



Γράφει ο Ιωάννης Αθ. Μπαλτζώης*

Η παρούσα ανάλυση αποτελεί προδημοσίευση μέρους του βιβλίου του Ελληνικού Ινστιτούτου Στρατηγικών Μελετών (ΕΛΙΣΜΕ), με τίτλο «Υβριδικοί Πόλεμοι», που πρόκειται να εκδοθεί στο άμεσο μέλλον.

Είναι μια συλλογική συγγραφική προσπάθεια, που θα αναφέρεται στην ιστορία και σε διάφορες μορφές και εφαρμογές του Υβριδικού Πολέμου σε περιοχές στην Ευρώπη και στην Μέση Ανατολή. Το παρόν απόσπασμα, αφορά μέρος του κεφαλαίου για τον Υβριδικό Πόλεμο του Ισλαμικού Κράτους, με πολλά άγνωστα μέχρι σήμερα στοιχεία.

Εισαγωγή.

Ο Υβριδικός Πόλεμος (ΥΠ) , Hybrid Warfare (HW) έχει γίνει ο πλέον δημοφιλής όρος στους ακαδημαϊκούς, στρατιωτικούς και πολιτικούς κύκλους. Αλλά τι σημαίνουν όντως ο όρος και πώς εφαρμόζεται αυτή η προσέγγιση του πολέμου από τους κρατικούς και μη κρατικούς φορείς στην πράξη; Ο όρος υβρίδιο σημαίνει κάτι ετερογενές, πολυμορφικό ή πολλαπλά ποικίλο. Όμως, όσον αφορά τον πόλεμο, τι σημαίνει αυτό; Ο όρος χρησιμοποιήθηκε ευρέως και διεθνώς μετά την αριστοτεχνική και πρωτοποριακή στην μεθοδολογία επιχείρηση κατάληψης της Κριμαίας από τους Ρώσους το 2014. Έτσι θα λέγαμε ότι ο ορισμός για τον Υβριδικό Πόλεμο χρησιμοποιήθηκε για να περιγράψει τις αλλαγές στον χαρακτήρα του πολέμου από το 2005. Ο όρος χρησιμοποιήθηκε

για να περιγράψει τη στρατηγική της Χεζμπολά στον πόλεμο του Λιβάνου το 2006. Ωστόσο, ορισμένοι παρατηρητές και στρατηγικοί αναλυτές υποστήριξαν ότι η σύγχρονη προέλευσή της βρίσκεται στον βαλκανικό πόλεμο και στην κατάρρευση της Γιουγκοσλαβίας. Άλλοι ισχυρίστηκαν ότι στοιχεία υβριδισμού έχουν συμβεί σε πολλούς πολέμους μετά την άνοδο του «πολιτισμένου» πολέμου. **Συμβαίνει όταν ένας δρώντας (κρατικός ή μη κρατικός) που το ασκεί εναντίον ενός αντιπάλου εισάγει ένα «κοκτέιλ» συμβατικών στρατιωτικών δυνατοτήτων, πολιτικού πολέμου, τρομοκρατίας, ανατροπής, αντάρτικου πολέμου, οργανωμένου εγκλήματος και, στη σύγχρονη εποχή, κυβερνο-πόλεμου.** Μπορεί επίσης να περιλαμβάνει παραβιάσεις των διεθνών νόμων του πολέμου από τον χρήστη του υβριδικού πολέμου. Όταν ο όρος εμφανίστηκε για πρώτη φορά να περιγράφει αυτό που ορισμένοι αναλυτές όπως ο Frank Hoffman[1] είδαν ως αναδυόμενες τάσεις, κάποιοι αναρωτήθηκαν αν ο όρος πρόσθεσε κάτι νέο για να περιγράψει πολέμους διαφορετικούς από τους καθαρά συμβατικούς ή συμμετρική δύναμη στις συγκρούσεις δύναμης μεταξύ παρόμοιων στρατών. Άλλοι αναρωτιόντουσαν αν ο όρος πρόσθεσε κάτι στην υπάρχουσα πληθώρα όρων που περιγράφουν πολέμους διαφορετικούς από καθαρά συμβατικούς, όπως ακανόνιστοι, ανταρτοπόλεμοι, χαμηλής έντασης, τέταρτης γενιάς, ασυμμετρικοί, νέοι πόλεμοι, πόλεμος για πάντα, κλπ. Τελικά, ο Υ.Π. είναι ένας χρήσιμος όρος επειδή αναδεικνύει - επισημαίνει ορισμένα χαρακτηριστικά του σύγχρονου πολέμου από τα κράτη και τους μη κρατικούς φορείς που τον διεξάγουν[2].

ISIS. Περίπτωση Μελέτης.

Μία από τις πιο γνωστές και σύγχρονες περιπτώσεις ασύμμετρης υβριδικής απειλής, η ακόμη καλύτερα Υβριδικού Πολέμου, που θα εξετάσουμε, είναι το λεγόμενο Ισλαμικό Κράτος (I.K.) ή ISIS. Είναι γνωστόν σήμερα ότι το I.K. έχει περίπου εξαφανιστεί από τα εδάφη της Συρίας και του Ιράκ, εκτός από κάποιες απομονωμένες ολιγομελείς ομάδες του στην έρημο της Συρίας. Φυσικά υπάρχουν πολλοί μαχητές του ISIS, καθώς και άλλες ακραίες Ισλαμιστικές Οργανώσεις, παρόμοιας ιδεολογίας στον θύλακα του Ιντλίμπ, μια επαρχία στα ΒΔ της Συρίας, όπου εκεί έχουν μεταφερθεί σκόπιμα και με την έγκριση του ΟΗΕ δεκάδες χιλιάδες τζιχαντιστών μαχητών με τις οικογένειές των. Το ISIS είχε χαρακτηριστεί ως υβριδική απειλή λόγω της αποτελεσματικής ικανότητά του να αναπτύσσει, μια σειρά από συμβατικές και τρομοκρατικές τακτικές ταυτόχρονα. Επιπλέον το ISIS είχε τη δυνατότητα να λειτουργεί παγκόσμια δίκτυα προσηλυτισμού και στρατολόγησης προκειμένου να συσπειρώσει χιλιάδες μαχητές στη θρησκευτική ιδεολογία του. Ο πρώην Πρόεδρος των ΗΠΑ Barak Obama, υπογράμμισε αυτή την ιδέα όταν είπε ότι το ISIS αντιπροσώπευε, «ένα είδος ενός υβριδικού δικτύου και όχι μόνο ένα τρομοκρατικό τοιούτο, αλλά ένα δίκτυο με εδαφικές φιλοδοξίες, αλλά και με ένα πρόσωπο στρατηγικής και τακτικής ενός συμβατικού στρατού.» Το ISIS είχε τη δυνατότητα για σχηματισμό, να αναπτύσσεται, καθώς και να

διατηρεί συμβατικές δυνάμεις, και ταυτόχρονα να μεγιστοποιεί τη χρήση των παράνομων τακτικών του, προσαρμόζοντας το συνδυασμό του για να εκμεταλλευτεί την αδυναμία των αντιπάλου του[3]. Το ISIS, αν και μη κρατικός φορέας, παρουσίασε μια σχεδόν απaráμιλλη 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, και επωφελείται από την αποκεντρωμένη φύση των δικτύων και την ικανότητα των υποστηρικτών του, να δημιουργήσει και να λειτουργήσει το δικό του τμήμα δημοσίων σχέσεων για τη στήριξη της οργάνωσης. Ο πρωτοφανής αριθμός των ξένων μαχητών που είχαν επανδρώσει την οργάνωση, αποδεικνύει την επιτυχία της πολιτικής του και της εκστρατείας του.

EMNI. Η Τρομερή Υπηρεσία Πληροφοριών του ΙΚ.

Μια εξαιρετική και αποκαλυπτική μελέτη δημοσιεύτηκε στην πρώτη έκδοση του διεθνούς επιστημονικού περιοδικού «Perspectives on Terrorism» (Απόψεις Τρομοκρατίας) για το έτος 2017[4]. 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[5] είχε βοηθήσει σε αυτό. Δηλαδή όσα μάθαμε για τον υβριδικό πόλεμο του Ι.Κ. είναι στο μεγαλύτερο ποσοστό από αυτή την αποκάλυψη. Φυσικά μετά από αυτά πλείστες άλλες πληροφορίες είδαν το φως της δημοσιότητας, ώστε σήμερα να γνωρίζουμε πως λειτούργησε όλο το σύστημα πληροφοριών, προπαγάνδας και μεταβίβασης εντολών του Ι.Κ. Η μελέτη αυτή έγινε από την Anne Speckhard [6] και τον Ahmet S. Yayla[7] και βασίζεται σε συνεντεύξεις από 42 πρώην μέλη- αποστάτες της τρομοκρατικής οργάνωσης Ισλαμικό Κράτος αλλά και προηγούμενες επιστημονικές μελέτες, όπως το δημοσιογραφικό ερευνητικό έργο του Christoph Reuter της Der Spiegel, ο οποίος πρώτος δημοσίευσε την ανακάλυψη των αρχείων του Haji Bakr, που ήταν ο δημιουργός της EMNI, όπως θα δούμε παρακάτω. Τα χαρακτηριστικά και η μεθοδολογία των συνεντεύξεων επεξηγούνται από τους ερευνητές και είναι πρωτοπόρα και ενδιαφέροντα[8].

Η προέλευση της EMNI αποκαλύφθηκε από σύμπτωση με την ανεύρεση το 2014 εγγράφων, που ανήκαν στον Haji Bakr (Χάτζι Μπακρ), (δηλαδή του Σαμίρ Αμπντ Μωχάμεντ αλ-Καχλιφάουι), ενός πρώην σημειάρχου της υπηρεσίας πληροφοριών του Santam Hussein, ο οποίος ήταν ο αρχιτέκτονας και δημιουργός της EMNI. Είχε προηγουμένως φυλακιστεί στις φυλακές Abu Ghraib και στη Βάση Buqa, 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 πρώην Σμήναρχος πληροφοριών του Ιράκ Haji Bakr

Ο Haji Bakr εστάλη από την οργάνωση στη Συρία, τα τέλη του 2012, ως μέλος ενός μικροσκοπικού πυρήνα, με αποστολή να βοηθήσει στο σχεδιασμό των βημάτων για το μελλοντικό «Ισλαμικό Κράτος», ώστε να κατακτήσει όσο περισσότερο έδαφος γίνεται στη Συρία και το Ιράκ.. Τα έγγραφα με τις σημειώσεις του, που βρέθηκαν μετά το θάνατο του (2014), αποτελούνταν από 31 σελίδες χειρόγραφων σημειώσεων, οργανογραμμάτων, λιστών, και προγραμμάτων και περιγράφουν βήμα-βήμα πώς να υποτάξεις ένα έθνος. . Ο Christoph Reuter[9], ο οποίος πρώτος ανέλυσε τα έγγραφα, έγραψε: «Αποκαλύπτουν μία πολυεπίπεδη σύνθεση και οδηγίες δράσης, μερικά ήδη δοκιμασμένα και άλλα καινούργια για κατάσταση αναρχίας στις περιοχές που κρατούν οι αντάρτες στη Συρία. Κατά ένα τρόπο, τα έγγραφα είναι ο πηγαίος κώδικας για το πιο επιτυχημένο τρομοκρατικό στρατό στη πρόσφατη ιστορία». Επιπρόσθετα, ήταν ο κώδικας για μία ομάδα αποφασισμένων τρομοκρατών να ενωθούν όχι μόνο για ανούσιες βάρβαρες τρομοκρατικές οργανώσεις, αλλά επίσης για ένα απολυταρχικό κράτος, ικανό να κυριαρχεί αδίστακτα στους πολίτες και τη περιοχή του.



Το οργανόγραμμα του Χάτζι Μπακρ

Μεθοδολογία του Ι.Κ.

Συνοπτικά να αναφέρουμε μερικές μεθόδους που εφάρμοσε το ΙΚ: Νέα έγγραφα που βρέθηκαν στο Χαλέπι επιβεβαιώνουν το εσωτερικό σύστημα παρακολούθησεων στο ΙΚ όπως επίσης και ένα υψηλής πολυπλοκότητας σύστημα διείσδυσης και παρακολούθησης σε όλες τις οργανώσεις που τους εναντιώνονταν. Στα κατασχεθέντα αρχεία του ΙΚ από το Χαλέπι υπήρχαν μεγάλες λίστες με πληροφοριοδότες εγκατεστημένους σε κάθε επαναστατική ομάδα και ακόμη και στον κυβερνητικό στρατό. Οι λίστες επίσης επιβεβαιώνουν σαφείς οδηγίες προς τα στελέχη του ΙΚ να παντρεύονται γυναίκες από ισχυρές οικογένειες πριν τη κατάληψη των χωριών, ώστε να κερδίζουν πίστη και συμμαχία από τις ισχυρές οικογένειες του χωριού, προτού το ΙΚ πάρει τον πλήρη έλεγχο[10].

Το χειρόγραφο οργανόγραμμα[11] του Haji Bakr δείχνει το όραμα του για την EMNI, καθώς σχεδίασε την αλυσίδα συλλογής, ταξινόμησης, αξιολόγησης, και εκμετάλλευσης των πληροφοριών, καθώς και την διοίκηση που περιλαμβάνει έναν εμίρη, ή διοικητή, να είναι υπεύθυνος για δολοφονίες, απαγωγές, ελεύθερους σκοπευτές, επικοινωνίες, και κρυπτογράφηση, όπως επίσης και έναν εμίρη να επιβλέπει τους άλλους εμίρηδες «για τη περίπτωση που δε κάνουν καλά τη δουλειά τους». Δηλαδή ένα ολοκληρωτικό σύστημα παρακολούθησης όλων, που ομοιάζει πολύ με το σοβιετικό σύστημα παρακολούθησης των πάντων, από τα πιο χαμηλά, μέχρι τα πιο υψηλά επίπεδα της δημόσιας και κομματικής ιεραρχίας.

Τα κεντρικά της EMNI βρίσκονταν στη Συριακή πόλη Αλ-Μπαμπ. Ο τελευταίος γνωστός αρχηγός ήταν ο 39χρονος εκπρόσωπος τύπου του ΙΚ, ο Σύριος Abu Mohamed al Adhani, που σκοτώθηκε τον Αύγουστο του 2016 από βομβαρδισμό των ΗΠΑ στη πόλη αλ-Μπαμπ. Στην μελέτη αναφέρεται ότι στην EMNI εργαζόταν πολύ μεγάλος αριθμός Μπααθιστών Αξκών, που υπηρετούσαν στις υπηρεσίες πληροφοριών του Saddam Hussein (Σαντάμ Χουσεΐν), καθώς και την μεθοδολογία που εφάρμοζαν για συλλογή και αξιολόγηση των πληροφοριών κάθε μορφής, για ανακρίσεις, βασανιστήρια, για εξόντωση αντιπάλων και διαφωνούντων, για οργάνωση διαφόρων μορφών επιχειρήσεων για την επίτευξη ενός ΑΝΣΚ, σε μεγάλο βαθμό παρεμφερή με την μεθοδολογία που εφαρμόζονταν στο Ιράκ επί Σαντάμ Χουσεΐν. Τα στελέχη της EMNI θεωρούνταν η «αφρόκρεμα» της οργάνωσης και επιλέγονται ανάλογα, βάση της πίστης και των ικανοτήτων τους[12].

Η Παρακολούθηση και η Χρήση του Διαδικτύου

Ας δούμε τώρα πως λειτουργούσε όλο το σύστημα πληροφοριών, ενημέρωσης και έκδοσης διαταγών για τρομοκρατικές ενέργειες ή άλλης μορφής

δράσεις. Πρόσβαση στο διαδίκτυο παρείχετο σε μαχητές του ΙΚ και πολίτες, σε καφετέριες που το ΙΚ αποκαλούσε «ταχυδρομεία». Το ΙΚ δεν βασιζέτο σε οποιαδήποτε υψηλού επιπέδου τεχνική παρακολούθηση της χρήσης του διαδικτύου, αλλά αντίθετα τοποθετούσε στελέχη του ΙΚ 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). Από τεχνικής πλευράς, οι υπολογιστές παρακολουθούνται με χαμηλού επιπέδου τεχνικές για το ιστορικό επισκέψεων, ενώ ευρέως διαδεδομένα δωρεάν προγράμματα παρακολουθούν εάν γίνεται πρόσβαση σε ιστοσελίδες που απαγορεύουν. Πρόσβαση στο διαδίκτυο δίχως παρακολούθηση είναι εφικτή μέσω κινητών τηλεφώνων σε συγκεκριμένες περιοχές του εδάφους του ΙΚ αλλά όποιος το κάνει κινδυνεύει να ανακαλυφθεί τι έκανε εάν εντοπιστεί και κάνουν έρευνα στη συσκευή του. 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.

Για τις προσωπικές τους επικοινωνίες, τα μέλη της EMNI έμαθαν από τις προκάτοχες τρομοκρατικές οργανώσεις, να μη χρησιμοποιούν e-mail ή τηλέφωνα που μπορούν να εντοπιστούν από ξένες υπηρεσίες πληροφοριών. Προτιμούσαν την επικοινωνία πρόσωπο με πρόσωπο. Αυτό ήταν δύσκολο, ωστόσο, ειδικά στις περιπτώσεις όπου η EMNI χρειάζονταν να επικοινωνήσει με ξένους μαχητές που είχαν στρατολογηθεί και επιχειρούσαν εκτός Συρίας και Ιράκ. Για αυτές τις περιπτώσεις υπήρχαν ειδικές διαδικασίες. Αν και τα απλά μέλη του ΙΚ συχνά χρησιμοποιούν τηλεφωνικές επικοινωνίες μέσω κρυπτογραφημένων εφαρμογών μέσω κοινωνικής δικτύωσης όπως το Telegram και το Whats App, η EMNI αποφεύγει τη χρήση τους. Αντίθετα, για την αποφυγή εντοπισμού και μέτρων ασφαλείας, τα στελέχη της EMNI βασίζονται 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, χρησιμοποιούν 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. Οι αποστάτες επίσης ανέφεραν ότι η EMNI 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. Αντίστοιχα, η EMNI επίσης χρησιμοποιούσε νέους μυστικούς πράκτορες της στην Ευρώπη για υπηρεσίες όπως πρόσωπο-με-πρόσωπο επαφή και μεταφορά

μηνυμάτων και σε άλλα επιχειρησιακά στελέχη. Σύμφωνα με αναφορές ανακρίσεων από συλληφθέντα μέλη του ΙΚ στην Ευρώπη και Αυστραλία, η EMNI έχει στείλει επιχειρησιακά στελέχη σε Αυστρία, Γερμανία, Ισπανία, Λίβανο, Τυνησία, Μπαγκλαντές, Ινδονησία και Μαλαισία. Εσωτερικές αναφορές από πληροφοριοδότες του ΙΚ αποκάλυψαν ότι η EMNI έχει τοποθετήσει εκατοντάδες στελέχη της σε χώρες της Ευρωπαϊκής Ένωσης, μαζί με εκατοντάδες ακόμα στη Τουρκία. **Σήμερα είναι γνωστό ότι η EMNI εκπαίδευσε τους δράστες όλων των επιθέσεων στην Ευρώπη**, πριν διαταχθούν να εκτελέσουν την τρομοκρατική ενέργεια!! . Στελέχη της EMNI έχουν επίσης εμπλακεί στο σχεδιασμό και εκτέλεση πολύ περισσότερων επιθέσεων παγκοσμίως, συμπεριλαμβανομένων πολλών επιθέσεων σε Τουρκία, Τυνησία, και Μπαγκλαντές. Μία μελέτη των καταγεγραμμένων ανακρίσεων που παρείχαν οι Ευρωπαϊκές πρωτεύουσες στο New York Times αποκάλυψε ότι τα στελέχη της EMNI επιλέγονταν βάση εθνικότητας και ομαδοποιούνται με βάση γλώσσας (ιδιαίτερα της μητρικής των, για την καλύτερη επικοινωνία, αλλά και εμπιστοσύνη μεταξύ των) σε μικρές, διακριτικές ομάδες για την εκτέλεση των επιχειρήσεων[13].



Οι χώρες με τις τρομοκρατικές οργανώσεις ISIS και Al Qaida, ως το 2018.

Τόσο το Ι.Κ. με την EMNI, όσο και οι άλλες εξτρεμιστικές Ισλαμιστικές οργανώσεις αναπτύσσουν υβριδικές τεχνολογίες, όπως η τεχνητή νοημοσύνη και η μίμηση της ανθρώπινης συμπεριφοράς, Αυτές επιτρέπουν σε τρομοκρατικές οργανώσεις να μεταδίδουν τα μηνυμάτα τους με σκοπό την στρατολόγηση νέων μελών, καθώς και την δημιουργία ιστοτόπων, ή e-mails με δυνατότητα το hacking εχθρικού ιστοτόπου. Η υβριδική τεχνολογία επιτρέπει επίσης σε τζιχαντιστές να αμυνθούν από επιθέσεις που δέχονται από τις υπηρεσίες

ασφαλείας, ή από αντιπάλους τους. Επίσης αναπτύσσουν κρυπτογραφικές επικοινωνίες. Η κρυπτογραφία είναι η τέχνη να στέλνεις και να λαμβάνεις μηνύματα με κωδικούς. Πολλές τρομοκρατικές οργανώσεις δημιουργούν τις δικές τους πλατφόρμες για να προωθήσουν τα σχέδιά τους, κάνοντας δύσκολη κάθε προσπάθεια των υπηρεσιών ασφαλείας να σπάσουν τους κωδικούς, όπως είδαμε πιο πάνω με το Ισλαμικό Κράτος[14].

Τρόποι Χρήσης των ΜΚΔ από το Ισλαμικό Κράτος.

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 Instagram» κ.α, τα οποία έχουν ξεπεράσει τα μέχρι τώρα παντοδύναμα ΜΜΕ. Είναι σημαντικότερα «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 ενώ παράλληλα μέσω της επικοινωνίας ανταλλάσσονται πολύ γρήγορα σκέψεις, ενημέρωση, πληροφορίες και ενέργειες κάθε φύσης και περιεχομένου. 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.

Για να καταλάβουμε καλύτερα πως γίνεται η χρήση του διαδικτύου θα αναφερθούμε στην δομή του. Το διαδίκτυο, World Wide Web (WWW) χωρίζεται σε τρία μέρη. Το πρώτο είναι το «επιφανειακό διαδίκτυο, αυτό που χρησιμοποιούμε στις καθημερινές μας επαφές, με εφαρμογές όπως, Google, Twitter, Facebook, Yahoo, In, Gmail, YouTube κλπ, το οποίο είναι το 10% του χρησιμοποιούμενου διαδικτύου. Το επόμενο είναι το Deep Web, το οποίο αποτελεί το 90% του διαδικτύου. Και τέλος είναι το Dark Web, για το οποίο δεν υπάρχουν ακριβή στοιχεία και απαιτούνται ειδικά προγράμματα και εφαρμογές, όπως το TOR, καθώς και ειδικές τεχνικές και γνώσεις για να κάνεις χρήση.



Γραφική παράσταση του διαδικτύου.

Το Ισλαμικό Κράτος, χρησιμοποιούσε 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, κάτι που απαιτεί τεράστια προσπάθεια και ενισχυμένη φαντασία από πλευράς κρατών και αντιτρομοκρατικών οργανώσεων για να το αντιμετωπίσει. Το κυβερνο-τζιχάντ (Cyber-jihad) έχει πραγματοποιήσει εκπληκτική πρόοδο στην χρήση του κυβερνοχώρου, που εκ των πραγμάτων προσφέρει σημαντικές ευκαιρίες προς κάθε κατεύθυνση. Μέσα από τον κυβερνοχώρο προωθείται η ενημέρωση και η ριζοσπαστικοποίηση στελεχών, η προβολή και προπαγάνδα και η στρατολόγηση νέων μελών, ο εκφοβισμός και ο έλεγχος των μαζών διεθνώς, με άμεσες και πολύ δυνατές επιπτώσεις για την διεθνή ασφάλεια και όχι μόνο. Σήμερα, όποιος έχει ένα Smart Phone μπορεί να προωθήσει πολύ άνετα ριζοσπαστικά μηνύματα. Βρισκόμαστε σε εποχή μετασύγχρονων πολέμων. Το Ισλαμικό Κράτος χρησιμοποιεί «ελεύθερους συνεργάτες» μέσω των οποίων επιδιώκει τη δημιουργία επαφών και σχέσεων με Δυτικούς υποστηρικτές. Οι συνομιλίες γίνονται μέσω ειδικής πλατφόρμας όπως το «Telegram» και το «Surespot. Οι γνωστές εφαρμογές στο twitter είναι η «Αυγή» και ο «Ισλαμικός Κόμβος»: Η Αυγή είναι προσβάσιμη μέσω του “google play store”, της πλατφόρμας δηλαδή του Google για ινιτά που χρησιμοποιούν αυτό το λογισμικό, ενώ ο Ισλαμικός Κόμβος είναι διαθέσιμος για τους χρήστες του Iphone. Έχουμε μπροστά μας μια νέα γενιά κυβερνοτρομοκρατών. Έχουμε μπροστά μας ένα νέο «ALUMNI», πτυχιούχων από τα μέτωπα του Ιράκ της Συρίας και της Λιβύης. Το «cyber jihad» είναι πλέον η πραγματικότητα που συνεχώς εξελίσσεται.[\[15\]](#).



Είναι πλέον γνωστό , ότι το Ισλαμικό Κράτος, όπως και άλλες εξτρεμιστικές οργανώσεις σήμερα, ήταν η οργάνωση με την πιο επιτυχημένη διαδικτυακή προπαγάνδα. Έτσι τίθεται το ερώτημα πως οι τρομοκράτες έχουν πρόσβαση στο διαδίκτυο και με ποιο τρόπο το χρησιμοποιούν. Σύμφωνα με άρθρο του Spiegel, που αναδημοσιεύτηκε στο CNN Greece πίσω από την παροχή δικτύου βρίσκεται η Ευρώπη, τη στιγμή που υποτίθεται η Ε.Ε. και όλες οι χώρες του Δυτικού κόσμου, συμμετέχουν στη συμμαχία κατά των τζιχαντιστών. Όπως αποκαλύπτεται στο ρεπορτάζ, ευρωπαϊκές εταιρίες δίνουν τη δυνατότητα σε πολλές ακραίες οργανώσεις ακόμη και σήμερα, να έχουν πρόσβαση σε πλατφόρμες για να συνεχίζουν την προπαγάνδα τους και η απορία είναι γιατί δεν μπορεί να αντιμετωπιστεί. Αυτό που δεν γνωρίζουμε με βεβαιότητα, είναι εάν οι συγκεκριμένες εταιρίες, που παρέχουν διαδικτυακές υπηρεσίες γνωρίζουν, αν ανάμεσα στους «πελάτες» τους βρίσκονται και οι τζιχαντιστές. Όμως το Spiegel υποστηρίζει ότι έχει στην κατοχή του έγγραφα που αποδεικνύουν ότι η παροχή Ιντερνετ ενδέχεται να γίνεται εν γνώσει αυτών των εταιριών. Τούτο σημαίνει πως θα μπορούσαν να προχωρήσουν στην παύση παροχής διαδικτύου στον ISIS. Όπως αποκαλύπτει το γερμανικό περιοδικό, η τεχνολογία που χρειάζεται για να έχει κανείς διαδικτυακή πρόσβαση σε Ιράκ ή Συρία, πρέπει να αγοραστεί στην επαρχία Χατάι, στην Τουρκία κοντά στα συριακά σύνορα. Ο συνολικός εξοπλισμός φτάνει περίπου 500 δολάρια στη Συρία, χωρίς να συμπεριλαμβάνονται στην τιμή οι χρεώσεις από τον εκάστοτε πάροχο. Και ιδού μια άλλη απόδειξη για τον ύποπτο και επικίνδυνο ρόλο της Τουρκίας, εκτός των άλλων, για την δημιουργία και γιγάντωση των

τζιχαντιστικών οργανώσεων που δρούσαν και δρουν ακόμη στην Συρία και δη στον θύλακα του Ιντλίμπ. Άλλωστε υπάρχουν χιλιάδες δορυφορικά πιάτα που επιτρέπουν στους χρήστες την πρόσβαση στο διαδίκτυο μέσω δορυφόρου. Σύμφωνα πάντα με το Spiegel, τα δορυφορικά πιάτα φτάνουν στη Μέση Ανατολή μέσω Ρότερνταμ, μέσα σε κοντέινερ και να αποστέλλονται από το λιμάνι κάθε χρόνο σε προορισμούς σε όλο τον κόσμο, ενώ από τις εταιρίες που παρέχουν δορυφορική κάλυψη συγκαταλέγεται και μία γαλλική. Πρόκειται για τον γαλλικό όμιλο Eutelsat, ο οποίος βρίσκεται στην κορυφή της λίστας των εταιριών που προσφέρουν στους τζιχαντιστές τη δυνατότητα να συνεχίζουν την προπαγάνδα του τρόμου. Το περιοδικό επικοινωνήσε με την εταιρία, η οποία όμως υποστήριξε ότι δε μπορεί να ελέγξει πώς χρησιμοποιούνται τα τερματικά της και ότι δεν έχει επαφή με τους πελάτες. Και το Spiegel εξηγεί, ότι αυτός ο ισχυρισμός δεν ευσταθεί, καθώς οι χρήστες για να έχουν ολοκληρωμένη πρόσβαση στο Διαδίκτυο πρέπει μέσω GPS να δώσουν την ακριβή τοποθεσία τους. Την ίδια ώρα, πέρα από τη γαλλική εταιρία, η βρετανική Avanti Communications και η λουξεμβουργιανή SES, εικάζεται ότι «συνεργάζονται» με τις περιοχές που έχουν περάσει στα χέρια των τζιχαντιστών.

«Τα στοιχεία GPS που έχει στην κατοχή του το Spiegel από το 2014 έως και το 2015, ξεκάθαρα αποδεικνύουν ότι τα δορυφορικά πιάτα εντοπίζονται με ακρίβεια σε σημεία που τελούσαν υπό τον έλεγχο του Ισλαμικού Κράτους», αναφέρει το δημοσίευμα. Οι δε σύγχρονοι Αμερικανοί, Ρωσικοί, Ισραηλινοί και λοιποί δορυφόροι έχουν ακρίβεια και ευκρίνεια εκατοστών στην λήψη εικόνων .

Τρόποι Αντιμετώπισης. Η Κυβερνοεπίθεση στα πλαίσια του Διεθνούς Δικαίου. Το εγχειρίδιο του Ταλλίν.

Σύμφωνα με την τελευταία παρουσίαση που έκανε ο Διευθυντής της Εθνικής Ασφάλειας των ΗΠΑ, (DNI) Dan Coats, «*Ο ISIS έχει ακόμα στην υπηρεσία του χιλιάδες μαχητές στη Συρία, στο Ιράκ και παγκοσμίως. Διατηρεί την παρουσία του σε οκτώ χώρες και έχει υποστηρικτές στο Διαδίκτυο. Η ηγεσία της Αλ Κάιντα ενδυναμώνει τη δομή της οργάνωσης διεθνώς και συνεχίζει να υποστηρίζει τις επιθέσεις της κατά της Δύσης και των ΗΠΑ*»[16].

Πριν αναφερθούμε σε τρόπους και μεθόδους αντιμετώπισης ας εξετάσουμε τον κυβερνοπόλεμο από άποψη διεθνούς δικαίου. Το Άρθρο 51 του Καταστατικού Χάρτη του ΟΗΕ [17], 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*». Δηλαδή καθορίζεται σαφώς το δικαίωμα κάθε κρατικής οντότητας για νόμιμη άμυνα, έναντι ενόπλου όμως επιθέσεως. Έτσι 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, σύμφωνα με το δίκαιο του πολέμου (Jus ad bellum), όπως αυτό καθορίζεται από τον

Καταστατικό Χάρτη του ΟΗΕ και στο «Δίκαιο των Ενόπλων Συγκρούσεων» και αφετέρου τα κράτη είναι υποχρεωμένα να εφαρμόσουν και να σεβαστούν τους κανόνες του “Jus in bello”[18].

Για τον λόγο αυτό, το ΝΑΤΟ πριν λίγα χρόνια δημιούργησε μια ομάδα εργασίας, ανεξάρτητων νομικών και τεχνικών εμπειρογνομόνων, προκειμένου να συντάξουν μια μελέτη για το πώς οι διεθνείς κανόνες δικαίου μπορούν να έχουν εφαρμογή στον κυβερνοπόλεμο. Έτσι δημιούργησαν 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**” (το δίκαιο που εφαρμόζεται προ της έναρξης των εχθροπραξιών), αλλά και το “**Jus in Bello**” (το δίκαιο που εφαρμόζεται αμέσως μετά την έναρξη των εχθροπραξιών) ισχύουν και για τις επιχειρήσεις στον κυβερνοχώρο[19].

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 έχουν 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 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. Κάθε χώρα θα πρέπει να έχει μια κρυστάλλινη Εθνική Στρατηγική για τον Κυβερνοχώρο με δεδομένη ανεξάρτητη Αρχή, υπεύθυνη για τα θέματα της ασφάλειας στο διαδίκτυο και η οποία θα έχει ευρύτερη συνεργασία με τις μυστικές υπηρεσίες και τις υπεύθυνες αρχές για την ασφάλεια στο διαδίκτυο. Θα πρέπει να αναγνωριστεί επίσημα και υπεύθυνα από όλα τα κράτη ότι οι κυβερνοαπειλές αποτελούν ξεκάθαρη μορφή απειλών για την εθνική, συμμαχική, περιφερειακή και παγκόσμια ασφάλεια. Είναι απαραίτητο οι διάφορες Κοινωνίες της Πληροφορίας και άλλοι μη-κυβερνητικοί οργανισμοί να υποστηρίζουν πρωτοβουλίες που να έχουν ως στόχο την σωστή λειτουργία του διαδικτύου.

Ιδιαίτερη σημασία για την καταπολέμηση της ισλαμικής τρομοκρατίας έχει ο αποτελεσματικός έλεγχος των μαχητών του ISIS και της Αλ Κάιντα, που έχουν ευρωπαϊκά διαβατήρια και έχουν επιστρέψει στην Ευρώπη. Ειδικότερα θεωρείται πως αποτελούν μεγάλο κίνδυνο οι Βαλκάνιοι ισλαμιστές που προέρχονται από το Κόσοβο, την Αλβανία, τη Βόρεια Μακεδονία και τη Βοσνία-Ερζεγοβίνη και εδώ θα πρέπει να στραφεί η προσοχή των Εθνικών Υπηρεσιών Ασφαλείας των κρατών της Ε.Ε. και ιδιαίτερα των Βαλκανικών κρατών, που μας αφορά άμεσα.

*** Ο Ιωάννης Αθαν. Μπαλτζώης είναι αντιστράτηγος ε.α., πρώην Ακόλουθος Άμυνας στο Τελ Αβίβ, πρώην Αξιωματικός επιχειρήσεων της ECMM στον πόλεμο της Βοσνίας, Απόφοιτος Tactical Intelligence School (U.S. Army), με Μεταπτυχιακό (M.Sc.) στην Γεωπολιτική Ανάλυση, Γεωστρατηγική Σύνθεση και Σπουδές Άμυνας και Διεθνούς Δικαίου του Εθνικού Καποδιστριακού Πανεπιστημίου Αθηνών, μέλος του Δ.Σ. του Ελληνικού Ινστιτούτου Στρατηγικών Μελετών (ΕΛΙΣΜΕ).**

Πρώτη δημοσίευση στο 1ο τεύχος του νέου ηλεκτρονικού περιοδικού Militaire Magazine (κάντε κλικ να το ξεφυλλίσετε)

[1] Ο Dr. Hoffman, πρώην Αξχος του Πολεμικού Ναυτικού των ΗΠΑ, ήταν αναλυτής και ήταν καθηγητής στο the National Defense University, καθώς και στο Institute for National Strategic Studies. Περισσότερα στο <https://www.fpri.org/contributor/frank-hoffman/>

[2] Βλ. Καθηγητής Ahmed S. Hashim, <https://www.oxfordresearchgroup.org.uk/blog/state-and-non-state-hybrid-warfare>

[3] Βλ. Tim Cross, «Syria air strikes: Can the West win this new kind of hybrid war against Isis?», Independent, 26/9/14, διαθέσιμο στην ιστοσελίδα <https://goo.gl/mMFP8h> (πρόσβαση 15/5/19)

[4] Β λ. PERSPECTIVES ON TERRORISM Volume 11, Issue 1, Feb 2017. P2-14, επίσης:

Anne Speckhard, Ahmet S. Yayla , «The ISIS Emni: The Origins and Inner Workings of ISIS's Intelligence Apparatus», Perspectives on Terrorism, διαθέσιμο στην ιστοσελίδα <https://goo.gl/7QV5qk> (πρόσβαση 31-7-18)

[5] Το όνομα EMNI είναι παράγωγο της αραβικής ρίζας «amn», το οποίο στα αραβικά σημαίνει «εμπιστοσύνη», «ασφάλεια», και «προστασία και στα τουρκικά, η λέξη «emniyet» σημαίνει «ασφάλεια» και πάλι από την ίδια αραβική ρίζα. ο.π.

[6] Anne Speckhard, Ph.D. is Adjunct Associate Professor of Psychiatry at Georgetown University in the School of Medicine and Director of the International Center for the Study of Violent Extremism (ICSVE). Ο.π.

[7] Ahmet S. Yayla, Ph.D. is Adjunct Professor of Criminology, Law and Society at George Mason University. Ο.π.

[8] Σύμφωνα με την μελέτη οι συνεντεύξεις ελήφθησαν από 32 Σύριους στη Τουρκία, 5 πολίτες των Βαλκανίων, 3 Δυτικούς Ευρωπαίους, και 2 Ασιάτες κατά τη περίοδο από τον Οκτώβριο του 2015 έως το Φεβρουάριο του 2017. Τα άτομα είχαν ηλικίες από 15 έως 52 ετών και αποτελούνταν από 6 γυναίκες και 36 άντρες. Οι ρόλοι τους στο ΙΚ διέφεραν από μαχητές, διοικητές, προσωπικό υλικοτεχνικής υποστήριξης, φύλακες, αστυνομικοί – συμπεριλαμβανομένης και γυναικείας αστυνομίας, και σύζυγοι μαχητών. Κάθε συνέντευξη είχε διάρκεια από μία έως πέντε ώρες η τεχνική συνεντεύξεως ήταν ημι-δομημένη, πρώτα επιτρέποντας στο άτομο να πει την ιστορία του ή της και έπειτα γίνονταν μία σειρά από 45 ερωτήσεις εμβαθύνοντας στο τομέα όπου το άτομο είχε προσωπικές εμπειρίες. Οι αποστάτες κρίθηκαν αυθεντικοί με βάση το ότι έχουν καταδικαστεί για κατηγορίες τρομοκρατίας σε 10 υποθέσεις, ή μέσω πληροφοριών και επιβεβαίωσης από γνωστούς αποστάτες ή διακινητές σε 32 ακόμα υποθέσεις. Επιπρόσθετα αξιολογήθηκαν ως πραγματικοί αποστάτες του ΙΚ βάση συσχέτισης των ιστοριών τους με γνωστά στοιχεία για το ΙΚ και με ανάλυση των μετατραυματικών απαντήσεων τους ενώ μιλούσαν για τη βαρβαρότητα της οργάνωσης . Βλ. PERSPECTIVES ON TERRORISM Volume 11, Issue 1, p2-14

[9] Βλ. Βιογραφικό Christoph Reuter στο Spiegel on line, διαθέσιμο στο <https://goo.gl/iQ3yjd> (πρόσβαση 12/4/19)

[10] Βλ. PERSPECTIVES ON TERRORISM Volume 11, Issue 1, ο.π, σ 2-14

[11] Βλ. C. Reuter , «Secret Files Reveal the Structure of Islamic State», Spiegel, 18/4/15, διαθέσιμο στην ιστοσελίδα <https://goo.gl/Jakffz> (πρόσβαση 3/5/19)

[12] Βλ. PERSPECTIVES ON TERRORISM Volume 11, Issue 1, p2-14, ο.π. <https://goo.gl/7QV5qk>

[13] Βλ. PERSPECTIVES ON TERRORISM Volume 11, Issue 1, ο.π

[14] Βλ. Σπύρου Μπαμιατζή «Οι νέες επιχειρησιακές τακτικές του ISIS και της Αλ Κάιντα», διαθέσιμο στην ιστοσελίδα <https://slpress.gr/diethni/oi-nees-epicheirisiakes-taktikes-toy-isis-kai-tis-al-kainta> (πρόσβαση 11/7/19)

[15] Βλ. Philip Seib & Dana M. Janbek, *Global Terrorism and New Media*, Routledge, New York 2011, p58-62

[16] Βλ. Σπύρου Μπαμιατζή «Οι νέες επιχειρησιακές τακτικές του ISIS και της Αλ Κάιντα», διαθέσιμο στην ιστοσελίδα <https://slpress.gr/diethni/oi-nees-epicheirisiakes-taktikes-toy-isis-kai-tis-al-kainta> (πρόσβαση 11/7/19)

[17] Βλ. «Καταστατικός Χάρτης των Ηνωμένων Εθνών», διαθέσιμο στην ιστοσελίδα <https://goo.gl/bTnG5H> (πρόσβαση 12/6/19)

[18] Βλ. Διακλαδική Επιθεώρηση ΑΔΙΣΠΟ, *Ανχη (ΝΟΜΙΚΟΥ)* Θωμά Σκότη, τεύχος 360, σ 38

[19] Βλ. περισσότερα στο: Schmitt, Michael, *Tallinn Manual on the International Law Applicable to Cyber War*. N.Y, Cambridge University Press, 2013