη τάση, οπότε σήμερα είναι πολύ περισσότερα. Στα κανάλια Telegram δημοφιλή είναι οι στρατιωτικές επιχειρήσεις στη Συρία, οι πόλεμοι στην Γάζα και στην Ουκρανία. Ακολουθούν οι δραστηριότητες ισλαμιστικών οργανώσεων και τρομοκρατών διαφόρων αποχρώσεων, σε άλλα

μέρη του κόσμου, οι πολιτικές εξελίξεις στις ΗΠΑ και την Ευρώπη, θέματα που αφορούν την cyber security, και άλλα θέματα ισλαμικής τρομοκρατίας. στη Βόρεια Αμερική και την Ευρώπη. Και αυτό σημαίνει ότι ο ισλαμικός εξτρεμισμός και η «έγχρωμη» τρομοκρατία, όχι μόνο δεν έχουν εξαφανισθεί, αλλά υπάρχουν, αλλού εν υπνώσει και αλλού με δραστηριότητες και τρέφονται, συντηρούνται και γιγαντώνονται, μέσω του διαδικτύου από τα διάφορα μέσα προβολής του.

***Ο Ιωάννης Μπαλτζώης είναι αντγος (ε.α.) , με M.Sc. από ΕΚΠΑ και πρόεδρος ΕΛΙΣΜΕ.**

*Απόσπασμα του γράφοντος, από το βιβλίο του ΕΛΙΣΜΕ «Υβριδικοί Πόλεμοι».