ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
Τμήμα Ναυτιλίας και Επιχειρηματικών Υπηρεσιών

&

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
Τμήμα Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής

ΔΙΙΔΡΥΜΑΤΙΚΟ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΣΤΗ ΝΑΥΤΙΛΙΑ ΚΑΙ ΤΙΣ ΜΕΤΑΦΟΡΕΣ»

ΤΙΤΛΟΣ

Απειλές ασφάλειας και κυβερνοασφάλειας μικροδορυφόρων (cubesats)

ΤΙΤΛΟΣ ΑΓΓΛΙΚΑ

Microsatellites'(Cubesats') Security and Cybersecurity Threats

Ονοματεπώνυμο Σπουδαστή:

Λυκούδης Γρ. Ανδρέας

Ονοματεπώνυμο Υπεύθυνων Καθηγητών:

Νικητάκος Νικήτας

Μαντζούρης Γεώργιος

ΔΙΑΤΡΙΒΗ

Φεβρουάριος 2019

ΤΙΤΛΟΣ

Microsatellites'(Cubesats') Security and Cybersecurity Threats

ΟΝΟΜΑ ΦΟΙΤΗΤΗ

Λυκούδης Γρ. Ανδρέας

Μεταπτυχιακή Διατριβή που υποβάλλεται στο καθηγητικό σώμα για την μερική εκπλήρωση των υποχρεώσεων απόκτησης του μεταπτυχιακού τίτλου του Διιδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών «Νέες Τεχνολογίες στη Ναυτιλία και τις Μεταφορές» του Τμήματος Ναυτιλίας και Επιχειρηματικών Υπηρεσιών του Πανεπιστημίου Αιγαίου και του Τμήματος Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής του Πανεπιστημίου Δυτικής Αττικής.

Δήλωση συγγραφέα διπλωματικής διατριβής

Ο κάτωθι υπογεγραμμένος **Λυκούδης Ανδρέας**, του **Γρηγορίου**, με αριθμό μητρώου **106** φοιτητής του Διιδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών «Νέες Τεχνολογίες στη Ναυτιλία και τις Μεταφορές» του Τμήματος Ναυτιλίας και Επιχειρηματικών Υπηρεσιών του Πανεπιστημίου Αιγαίου και του Τμήματος Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι: *«Είμαι συγγραφέας αυτής της μεταπτυχιακής διπλωματικής διατριβής και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην διατριβή. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η διατριβή προετοιμάστηκε από εμένα προσωπικά ειδικά για τη συγκεκριμένη μεταπτυχιακή διπλωματική διατριβή».*

Ο δηλών **Ημερομηνία**

Λυκούδης Ανδρέας **__/__/____**

Περίληψη

Στη σύγχρονη εποχή οι νέες τεχνολογίες πληροφορικής και επικοινωνιών (ΤΠΕ), σε καθημερινή βάση, αναδεικνύονται ως οι πλέον απαραίτητες για την κάλυψη επαγγελματικών και μη αναγκών. Σε κάθε χώρο, όπως και στο ναυτιλιακό, τον οποίο καλείται να εξυπηρετήσει στην ευρύτερη έννοιά της η παρούσα εργασία, κριτήριο επιλογής, ανάμεσα σε ένα ικανό, αριθμητικά, πλήθος τέτοιων τεχνολογιών που προσομοιάζουν μεταξύ τους, αποτελεί, σε μεγάλο βαθμό, το επίπεδο της αποτελεσματικής διακίνησης πληροφοριών στον επιθυμητό χρόνο προκειμένου να επιτυγχάνεται το προσδοκώμενο αποτέλεσμα. Η χρήση δορυφορικών συστημάτων πλέον μοιάζει επιβεβλημένη και για το λόγο αυτό, ολοένα και περισσότερες εταιρείες του κλάδου της ναυτιλίας επιλέγουν να διερευνούν τις εξελίξεις σε αυτά, με τις διευκολύνσεις που διαφαίνεται να προσφέρουν οι μικροδορυφόροι (microsatellites/cubesats), να έχουν αυξανόμενη ζήτηση.

Ωστόσο, το τελευταίο χρονικό διάστημα, πέρα από την αποτελεσματική και ταχεία μετάδοση, έχει αρχίσει να συζητείται ολοένα και περισσότερο η ασφάλεια της πληροφορίας, ως προσδοκία από την όποια επιλεχθείσα τεχνολογική εφαρμογή. Οι πελάτες/χρήστες (clients/users), έχοντας υπόψη την ευκολία διείσδυσης σε εύθραυστες πληροφορικές εφαρμογές μέσω διαδικτύου και θέλοντας να διαφυλάξουν το «απόρρητο» και την βιωσιμότητα τους απέναντι σε «πειρατές» και «κακόβουλα λογισμικά», γίνονται πιο απαιτητικοί στις προδιαγραφές των σχεδιαζόμενων εφαρμογών επικοινωνίας που τους παρουσιάζονται, γεγονός που έμμεσα ή άμεσα επηρεάζει και το χώρο των εξελίξεων στις αεροδιαστημικές εφαρμογές.

Στην παρούσα εργασία, επιλέγοντας ως «αντικείμενο» έρευνας δύο μικροδορυφόρους που εκτέλεσαν επιτυχή αποστολή κατά το εγγύς παρελθόν, καταγράφονται η προσπάθεια εντοπισμού πιθανών κινδύνων (απειλών) και τρωτοτήτων ασφάλειας και κυβερνοασφάλειας (security's and cybersecurity's risks (threats) and vulnerabilities) στα υποσυστήματα τους (cubesat subsystems) και στην αποστολή και λήψη σήματος των «φορτίων» τους (payload), καθώς και η προσπάθεια κατηγοριοποίησής αυτών ως προς τη σημαντικότητά τους σε σχέση με τη λειτουργία των μικροδορυφόρων και το σκοπό της αποστολής τους. Επιπλέον, παρουσιάζεται η σημαντικότητα της διασφάλισης της διακινούμενης πληροφορίας μέσω μικροδορυφόρων και

αναφέρονται προτάσεις ενδυνάμωσης της ασφάλειας και κυβερνοασφάλειας σε αυτά τα συστήματα.

Λέξεις κλειδιά

Διασφάλιση πληροφορίας; Ασφάλεια και Κυβερνοασφάλεια; Απειλή; Τρωτότητα; Μικροδορυφόρος (cubesat)

Abstract

In modern times, the new information and communication technologies (ICT), on a daily basis, are emerging as vital to meet professional and non-business needs. In each sector, just as in maritime's, a criterion of choice, among a number of similar technologies, is, to a large extent, the level of effectiveness of transferring the information at the desired time, in order to achieve the expected outcome. The use of satellite systems seems imposed, and therefore more and more shipping companies are choosing to explore the new developments, with the trends that microsatellites / cubesats offer, to be in growing demand.

However, lately, in addition to efficient and rapid transmission, information security has increasingly begun to be discussed as an expectation of any selected technology. Clients / users, having regard to the ease of penetration of fragile IT applications over the Internet and wanting to preserve their "privacy" and viability against "pirates" and "malware", are becoming more demanding in the specifications of the proposed communication applications, which indirectly or directly influences the developments in aerospace applications.

In this study, through the selection of two cubesats that performed a successful mission in the near past as the "object" of research, the effort to identify security's and cybersecurity's risks (threats) and vulnerabilities in their subsystems and in the "send and receive" signal of their payload is presented, as well as the attempt to categorize these vulnerabilities in terms of their importance in relation to the operation of the cubesats and the purpose of their mission. In addition, the importance of the assurance of the transferring information through cubesats is presented, along with proposals for hardening security and cyber-security in these systems.

Keywords

Information assurance; Security and Cybersecurity; Threat; Vulnerability; Microsatellite (Cubesat)

Ευχαριστίες

Η εργασία αυτή, που αποτελεί προσπάθεια ανάδειξης σημαντικών εξελίξεων στο χώρο του διαστήματος, όπως εκτέθηκαν και κατά τη διάρκεια των μαθημάτων της τρίτης κατεύθυνσης «Σχεδιασμός και Λειτουργία Αεροδιαστημικών Συστημάτων και εφαρμογές στη Ναυτιλία», εκπονήθηκε στο πλαίσιο του Διιδρυματικού ΠΜΣ «Νέες Τεχνολογίες στη Ναυτιλία και τις Μεταφορές» του Τμήματος "Ναυτιλίας και Επιχειρηματικών Υπηρεσιών" του Πανεπιστημίου Αιγαίου και του Τμήματος "Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής" (πρώην "Τμήμα Αυτοματισμού Τ.Ε.") του Πανεπιστημίου Δυτικής Αττικής (πρώην Ανώτατου Εκπαιδευτικού Ιδρύματος Πειραιά ΤΤ).

Συναφώς, επιθυμία μου αποτελεί να προβώ σε ευχαριστίες ορισμένων ατόμων τα οποία συνέβαλαν στην ολοκλήρωση των σπουδών μου με διάφορους τρόπους και με ώθησαν στην πραγματοποίηση της παρούσας εργασίας.

Αρχικά, θα ήθελα να ευχαριστήσω τους καθηγητές του ΠΜΣ και ειδικότερα αυτούς της κατεύθυνσης «Σχεδιασμός και Λειτουργία Αεροδιαστημικών Συστημάτων και εφαρμογές στη Ναυτιλία», για την καθοδήγηση τους στην «είσοδό» μου σε ένα τόσο «νέο» και «διαφορετικό», για εμένα, επιστημονικό χώρο.

Επίσης, θα ήθελα να ευχαριστήσω τους επιβλέποντες καθηγητές της εργασίας μου, τον Καθηγητή κ. Νικητάκο Νικήτα και το Δρ. Μαντζούρη Γεώργιο, για τη συμβολή τους, με τις σημαντικές υποδείξεις τους και τις διορθώσεις τους, οι οποίες ήταν απαραίτητες για την επιτυχή ολοκλήρωση αυτής.

Επιπρόσθετα, θερμές ευχαριστίες θα επιθυμούσα να εκφράσω προς τους συμφοιτητές μου στο μεταπτυχιακό πρόγραμμα, οι οποίοι κατάφεραν να δημιουργήσουν ένα αρμονικό «μαθησιακό περιβάλλον», ικανό να προάγει την επιστήμη.

Πιο συγκεκριμένα όμως, ευχαριστίες εκφράζω στους συμφοιτητές μου – καλύτερα συνοδοιπόρους μου, θα τους αποκαλούσα – στην κατεύθυνση «Σχεδιασμός και

Λειτουργία Αεροδιαστημικών Συστημάτων και εφαρμογές στη Ναυτιλία», για τις αμέτρητες βραδινές και νυχτερινές ώρες συνεργασίας, με χρήση κάθε είδους τεχνολογικής εφαρμογής επικοινωνίας, προκειμένου να εκπονηθούν ομαδικές εργασίες, να λυθούν απορίες και να συζητηθούν προβληματισμοί, με απώτερο αποτέλεσμα την επιτυχή ολοκλήρωση των εκπαιδευτικών ενοτήτων του ΠΜΣ.

Ευχαριστώ ακόμη, τους φίλους μου και τους συναδέλφους μου για την υπομονή και την υποστήριξη τους, όλο αυτό το διάστημα.

Τέλος, ιδιαίτερες ευχαριστίες απευθύνω και στην οικογένειά μου. Οτιδήποτε περισσότερο θα ήταν περιττό να ειπωθεί για τους δικούς μου ανθρώπους εδώ. Γνωρίζουν άλλωστε πόσο σημαντικοί είναι για εμένα !!!

"To move forward,
what's required is
a unified space agenda
based on exploration, science,
development, commerce and
security."

Edwin Eugene Aldrin Jr.
(Buzz Aldrin)
One of the first two humans
to land on the Moon
AΩ

Πίνακας Περιεχομένων

Κατάλογος Πινάκων

Κατάλογος Εικόνων

Κατάλογος Σχημάτων

Κατάλογος Συντομογραφιών

Ελληνικές

• ΗΠΑ Ηνωμένες Πολιτείες Αμερικής
• ΤΠΕ Τεχνολογίες Πληροφορικής και Επικοινωνιών

Ξενόγλωσσες

- ADCS Attitude Determination and Control Subsystem
- AIS Automatic Identification System
- ASAT Anti-SATellite
- CD Cambridge Dictionary
- CDHS Command and Data Handling Subsystem
- CDMA Code Division Multiple Access
- COTS Commercial Off-The-Shelf Components
- CS Communications Subsystem
- DPC Data Processing Center
- EPS Electrical Power System
- FDMA Frequency Division Multiple Access
- GPS Global Positioning System
- ICT Information and Communication Technologies
- IT Information Technologies
- ITU International Telecommunication Union
- MCC Mission Control Center
- MF-TDMA Multi Frequency Time Division Multiple Access
- OD Oxford Dictionaries
- Pentest Penetration testing
- POCC Payload Operations Control Center
- PPP Public Private Partnership,
- PS Propulsion Subsystem
- SCPC Single Channel per Carrier

- SOCC Spacecraft Operations Control Center
- SS Structural Subsystem
- TCS Thermal Control Subsystem

Σελίδα κενή

1. Εισαγωγή

1.1 Περιγραφή ερευνητικού προβλήματος

Κατά τη διάρκεια μιας ιστορικής αναζήτησης των τρόπων μετάδοσης οποιασδήποτε πληροφορίας μεταξύ ανθρώπων σε απόσταση, εύκολα αναδεικνύεται η τεχνολογική καινοτομία που λάμβανε χώρα κατά περιόδους. Στην αρχαία Ελλάδα, για παράδειγμα, αξιοποιούνταν οι φρυκτωρίες, η χρήση πυρσών δηλαδή στις κορυφές των βουνών, οι οποίες αναφέρονται ακόμη και στο έργο του Αισχύλου «Αγαμέμνων», καθώς κάλυψαν μέσω ενός δικτύου τέτοιων κατασκευών, περίπου 550 χιλιόμετρα και από την Τροία και το όρος Ίδη έφτασε στο Παλάτι των Μυκηνών το μήνυμα της νίκης του Αγαμέμνονα σε μια νύχτα, όπως φαίνεται και στο ακόλουθο απόσπασμα:
«*ΧΟΡΟΣ: Και πότε κούρσεψαν την πόλη;*
ΚΛΥΤΑΙΜΝΗΣΤΡΑ: Τη νύχτα, σου είπα, που το φως γέννησε τούτο.
ΧΟΡΟΣ: Τόσο γοργά ποιος θα 'ρχονταν μαντατοφόρος;
ΚΛΥΤΑΙΜΝΗΣΤΡΑ: Ο Ήφαιστος, λαμπρός στέλνοντας φέγγος από την Ίδη. Συναλλάζοντας οι φλόγες την έτοιμη φωτιά, μια με την άλλη, τη φέραν ως εδώ. (...) Αυτό σου λέω το ξάστερο σημάδι από την Τροία και το μαντάτ' ο άντρας μου έχει στείλει.»[1]

Από τότε, έως και την πιο σύγχρονη εποχή, όπου εξελίξεις σε διάφορες περιόδους, όπως αυτή του Ψυχρού Πολέμου ανάμεσα στις δύο υπερδυνάμεις, ΗΠΑ και Σοβιετικής Ένωσης, καθώς και η παγκόσμια άνθιση τομέων επιχειρηματικότητας όπως η θαλάσσια διακίνηση εμπορευμάτων, επέβαλαν τη χρήση δορυφορικών συστημάτων, η αναγκαιότητα ταχείας και επιτυχούς μετάδοσης κάθε είδους πληροφορίας έχει προκαλέσει σημαντικά τεχνολογικά επιτεύγματα. Και εάν θεωρούταν έως πριν από μία δεκαετία η χρήση συστοιχιών δορυφορικών συστημάτων ως το πιο καινοτόμο επίτευγμα για την κάλυψη της ανάγκης μετάδοσης της πληροφορίας, σήμερα, κυρίως ο παράγοντας κόστος κατασκευής σε συνδυασμό με το νόμο του Moore, ότι δηλαδή ο αριθμός των τρανζίστορ ενός ολοκληρωμένου

[1] ΑΙΣΧΥΛΟΥ, ΑΓΑΜΕΜΝΩΝ, Στίχοι 263-304, Αποσπάσματα, Μετάφραση Τ. ΡΟΥΣΣΟΥ, *ΚΑΚΤΟΣ*, 1992

κυκλώματος διπλασιάζεται κάθε δύο χρόνια, οδηγούν σε νέες λύσεις, με κύριο εκπρόσωπο την ανάπτυξη συστοιχιών μικροδορυφορικών συστημάτων (cubesats constellation).

Οι δυνατότητες αυτών των μικροδορυφόρων ολοένα και ανταποκρίνονται καλύτερα στις προδιαγραφές των κατασκευαστών τους, καθώς και στις απαιτήσεις των πελατών-χρηστών τους, με αποτέλεσμα να καθίστανται πιο δημοφιλείς, ειδικά σε θέματα μετάδοσης πληροφοριών. Το μικρότερο κόστος κατασκευής, όπως προαναφέρθηκε, σε συνδυασμό με το μικρό τους μέγεθος και άρα το μικρότερο τους βάρος και η εξελισσόμενη τεχνολογία των εξαρτημάτων που φέρουν ως «ωφέλιμο φορτίο» (payload), οδηγούν σε μεγαλύτερη αποδοχή καθώς οι εν δυνάμει πελάτες-χρήστες αποκτούν ταχεία πρόσβαση σε χρήσιμες, για την ομαλή λειτουργία τους, πληροφορίες, μειώνοντας τα έως πρότινος έξοδα τους.

Ωστόσο, το βασικότερο μέλημα στη μετάδοση οποιασδήποτε πληροφορίας θεωρούταν και εξακολουθεί να θεωρείται, η προστασία της από οποιαδήποτε απειλή. Η ασφάλεια στη μετάδοση μιας πληροφορίας, η οποία σημειωτέον έχει αποτελέσει πηγή δημιουργίας μιας από τις σημαντικότερες νέες επιστήμες, ιδιαίτερα από τα μέσα του προηγούμενου αιώνα, αυτή δηλαδή της κρυπτολογίας, οφείλει να αποτελεί και βασικό χαρακτηριστικό οποιασδήποτε νέας μεθόδου και νέας τεχνολογίας. Ιδιαίτερα τη στιγμή που οι πελάτες-χρήστες, εκδηλώνουν ολοένα και περισσότερο την επιθυμία να διαφυλάξουν το «απόρρητο» και τη βιωσιμότητά τους απέναντι σε επιθέσεις και κυβερνο-επιθέσεις από «πειρατές». Ανάμεσα στις τεχνολογίες αυτές, ως φυσικό επακόλουθο, θα έπρεπε να συγκαταλέγονται τόσο οι δορυφόροι όσο και οι μικροδορυφόροι.

Εντούτοις, η κατεύθυνση που τηρούταν έως πρόσφατα, στο πλαίσιο της επικοινωνίας των σταθμών εδάφους με τους δορυφόρους, αλλά και τους μικροδορυφόρους (τόσο σε λειτουργικό επίπεδο αυτών, όσο και σε επίπεδο αποστολής και λήψης σήματος του payload) ήταν να καθίσταται αυτή η επικοινωνία κατά κύριο λόγο «επιτυχής» εξαιτίας της απόστασης και της αντικειμενικής δυσκολίας επίτευξης της, λαμβάνοντας λιγότερο υπόψη την ασφάλειά της.

Πλέον, όμως, η κατεύθυνση αυτή φαίνεται να αλλάζει, καθώς η ασφάλεια και κυβερνοασφάλεια αποκτούν νέα δυναμική, στο πλαίσιο των γενικότερων οδηγιών – πολιτικών διαφόρων κρατών για την αντιμετώπιση επιθέσεων και κυβερνοεπιθέσεων, αλλά και των απαιτήσεων των πελατών-χρηστών αεροδιαστημικών εφαρμογών. Χαρακτηριστικό παράδειγμα της αλλαγής πλεύσης είναι η *δήλωση στο αμερικανικό Κογκρέσο, του διευθυντή της αντίστοιχης Διεύθυνσης Εθνικών Πληροφοριών των ΗΠΑ, Dan Coats* (όπ. αναφ. ο Logan, (2018))[2] *ότι «οι αντίπαλοι – ανταγωνιστές των ΗΠΑ συνεχίζουν να προσπαθούν να αποκτήσουν αντι-δορυφορικά όπλα (anti-satellite [ASAT] weapons»*. Με βάση τη δήλωση αυτή, και λαμβάνοντας υπόψη ότι το πεδίο μάχης καλύπτει πέραν των ASAT, τα αμιγή οπλικά συστήματα δηλαδή, όσο και τα «κυβερνο-όπλα» στην ευρύτερη έννοιά τους, που σκοπό έχουν τη «βλάβη», μόνιμη ή μη, δορυφορικών συστημάτων, αναδεικνύεται η σοβαρότητα που έχει αρχίσει να εγείρει το θέμα της ασφάλειας και κυβερνοασφάλειας.

[2] Logan T., (2018), The US must secure its supply chain in the face of anti-satellite weapons,C4ISRNET https://www.c4isrnet.com/opinion/2018/05/16/the-us-must-secure-its-supply-chain-in-the-face-of-anti-satellite-weapons/

1.2 Περιληπτική περιγραφή των κεφαλαίων

Έχοντας υπόψη τα παραπάνω και σε συνδυασμό με το γεγονός ότι οι κατασκευαστές αναγνωρίζοντας τη σημαντικότητα της πληροφορίας, σταδιακά προβαίνουν στην ενδυνάμωση της ασφάλειας αλλά και της κυβερνοασφάλειας (security and cybersecurity hardening) των μικροδορυφόρων, η παρούσα εργασία σκοπό έχει την καταγραφή πιθανών τρωτοτήτων ασφάλειας και κυβερνοασφάλειας σε κάθε ένα από τα υποσυστήματα ενός μικροδορυφόρου.

Πιο αναλυτικά, σκοπός αποτελεί ο εντοπισμός και η κατηγοριοποίηση πιθανών τρωτοτήτων ασφάλειας και κυβερνοασφάλειας στο επίπεδο λειτουργίας του μικροδορυφόρου, ήτοι κατά τη μετάδοση των εντολών λειτουργίας του σε σχέση με την εκτέλεση ή μη αυτών, όχι ως σφάλμα του συστήματος ή εξαιτίας άλλου τυχαίου γεγονότος (π.χ. ηλιακή καταιγίδα), αλλά ως επιρροή εξωγενούς παράγοντα.

Ομοίως θα διενεργηθεί προσπάθεια αντίστοιχου εντοπισμού και κατηγοριοποίησης πιθανών κενών ασφάλειας και κυβερνοασφάλειας στο επίπεδο αποστολής και λήψης σήματος του payload, σε σχέση με τη δυνατότητα επιρροής του από εξωτερικούς παράγοντες. Για την εκπλήρωση του σκοπού θα επιλεγούν οι περιπτώσεις δύο μικροδορυφόρων, οι οποίοι εκτέλεσαν επιτυχή αποστολή κατά το εγγύς παρελθόν.

Στο σημείο αυτό πρέπει να σημειωθούν και να καταστούν απόλυτα σαφείς οι ακόλουθες δύο παρατηρήσεις – δηλώσεις:
α) *Η εργασία αυτή* ***δεν αποτελεί*** *προσπάθεια μείωσης της σημαντικότητας της επιτυχίας των δύο μικροδορυφόρων. Αντιθέτως, η προσπάθεια ανάδειξης πιθανών τρωτοτήτων σε επιτυχημένα μοντέλα υλοποίησης μικροδορυφορικών αποστολών, στόχο έχει τη δημιουργία συναίσθησης της σημαντικότητας που πρέπει να δοθεί στον τομέα της ασφάλειας και κυβερνοασφάλειας. Με άλλα λόγια, στόχος είναι η εδραίωση της αντίληψης ότι η ασφάλεια (security) και κυβερνοασφάλεια πλέον οφείλει να αποτελεί μέρος των διαδικασιών σχεδιασμού και κατασκευής ενός μικροδορυφορικού συστήματος*.

*β) Η παρούσα εργασία **αποτελεί** προσπάθεια «ποιοτικού» προσδιορισμού της βλάβης/των βλαβών, από τρωτότητες. Έτσι, η διερεύνηση ενός κώδικα λειτουργίας με σκοπό τον εντοπισμό τρωτοτήτων σε αυτό, ουσιαστικά με πρόκληση κυβερνο-επίθεσης σε αυτό, ή η διερεύνηση δημιουργίας κατάλληλου οπλικού συστήματος για εντοπισμό τρωτοτήτων, μπορούν να αποτελέσουν αντικείμενα επόμενης εργασίας. Επίσης, ο εντοπισμός στα λογισμικά των commercial off-the-shelf (COTS) components, διαφόρων τρωτοτήτων, σε ερευνητική εργασία, πρέπει να γίνει με πολύ μεγάλη προσοχή, γιατί μπορεί να επηρεαστεί η αντίστοιχη αγορά και να υποστηριχθεί από τις «θιγόμενες» παρασκευάστριες εταιρείες ότι καταβάλλεται προσπάθεια νόθευσης του ανταγωνισμού, με αρνητικά αποτελέσματα στον ερευνητή. Συναφώς, η διερεύνηση κώδικα που δημιουργείται εξ ολοκλήρου από ομάδα του κατασκευαστή, στο πλαίσιο custom made component, απουσία χρήσης COTS, διαφαίνεται δύσκολο εγχείρημα, εάν δεν πραγματοποιηθεί με σύμφωνη γνώμη των κατασκευαστών.*
Σε κάθε περίπτωση, αυτές οι ανησυχίες μπορούν να είναι μέλημα μιας επόμενης, όπως προαναφέρθηκε, ερευνητικής εργασίας.

Στόχοι θα αποτελέσουν η ανάδειξη των κινδύνων, η σημαντικότητα αυτών στη λειτουργία του μικροδορυφόρου και η διασφάλιση της μετάδοσης της πληροφορίας από και προς αυτόν και θα αναφερθούν προτάσεις ενδυνάμωσης της ασφάλειας και κυβερνοασφάλειας αυτού.

Υπό μορφή κατηγοριοποίησης, η παρούσα εργασία αποτελείται από τα ακόλουθα κεφάλαια, για τα οποία παρατίθεται μια πολύ σύντομη περιγραφή προκειμένου να βοηθηθεί ο αναγνώστης:

- *Μετάδοση της πληροφορίας*. Τι είναι πληροφορία, γιατί έχει σημασία, πως μεταδίδεται. (Κεφάλαιο 2ο)
- *Μικροδορυφόρος*. Τι είναι, ποια είναι η χρήση του, από ποια υποσυστήματα αποτελείται γενικά. (Κεφάλαιο 3ο)
- *Ασφάλεια και Κυβερνοασφάλεια*. Σχέση της ασφάλειας και κυβερνοασφάλειας με τη διαφύλαξη της πληροφορίας. Τρωτότητα, τι καλείται, τι προκαλεί στην πληροφορία και ποια η μεθοδολογία εντοπισμού της (Κεφάλαιο 4ο)

- *Εντοπισμός τρωτοτήτων ασφάλειας και κυβερνοασφάλειας σε επίπεδο λειτουργίας του μικροδορυφόρου*. Επιλογή δύο μικροδορυφόρων, καταγραφή των υποσυστημάτων τους, κοινά υποσυστήματα μεταξύ των δύο μικροδορυφόρων, ποιες οι τρωτότητες σε κάθε υποσύστημα (Κεφάλαιο 5^{ο})
- *Εντοπισμός τρωτοτήτων ασφάλειας και κυβερνοασφάλειας αποστολής – λήψης σήματος του φορτίου (payload)*. Περιγραφή φορτίου (payload) των δύο μικροδορυφόρων, με βάση την αποστολή τους, που εντοπίζονται τρωτότητες (Κεφάλαιο 6^{ο})
- *Συμπεράσματα – Προτάσεις*. Ποια είναι τα συμπεράσματα που προκύπτουν, τι μπορεί να γίνει (Κεφάλαιο 7^{ο})

2. Μετάδοση της πληροφορίας

Αρκεί κάποιος να αναρωτηθεί πως θα μπορούσε να οριστεί η λέξη πληροφορία και θα αντιληφθεί ότι η λέξη αυτή έχει ένα βαθμό ιδιαιτερότητας. Όπως αναφέρθηκε παραπάνω, η πληροφορία της επιτυχίας της πτώσης της Τροίας, αποτελούσε το αντικείμενο μεταφοράς με συγκεκριμένη μέθοδο. Αντίστοιχα, η πληροφορία ήταν αυτό που αναζητούσαν να μεταφέρουν ή να υποκλέψουν εκατέρωθεν οι υπερδυνάμεις κατά τον Ψυχρό Πόλεμο προκειμένου να επικρατήσουν σε κάθε τομέα. Ακόμη και στο χώρο του θαλάσσιου εμπορίου, στην ενδυνάμωση και εξέλιξη του οποίου αποσκοπεί και η παρούσα εργασία, η πληροφορία είναι αυτή που θα σημάνει την επιτυχία μιας επιχείρησης απέναντι στους ανταγωνιστές της. Προκύπτει λοιπόν η ανάγκη να περιγραφεί η έννοια αυτή κατά το δυνατό καλύτερα, να καταγραφεί η σημαντικότητά της, να περιγραφεί ο τρόπος διάδοσής της μέσω δορυφορικών συστημάτων επικοινωνίας και να σημειωθεί το κανονιστικό πλαίσιο μέσα στο οποίο οφείλει να λειτουργεί όποιος επιθυμεί να ασχοληθεί με το χώρο των αεροδιαστημικών εφαρμογών προκειμένου να πετύχει τα επιθυμητά αποτελέσματα.

2.1 Ορισμός πληροφορίας – Γενική περιγραφή

«Πληροφορία: (1) στοιχείο, μήνυμα (είδηση, ανακοίνωση, δήλωση, αναφορά κτλ.) που περιέχει και μεταδίδει μια γνώση για κπ. ή για κτ.; (2α) ποιοτικός συντελεστής, που καθορίζει τη θέση ή την κατάσταση ενός συστήματος ελέγχου; (2β) το περιεχόμενο ενός μηνύματος, που συντίθεται από σημεία ενός κώδικα»

Το παραπάνω αποτελεί τον ορισμό του όρου «πληροφορία» όπως αναφέρεται στο διαδικτυακό Λεξικό της Κοινής Νεοελληνικής[3]. Όμως, παρόλο που στην ελληνική γλώσσα ο όρος φαίνεται να έχει σαφή προσδιορισμό, εάν αναζητήσει κάποιος τον ορισμό στην αγγλική, τότε προκύπτει ένα ενδιαφέρον αποτέλεσμα, που μάλλον ανατρέπει και την πρώτη εντύπωση που αποκόμισε στην ελληνική. Αυτό διότι στην αγγλική, όπως αναφέρεται στο διαδικτυακό CD [4], δεν φαίνεται να ορίζεται η λέξη, πέρα από το γενικό «γεγονότα σχετικά με μια κατάσταση, άτομο, συμβάν κ.α.», αλλά προσδιορίζεται καλύτερα αναλόγως του πεδίου που καλύπτει. Το τελευταίο εκτίθεται στο διαδικτυακό OD[5], όπου μεταξύ άλλων ο όρος «πληροφορία» εξετάζεται πλέον στην εννοιολογική του ερμηνεία, πέρα από μια απλοϊκή περιγραφή. Σημειώνεται η ιστορικότητά του και η τροποποίηση της χρήσης του στην πάροδο του χρόνου, καθώς και αναγνωρίζεται ότι σε μια τελευταία καταγραφή των πιο χρησιμοποιούμενων λέξεων, η πληροφορία κατέχει την 22η θέση, από την 346η που βρισκόταν το 1967.

Σύμφωνα με τον Madden (2000)[6], στην προσπάθειά του να περιγράψει την έννοια της πληροφορίας, με σκοπό να γίνει ευρύτερα αντιληπτή στο πεδίο της διαχείρισης της (Information Management), καταλήγει πως αντί της προσπάθειας ορισμού της λέξης με βάση τη μια επιστημονική θεωρία ή την άλλη, προς αποφυγή παρερμηνειών οι οποίες μπορεί να δημιουργηθούν ανάλογα με το θεωρητικό υπόβαθρο του αποστολέα και του παραλήπτη, προτιμότερο είναι να προσδιορίζεται ως *«… information should be defined as: a stimulus originating in one system that affects the interpretation by another system of either the second system's relationship to the first*

[3] Ινστιτούτο Νεοελληνικών Σπουδών (Ίδρυμα Μανόλη Τριανταφυλλίδη) (1998), *Λεξικό της κοινής νεοελληνικής*, http://www.greek-language.gr/greekLang/modern_greek/tools/lexica/triantafyllides/search.html?lq=πληροφορία&dq=

[4] Cambridge University Press (2019), *Cambridge Dictionary*, https://dictionary.cambridge.org/dictionary/english/information#dataset-cald4

[5] Oxford University Press (2019), Oxford Dictionaries, https://en.oxforddictionaries.com/definition/information; https://public.oed.com/blog/word-stories-information/#

[6] Madden A.D., October 2000, A definition of information, *Aslib Proceedings*, Vol 52, No.9, (343-349)

or of the relationship the two systems share with a given environment» (σελ. 348), δηλαδή «*... πληροφορία μπορεί να καλείται το πηγάζον σε ένα σύστημα κίνητρο που επηρεάζει την ερμηνεία από ένα άλλο σύστημα με βάση είτε τη σχέση του δεύτερου συστήματος με το πρώτο, είτε την κοινή σχέση των δύο συστημάτων με ένα συγκεκριμένο περιβάλλον*». Με τον τρόπο αυτό πιθανολογείται ότι το κοινό περιβάλλον, ή το πλαίσιο στο οποίο προκαλείται η επικοινωνία, προσδιορίζουν ορθότερα την έννοια της πληροφορίας και την κωδικοποιούν με τέτοιο τρόπο ώστε να γίνεται αντιληπτή από τους συνδιαλλαζόμενους.

Από τα ανωτέρω εμφανίζεται ανάγκη να ορίζεται κάθε φορά το πλαίσιο που θα περιβάλλει τον όρο πληροφορία. Για παράδειγμα, στη συγκεκριμένη εργασία, δε μπορεί να έχει την ίδια έννοια η πληροφορία που αποστέλλεται από το σταθμό εδάφους σε ένα μικροδορυφόρο και αντίστροφα για τους σκοπούς της λειτουργίας του, με την αναφορά στην πληροφορία που λαμβάνει και αποστέλλει μια κάμερα η οποία λειτουργεί ως το ωφέλιμο φορτίο (payload) ενός μικροδορυφόρου προς το σταθμό εδάφους και η οποία αποτελεί το σκοπό της αποστολής του.

Για να αποφευχθεί λοιπόν η όποια πιθανή παρερμηνεία στην παρούσα εργασία, ή έστω η απαίτηση προσδιορισμού του πεδίου στο οποίο αντιστοιχεί κάθε φορά που αναφέρεται, θα ληφθεί ως κοινό περιβάλλον της πληροφορίας, αυτό που περιγράφεται στη Θεωρία Πληροφορίας. Σύμφωνα με τον Ζορκάδη (2002)[7]

> «*Η συντακτική πληροφορία σχετίζεται με τα σύμβολα και τις σχέσεις μεταξύ αυτών, από τα οποία αποτελούνται τα μηνύματα. Η σημασιολογική πληροφορία σχετίζεται με τη σημασία και η πραγματική με τη χρήση και τη δυνατή επίπτωση των μηνυμάτων. Έτσι, ενώ ο συντακτικός τύπος της πληροφορίας αναφέρεται στη μορφή, ο σημασιολογικός και ο πραγματικός αναφέρονται στο περιεχόμενο*» (σελ.15)

και

> «*... η Θεωρία Πληροφορίας αναφέρεται στη συντακτική πληροφορία, δηλαδή η πληροφορία εξαρτάται από την πιθανότητα εμφάνισης των μηνυμάτων και όχι από τη σημασία τους*» (σελ.15-16).

[7] Ζορκάδης Β. (2002), Θεωρία Πληροφορίας και Κωδικοποίησης, Πάτρα, ΕΑΠ https://eclass.uop.gr/modules/document/file.php/TST244/Θεωρία Πληροφορίας και Κωδικοποίησης.pdf

Η επιλογή αυτή καθιστά δυνατή την ενιαία αντίληψη της πληροφορίας, αφού θα γίνεται αναφορά στον όγκο δεδομένων αποστολής και λήψης από το σταθμό εδάφους προς το μικροδορυφόρο και αντίστροφα, ανεξαρτήτως εάν αντιστοιχεί σε λειτουργική πληροφορία του συστήματος ή σε πληροφορία που απασχολεί τον σκοπό της αποστολής του μικροδορυφόρου.

Παράλληλα, έχοντας θέσει το περιβάλλον στο οποίο εντάσσεται η πληροφορία, είναι πλέον δυνατή και η ανάδειξη της σημαντικότητάς της σε σχέση με την επιτυχία ή μη της αποστολής ενός μικροδορυφόρου. Αυτό μπορεί να γίνει, εφόσον ληφθεί υπόψη ότι η σημασιολογική και η πραγματική πληροφορία, αφορούν ουσιαστικά στην ποιότητα των δεδομένων που αποστέλλονται και λαμβάνονται, δημιουργώντας μια ολότητα στην αξιολόγηση της πληροφορίας, αναγκαία προϋπόθεση για την μετέπειτα επιλογή εξασφάλισής της από πιθανές επιθέσεις και κυβερνοεπιθέσεις.

2.2 Μετάδοση πληροφορίας

Η μετάδοση πληροφορίας σε μια αποστολή μικροδορυφόρου αποτελεί έως σήμερα το κύριο μέλημα. Ανεξαρτήτως εάν αυτή επιτυγχάνεται επαναλαμβανόμενα ή μη, εάν είναι ολοκληρωμένη ή όχι, πολλές φορές ο μικροδορυφόρος θεωρείται ως έχοντας ολοκληρώσει επιτυχώς την αποστολή του, εφόσον έστω και μια φορά έχει καταφέρει να επικοινωνήσει με τον επίγειο σταθμό. Είναι αντιληπτό, η επιτυχία αυτή να εξαρτάται κυρίως από την δυνατότητα που παρέχεται από την εφαρμογή της τεχνολογίας επικοινωνίας δορυφόρων και πέρα από απρόβλεπτους παράγοντες, όπως κάποια βλάβη του συστήματος ή επαφή του μικροδορυφόρου με τα λεγόμενα «σκουπίδια του διαστήματος» (debris).

Από τη βιβλιογραφία (Elbert, (2008)[8]; Ippolito, (2017)[9]; Maral και Bousquet, (2009)[10]) προκύπτει ότι όλες οι ακολουθητέες τεχνικές πρόσβασης (MF-TDMA, SCPC, FDMA κ.α.), βασίζονται στην αρχή διάδοσης (εξίσωση ζεύξης- λαμβανόμενης ισχύος), όπου προβλέπεται πως ότι αποστέλλεται από ένα πομπό Tx, κεραίας εκπομπής κέρδους G_T, εκπεμπόμενης ισχύος P_T, με απόδοση διάδοσης που να μετράται από την ισοδύναμη ισοτροπικά ακτινοβολούμενη ισχύ EIRP, λαμβάνεται από ένα δέκτη Rx, κεραίας λήψης κέρδους G_R, μειούμενο από τις απώλειες της διαδρομής L_{FS}, ή όπως περιγράφεται σε μορφή μαθηματικών εξισώσεων (με κατάλληλη επιλογή μονάδων για κάθε μια)

$$EIRP = P_T * G_T \qquad \Rightarrow$$

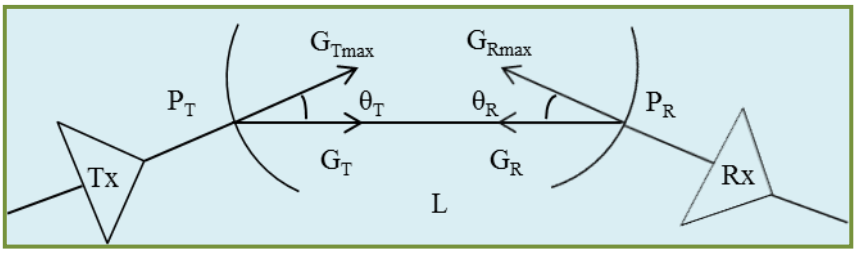
$$P_R = EIRP + G_R - L_{FS}$$

Σχηματικά η εξίσωση, σε απλοϊκή μορφή, περιγράφεται από το Σχήμα 1.

[8] Elbert B.R. (2008), Introduction to Satellite Communication, Third Edition, ARTECH HOUSE INC.

[9] Ippolito L.J. Jr. (2017), Satellite Communications Systems Engineering; Atmospheric Effects, Satellite Link Design and System Performance, Second Edition, JohnWiley & Sons Ltd

[10] Maral G. & Bousquet M. (2009), Satellite Communications Systems; Systems, Techniques and Technology, Fifth Edition, John Wiley & Sons Ltd



Σχήμα 1. Σχηματική απεικόνιση ζεύξης

Στο σημείο αυτό δεν πρέπει να παραβλεφθεί, ότι όλες οι επικοινωνίες που χρησιμοποιούν δορυφορικά συστήματα, όπως ορίζεται από τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunication Union – (ITU)) στα Κράτη – Μέλη της, αλλά και στις ιδιωτικές επιχειρήσεις που συμμετέχουν επίσης ως μέλη σε αυτή, αφού η Ένωση αποτελεί συνεργασία δημόσιου – ιδιωτικού τομέα (Public Private Partnership, PPP)), οφείλουν να συμπλέουν με τις κανονιστικές – ρυθμιστικές διατάξεις που έχουν θεσπιστεί. Σε ποιες συχνότητες (frequency bands) οφείλουν να λειτουργούν, το κόστος χρήσης των επικοινωνιακών συστημάτων σε αυτές και άλλα παρόμοια θέματα,, αποτελούν στοιχεία ανάδειξης της σημασίας που δίνεται στη μετάδοση της πληροφορίας και με τη χρήση αεροδιαστημικών εφαρμογών.

Τα βασικά στοιχεία λοιπόν, διασύνδεσης της μετάδοσης της πληροφορίας με την τεχνολογία επικοινωνίας δορυφόρων, σε συνδυασμό με τη Θεωρία Πληροφορίας και τη συμμόρφωση με τις κανονιστικές – ρυθμιστικές διατάξεις της ITU, όπως περιγράφηκαν συνοπτικά, δημιουργούν πλέον ένα πιο ολοκληρωμένο υπόβαθρο για την εξέλιξη της παρούσας έρευνας. Ειδικότερα, έχει καταστεί σαφές ότι ο όγκος της πληροφορίας και η ποιότητά της, δύο σημαντικά στοιχεία της αποστολής ενός μικροδορυφόρου, μπορούν να θεωρούνται ρυθμισμένα σε τέτοιο βαθμό ώστε να διασφαλίζεται η επιτυχής διάδοσή της και πιθανόν να είναι ήδη πρόσφορο το πεδίο ενίσχυσης της ασφάλειάς της από επιθέσεις και κυβερνοεπιθέσεις.

3. Μικροδορυφόρος

Στο κεφάλαιο αυτό θα περιγραφεί, όχι σε εκτενή βαθμό, καθώς κάτι τέτοιο θα μπορούσε να αποτελέσει αντικείμενο μιας άλλης επιστημονικής έρευνας, το σύστημα μικροδορυφόρος και συγκεκριμένα το σύστημα cubesat. Θα παρατεθεί το σύνολο των συνήθων υποσυστημάτων που αποτελούν και το τυπικό, ή ενδεικτικό θα υποστήριζε άλλος, λειτουργικό του σύστημα. Σε αυτό το κεφάλαιο δε θα αναλυθεί τι συμβαίνει με το ωφέλιμο φορτίο (payload) καθώς αυτό αποτελεί επιλογή κάθε κατασκευαστή μικροδορυφόρων, έπειτα από τις απαιτήσεις που θέτονται, είτε από τον ίδιο, είτε από τους πελάτες – χρήστες, με βάση την αποστολή που πρέπει να εκτελεστεί. Αντιθέτως θα απαριθμηθούν κάποια ωφέλιμα φορτία που χρησιμοποιούνται, αλλά και κάποια πιο σπάνια που αναδεικνύουν ωστόσο τις δυνατότητες των μικροδορυφόρων.

3.1 Cubesat– Γενική περιγραφή – Πεδίο χρήσης

Για αρχή θα πρέπει να υπάρξει ένας βασικός διαχωρισμός στις έννοιες μικροδορυφόρος και cubesat, καθώς όπως αναφέρεται στη βιβλιογραφία (Chin κ.συν. (2017)[11]) μικροδορυφόρος μπορεί να θεωρείται κάθε μικρού μεγέθους δορυφορικό σύστημα που έχει βάρος κάτω από 300 kgr, σε αντίθεση με τον cubesat που όχι μόνο ζυγίζει πολύ πιο λίγο, αλλά έχει συγκεκριμένες διαστάσεις και σχήμα που οδηγούν και σε πολύ χαμηλότερο κόστος κατασκευής. Παράλληλα, η τυποποίηση του (σχήμα, διαστάσεις και βάρος) οδηγεί και στη δημιουργία μαζικής παραγωγής, τελευταίας λέξης της τεχνολογίας, ετοιμοπαράδοτων και εύκολων στη χρήση μερών (COTS) που συντελούν στην ακόμη περισσότερο μείωση του κόστους παραγωγής του.

Πιο συγκεκριμένα, ο cubesat, που όπως είναι ευνόητο πήρε την ονομασία του από το σχήμα του που κυβίζει, έχει ως βασικό μέγεθος μονάδας το 1U. Το 1U ανταποκρίνεται σε κύβο μεγέθους πλευράς 10 cm με μάζα βάρους περίπου 1 με 1.33 kgr, ενώ πλέον υπάρχουν cubesats με μέγεθος 1.5U, 2U, 3U και 6U. Όπως είναι αντιληπτό η αντιστοιχία στο μέγεθος πηγάζει στη δημιουργία cubesats με τετραγωνική βάση και ύψος τέτοιο που να προκύπτει ο πολλαπλάσιος όγκος.

Ένας, τόσο συγκεκριμένου μεγέθους, μικροδορυφόρος, μπορεί να μεταφέρει περιορισμένα ωφέλιμα φορτία. Ως εκ τούτου, γεννάται το ερώτημα ποιους τομείς μπορεί να εξυπηρετήσει ένας cubesat και πόσους παράλληλα στην αποστολή του σύμφωνα με το μέγεθός του. Σε αυτό το ερώτημα ως αρχική απάντηση, καθώς παρακάτω θα σημειωθούν, όπως προαναφέρθηκε, κάποια ωφέλιμα φορτία που χρησιμοποιούνται, μπορεί να δοθεί από στοιχεία που αναφέρονται σε πίνακα του 2014 των Jakhu & Pelton (όπως αναφέρουν οι Madry, Martinez, Laufer (2018)[12]). Εντούτοις κάποια στοιχεία έχουν πλέον τροποποιηθεί σε σχέση με το 2014, καθώς με cubesats εξυπηρετούνται πλέον και περισσότεροι τομείς, όπως για παράδειγμα η μετεωρολογία ή αυξάνεται η χρήση των cubesats σε άλλους, σύμφωνα με το

[11] Chin J. κ.συν., (2017), CubeSat 101: Basic Concepts and Processes for First-Time CubeSat Developers, Revision, NASA CubeSat Launch Initiative

[12]Madry S., Martinez P., Laufer R. (2018), Innovative Design, Manufacturing and Testing of Small Satellites, Springer Praxis Books, Springer International Publishing AG, part of Springer Nature

διαδικτυακό τόπο nanosats.eu[13], όπου αναφέρονται σε βάση δεδομένων σχεδόν το σύνολο των μικροδορυφόρων που έχουν εκτελέσει, εκτελούν και πρόκειται να εκτελέσουν αποστολή. Ενδεικτικά στον Πίνακα 1 σημειώνονται μερικά από αυτά.

Τομείς που εξυπηρετούνται από cubesats 1U έως 6U	**Συχνότητα**
Τηλεπικοινωνία	Σπάνια με αυξητική τάση σε επίπεδο έρευνας
Μετάδοση πληροφορίας (δεδομένα/μηνύματα)	Συχνά με αυξητική τάση
Τηλεπισκόπηση	Ολοένα και περισσότερο
Αναμετάδοση από επίγεια συστήματα	Συχνά
Μετεωρολογία	Περιστασιακά με αυξητική τάση

Πίνακας 1. Συνήθεις τομείς που αξιοποιούν cubesats

[13] https://www.nanosats.eu/#database

3.2 Υποσυστήματα μικροδορυφόρου – Περιγραφή

Στη συνέχεια θα αναφερθούν περιληπτικά τα λειτουργικά συστήματα ενός cubesat (cubesat platform), με βάση τη βιβλιογραφία (Madry, Martinez, Laufer (2018)[14], Amandine Denis κ.συν. (2015)[15]; Bonyan (2010)[16]; Addaim, Kherras, Zantou (2010)[17]), τα πιθανότερα ωφέλιμα φορτία (payload) που χρησιμοποιούνται, καθώς και κάποια ακόμη υποσυστήματα που οφείλεται να περιλαμβάνονται ως μέρος του συνόλου του συστήματος μικροδορυφόρος (cubesat), προκειμένου να είναι δυνατό να λεχθεί ότι έχει ολοκληρωθεί η συνοπτική περιγραφή για τους σκοπούς της παρούσας εργασίας.

3.2.1 Λειτουργικά υποσυστήματα – cubesat platform

Τα λειτουργικά υποσυστήματα ενός cubesat που απαντώνται συνηθέστερα είναι τα ακόλουθα:

- Δομικό Υποσύστημα (Structural subsystem – (SS))
- Υποσύστημα Ελέγχου Θέσης στο Χώρο (Attitude Determination and Control Subsystem – (ADCS))
- Υποσύστημα ηλεκτρικής τροφοδοσίας (Electrical Power System – (EPS))
- Υποσύστημα Τηλεμετρίας, Εντοπισμού και Ελέγχου (Telemetry, Tracking & Command – (TT&C))
- Υποσύστημα ελέγχου θερμοκρασίας (Thermal Control Subsystem – (TCS))
- Υποσύστημα Ελέγχου (Command and Data Handling Subsystem – (CDHS))

Πιο κάτω αναλύονται περιληπτικά

[14] Madry S., Martinez P., Laufer R. (2018), Innovative Design, Manufacturing and Testing of Small Satellites, Springer Praxis Books, Springer International Publishing AG, part of Springer Nature
[15] Amandine Denis κ.συν. (2015), QB50 System Requirements and Recommendations, Issue 7, VKI
[16] Bonyan H. (2010), Looking into Future - Systems Engineering of Microsatellites, In Thawar T. Arif (Ed.)Aerospace Technologies Advancements, InTech
[17] Addaim A., Kherras A., Zantou El B., (2010) Design of Low-cost Telecommunications CubeSat-class Spacecraft, In Thawar T. Arif (Ed.)Aerospace Technologies Advancements, InTech

- Δομικό Υποσύστημα (**Structural subsystem – (SS)**)

Τα χαρακτηριστικά που αναφέρθηκαν στην παράγραφο 3.1 αποτελούν ουσιαστικά το πρώτο υποσύστημα ενός cubesat. Για να θεωρείται ως τέτοιος και να γίνει αποδεκτός κατά την αξιολόγησή του προ πτήσης, θα πρέπει να πληροί το μέγεθος, το βάρος και το σχήμα στα οποία αντιστοιχεί, δηλαδή σε 1U, 1.5U, 2U, 3U ή 6U. Σύμφωνα με τα σχέδια του (blueprints), το δομικό πλαίσιο ή αλλιώς ο σκελετός, που θα περιβάλλει τα υπόλοιπα υποσυστήματα θα δημιουργηθεί από συγκεκριμένο ανθεκτικό υλικό.

- Υποσύστημα Ελέγχου Θέσης στο Χώρο (**Attitude Determination and Control Subsystem – (ADCS)**)

Είναι υπεύθυνο για την επαναφορά του cubesat στην προϋπολογισθείσα θέση του στο χώρο (άξονες x, y, z), μετά την εκτόξευσή του από το διαστημικό σταθμό, ώστε να εκπληρώσει την αποστολή του, αλλά και τη διόρθωση – μεταβολή της θέσης αυτής, εφόσον κριθεί σκόπιμο κατά τη διάρκεια της αποστολής, καθώς και επαναφοράς σε περιπτώσεις περιδίνησης. Για το σκοπό αυτό, προκειμένου δηλαδή να γίνεται αντιληπτή η ανάγκη επαναφοράς, χρησιμοποιούνται magnetorques για τη σταθεροποίηση, και μαγνητόμετρα (magnetometers) και γυροσκόπια (gyroscopes) για να καθίσταται αυτή επιτυχής.

- Υποσύστημα ηλεκτρικής τροφοδοσίας (**Electrical Power System – (EPS)**)

Από τον τίτλο είναι προφανές ότι αποτελεί το υποσύστημα παροχής ηλεκτρικής ενέργειας στα υπόλοιπα υποσυστήματα. Θα πρέπει να είναι ικανό να διατηρήσει την παροχή ηλεκτρικής ενέργειας καθ’ όλη τη διάρκεια της αποστολής του cubesat, και να τεθεί σε λειτουργία όταν ο cubesat εκτοξευθεί από το διαστημικό σταθμό σε τροχιά γύρω από τον πλανήτη. Το ποσοστό αποφόρτισης της μπαταρίας του μπορεί να προβλεφθεί από την κατανάλωση των υπολοίπων υποσυστημάτων, συμπεριλαμβανομένου και του μη λειτουργικού του υποσυστήματος, δηλαδή του υποσυστήματος ωφέλιμου φορτίου (payload), το οποίο θα αποστέλλει πληροφορίες που αφορούν το σκοπό της αποστολής. Επίσης, να σημειωθεί ότι υπάρχει η

δυνατότητα επαναφόρτισης της μπαταρίας με τη συλλογή ηλιακής ενέργειας, εφόσον υπάρχει, κατασκευαστικά, η δυνατότητα προσθήκης φωτοβολταϊκών συλλεκτών.

- Υποσύστημα Τηλεμετρίας, Εντοπισμού και Ελέγχου (**Telemetry, Tracking & Command – (TT&C)**)

Το υποσύστημα αυτό είναι υπεύθυνο για την μετάδοση των μοναδικών σημάτων που εκπέμπει ο cubesat προκειμένου να αναγνωριστεί ανάμεσα σε πολλά άλλα αντίστοιχα σήματα που λαμβάνει ο σταθμός εδάφους από άλλους cubesats ή δορυφορικά συστήματα. Επίσης είναι υπεύθυνο για την επικοινωνία με το σταθμό εδάφους όσον αφορά την ομαλή λειτουργία του cubesat και τις όποιες πιθανές νέες εντολές σταλούν προς αυτό για τη λειτουργία του. Έχει το ρόλο του διακόπτη ενεργοποίησης όταν ο cubesat εκτοξευθεί από το διαστημικό σταθμό για την εκτέλεση της αποστολής του. Χρησιμοποιούνται για τη λειτουργία του αρχές επικοινωνιών μετάδοσης δεδομένων, με αξιοποίηση της κεραίας ή των κεραιών που έχει ο cubesat.

- Υποσύστημα ελέγχου θερμοκρασίας (**Thermal Control Subsystem – (TCS)**)

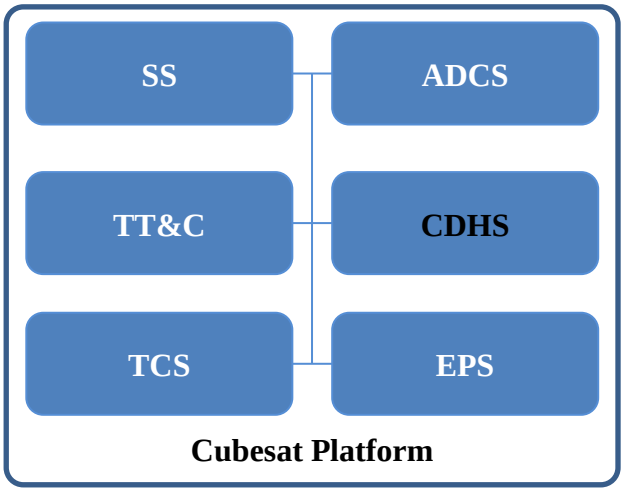
Δεδομένης της εναλλασσόμενης εξαιρετικά υψηλής και εξαιρετικά χαμηλής θερμοκρασίας που συναντά κατά την τροχιά του γύρω από τον πλανήτη ο cubesat, το υποσύστημα αυτό είναι υπεύθυνο για τη διατήρηση της λειτουργικής θερμοκρασίας των ηλεκτρονικών συστημάτων όταν αυτά είναι σε λειτουργία και σε κατάσταση επιβίωσης όταν δεν λειτουργούν. Για αυτό χρησιμοποιούνται τεχνικές βασισμένες στη θεωρία της μεταφοράς θερμότητας, όπως η τοποθέτηση ενεργητικών ή παθητικών μέσων. Για παράδειγμα χρησιμοποιούνται shutters, cryogenics, coatings, heaters/coolers και insulation blankets, heat pipes, sun shields, radiation fins, αντίστοιχα.

- Υποσύστημα Ελέγχου (**Command and Data Handling Subsystem – (CDHS)**)

Είναι το υπεύθυνο υποσύστημα για τον έλεγχο της καλής λειτουργίας του cubesat. Από αυτό μεταδίδονται όλες οι πληροφορίες στα υπόλοιπα υποσυστήματα για την

εκτέλεση των εργασιών τους και συντονίζει τη μεταφορά των δεδομένων με τέτοιο τρόπο ώστε το συνολικό σύστημα να εκτελεί τη αποστολή του σύμφωνα με το σχεδιασμό. Αξιοποιεί τα στοιχεία που παρέχονται από το υποσύστημα τηλεμετρίας, εντοπισμού και ελέγχου προκειμένου να «αντιλαμβάνεται» το σύστημα τη θέση του, το χρόνο, την ομαλή «πλεύση» του και να αξιοποιεί τις εντολές του σταθμού εδάφους. Για τις δυνατότητες αυτές αξιοποιείται το λογισμικό που λειτουργεί στον ηλεκτρονικό υπολογιστή που φέρει ο cubesat και οι αισθητήρες του.

Στο σχήμα 2 που ακολουθεί φαίνεται μια συνήθης ή αλλιώς τυπική διασύνδεση, όχι μοναδική, των λειτουργικών υποσυστημάτων ενός cubesat.



Σχήμα 2. Συνήθης cubesat platform

Σε αυτό το σημείο οφείλεται να σημειωθεί ότι, τα παραπάνω καταγράφηκαν ως τα συνηθέστερα απαντώμενα υποσυστήματα, αλλά πλέον έχει αρχίσει να χρησιμοποιείται ολοένα και περισσότερο και το υποσύστημα πρόωσης (**Propulsion Subsystem – (PS)**) με χρήση μικροπροωθητήρων (microthrusters), προκειμένου να καθίσταται εφικτή η διόρθωση της τροχιάς του cubesat και η συνέχιση της εκτέλεσης της αποστολής του. Αυτό, σε συνδυασμό με δυνατότητες τις οποίες μπορεί να παρέχει ένα κατάλληλο EPS, το οποίο με επαναφόρτιση να μπορεί δηλαδή να επιμηκύνει τη διάρκεια ζωής και λειτουργίας του cubesat, είναι ικανό να καταστήσει το μικροδορυφόρο μια ευρύτερη τεχνολογική λύση στην αγορά.

3.2.2 Ωφέλιμο φορτίο (payload)

Όπως σημειώθηκε στην αρχή του κεφαλαίου, το ωφέλιμο φορτίο (payload) είναι διαφορετικό για κάθε σύστημα και εξαρτάται από τις απαιτήσεις του πελάτη – χρήστη ή του κατασκευαστή. Μερικά από αυτά, όπως έχουν καταχωρηθεί στη βάση δεδομένων του διαδικτυακού τόπου nanosats.eu[18] και τα οποία αντιστοιχούν και στους τομείς που εξυπηρετούνται από τη χρήση των cubesats, είναι συσκευές μετάδοσης σήματος AIS και GPS, κάμερες, κεραίες νέας τεχνολογίας με δυνατότητας αποστολής και λήψης μεγαλύτερου όγκου δεδομένων ανά κανάλι επικοινωνίας και αισθητήρες για μετρήσεις μετεωρολογικών προγνώσεων. Φυσικά υπάρχουν και πιο σπάνια ωφέλιμα φορτία, όπως για παράδειγμα η μελέτη του γραφενίου που αποτέλεσε payload για το Lambdasat, καθώς και υπηρεσίες φωνητικής επικοινωνίας με χρήση κατάλληλων routers, που αποτελεί payload συστοιχιών (αστερισμού) cubesats (cubesats' constellation), όπως οι Diamond Blue, Diamond Red και Diamond Green.

3.2.3 Υπόλοιπα υποσυστήματα

Επίσης, στο σύστημα cubesat σύμφωνα με τη βιβλιογραφία (Chin κ.συν. (2017)[19]) οφείλουν να συγκαταλέγονται το σύστημα διανομής και το σύστημα εκτόξευσης, cubesat dispenser system και launch system (launch rocket) αντίστοιχα. Για να λάβει θέση στο σύστημα εκτόξευσης ο cubesat πρέπει πρώτα να τοποθετηθεί σε κατάλληλα διασκευασμένο διανομέα που συνήθως έχει χωρητικότητα 3U ή 6U, μπορεί δηλαδή να περιέχει έως τρεις ή έξι μεγέθους 1U cubesats αντίστοιχα, ή οποιοδήποτε άλλο συνδυασμό που να συμπληρώνει τον όγκο. Ρόλος του είναι η προστασία του cubesat έως τη στιγμή που θα αφεθεί στο διάστημα για να εκτελέσει την αποστολή του. Όσο για το σύστημα εκτόξευσης, αυτό ως μέσο αποστολής του cubesat στο διαστημικό σταθμό από όπου θα προωθηθεί στο διάστημα για την εκτέλεση της αποστολής του,

[18] https://www.nanosats.eu/#database

[19] Chin J. κ.συν., (2017), CubeSat 101: Basic Concepts and Processes for First-Time CubeSat Developers, Revision, NASA CubeSat Launch Initiative

μπορεί να είναι οποιοσδήποτε πύραυλος που αποστέλλεται για οποιαδήποτε άλλη αποστολή προς το διάστημα, όπως για παράδειγμα μια αποστολή εφοδιασμού.

Τέλος, σε όλη αυτή την περιγραφή δεν μπορεί να απαλειφθεί το υποσύστημα του σταθμού εδάφους, προκειμένου να υπάρξει μια συνολική περιγραφή του συστήματος μικροδορυφόρος (cubesat). Στο σταθμό εδάφους σύμφωνα με τη βιβλιογραφία (Agasid κ.συν. (2015)[20]) πρέπει να περιλαμβάνονται τα ακόλουθα

- Επιχειρησιακό κέντρο ελέγχου πλατφόρμας (**Spacecraft Operations Control Center – (SOCC)**)
- Επιχειρησιακό κέντρο ελέγχου ωφέλιμου φορτίου (**Payload Operations Control Center – (POCC)**)
- Κέντρο Ελέγχου αποστολής (**Mission Control Center – (MCC)**)
- Κέντρο επεξεργασίας δεδομένων (**Data Processing Center – (DPC)**)

Φυσικά, δεν έχει σημασία εάν όλα αυτά βρίσκονται στον ίδιο χώρο. Όμως, όπως γίνεται αντιληπτό, για κάθε κέντρο πρέπει να αντιστοιχούν λογισμικά επεξεργασίας δεδομένων που αναλύουν τη λειτουργία του cubesat, τη λειτουργία και απόδοση του ωφέλιμου φορτίου καθώς και βοηθούν στην αξιολόγηση του συνόλου της αποστολής. Ως προς το hardware που απαιτείται, εκεί περιλαμβάνονται υπολογιστής ή υπολογιστές και η απαραίτητη κεραία.

[20] Agasid E. κ.συν. (2015), Small Spacecraft Technology State of the Art, Mission Design Division Ames Research Center, Moffett Field, NASA, California

4. Ασφάλεια και Κυβερνοασφάλεια – Τρωτότητες – Γενική περιγραφή

Όπως περιγράφηκε παραπάνω, η μετάδοση της πληροφορίας αποτελεί το σημαντικότερο μέλημα επιτυχίας της αποστολής ενός μικροδορυφόρου. Αυτό όμως, ταυτόχρονα αναδεικνύεται και ως πρόβλημα, αφού η σημαντικότητα αυτή «ελκύει» και τον αρνητισμό. Η επιθυμία αποτυχίας μιας αποστολής, μπορεί ίσως να ξεπερνά αυτή της επιτυχίας. Ειδικά όταν διακυβεύονται μεγάλα συμφέροντα, όπως για παράδειγμα η επικράτηση στο χώρο του διαστήματος, η διατήρηση του αισθήματος της ασφάλειας των πολιτών μιας χώρας αλλά και η οικονομική επικράτηση στο χώρο της επιχειρηματικότητας. Με άλλα λόγια, η αποτυχία της αποστολής ενός αεροδιαστημικού συστήματος, ή έστω η απειλή της ομαλής διεξαγωγής της, σε μια εποχή που η χρήση ψηφιακής διασύνδεσης καλύπτει τομείς, όπως χωρική κυριαρχία, ασφάλεια, δημόσια διοίκηση και οικονομία, ίσως να απασχολεί περισσότερους «παίκτες» παγκοσμίως, από όσους φαντάζεται κάποιος.

Για το λόγο αυτό στις επόμενες ενότητες του παρόντος κεφαλαίου, θα γίνει προσπάθεια περιγραφής εννοιών που αφορούν την ασφάλεια και κυβερνοασφάλεια, προκειμένου και σε αυτό το πεδίο να δημιουργηθεί ένα ομογενές υπόβαθρο για την περαιτέρω πορεία της εργασίας. Μερικές από τις έννοιες αυτές είναι: ασφάλεια διαστήματος και κυβερνοασφάλεια (space security και cybersecurity), επιθέσεις και κυβερνο-επιθέσεις (security attacks και cyber-attacks), κίνδυνος (risk) και τρωτότητα (vulnerability). Παράλληλα, θα σημειωθούν η σχέση της ασφάλειας και κυβερνοασφάλειας με τη διαφύλαξη της πληροφορίας, η επιβλαβής σχέση ανάμεσα στην ύπαρξη τρωτότητας σε ένα σύστημα και στην πληροφορία, καθώς και ποια μπορεί να είναι η μεθοδολογία εντοπισμού της τρωτότητας, προκειμένου να αντιμετωπιστεί.

4.1 Ασφάλεια και Κυβερνοασφάλεια

Για να ολοκληρωθεί ο λειτουργικός «οδικός χάρτης» της παρούσας εργασίας, ώστε στη συνέχεια να καταγραφούν ομοιογενώς και να αναλυθούν οι δύο μικροδορυφόροι που έχουν επιλεγεί ως αντικείμενο της έρευνας, θα πρέπει να τεθούν υπόψη κάποιες παράμετροι και στο πεδίο της ασφάλειας. Πιθανόν πολλοί να αντιλαμβάνονται, ή και να χρησιμοποιούν, τον όρο κυβερνοασφάλεια, ως ότι αυτός αποτελεί το υπερσύνολο όλων των θεμάτων ασφαλείας που αφορούν τις δορυφορικές εφαρμογές, δεδομένου ότι τα δορυφορικά συστήματα χρησιμοποιούν τεχνολογίες ΤΠΕ. Πρέπει να σημειωθεί, ότι δεν ισχύει αυτό, καθώς η κυβερνοασφάλεια λειτουργεί περισσότερο ως υποσύνολο της «ασφάλειας του διαστήματος» και επικεντρώνεται σε πιο εξειδικευμένα θέματα. Άλλωστε όπως επισημαίνουν οι Livingstone και Lewis (2016)[21]

> «*The intersection of space security and cybersecurity is not a new problem, but it has remained largely unrecognized as a potentially significant vulnerability. It thus remains unaddressed in practical mechanisms. This is despite the increasing dependence on the space-related goods and services to support modern communities as space becomes increasingly intrinsic to all elements of national and international infrastructure*»,

δηλαδή

> «*Η διασταύρωση της ασφάλειας του διαστήματος και της κυβερνοασφάλειας δεν αποτελεί νέο πρόβλημα, αλλά παραμένει ως επί το πλείστον μη αναγνωρισμένο ως δυνητικά σημαντική τρωτότητα. Συνεπώς, παραμένει αδιευκρίνιστο σε πρακτικούς μηχανισμούς. Αυτό συμβαίνει παρά την αυξανόμενη εξάρτηση από τα αγαθά και τις υπηρεσίες που σχετίζονται με το διάστημα για τη στήριξη των σύγχρονων κοινοτήτων καθώς το διάστημα γίνεται όλο και περισσότερο εγγενές σε όλα τα στοιχεία της εθνικής και διεθνούς υποδομής*».

Συμπερασματικά, σχέση μεταξύ των δύο ειδών ασφάλειας υφίσταται, ως η ένωση των δύο συνόλων, η ύπαρξη δηλαδή κοινών στοιχείων, εάν ακολουθηθεί η αντίστοιχη Θεωρία Συνόλων, ωστόσο οφείλεται να προσδιοριστεί η σχέση αυτή διεξοδικότερα,

[21] Livingstone D., Lewis P., (2016), "Space, the Final Frontier for Cybersecurity?", London, The Royal Institute of International Affairs Chatham House

για να μην θεωρείται δυνητική τρωτότητα. Για την παρούσα εργασία, η προσπάθεια αυτή, η οποία διενεργείται μόνο σε επίπεδο καταχώρησης των εννοιών για να υπάρξει μια τυπική αντίληψη των διαφορών των δύο συνόλων, θα βασιστεί στην αξιοποίηση των όρων, όπως αυτοί περιγράφονται σε κείμενα της Μεγάλης Βρετανίας και της Ελλάδας.

Συναφώς, ο όρος «ασφάλεια του διαστήματος» εμφανίζεται για τη Μεγάλη Βρετανία στη Εθνική Πολιτική για την Ασφάλεια στο Διάστημα (2014)[22] με την ακόλουθη φράση: «*We define space security as having safe, assured and sustainable access to space capabilities, with adequate resilience against threats and hazards*» (σελ.7), δηλαδή «*ορίζουμε την ασφάλεια του διαστήματος σαν να έχουμε ασφαλή, επιβεβαιωμένη και βιώσιμη πρόσβαση στις δυνατότητες στο διάστημα, με επαρκή ανθεκτικότητα έναντι απειλών και κινδύνων*».

Αντίστοιχα, όπως σημειώνεται στην Εθνική Στρατηγική Κυβερνοασφάλειας της χώρας μας (Υπουργείο Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης (2018)[23])

> «*Ο όρος "κυβερνοασφάλεια" αναφέρεται σε όλες εκείνες τις δράσεις και τις ενέργειες που ενδείκνυνται και πρέπει να γίνουν, προκειμένου να διασφαλιστεί η προστασία του κυβερνοχώρου από εκείνες τις απειλές που είναι άμεσα συνυφασμένες με αυτόν και που μπορούν να βλάψουν τα αλληλοεξαρτώμενα συστήματα Τεχνολογιών Πληροφορικής και Επικοινωνιών ΤΠΕ*»,

Στο σημείο αυτό οφείλει να παρατηρηθεί ότι κοινός παρονομαστής στους δύο ορισμούς προκύπτει να είναι η έννοια «απειλή» η οποία θα περιγραφεί σε επόμενη ενότητα του κεφαλαίου αυτού.

[22] HM Government, (2014), National Space Security Policy

[23] Υπουργείο Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, (2018), Εθνική Στρατηγική Κυβερνοασφάλειας, 3η Αναθεώρηση

Χρήσιμη κρίνεται και η περιγραφή του όρου «ανθεκτικότητα» (resilience). Στη βιβλιογραφία απαντάται αρκετά (Thompson, Ryan, Slay και McLucas (2016)[24]; Ercan και Kale (2017)[25]), καθώς αποτελεί το επόμενο στάδιο στο οποίο πρέπει να μετακινηθεί ένα σύστημα για να επέλθει κανονικότητα στη λειτουργία του και στην ασφάλειά του, όταν η ασφάλεια του έχει παραβιαστεί. Η ανθεκτικότητα, στην παρούσα εργασία θα χρησιμοποιηθεί με την ευρεία έννοια που ορίστηκε εδώ, προς διευκόλυνση του αναγνώστη, καθώς στη βιβλιογραφία σημειώνονται και ειδικότερες καταστάσεις του όρου και υποκατηγορίες προσδιορισμού του, όπως η ανίχνευση (detection), η αντικατάσταση (replacement), η ανάλυση (resolution), η διάσπαση (disaggregation), η κατανομή (distribution), η διαποικίληση (diversification), η εξαπάτηση (deception), ο πολλαπλασιασμός (proliferation) και η προστασία (protection), οι οποίες όμως θεωρούνται εξειδικευμένες.

[24] Thompson M.A., Ryan M.J., Slay J. and McLucas A.C., 2016, Harmonized taxonomies for security and resilience, Information Security Journal: A Global Perspective, Vol. 25, Nos. 1–3, 54–67, Taylor & Francis

[25] Ercan C., Kale İ., 2017, The role of space in the security and defence policy of Turkey. A change in outlook: Security in space versus security from space, Space Policy, 42, 17–25, Elsevier Ltd.

4.2 Τρωτότητες

Όπως προκύπτει από τη βιβλιογραφία (Thompson, Ryan, Slay και McLucas (2016)[26]), η αποσαφήνιση, και σε αυτή την ενότητα, των χρησιμοποιούμενων όρων είναι χρήσιμη. Για τις ανάγκες, λοιπόν, της εργασίας, θα καταγραφούν πολύ περιληπτικά οι έννοιες

- Κίνδυνος (risk)
- Απειλή (threat)
- Τρωτότητα (vulnerability)
- Επίθεση και Κυβερνο-επίθεση (attack και cyberattack)
- Κενό ασφαλείας (cybersecurity breach)
- Τρόποι και μέσα επίθεσης (counterspace weapons)
- Αντίμετρα (countermeasure)

και θα αναδειχθεί η συσχέτισή τους.

Κίνδυνος

Ως κίνδυνος συνήθως περιγράφεται η πιθανότητα ένα συμβάν να λάβει χώρα, όπως μια απειλή που εκμεταλλεύεται τρωτότητες ενός συστήματος και οι επιπτώσεις που επιφέρει σε σημαντικά στοιχεία, για παράδειγμα σε λειτουργικό υποσύστημα ενός μικροδορυφόρου.

Απειλή

Απειλή μπορεί να χαρακτηριστεί ως το ενδεχόμενο πραγματοποίησης μιας μη εξουσιοδοτημένης ενέργειας σε ένα μέσο, όπως για παράδειγμα το ενδεχόμενο παροχής εντολής παύσης λειτουργίας σε ένα σύστημα χωρίς έγκριση.

Για την έννοια αυτή, όπως προαναφέρθηκε και στην εισαγωγή του κεφαλαίου, οφείλεται να καταγραφεί ότι μπορεί να έχει επιρροή σε πολλούς τομείς.

[26] Thompson M.A., Ryan M.J., Slay J. and McLucas A.C., 2016, Harmonized taxonomies for security and resilience, Information Security Journal: A Global Perspective, Vol. 25, Nos. 1–3, 54–67, Taylor & Francis

Το ερώτημα που μπορεί να τεθεί είναι, για ποιο λόγο κάποιος να προβεί σε εφαρμογή ασφαλείας και κυβερνοασφάλειας σε ένα μικροδορυφόρο, ή διαφορετικά, για ποιο λόγο κάποιος να αναλωθεί σε μια επίθεση ή κυβερνο-επίθεση προς ένα μικροδορυφόρο. Ως δυνατή απάντηση που πιθανόν να δοθεί, είναι, ότι πρέπει πρώτα να εντοπιστεί ο αντίκτυπος που θα έχει μια τέτοια επίθεση, προκειμένου να αιτιολογηθεί εάν αξίζει να προβεί κάποιος σε μια τέτοια ενέργεια.

Ο αντίκτυπος κάθε επίθεσης και κυβερνο-επίθεσης, έχει άμεση σχέση με την έμμεση βλάβη στον πελάτη – χρήστη, για τον οποίο εκτελεί αποστολή ή γενικότερα εξυπηρετεί, ο «στόχος» που πλήγεται. Για το σκοπό αυτό, θα παρατεθούν μερικοί τομείς, μέσα από τους οποίους μπορούν να εντοπιστούν δυνητικοί πελάτες – χρήστες που μπορεί να απειληθούν, καθώς και θέσεις ερευνητών που υποστηρίζουν αυτή την ύπαρξη απειλής προς τους τομείς αυτούς.

Χωρική κυριαρχία – Ασφάλεια.

Η επίγνωση των φίλιων θέσεων και της κατάστασης ετοιμότητάς τους, καθώς και των εχθρικών, έχει σημαντικό ρόλο στην άμυνα μιας χώρας, τα μετεωρολογικά στοιχεία προκειμένου να σχεδιαστούν τα στρατηγικά πλάνα για την ισχυροποίηση της ομοίως, αλλά και η επιτήρηση, χερσαία και θαλάσσια, είτε ως situational awareness είτε ως surveillance, ώστε να διαφυλάσσεται η ασφάλεια των πολιτών από εγκληματικές ενέργειες, έχουν τη δική τους αξία και τα δεδομένα (πληροφορίες) που διακινούνται για την δυνατότητα αυτή κρίνονται ως ζωτικής σημασίας.
Τα παραπάνω εκτεθέντα, αποτελούν ήδη θέμα διερεύνησης στη γειτονική Τουρκία, όπου δίνεται ιδιαίτερη προσοχή και σημασία στη διαφύλαξη αυτών των δεδομένων που προαναφέρθηκαν, όπως καταγράφουν και οι Ercan και Kale (2017)[27] ,

> «*... in-orbit SBA are invaluable tools for Turkey's security and defence strategies too. Missile defence systems, satellite communication, and meteorological data provided from space are desperately needed by the decision makers to be able to*

[27] Ercan C., Kale İ., 2017, The role of space in the security and defence policy of Turkey. A change in outlook: Security in space versus security from space, Space Policy, 42, 17–25, Elsevier Ltd.

see the risks/vulnerabilities and to predict the following stages of defence and security»,

δηλαδή

«*…τα σε τροχιά SBA είναι ανεκτίμητα εργαλεία για τις στρατηγικές ασφαλείας και άμυνας της Τουρκίας. Τα αμυντικά πυραυλικά συστήματα, η δορυφορική επικοινωνία και τα μετεωρολογικά δεδομένα που παρέχονται από το διάστημα είναι απόλυτης ανάγκης για τους υπεύθυνους λήψης αποφάσεων για να δουν τους κινδύνους/τρωτότητες και να προβλέψουν τα ακόλουθα στάδια άμυνας και ασφάλειας*»

Δημόσια Διοίκηση.

Σε όλες τις αναπτυγμένες χώρες, αλλά και στις αναπτυσσόμενες, η στροφή στην ηλεκτρονική διακυβέρνηση αποτελεί βασικό στοιχείο εκσυγχρονισμού. Το μοντέλο χρήσης τεχνολογιών ΤΠΕ, με διαδικτυακή και δορυφορική μεταφορά δεδομένων, οδηγεί τις νέες εφαρμοζόμενες μεθόδους της δημόσιας διοίκησης και εξυπηρέτησης των πολιτών. Διακινούμενα έγγραφα και αρχεία με απομακρυσμένη πρόσβαση, μετεωρολογικά στοιχεία (για τα οποία αναδεικνύεται η σημαντικότητά τους πέρα από τους τομείς άμυνας και ασφάλειας), χωροταξικός σχεδιασμός, θαλάσσιος και μη, ρύθμιση κυκλοφορίας, τηλεϊατρική, είναι μόνο μερικές από αυτές τις εφαρμογές που χρησιμοποιούν δεδομένα (πληροφορίες) και που μπορούν να δημιουργήσουν δυσλειτουργία ή και ανεπίστρεπτες βλάβες στην δημόσια διοίκηση με την ευρύτερη της έννοια.

Ο Farmer σε δημοσίευση του (οπ. αναφ. από τους Harrison, Johnson και Roberts, (2018)[28]) παρουσίασε την είδηση ότι

«*In 2014, a 25-year old British citizen was arrested for hacking into an unnamed satellite system used by the U.S. military, where he accessed hundreds of Pentagon employees' personal information. In the same attack, the hacker also accessed data from about 30,000 satellite phones*»,

δηλαδή

[28] Harrison T., Johnson K., Roberts T.G., 2018, Space Threat Assessment 2018, Center for Strategic and International Studies

«*Το 2014, ένας 25χρονος Βρετανός πολίτης συνελήφθη για hacking σε ένα ανώνυμο δορυφορικό σύστημα που χρησιμοποιούσε ο αμερικανικός στρατός, όπου απέκτησε πρόσβαση σε προσωπικές πληροφορίες εκατοντάδων εργαζομένων του Πενταγώνου. Στην ίδια επίθεση, ο hacker απέκτησε επίσης πρόσβαση σε δεδομένα από περίπου 30.000 δορυφορικά τηλέφωνα*».

Ναυτιλία.

Από το χώρο της οικονομίας, επιλέγεται η ναυτιλία ως χαρακτηριστικό παράδειγμα. Η χρήση των νέων εφαρμογών ΤΠΕ και των δορυφορικών συστημάτων, έχουν δώσει ώθηση για τη δημιουργία υπερσύγχρονων πλοίων που λειτουργούν με περισσότερους αυτοματισμούς, που παρουσιάζουν μεγαλύτερες δυνατότητες πλεύσης, που λαμβάνουν ταχύτερα ενημερώσεις για ναυτιλιακούς κινδύνους και επικίνδυνα καιρικά φαινόμενα, που προσδιορίζουν τη θέση τους, που επικοινωνούν και μεταφέρουν δεδομένα (πληροφορίες), που κινούνται ταχύτερα με μικρότερη κατανάλωση, μειώνοντας δηλαδή το χρόνο πλεύσης, το κόστος συντήρησης και το επιχειρησιακό τους κόστος και ουσιαστικά αυξάνοντας τον ανταγωνισμό, αλλά κυρίως το παραγόμενο κέρδος για τις εταιρείες που τις υιοθετούν.

Όπως σημειώνει και ο Shaikh (2017)[29], «*Three examples of such attacks are found in the maritime sector: ... [ ] ...US Transportation Command (Transcom) contractors compromised by several advanced cyber-attacks, targeting onboard systems with potential loss of confidential data (Stamford, 2014)*», δηλαδή «*Τρία παραδείγματα τέτοιων επιθέσεων έχουν εντοπιστεί στο κλάδο της ναυτιλίας: ... [ ] ... εργολήπτες της αμερικανικής Διοίκησης Μεταφορών (Transcom) συμβιβάστηκαν από αρκετές υψηλού επιπέδου κυβερνο-επιθέσεις, που στόχευαν σε συστήματα επί πλοίων με πιθανή απώλεια εμπιστευτικών δεδομένων*».

Επανερχόμενοι έτσι στο ερώτημα που τέθηκε νωρίτερα, η απάντηση μπορεί να είναι πως ναι, κάποιος, για λόγους που δεν μπορούμε να γνωρίζουμε εκ των προτέρων, μπορεί να ασχοληθεί με το να προβεί σε επίθεση ή κυβερνο-επίθεση ακόμη και σε ένα

[29] Shaikh S.A. (2017), Future of the Sea: Cyber Security, UK Government Office for Science, Crown

μικροδορυφόρο, από τη στιγμή που θα προκύψει κέρδος οποιασδήποτε φύσεως, είτε για τον ίδιο, είτε για τον εντολέα του.

Τρωτότητα

Τρωτότητα μπορεί να καλείται η έκθεση σε πιθανότητα αποτυχίας μιας υπηρεσίας ασφαλείας σε περίπτωση επίθεσης, όπως για παράδειγμα η αδυναμία προστασίας ενός υπολογιστή από ένα μη ανανεωμένο λογισμικό προστασίας.

Πρέπει να αναδειχθεί ότι η τρωτότητα κατέχει, ως συνέπεια της απειλής, αρκετά σημαντικό ρόλο στο πεδίο της ασφάλειας αεροδιαστημικών εφαρμογών και δη δορυφορικών συστημάτων. Κάθε συστατικό (component) του συστήματος μικροδορυφόρος που δεν έχει μελετηθεί η χρήση του με προσοχή, δηλαδή να μην παρέχεται σωστή πληροφόρηση περί εκείνων των σημείων που χρειάζονται ενίσχυση κατά τη διάρκεια του σχεδιασμού της ασφάλειάς του, μπορεί εφόσον ευοδώσει μια επίθεση εναντίον του, να προκαλέσει ανεπίστρεπτη βλάβη στη λειτουργία όλου του συστήματος έως και την καταστροφή του ή ακόμη και την καταστροφή επιπλέον αεροδιαστημικών συστημάτων, με τα οποία δυνητικά θα μπορεί να συγκρουστεί. Αλλά ακόμη και αυτό να μη συμβεί, το γεγονός ότι θα πρέπει να συνεχίσει την αποστολή του το σύστημα, έχοντας πιθανόν και άλλα τρωτά σημεία, θα το καταστήσει σταδιακά αναξιόπιστο με συνέπεια την τελικά πλήρη απαξίωση του. Αυτό σημαίνει ότι πρέπει να λαμβάνονται υπόψη στο σχεδιασμό ασφαλείας, όλα τα υποσυστήματα της πλατφόρμας του μικροδορυφόρου, του ωφέλιμου φορτίου συμπεριλαμβανομένου και του σταθμού εδάφους. Άλλωστε, εφόσον υπάρχουν τρωτότητες, σε μια εποχή που ολοένα και περισσότερο αξιοποιούνται τα συστήματα αυτά, πιθανόν να δημιουργηθούν μεγαλύτερα προβλήματα. Όπως αναφέρουν οι Livingstone και Lewis (2016)[30] «*Cyber vulnerabilities in space therefore pose serious risks for groundbased critical infrastructure, and insecurities in the space environment will hinder economic development and increase the risks to society*», δηλαδή «*Οι τρωτότητες στο διάστημα συνεπώς δημιουργούν σοβαρούς κινδύνους για κρίσιμες επίγειες υποδομές, και οι*

[30] Livingstone D., Lewis P., (2016), "Space, the Final Frontier for Cybersecurity?", London, The Royal Institute of International Affairs Chatham House

ανασφάλειες στο διαστημικό περιβάλλον θα παρεμποδίσουν την οικονομική ανάπτυξη και θα αυξήσουν τους κινδύνους για την κοινωνία».

Επίσης, οφείλεται να σημειωθεί η μεγάλη δυναμική που έχει ο όρος στον τομέα διαχείρισης ενός συστήματος. Η διαχείριση διακινδύνευσης (risk management), για τα μέρη που αφορούν την ασφάλεια (security) ενός συστήματος, όχι δηλαδή εξαιτίας σφαλμάτων του ίδιου του συστήματος ή άλλων τυχαίων γεγονότων (φυσικών παραγόντων), αλλά λόγω επιρροής εξωγενών παραγόντων (ανθρώπινων) που με πρόθεση παρεμβαίνουν σε αυτό, σχετίζεται άμεσα με την τρωτότητα (βλ. ορισμό κινδύνου στην αρχή της ενότητας). Δεν είναι τυχαίο που πλέον υφίσταται πέρα από την εκτίμηση διακινδύνευσης (risk assessment) και εκτίμηση τρωτότητας (vulnerability assessment), ως πεδίο έρευνας, αλλά και αξιοποίησης της από χώρες όπως οι ΗΠΑ (Chatfield, Reddick, 2018[31]).

Επίθεση και Κυβερνο-επίθεση

Επίθεση νοείται ως το σύνολο πραγματοποίησης απειλών εναντίον ενός συστήματος με σκοπό την πρόκληση μόνιμης ή μη βλάβης. Συναφώς, κυβερνο-επίθεση θεωρείται το αποτέλεσμα μίας ή μιας σειράς πραγματοποίησης συντονισμένων απειλών εναντίον υπολογιστικών συστημάτων ή δικτύων με σκοπό τον προαναφερθέντα.

Τρόποι και μέσα επίθεσης

Έχοντας υπόψη τα παραπάνω, προκύπτει η αναγκαιότητα να γίνει αναφορά στους τρόπους και τα μέσα με τα οποία μπορεί κάποιος να προβεί σε τέτοιες ενέργειες. Γενικά στη βιβλιογραφία απαντώνται περιγραφές που εντάσσονται σε δύο ή περισσότερες κατηγορίες (Harrison, Johnson και Roberts (2018)[32]; Livingstone και

[31] Chatfield A.T., Reddick C.G., 2018, Crowdsourced cybersecurity innovation: The case of the Pentagon's vulnerability reward program, Information Polity: The International Journal of Government & Democracy in the Information Age, Vol. 23, Issue 2, p177-194, IOS Press

[32] Harrison T., Johnson K., Roberts T.G., 2018, Space Threat Assessment 2018, Center for Strategic and International Studies

Lewis (2016)[33]; Moranta, Pavesi, Perrichon, Plattard, Sarret (2018)[34]; Pindják (2016)[35]; Thompson, Ryan, Slay και McLucas (2016)[36]). Προτιμότερη και πληρέστερη, αφού αναφέρει σε συσχέτιση τα μέσα με τον τρόπο και το πεδίο που ανήκουν αυτά, κρίνεται η κατηγοριοποίηση σύμφωνα με τους Harrison, Johnson και Roberts (2018), για τους οποίους το σύνολό της αποτελεί τα επονομαζόμενα Counterspace Weapons.

Σημειώνεται ότι η κατηγοριοποίηση θα παραμείνει στην αγγλική της έκδοση για αποφυγή παρανοήσεων και η οποία εμπεριέχει τα ακόλουθα:

- *Kinetic physical*
- *Non-kinetic physical*
- *Electronics*
- *Cyber*

Ακολουθεί συνοπτική περιγραφή των μέσων που απαρτίζουν κάθε κατηγορία από αυτές, καθώς κρίνεται σημαντική στην αποτύπωση τους για την παρούσα εργασία.

- *Kinetic physical*

Στην κατηγορία αυτή ανήκουν τα ASAT, τα αμιγή οπλικά συστήματα δηλαδή, που μπορούν να βάλλουν είτε κατά του δορυφόρου, είτε κατά του σταθμού εδάφους και τα οποία μπορούν να προκαλέσουν μόνιμη καταστροφή στους στόχους. Ωστόσο, θεωρητικά, μπορούν να γίνουν εύκολα εντοπίσιμα και να αποδοθεί ποιος τα χρησιμοποίησε.

- *Non-kinetic physical*

[33] Livingstone D., Lewis P., (2016), "Space, the Final Frontier for Cybersecurity?", London, The Royal Institute of International Affairs Chatham House

[34] Moranta S., Pavesi G., Perrichon L., Plattard S., Sarret M., 2018, Security in Outer Space: Rising Stakes for Europe, ESPI Report 64, European Space Policy Institute (ESPI)

[35] Pindják P., 2016, A Stronger EU in Cosmos: Embracing the Concept of Space Security, INCAS Bulletin, Volume 8, Issue 3, pp. 91 – 97

[36] Thompson M.A., Ryan M.J., Slay J. and McLucas A.C., 2016, Harmonized taxonomies for security and resilience, Information Security Journal: A Global Perspective, Vol. 25, Nos. 1–3, 54–67, Taylor & Francis

Στην κατηγορία αυτή συναντώνται τα lasers, τα high-powered microwaves και τα electromagnetic pulse οπλικά συστήματα. Αυτά δεν έρχονται σε επαφή με το στόχο σε αντίθεση με τα kinetic, ενώ παράλληλα είναι δύσκολο να αποδοθεί ποιος τα χρησιμοποίησε. Επίσης προκαλούν καταστροφή των στόχων, αν και ο επιτιθέμενος αδυνατεί να αντιληφθεί άμεσα εάν η επίθεση ήταν επιτυχής.

- *Electronics*

Εδώ συγκαταλέγονται οι συσκευές jamming και spoofing. Στόχοι είναι τα συστήματα επικοινωνίας των δορυφόρων, αυτά δηλαδή που αποστέλλουν και παραλαμβάνουν δεδομένα (πληροφορίες) μέσω ραδιοσυχνοτήτων. Το jamming προκαλεί αναστρέψιμη βλάβη, αφού το σύστημα μπορεί να επιστρέψει στην κανονικότητά του όταν λήξει η επίθεση. Από την άλλη το spoofing, ουσιαστικά ξεγελάει με ψευδές σήμα τον δέκτη και έτσι αποστέλλονται ψευδή στοιχεία από και προς το δορυφόρο, με αποτέλεσμα ο χρήστης να θεωρεί ότι όλα βαίνουν σύμφωνα με το σχεδιασμό αλλά στην πραγματικότητα αυτό να μην ισχύει. Και οι δύο συσκευές θεωρούνται απλής κατασκευής, αυτές του jamming, κυκλοφορούν ευρέως στην αγορά, ενώ αυτές του spoofing κατασκευάζονται και όσο για το κόστος είναι χαμηλό σχετικά και για τα δύο είδη. Δεν εντοπίζονται εύκολα και δεν αποδίδεται ευθύνη για τη χρήση τους.

- *Cyber*

Τα μέσα αυτά που είναι υψηλής τεχνολογίας, επιτίθενται τόσο στα δεδομένα (πληροφορίες) που διακινούνται (μεταδίδονται) όσο και στα συστήματα που χρησιμοποιούν αυτά τα δεδομένα. Τα μέσα αυτά, τα οποία παρόλο που δεν απαντώνται ευρέως στην αγορά, είναι εύκολο να χρησιμοποιηθούν εφόσον αγοραστούν οι υπηρεσίες κάποιου που τα διαθέτει και γνωρίζει το πώς λειτουργούν. Μπορούν να προκαλέσουν απώλεια δεδομένων (πληροφοριών), ακόμη και να χαθεί εντελώς ο δορυφόρος, ενώ και αυτά είναι δύσκολο, ίσως και αδύνατο, να εντοπιστούν και να αποδοθούν ευθύνες.

Με βάση τα παραπάνω, γίνεται σε αυτό το σημείο αντιληπτό ότι, από τη στιγμή που δεν έχει καταστεί ολοκληρωμένη η διαδικασία του διαχωρισμού του security και του cybersecurity στο διάστημα, όπως δηλαδή αναφέρθηκε στην αρχή της πρώτης ενότητας αυτού του κεφαλαίου, υπάρχει η πιθανότητα να θεωρηθούν ως κυβερνο-επιθέσεις, επιθέσεις που κατατάσσονται σε άλλη κατηγορία, όπως αυτές που προκαλείται με χρήση συσκευών spoofing και συσκευών jamming για παράδειγμα. Για αρκετούς μελετητές, αυτό βέβαια ισχύει, καθώς αποδέχονται άλλες κατηγοριοποιήσεις, γενικότερης κλίμακας. Βλέπουμε έτσι να θεωρούνται το jamming και το spoofing κυβερνο-επιθέσεις, ενώ για να ισχύει αυτό ίσως θα πρέπει να προσδιοριστεί εάν ο κυβερνοχώρος συμπεριλαμβάνει μόνο τα δεδομένα και τη χρήση τους, ή και τη μετάδοση αυτών από ραδιοσυχνότητες.

Σε κάθε περίπτωση το εκπονούμενο αποτέλεσμα είναι ότι η πληροφορία βάλλεται, ανεξάρτητα της κατηγορίας των συστημάτων που το επιτυγχάνουν αυτό. Όπως προκύπτει, κρίνεται πως στην παρούσα εργασία οφείλεται να μελετηθούν τόσο τα ενδεχόμενα επίθεσης όσο και κυβερνο-επίθεσης, ώστε να αναδειχθεί η σημαντικότητά τους.

Κενό ασφαλείας

Ως κενό ασφαλείας νοείται η συνέπεια μιας επίθεσης που ολοκληρώθηκε με επιτυχία. Αυτά τα κενά ασφαλείας είναι που η «ανθεκτικότητα» καλείται να αντιμετωπίσει και να επαναφέρει την κανονικότητα της ασφάλειας του συστήματος. Όπως είναι αντιληπτό, στην ανθεκτικότητα καλείται ο υπεύθυνος χειριστής, να προϋπολογίσει κατά το στάδιο του σχεδιασμού την πιθανότητα ύπαρξης κενών, χωρίς ωστόσο να γνωρίζει ποια θα είναι αυτά, καθώς δεν μπορεί να προκαταβάλει τι είδους επίθεση θα δεχθεί, πέρα από αυτές που έχει ήδη αντιστοιχίσει με το σχεδιασμό της ασφάλειας.

Αντίμετρα

Αντίμετρα καλούνται διάφορες λειτουργίες συστημάτων ασφαλείας, που ρόλο έχουν

την αφαίρεση τρωτοτήτων ή την αντιστάθμιση απειλών, αφαιρώντας ουσιαστικά τα κενά ασφαλείας.

Όπως είναι αντιληπτό, τα αντίμετρα ενεργοποιούνται ουσιαστικά μετά την κυβερνο-επίθεση, όταν δηλαδή το σύστημα είτε λειτουργεί προς, είτε έχει φτάσει στη νέα κανονικότητα της ασφάλειας του, έχει ενεργοποιηθεί και υλοποιηθεί, με άλλα λόγια, το στάδιο της «ανθεκτικότητας» του συστήματος.

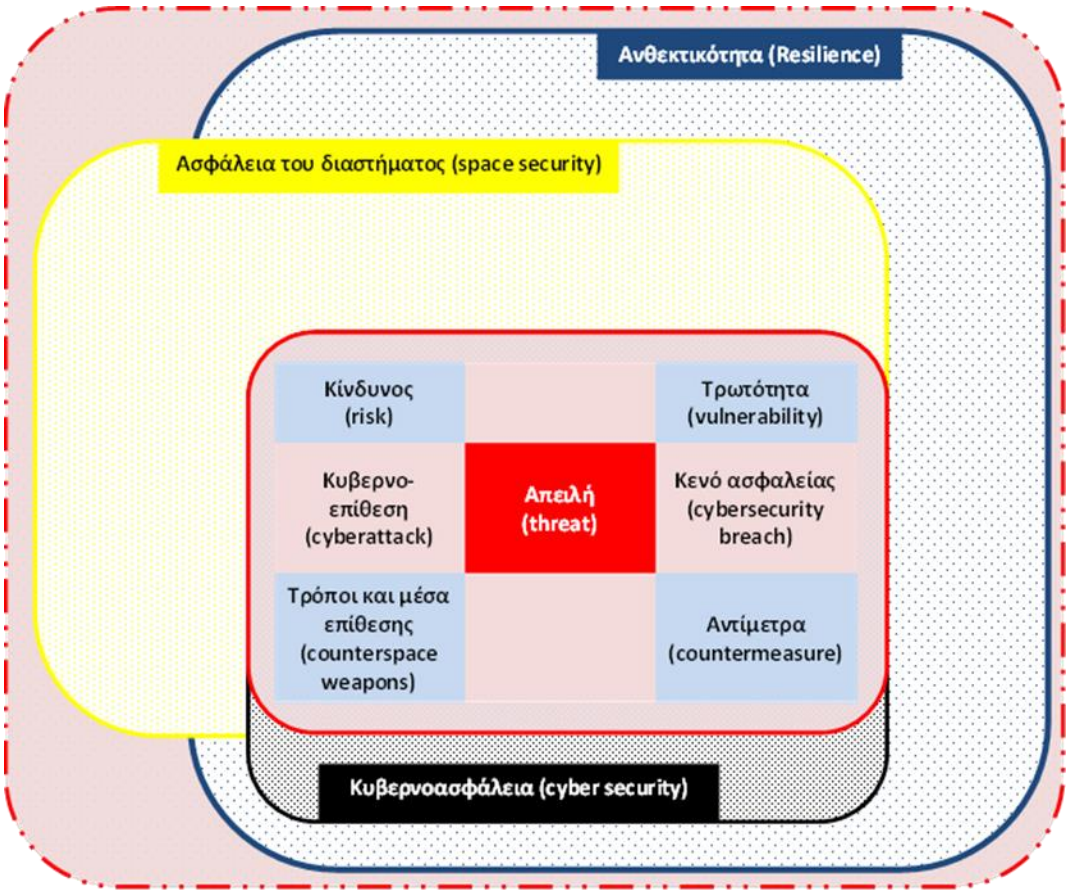
Σύμφωνα με τους Ercan και Kale (2017)[37], τα αντίμετρα μπορούν να είναι μεταξύ άλλων:

- *Τεχνικές anti-jamming*
- *Περιορισμένες περιοχές κάλυψης*
- *Προσαρμοζόμενη κωδικοποίηση*
- *Ψηφιακά προγραμματίσιμους δορυφόρους*
- *Κρυπτογράφηση (συμπεριλαμβανομένων της τηλεμετρίας, του τηλεχειρισμού και των δεδομένων διαστήματος)*
- *Πιστοποίηση και αναγνώριση χρηστών σταθμών εδάφους και δορυφόρων.*
- *Εσωτερικές δορυφορικές διασυνδέσεις για μείωση κυβερνο-επιθέσεων*
- *Περιοριστή RF*

Έχοντας αναφέρει όλα τα παραπάνω, στο σχήμα 3 παρουσιάζεται μια πρόταση συσχέτισης των εννοιών που αναλύθηκαν στις δύο προηγούμενες ενότητες, υπό τη μορφή συνόλων, προκειμένου να υπάρξει μια εικονική διασύνδεση αυτών. Η πρόταση βασίζεται αποκλειστικά στο εύρος των πεδίων που αντίστοιχα καλύπτουν οι έννοιες, όπως αυτό περιγράφηκε. Σημειώνεται ότι εκτιμάται πως το σύνολο ανθεκτικότητα, έχει μια πιο ευρεία υπόσταση, δεδομένης της αοριστίας που έχει να αντιμετωπίσει στην αποστολή του. Επίσης, η τομή του συνόλου ασφάλεια του διαστήματος με το σύνολο κυβερνοασφάλεια αποτελεί το σύνολο των εννοιών που καλούνται να αντιμετωπίσουν, που έχει ως σημαντικότερο υποσύνολο του την απειλή. Ωστόσο,

[37] Ercan C., Kale İ., 2017, The role of space in the security and defence policy of Turkey. A change in outlook: Security in space versus security from space, Space Policy, 42, 17–25, Elsevier Ltd.

θεωρείται πως το τελευταίο αυτό σύνολο λειτουργεί διασταλτικά, καθώς ταυτόχρονα, πέρα από τομή των δύο συνόλων ασφάλειας, αποτελεί και υπερσύνολο όλων, αφού η αοριστία του αριθμού των πιθανών απειλών και των υπολοίπων υποσυνόλων που την ακολουθούν, του δημιουργεί τέτοια δυναμική που δεν μπορεί παρά να περιβάλλει τα υπόλοιπα. Άλλωστε, κανένα σύστημα ασφαλείας δεν μπορεί για πάντα να μένει αλώβητο, ούτε πάντοτε να επέρχεται κανονικότητα σε αυτό. Σε αντίθεση, πάντα απειλές θα υφίστανται και θα αποτελούν κίνδυνο για κάποιο σύστημα.



Σχήμα 3. Απεικόνιση διασύνδεσης εννοιών με τη μορφή συνόλων

4.3 Μέθοδοι εντοπισμού κινδύνου/τρωτότητας

Στην ενότητα αυτή, θα καταγραφούν διάφορες μεθοδολογίες που μπορεί να ακολουθηθούν για την ολοκλήρωσή των στόχων της εργασίας. Πρώτα ωστόσο, οφείλεται να οριστεί το ρυθμιστικό πλαίσιο που θα καλύπτει την ορθότητα της επιλογής αυτής. Με άλλα λόγια, για να αποδειχθεί ορθή η επιλογή μεθοδολογίας, θα υποτεθεί ότι τα συστήματα που θα διερευνηθούν αποτελούν μέρος ενός έργου, στη διαχείριση (project management) του οποίου εμπίπτει και η διαχείριση διακινδύνευσης (risk management).

Με την υπόθεση αυτή, η επιλογή προσφορότερης μεθοδολογίας για τη διεξαγωγή της έρευνας θα βασίζεται σε καθορισμένους κανόνες, σε ρυθμισμένες διεργασίες που θα πρέπει να ακολουθηθούν και γενικότερα θα έχει αποφασιστεί σε κατάλληλο έδαφος για τη βασιμότητά της. Υπενθυμίζεται ότι, ο προσδιορισμός των κινδύνων ή των απειλών και των τρωτοτήτων προκαλεί μεν, αντικειμενικές δυσκολίες στο σχεδιασμό κάθε συστήματος, αλλά με την επιλογή πρόσφορης μεθοδολογίας για την καταγραφή και την αντιμετώπισή τους, κρίνεται κατά ένα μέρος, εάν το έργο μπορεί να στεφθεί με επιτυχία ή όχι. Βέβαια, επισημαίνεται ότι δε θα πραγματοποιηθεί διαχείριση διακινδύνευσης με την συνολική της μορφή, καθώς αυτό εκφεύγει από τους σκοπούς της εργασίας. Θα επιλεγούν τα μέρη εκείνα που θα οδηγήσουν ουσιαστικά σε εκτίμηση τρωτότητας, από εξωγενείς παράγοντες (ανθρώπινους) που σκοπό έχουν να πλήξουν το σύστημα, προκαλώντας του βλάβη ή αφήνοντας το με ανεπίστρεπτη ζημιά. Έτσι θα αποκλειστούν έλεγχοι για κινδύνους από περιβαλλοντικούς φυσικούς παράγοντες καθώς και πιθανά σφάλματα των μερών του συστήματος από αστοχία υλικού ή άλλα απρόβλεπτα, χωρίς παρέμβαση, αίτια.

Στο σημείο αυτό, θα περιγραφούν κάποιες έννοιες που αποτελούν βασικές αρχές στη διαχείριση διακινδύνευσης και θα υποβοηθήσουν στην επιλογή της μεθοδολογίας. Σύμφωνα με τη βιβλιογραφία (Greene, Stellman (2014) [38], Greiman (2013) [39]), θα αναφερθούν οι έννοιες:

[38] Greene J., Stellman A., 2014, Head First PMP, Third Edition, O'Reilly Media, Inc.

[39] Greiman V. A., 2013, Megaproject Management Lessons on Risk and Project Management from the Big Dig, John Wiley & Sons, Inc., Project Management Institute, Inc.

Εκτίμηση διακινδύνευσης (Risk assessment), που δεν είναι άλλο παρά η διαδικασία που αφορά στην εξεύρεση απαντήσεων για πλήθος ερωτημάτων, όπως του τι μπορεί να πάει λάθος σε ένα σύστημα, ποιος κίνδυνος δηλαδή να πραγματοποιηθεί, με τι συχνότητα και τι συνέπειες.

Επίσης, πρέπει να λαμβάνεται υπόψη ότι όλα βασίζονται στην αντίληψη κινδύνου (risk perception), δηλαδή στην υποκειμενική κρίση περί των χαρακτηριστικών και της δυναμικής του κινδύνου. Εάν για παράδειγμα, το μοντέλο που χρησιμοποιεί το σύστημα έχει βασιστεί σε υποθέσεις (assumptions) που είναι ατεκμηρίωτες, τότε η εκτίμηση θα είναι ασαφής και πιθανόν καταστροφική. Επιπρόσθετα, οι υποθέσεις αυτές, απαιτητό είναι να αντικατοπτρίζουν την ισχύουσα κατάσταση, αλλιώς μπορεί η λανθασμένη ιεράρχηση των κινδύνων, να προκαλέσει μεγαλύτερη ζημιά στο σύστημα. Αν δηλαδή προκριθεί ένας κίνδυνος που μπορεί να μην ενσαρκωθεί ποτέ, επειδή η εκτίμηση πραγματοποιήθηκε χωρίς να έχουν ληφθεί υπόψη οι ισχύουσες συνθήκες, σε σχέση με ένα κίνδυνο που μπορεί να προκληθεί από μια τρωτότητα που θα έχει θεωρηθεί χαμηλότερης σημασίας, τότε ενώ το σύστημα θα έχει σχεδιαστεί για να αντιμετωπίσει κυρίως τον πρώτο, βλάβη πιθανότερο είναι να προκαλέσει ο δεύτερος. Επιπλέον, οι υποθέσεις θα πρέπει να βασίζονται σε ιστορικά στοιχεία, εάν έχει προκληθεί παρόμοιο συμβάν στο παρελθόν δηλαδή, είτε στο ίδιο σύστημα σε περίπτωση επανασχεδιασμού του, είτε σε παρόμοιο. Ακόμη να βασίζονται και στην έρευνα καθώς και στην εμπειρία, ώστε να είναι ενήμερη (up to date) κάθε φορά, η ισχύουσα κατάσταση.

Σε όλα αυτά, ρόλο έχει και η ανοχή κινδύνου (risk tolerance), ως προς την επικινδυνότητα, που αντιστοιχεί στο σημείο, από το οποίο και μετά ένας κίνδυνος δεν γίνεται αποδεκτός.

Συναφώς, αναφέρεται και η έννοια της ανάλυσης σεναρίων (scenario analysis) που είναι η τεχνική η οποία απαντάται συνηθέστερα στην ανάλυση κινδύνου.

Στο σημείο αυτό, πρέπει να σημειωθούν και οι έννοιες της ποιοτικής και ποσοτικής εκτίμησης κινδύνου.

Ποιοτική εκτίμηση (qualitative analysis), στην οποία κατηγοριοποιούνται και ιεραρχούνται οι κίνδυνοι. Εκτιμάται με άλλα λόγια, αφενός η πιθανότητα ένας συγκεκριμένος κίνδυνος να πραγματοποιηθεί και αφετέρου το αντίκτυπο, ή αλλιώς οι επιπτώσεις, που θα έχει αυτή η εξέλιξη σε τομείς, όπως η απόδοση του συστήματος, το επίπεδο διατήρησης της ποιότητάς του κ.α.

Ποσοτική εκτίμηση (quantitative analysis), στην οποία υπολογίζονται μεν, συγκεκριμένα χαρακτηριστικά των κινδύνων αλλά και δίνεται ιδιαίτερη προσοχή σε αυτούς που κατέχουν τις υψηλότερες θέσεις στη λίστα ιεράρχησης εκθέσεων του συστήματος σε κίνδυνο. Επίσης, συμπεριλαμβάνεται και η αξιολόγηση των κινδύνων σε σχέση με την καταγραφή εκτίμησης του εύρους των πιθανών αποτελεσμάτων που θα προκύψουν από την πραγματοποίησή τους. Για το λόγο αυτό χρησιμοποιούνται στατιστικές μέθοδοι και η Θεωρία των Πιθανοτήτων, καθώς ένας μεμονωμένος παράγοντας κινδύνου μπορεί να οδηγήσει σε πολλαπλά αποτελέσματα.

Για να μπορέσει όμως να εκπονηθεί η οποιαδήποτε εκτίμηση τρωτότητας (vulnerability assessment), όπως προαναφέρθηκε στην αρχή της ενότητας, χρειάζεται να επιλεχθεί κατάλληλη μεθοδολογία εντοπισμού των τρωτοτήτων και να πραγματοποιηθεί αυτή σαν να υλοποιούταν κατά τη διάρκεια σχεδιασμού του συστήματος.

Για το λόγο αυτό, κρίνεται ότι πρέπει, εδώ, στο πλαίσιο τήρησης των προβλεπόμενων διαδικασιών που οφείλεται να ακολουθηθούν για τη διασφάλιση των αποτελεσμάτων, να σημειωθούν τα στάδια που θα επιλεγούν για να απαντηθούν τα υποθετικά ερωτήματα της παρούσας εργασίας, και που εμπεριέχονται σε κάθε εκπόνηση εκτίμησης, είτε κινδύνου, είτε τρωτότητας:

1. Καταγραφή σε κατάλογο των στοιχείων και πόρων σε ένα σύστημα
2. Προσθήκη ποιοτικής αξίας και σημασίας στους πόρους. Ιεράρχηση
3. Προσδιορισμός των κινδύνων, των τρωτοτήτων αντίστοιχα, ή πιθανών απειλών για κάθε πόρο
4. Μείωση ή εξάλειψη των πιο σοβαρών τρωτοτήτων για τους πιο πολύτιμους πόρους.

Έχοντας αποτυπώσει πλέον τα βήματα που θα αποτελέσουν το πλαίσιο της έρευνας, απομένει, για να προσδιοριστούν οι κίνδυνοι και οι τρωτότητες ή οι απειλές σε ένα σύστημα, να επιλεχθεί η μέθοδος. Πιο κάτω αναφέρονται ενδεικτικές μέθοδοι που μπορούν να ακολουθηθούν.

Root Cause Avalysis

Όπως προϊδεάζει ο τίτλος της, με βάση ένα συμβάν, αναλύονται οι βαθύτερες αιτίες που το προκάλεσαν ώστε να αντιμετωπιστεί αυτό ακριβώς στην πηγή δημιουργίας του, αντί απλά να τηρηθεί μια τυπική διαδικασία καταγραφής αυτού, χωρίς να διαλευκανθεί το πώς και το γιατί συνέβη. Στην ανάλυση, αναγνωρίζονται τα υποκρύπτοντα ελαττώματα σε ένα σύστημα ασφαλείας και καταγράφονται ώστε, εάν αυτά διορθωθούν, να προφυλάξουν το σύστημα τόσο από την επανάληψη τους, αλλά και να αποφευχθεί παρόμοια ατυχήματα να του συμβούν. Το root cause analysis λογίζεται ότι είναι μια επαναλαμβανόμενη διαδικασία και θεωρείται ως εργαλείο συνεχούς βελτίωσης του συστήματος.

Συναφώς η ανάλυση root cause δεν θεωρείται ως μια αυστηρά προσδιορισμένη μεθοδολογία. Εντοπίζονται πολλές άλλες διαφορετικές μεθοδολογίες, εργαλεία και διαδικασίες βασιζόμενες σε διαφορετικές φιλοσοφίες, που έχουν όμως το μέλημα να εντοπίσουν και να διορθώσουν την πηγή του προβλήματος όπως δηλαδή και η root cause analysis.

Ανεξάρτητα λοιπόν από τη φιλοσοφία που τις διακατέχει, δηλαδή εάν έχουν εφαλτήριο την ασφάλεια, την αποτυχία ή το σύστημα ως βάση, έχουν τα ακόλουθα κοινά στοιχεία που τις κατατάσσει σε μια ευρύτερη κατηγορία ανάλυσης root cause.
- Αναγνώριση του πραγματικού προβλήματος, συσχέτισή του με το συμβάν και ιεράρχησή του ως κύριο
- Αναγνώριση των αιτίων του προβλήματος. Παράγοντες που το δημιουργούν.

- Καθορισμός της σημαντικότητας του προβλήματος. Ποιες οι επιπτώσεις, θα υπάρξει επαναληψιμότητα ή όχι, θα είναι διαφορετικές σε πιθανά επόμενο παρόμοιο συμβάν, είναι τυχαίο και μεμονωμένο συμβάν λάθος χειρισμού ή υπάρχει ελάττωμα.
- Αναγνώριση των λόγων ύπαρξης των αιτίων του προβλήματος. Εντοπισμός της πηγής, ώστε η αντιμετώπισή της να εκμηδενίσει το πρόβλημα.

Counterfactual Risk Analysis

Επίσης, μπορεί να ακολουθηθεί η μέθοδος counterfactual risk analysis, στην downward έκδοσή της. Η ανάλυση αυτή, κυρίως αναγνωρίσιμη ως ποσοτική, η οποία αποτελεί μια πιο αντισυμβατική μέθοδο, δεδομένης της ιδέας στην οποία βασίζεται, μπορεί να εφαρμοστεί σε κάθε είδους κίνδυνο. Ανεξάρτητα εάν υπάρχουν δεδομένα απωλειών που να έχουν καταγραφεί ιστορικά, εάν αυτά είναι αρκετά για να δημιουργηθούν κατάλληλα μοντέλα πρόβλεψης και να καταρτιστούν στρατηγικές και τρόποι αντιμετώπισης, η βάση της ανάλυσης αυτής, είναι η αναζήτηση στο χρόνο ιστορικών γεγονότων που να αντιστοιχούν στο γεγονός που απασχολεί, αλλά και ιστορικών γεγονότων που να μην είχαν το αποτέλεσμα του συγκεκριμένου γεγονότος και η δημιουργία σεναρίων από αυτά. Άμεσα η ανάλυση δημιουργεί μεγαλύτερο πλήθος δεδομένων και οποιοδήποτε μοντέλο ανάλυσης θα καταλήξει σε πιο ακριβή αποτελέσματα, συντελώντας έτσι σε εξαγωγή πιο ασφαλών συμπερασμάτων. Στην αντιστοίχιση των γεγονότων όμως υπάρχουν δύο εκδόσεις αντιμετώπισης. Η πρώτη είναι η upward, η οποία είναι και πιο κατανοητή για την ανθρώπινη σκέψη, αφού γενικότερη ανθρώπινη προτίμηση είναι η θετική σκέψη. Αντίστοιχα υφίσταται και η downward έκδοση, η οποία οδηγεί την ανάλυση μέσω της καταστροφικής σκέψης, τι θα γινόταν δηλαδή εάν το γεγονός είχε μεγαλύτερες επιπτώσεις. Χαρακτηριστικό παράδειγμα είναι αυτό που αναφέρεται από τους Woo, Maynard και Seria (2017)[40]

> «*As a salient illustration of the power of downward counterfactual thinking, consider 9/11, the epitome of a Black Swan event (Taleb, 2007). This terrorist attack spawned numerous upward counterfactual thoughts: if only the FBI had the*

[40] Woo G., Maynard T., Seria J., 2017, Reimagining history: Counterfactual risk analysis, Emerging Risk Report 2017, Understanding risk, Emerging Risk Report 2017, Lloyd's-RMS

legal authority to open the computer of a terrorist suspect; ... [] ... A natural upward counterfactual question that was regularly asked is: 'Why did this happen?' The less natural but more searching downward counterfactual question following 9/11 is: 'Why didn't this happen before?'... [] ... As observed by his aide-de-camp, Nasir Al Wuhayshi, Osama bin Laden himself had the downward counterfactual thought that if a passenger jet leaving JFK could be ditched into the sea through malicious pilot action, it could also be flown into buildings (Joscelyn,2016).»

δηλαδή

«*Ως προεξέχουσα απεικόνιση της δύναμης της downward counterfactual σκέψης, εξετάζεται η 9/11, η επιτομή ενός γεγονότος Black Swan (Taleb, 2007). Αυτή η τρομοκρατική επίθεση δημιούργησε πολυάριθμες upward counterfactual σκέψεις: εάν το FBI είχε τη νομική εξουσία να ανοίξει τον υπολογιστή ενός υπόπτου τρομοκρατίας, ... [] ... Ένα φυσικό upward counterfactual ερώτημα που τέθηκε τακτικά είναι: «Γιατί συνέβη αυτό;». Η λιγότερο φυσική αλλά πιο ερευνητική downward counterfactual ερώτηση μετά την 9/11 είναι: «Γιατί δεν συνέβη αυτό πιο πριν;» ...[] ... Όπως παρατηρήθηκε από τον υπασπιστή του, Nasir Al Wuhayshi, ο ίδιος ο Οσάμα Μπιν Λάντεν, είχε την downward counterfactual σκέψη ότι εάν ένα επιβατικό αεροπλάνο που θα απογειωνόταν από το JFK μπορούσε να βυθιστεί στη θάλασσα μέσω κακόβουλων πιλοτικών ενεργειών, θα μπορούσε επίσης να πετάξει σε κτίρια (Joscelyn, 2016).*»

Penetration Testing

Η μέθοδος αυτή, που λανθασμένα θεωρείται μέρος της εκτίμησης τρωτότητας ή ακόμη και η ίδια η εκτίμηση τρωτότητας, προσδιορίζεται σύμφωνα με τρεις από τις μεγάλες εταιρείες του χώρου παροχής υπηρεσιών κυβερνοασφάλειας, δηλαδή τη Cisco[41], τη SecureAuth[42] και την Imperva Incapsula[43], ως μια προσομοίωση κυβερνο-επίθεσης στον υπολογιστή ή το δίκτυο του χρήστη, σε ασφαλές περιβάλλον με σκοπό τον εντοπισμό κενών ασφαλείας που προκαλούνται από τρωτότητες. Το

[41] https://www.cisco.com/c/en/us/products/security/what-is-pen-testing.html
[42] https://www.secureauth.com/products/penetration-testing
[43] https://www.incapsula.com/web-application-security/penetration-testing.html

pentest, όπως είναι πιο διαδεδομένο, είναι η προσπάθεια δηλαδή του εντοπισμού μέσω πραγματικών επιθέσεων των τρωτοτήτων κατά τη διάρκεια λειτουργίας του συστήματος, από τον ίδιο το χρήστη, είτε με ιδία μέσα, είτε με υποβοήθηση από κατάλληλο ειδικευμένο προσωπικό. Χρησιμοποιείται, όπως είναι εμφανές, σε θέματα κυβερνοασφάλειας και είναι αρκετά διαδεδομένο σε μεγάλες επιχειρήσεις, οι οποίες θέλουν να έχουν καλύτερη άμυνα και μεγαλύτερη ασφάλεια, απέναντι σε κυβερνο-επιθέσεις, οποιασδήποτε μορφής.

Interviews

Η μέθοδος αυτή, χρησιμοποιεί την εκ του σύνεγγυς ή εξ αποστάσεως λήψη συνέντευξης με κατά κύριο λόγο δομημένα ή ημιδομημένα ερωτηματολόγια, προκειμένου σε δεύτερο χρόνο με χρήση συγκεκριμένων μοντέλων ποσοτικού ή ποιοτικού προσδιορισμού, να καταλήξει σε συμπεράσματα από απαντήσεις ατόμων που ασχολούνται με το αντικείμενο της έρευνας αυτό καθ' εαυτό, καθώς και από εμπειρογνώμονες του χώρου. Καταχωρείται ανάμεσα στις τέσσερις πιο διαδεδομένες μεθόδους, μαζί με τη Root Cause Analysis, τη Delphi Technique και το Brainstorming (Greene, Stellman, 2014)[44]

Δεδομένης της βασικής υπόθεσης για την εξέλιξη της έρευνας, ότι δηλαδή τα συστήματα των δύο μικροδορυφόρων τελούν υπό σχεδιασμό, η μέθοδος που θα ακολουθηθεί, θα αποτελεί ουσιαστικά συνδυασμό ποιοτικής ανάλυσης με χρήση αρχών των μεθόδων Counterfactual Risk Analysis και Root Cause Analysis.

[44] Greene J., Stellman A., 2014, Head First PMP, Third Edition, O'Reilly Media, Inc.

5. Εντοπισμός τρωτοτήτων ασφάλειας και κυβερνοασφάλειας σε επίπεδο λειτουργίας του μικροδορυφόρου

Στο ακόλουθο κεφάλαιο, έχοντας πλέον μια πλήρη εικόνα σχετικά με τις έννοιες πληροφορία, cubesat, ασφάλεια και κυβερνοασφάλεια και τρωτότητα, θα καταβληθεί προσπάθεια εξέτασης δύο cubesats ως προς τα λειτουργικά τους υποσυστήματα. Τα υποσυστήματα αυτά θα καταγραφούν σε πρώτο επίπεδο, θα διερευνηθεί εάν υπάρχουν ομοιότητες μεταξύ τους και ακολούθως για κάθε ένα από αυτά θα λάβει χώρα ποιοτικός έλεγχος σε σχέση με πιθανές τρωτότητες που θα μπορούσαν να τα επηρεάσουν. Ουσιαστικά θα ακολουθηθεί η μεθοδολογία εντοπισμού τρωτότητας που περιγράφηκε σε προηγούμενο κεφάλαιο.

Η ερευνητική υπόθεση που οφείλεται να επιβεβαιωθεί, είναι, μέσω βιβλιογραφικής έρευνας να βρεθούν οι τρωτότητες ασφάλειας και κυβερνοασφάλειας στο λειτουργικό επίπεδο του μικροδορυφόρου. Για το στόχο αυτό, θα πρέπει να απαντηθούν τα ακόλουθα ερωτήματα:

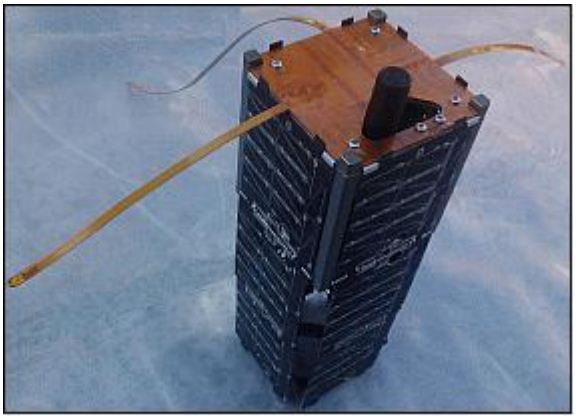
- Υπάρχουν τρωτότητες ασφάλειας και κυβερνοασφάλειας στο λειτουργικό επίπεδο του μικροδορυφόρου.
- Σε ποιο υποσύστημα υπάρχουν περισσότερες τρωτότητες.
- Οι κίνδυνοι που προκύπτουν από τις τρωτότητες ανά υποσύστημα μπορούν να κατηγοριοποιηθούν σε σημαντικούς ή μη για τη λειτουργία του συστήματος.

Στο σημείο αυτό σημειώνεται ότι η επιλογή των δύο cubesats έγινε με βάση αφενός την επιτυχή ολοκλήρωση της αποστολής τους και αφετέρου το ωφέλιμο φορτίο τους, που είναι το σύστημα AIS, καθώς αυτή η προσπάθεια κρίθηκε ότι θα βοηθήσει την όποια περαιτέρω έρευνα που να σχετίζει τις αεροδιαστημικές εφαρμογές με τη ναυτιλία. Οι cubesats αυτοί επιλέχθηκαν από ένα σύνολο cubesats, που προέκυψε ως αποτέλεσμα αναζήτησης στη βάση δεδομένων που τηρείται στο διαδικτυακό τόπο nanosats.eu[45], θέτοντας φίλτρο αναζήτησης για αυτούς που έχουν payload AIS. Ακολούθως, τα χαρακτηριστικά τους εντοπίστηκαν σε βάση δεδομένων που τηρείται

[45] https://airtable.com/shrafcwXODMMKeRgU/tbldJoOBP5wlNOJQY

στο διαδικτυακό τόπο Earth Observation Portal (eoPortal)[46] και με τον τρόπο αυτό επιτυγχάνεται η παρακάτω καταγραφή και παρουσίασή τους. Σημειώνεται ότι λόγω των τεχνικών ορολογιών δεν θα υπάρξουν τεράστιες αποκλίσεις στον τρόπο καταγραφής και περιγραφής τους σε σχέση με αυτόν που αναφέρονται στο διαδικτυακό τόπο eoPortal.

Ο πρώτος εκ των δύο cubesats που επιλέχθηκαν για την έρευνα, είναι ο Lambdasat (Λ-sat), ο έτερος είναι ο AAUSat3 και στις ακόλουθες εικόνες (Εικόνα 1 και Εικόνα 2, αντίστοιχα) φαίνονται κατά τη διάρκεια της προετοιμασίας τους για αποστολή.



Εικόνα 1. Lambdasat (Λ-sat)

(image credit: NASA, Periklis Papadopoulos) [47]

Εικόνα 2. AAUSat3

(image credit: AAU) [48]

[46] https://directory.eoportal.org/web/eoportal/home
[47] https://directory.eoportal.org/web/eoportal/satellite-missions/L/LAMBDASAT
[48] https://directory.eoportal.org/web/eoportal/satellite-missions/a/aausat3

5.1 Lambdasat (Λ-sat) [49],[50],[51]

Ο Lambdasat (Λ-sat), ο οποίος θεωρείται ο πρώτος ελληνικός cubesat που σχεδιάστηκε και υλοποιήθηκε από Έλληνες, κατασκευάστηκε στις ΗΠΑ από μια διεθνή ομάδα που περιείχε κυρίως Έλληνες επιστήμονες και φοιτητές από το SJSU (San Jose State University), Σαν Χοσε, Καλιφόρνια, την επονομαζόμενη Ομάδα Λάμδα (Lambda Team). Εμπνευστής της ήταν ο καθηγητής Μηχανολόγων Μηχανικών και Αεροναυπηγικής στο εν λόγω Πανεπιστήμιο, κ. Περικλής Ε. Παπαδόπουλος, ελληνικής καταγωγής. Από πλευράς ελληνικών εκπαιδευτικών ιδρυμάτων συμμετείχε το Πανεπιστήμιο Αιγαίου, με τον καθηγητή κ. Νικητάκο Νικήτα και τον κ. Μαντζούρη Γεώργιο. Το εγχείρημα της Ομάδας Λάμδα χρηματοδοτήθηκε από τη NASA. Για ιστορικούς λόγους, οφείλεται να σημειωθεί ότι το γράμμα Λ επιλέχθηκε από το πρώτο γράμμα των Λακεδαιμονίων, τιμώντας έτσι την ιστορία της χώρας.

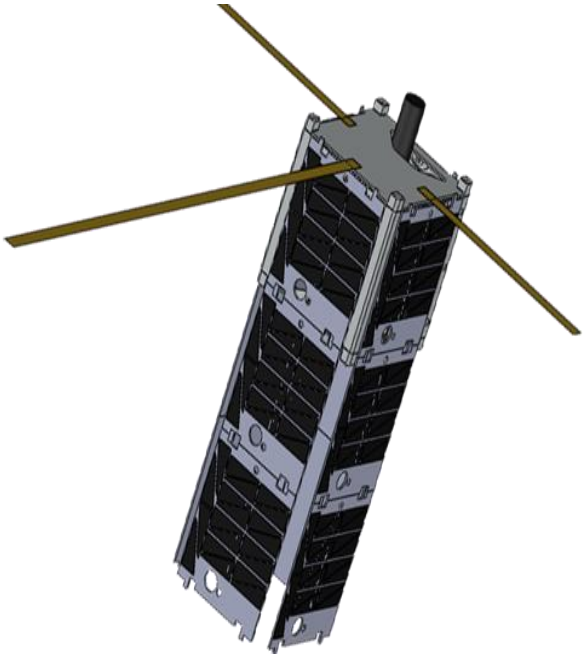
Ο μικροδορυφόρος είναι ένας cubesat, με πλευρά κύβου διαστάσεων 10 cm και βάρος 1.5 kgr., σε πλήρη αντιστοιχία με το μέγεθος 1U που προσδιορίζει ένα cubesat. Τα στοιχεία που τον απαρτίζουν είναι ένας κεντρικός υπολογιστής και ένα κύριο power board για ρύθμιση του διαύλου ισχύος (power bus) που χρησιμοποιεί παραγωγή ηλιακής ενέργειας από φωτοβολταϊκά panels, τα οποία στην πλήρη έκτασή τους δημιουργούν την επιφάνεια ενός 3U cubesat. Τα δομικά του υλικά (σκελετός) είναι από την Pumpkin Inc που έχει έδρα το Σαν Φρανσίσκο των ΗΠΑ. Το σύστημα ενέργειας (τροφοδοσίας), το οποίο είναι ειδικά σχεδιασμένο, καθώς και ο κύριος υπολογιστής, που έχουν σχεδιαστεί για να ικανοποιούν απαιτήσεις ανοχής διαστήματος τριών σφαλμάτων, λειτουργούν όλα τα ηλεκτρονικά συστήματα της NanoRacks.

[49] https://directory.eoportal.org/web/eoportal/satellite-missions/L/LAMBDASAT

[50] http://lambdasat.com/

[51] Mantzouris G., Papadopoulos P., Nikitakos N., Manso M., Bordetsky A., Sarris Z., Markarian G., Kourousis K., 2015, Picosatellites for Maritime Security Applications – the Lambdasat Case, Journal of Aerospace Technology and Management, Vol.7, No 4, pp.490-503

Οι τηλεπικοινωνίες επιτυγχάνονται μέσω Short Burst Data μόντεμ, χρησιμοποιώντας τον αστερισμό (συστοιχία) των δορυφόρων Iridium, που δίνει δυνατότητες ταχείας αποστολής δεδομένων μετά την απόκτησή τους. Οι επικοινωνίες με τους σταθμούς εδάφους θα πραγματοποιούνται με UHF μεταδότη και UHF δέκτη, που λειτουργεί σε συχνότητα που χρησιμοποιείται για ραδιοερασιτεχνισμό, ήτοι 437.462 MHz. Ο διαβιβαστής (transmitter) του Lambdasat αποτελείται από ένα ραδιοφάρο Stensat (radio beacon), ένα μικρό πομπό FM ικανό να παράγει AX.25 πακέτα μη αριθμημένων πληροφοριών (UI) με ρυθμό downlink στα 1.2 kbps AFSK (UHF) και uplink στα 9.6 kbps GFSK (UHF) και με ενέργεια μετάδοσης έως το 1 W λειτουργώντας με μία απλή τροφοδοσία 5 V. Στο δορυφόρο έχει τοποθετηθεί μονοπολική κεραία, με μήκος από 15 έως 20 cm. Ο λόγος της αυξομείωσης στο μήκος, είναι πως στην ουσία έχουν τοποθετηθεί τρεις διαφορετικές κεραίες πολύ απλές, μονοπολικές, μήκους 10 cm, 10 cm και 5 cm αντίστοιχα σε δύο από τους τρεις άξονες του δορυφόρου στις κατευθύνσεις x και y, όπως φαίνεται και στην εικόνα 1 παραπάνω. Οι κεραίες αυτές εξυπηρετούν στην καλύτερη επικοινωνία με το σταθμό εδάφους.



Σχήμα 4. Η διάταξη των κεραιών του Lambdasat (Λ-sat) (image credit: Lambda Team)[52]

Σημειώνεται ότι, όπου EPS περιλαμβάνεται το power board και τα φωτοβολταϊκά panels, το OBDH αντιστοιχίζεται με τον κύριο υπολογιστή, υπεύθυνο για όλες τις

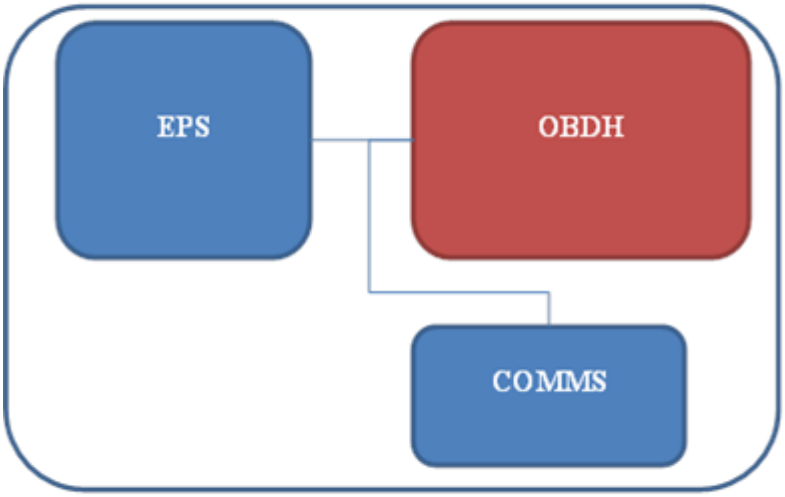
[52] https://directory.eoportal.org/web/eoportal/satellite-missions/L/LAMBDASAT

λειτουργίες του δορυφόρου, την επεξεργασία των εντολών που του δίνονται και τη μετάδοσή τους στα υπόλοιπα υποσυστήματα και το comms με τις κεραίες, το ραδιοφάρο και την επικοινωνία με τον αστερισμό του Iridium.

Περαιτέρω προδιαγραφές του Lambdasat (Λ-sat) είναι:

• Bands available: 2 m, 70 cm.
• Radio Frequency (RF) output power 0 to 1 W programmable.
• Operating voltage (Vdd) of 5.0 V.
• Operating current of 650 mA in transmission, 40 mA when idle.
• Serial interface rate of 38.4 Kbaud UART 8 bit, no parity, one stop bit.
• Dimensions: 1.75 × 3.10” × 1.00”/44.45 × 78.74 mm.
• Mass: approximately 50 g.
• Digital input signal specifications: high signal > 0.7 Vdd.
• Low signal < 0.3 Vdd; 10 uA.
• Digital output signal specifications: high signal > 2.0 V.
• Low signal < 0.4 V; 3 mA sink.
• Mounting holes: 0.125’’; 4 – 40 mounting hardware.

Η τροχιακή ζωή LambdaSat (Λ-sat) εκτιμάται πως μετά βίας θα ξεπεράσει τις εκατόν εβδομήντα (170) ημέρες μετά την εκτόξευσή του από το Διεθνή Διαστημικό Σταθμό (ISS) και την ανάπτυξη του. Υπολογίζεται μετά το πέρας των ημερών αυτών, να ακολουθήσει τις απαιτήσεις που έχουν οριστεί ως απαιτήσεις τροχιάς «υπολειμμάτων» (debris) και θα αποσυντεθεί κατά τη διάρκεια της επανεισόδου του στο τέλος της ζωής της αποστολής του.



Σχήμα 5. Διασύνδεση των λειτουργικών υποσυστημάτων του Lambdasat (Λ-sat).

Από τα παραπάνω προκύπτει ότι σχηματικά η διασύνδεση των λειτουργικών υποσυστημάτων (απουσία payload) του Lambdasat (Λ-sat) θα είναι όπως φαίνεται στο Σχήμα 5. Εάν τώρα αναζητήσει κάποιος παρόμοια διασύνδεση, θα εντοπίσει ότι σχεδιαστικά, σε πολύ βασικές αρχές, στα υποσυστήματα προσοσμοιάζει ο Lambdasat (Λ-sat) με τον TechEdSat CubeSat της NASA, ενώ σίγουρα ο σχεδιασμός αυτός είναι πιο μακριά από τον τυπικό και συνήθη που περιγράφηκε στο κεφάλαιο 3 της παρούσας εργασίας.

5.2 AAUSat3 [53],[54],[55]

Ο cubesat αυτός, ο οποίος είναι ο τρίτος στη σειρά που δημιουργήθηκε στο πανεπιστήμιο του Ααλμπεργκ της Δανίας, απασχολεί φοιτητές ως έργο που πρέπει να διαχειριστούν. Η διαχείριση από τους φοιτητές, με τη μελέτη, τη συμπλήρωση των εγγράφων, το σχεδιασμό, την τήρηση των χρονοδιαγραμμάτων και τη συναρμολόγηση του cubesat, είναι το μέλημα για το οποίο δημιουργείται διαστημική τεχνολογία και δη cubesats από το πανεπιστήμιο. Ακόμη και η συνεργασία, ομάδων διαφορετικών επιστημονικών πεδίων που εμπλέκονται στο έργο, αποτελεί σκοπό αυτού. Όταν ο cubesat θα τεθεί σε τροχιά, επαφίεται στους φοιτητές εάν θα έχει λειτουργικότητα, καθώς οι φοιτητές καθορίζουν την πορεία του έργου ασκώντας τηλεμετρία από το σταθμό εδάφους και αντίστροφα.
Έτσι αυτό που έχει πρωτίστως σημασία για το πανεπιστήμιο είναι να μπορούν να δημιουργούν λειτουργικούς μικροδορυφόρους, οι οποίοι να αξιοποιούνται στη συνέχεια και σε δεύτερο χρόνο να λειτουργούν βάζοντας σε αυτούς διαφορετικά payloads.

Ο AAUSat3 είναι ένας επίσης χαρακτηριστικός cubesat μεγέθους 1U, αφού έχει μήκος πλευράς βάσης τετραγώνου 10 cm, ύψος 11.3 cm και βάρος μάζας 0.8 kgr.
Ο AAUSat3 έχει σχεδιαστεί με μέλημα την άρθρωση και την κατανομή στη μορφοποίησή του, με απαρέγκλιτα συγκεκριμένου προσδιορισμού υποσυστήματα συνεργαζόμενα για τις εργασίες τους με κατάλληλες διεπαφές. Ο νέος αυτός cubesat έχει πολλές ριζικές αλλαγές σε σχέση με τον προηγούμενο AAUSat-2, καθώς εκείνος ήταν σχεδιασμένος να βασίζεται σε ένα κεντρικό υπολογιστή OBC, που παραπέμπει σε παλαιότερη εποχή δομής και λειτουργίας συστήματος, ενώ τώρα παρουσιάζονται αρκετά πλεονεκτήματα, με κύριο την παράλληλη ανάπτυξη και δοκιμή των υποσυστημάτων.

[53] https://directory.eoportal.org/web/eoportal/satellite-missions/a/aausat3
[54] http://www.space.aau.dk/aausat3/index.php
[55] Andrieu J., El haouzianC.N., 2010, Design and Development of a QOS Policy for AAUSAT3 Communication Protocol, AAUSAT3 Project, Department of Electronics, Networks & Distributed Systems, Aalborg University

Πέρα από αυτό, πλέον, εφαρμόζεται λειτουργία προγραμματισμού πτήσης (flight planner functionality - FP) για έλεγχο της έρευνας (έλεγχος των πειραμάτων που τυχόν πραγματοποιούνται και της απόδοσης των payloads). Επιβάλλεται με τον τρόπο αυτό και προσπάθεια δυνατότητας τα υποσυστήματα να λειτουργούν στη βασική τους λειτουργική θέση και το υποσύστημα ηλεκτρικής ενέργειας (EPS) να αναλαμβάνει το ρόλο του συντονιστή, ως το κύριο υποσύστημα της πλατφόρμας, υπεύθυνο για την ενεργοποίηση των υπολοίπων υποσυστημάτων. Αυτό βέβαια είναι κάτι που σχεδιάζεται στο στάδιο κατάρτισης των λειτουργιών του cubesat, όπου υπολογίζεται η κατάλληλη διαθέσιμη ενέργεια για τις λειτουργίες αυτές.

Στον AAUSat3, τα υποσυστήματα που τον αποτελούν είναι:
-Το υποσύστημα παροχής ηλεκτρικής ενέργειας (Electrical Power Supply - EPS),
-το υποσύστημα προγραμματισμού πτήσης (Flight Planner - FP),
- Υποσύστημα Ελέγχου Θέσης στο Χώρο (Attitude Determination and Control Subsystem –ADCS)
-το υποσύστημα καταγραφής – ημερολόγιο (LOGging - LOG) και
-το υποσύστημα επικοινωνιών (COMmunication – COM ή RF),
και τα οποία απαρτίζουν τον πυρήνα του, ή αλλιώς αποτελούν το σύνολο των λειτουργικών υποσυστημάτων του συστήματος στην πλατφόρμα.

Είναι σημαντικό να διευκρινιστεί ότι το EPS στη συγκεκριμένη δομή, είναι υπεύθυνο για την έναρξη της λειτουργίας του cubesat, όταν αυτός εκτοξεύεται από το διαστημικό σταθμό σε τροχιά, οφείλει να είναι λειτουργικό συνέχεια, ενώ τα υπόλοιπα μπορούν να ενεργοποιούνται όταν τους δοθεί εντολή. Ακόμη ότι, για να διατηρεί την παρεχόμενη ενέργεια για τη λειτουργία του cubesat, οφείλει να υποστηρίζεται από ενσωματωμένα φωτοβολταϊκά panels επιφανείας, η μπαταρία του, υπεύθυνη για τη διανομή και την αποθήκευση ενέργειας, να είναι λιθίου LiION 8.2V 2200 mAh και να έχει ρυθμισμένο διανομέα ισχύος: 3.3 και 5V.

Με δεδομένο ότι το EPS έχει το σπουδαιότερο ρόλο στον AAUSat3, παρακάτω αναλύονται και τα υποσυστήματα που το συντελούν, υπενθυμίζοντας ωστόσο ότι το υποσύστημα αυτό μεταφέρει ενέργεια σε όλα τα άλλα υποσυστήματα, και αυτό το

επιτυγχάνει ρυθμιζόμενα μέσω μεμονωμένων, ατομικών καναλιών. Αυτά παρακολουθούνται και τίθενται σε λειτουργία ή βγαίνουν εκτός λειτουργίας από το ίδιο το EPS.

Το υποσύστημα ενέργειας έχει δύο μπαταρίες και ένα υψηλής ενέργειας σημειακού εντοπισμού (Maximum Power Point Tracking - MPPT) φορτιστή ηλιακής συστοιχίας. Το υποσύστημα βασίζεται σε ένα 8-bit AVR MCU (AT90CAN128). Κατά την επιχειρησιακή του λειτουργία, το υποσύστημα χειρίζεται τη φόρτιση και την εκφόρτιση των δύο μπαταριών και παρακολουθεί την ομαλή λειτουργία και την υγεία του cubesat.

Υποσυστήματα του EPS είναι τα

-PV Cells

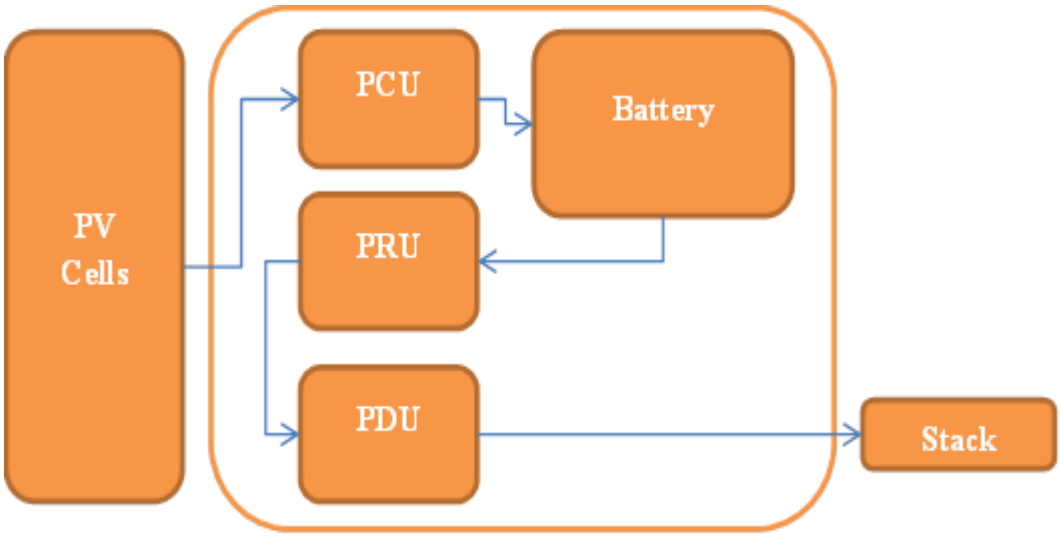
-Battery

-PCU

-PRU

-PDU

και σχηματικά φαίνονται στο σχήμα 6.



Σχήμα 6. Διάταξη υποσυστημάτων στο EPS

PV Cells

Φωτοβολταϊκά κελιά υπάρχουν στις πέντε πλευρές του κύβου, είναι τύπου TJ Solar Cell 3G28C από την Azurspace. Είναι δυνατό κάθε κελί να φέρει 1.15 W σε μέγιστο σημείο, στους 28°C και ακτινοβολία of 1367 W/m^2. Δύο κελιά συνδέονται σε σειρά σε κάθε πλευρά, δίνοντας μέγιστη τάση 4.7 V και όλα συνδέονται μεταξύ τους με δίοδο blocking.

Battery

Αποτελείται από δύο Li-Ion σε σειρά μπαταρίες, δίνοντας συνολική τάση από 6 V έως 8.2 V και χωρητικότητα 2 Ah η κάθε μία. Είναι CGR18650AF-1S1P από την Panasonic.

PCU

Η Μονάδα Μετατροπής Ισχύος είναι υπεύθυνη για τη μετατροπή της συλλεγόμενης από τα φωτοβολταϊκά panels ενέργειας σε αποθηκευμένη ενέργεια στις μπαταρίες. Έχει ένα μετατροπέα ώθησης που μπορεί να ενισχύσει τα 3 V - 5 V των φωτοβολταϊκών σε τάση μπαταρίας 6 V - 8,2 V. Με ένα ψηφιακό ποτενσιόμετρο επιτρέπεται στο EPS να ελέγχει την τάση των φωτοβολταϊκών. Η μονάδα PCU έχει τερματισμό φόρτισης hardware και software. Ο τερματισμός του υλικού υλοποιείται έτσι ώστε η μετασχηματισμένη ώθηση να απενεργοποιείται εάν η τάση της μπαταρίας φθάσει τα 8,2 V. Ο μετατροπέας ώθησης μπορεί επίσης να απενεργοποιηθεί και από το MCU που προαναφέρθηκε. Το MCU θα απενεργοποιήσει τη φόρτιση όταν η τάση της μπαταρίας φτάσει τα 8 V, προκειμένου να αυξηθεί ο χρόνος ζωής των μπαταριών. Αυτό το όριο είναι προσδιορίσιμο και από το σταθμό εδάφους.

PRU

Η μονάδα ρύθμισης ισχύος είναι υπεύθυνη για τη μετατροπή της τάσης της μπαταρίας σε 3,3 V και 5 V για τα υποσυστήματα. Το PRU αποτελείται από τρεις μετατροπείς buck. Ένας για τα κανάλια 3.3 V και 5 V που χρησιμοποιούνται από τα υποσυστήματα. Όμως και ο ενισχυτής ισχύος του UHF έχει δικό του ειδικό μετατροπέα 3,3 V. Ο

κύριος μετατροπέας 3,3 V έχει προστασία χαμηλής τάσης και η έξοδός της τροφοδοτείται και στους τρεις μετατροπείς. Όταν η μπαταρία φθάσει τα 7 V, οι μετατροπείς απενεργοποιούνται και η κατανάλωση ενέργειας μειώνεται στο ελάχιστο. Η μονάδα PCU είναι ακόμα ενεργή, για να φορτίζουν τα φωτοβολταϊκά. Κάθε μετατροπέας είναι δυνατό να παραδώσει περίπου 1,2 A.

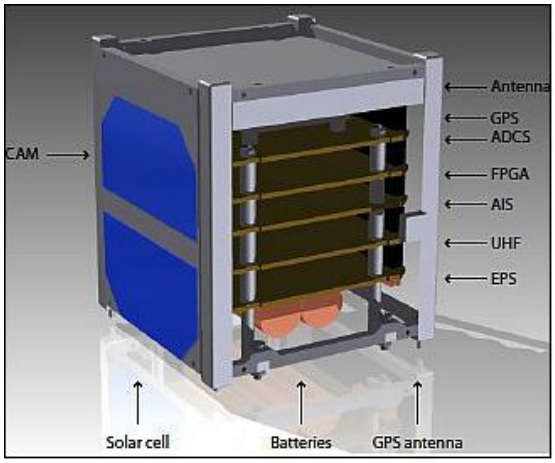
PDU

Η Μονάδα Διανομής Ηλεκτρικής Ενέργειας είναι υπεύθυνη για τον έλεγχο και την παρακολούθηση των καναλιών παροχής ενέργειας του συστήματος. Συνολικά είναι 12 κανάλια. Ελέγχονται ξεχωριστά. Εάν η μονάδα MCU αντιληφθεί διακοπή, με την ενεργοποίηση μίας από τις λειτουργίες προστασίας από το κλείστρο που έχει κάθε κανάλι, ο δίαυλος ισχύος παραμένει εκτός λειτουργίας μέχρι να επανενεργοποιηθεί από το έδαφος.

Επίσης, άλλη μια καινοτομία, είναι η επιλογή ξεχωριστών hardware για κάθε ένα από τα EPS, COM και ADCS, παράλληλα με τη λειτουργία τους στο δικό τους PCB (Printed Circuit Board) που τους δίνει τη δυνατότητα να τίθενται σε λειτουργία default, ακόμα και όταν βρίσκεται το σύστημα κάτω από κρίσιμες καταστάσεις. Επιπλέον, τα EPS, COM και ADCS είναι συνδεδεμένα με τα input και τα output (μπαταρίες, φωτοβολταϊκά panels, πομπός, κεραίες, magnetorques και αισθητήρες) του hardware.

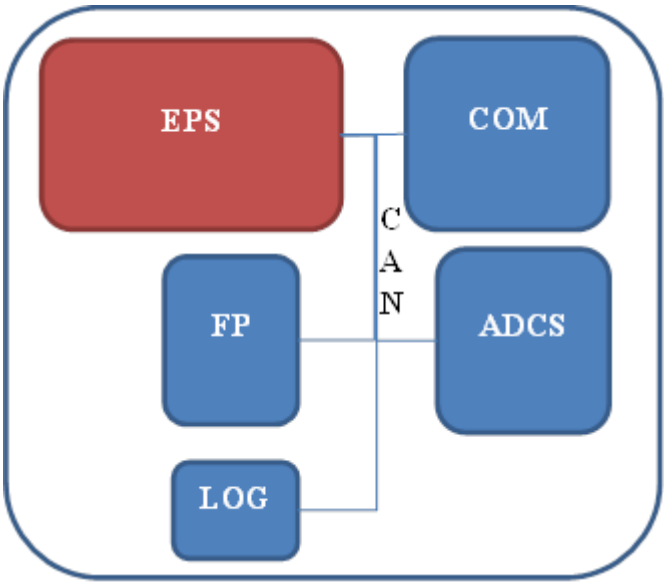
Η διάρκεια ζωής του AAUSat3 υπολογίζεται στην ελάχιστη τιμή της, σε ένα (01) μήνα, ενώ δεν τίθεται πάνω όριο, καθώς σχεδιαστικά είναι σε θέση να «μακροημερεύσει».

Στο επόμενο σχήμα (Σχήμα 7) φαίνεται πως εφαρμόζονται τα προεκτεθέντα σχετικά με το hardware και το PCB και πως τοποθετούνται στο χώρο του cubesat.



Σχήμα 7: Σχηματική δομή του AAUSat3 (image credit: AAU)[56]

Στο σχήμα 8 φαίνεται η διασύνδεση των υποσυστημάτων, όπως περιγράφηκαν. Όπως φαίνεται, στο EPS έχει κόκκινο χρώμα για να αναδειχθεί η σημαντικότητά του σε σχέση με τα υπόλοιπα τέσσερα (04) υποσυστήματα, ενώ και τα υπόλοιπα εμφανίζονται με αντιστοιχία στο μέγεθός τους ως σημαντικά (μεγάλο, μικρό, πιο μικρό), όπως δηλαδή κατατάσσονται σύμφωνα με τους κατασκευαστές.



Σχήμα 8. Διασύνδεση των λειτουργικών υποσυστημάτων του **AAUSat3**

RF επικοινωνίες (ή όπως διαφορετικά έχει αναφερθεί COM)

Η επικοινωνία μεταξύ του δορυφόρου και του επίγειου σταθμού γίνονται μέσω UHF με χρήση Πρωτοκόλλου Εμπρόσθιας Διόρθωσης Σφαλμάτων (Forward Error

[56] https://directory.eoportal.org/web/eoportal/satellite-missions/a/aausat3

Correction - FEC). Το COM λειτουργεί ως διαφανής συσκευή δρομολόγησης (transparent routing device), που επιτρέπει σε όλα τα υποσυστήματα να έχουν τη δική τους επικοινωνία με το σταθμό εδάφους και παρέχει τη δυνατότητα απευθείας λήψης δεδομένων από το έδαφος.

Χαρακτηριστικά

• 162 MHz "uplink" for the AIS payload

• 437 MHz uplink/downlink for S/C επικοινωνία

• Radiolink Viterbi and Reed Solomon κωδικοποίηση

Για να πετύχει μια μετάδοση δεδομένων και προς τις δύο κατευθύνσεις αλλά όχι ταυτόχρονα (half duplex solution), χρησιμοποιείται ένας πομποδέκτης στενής ζώνης υψηλής απόδοσης (high performance narrow-band transceiver) της Analog Devices, ADF 7021.

Με τον τρόπο αυτό κάθε υποσύστημα για τη λειτουργία του χρειάζεται το EPS και το COM.

Οι εσωτερικές επικοινωνίες παρέχονται από ένα φορέα δικτύου περιοχικού ελέγχου (Controller Area Network Bus - CAN), με χρήση ενός επιπέδου δικτύου CSP (Cubesat Space Protocol), το οποίο δημιουργήθηκε από προσπάθεια κοινότητας ανοικτής πηγής (open source community) και συντηρείται από τους φοιτητές του πανεπιστημίου. Σημειώνεται ότι το CSP επιτρέπει στους προγραμματιστές υποσυστημάτων να χρησιμοποιήσουν επικοινωνία socket-like ανάμεσα στα υποσυστήματα με την ανάθεση διευθύνσεων σε υποσυστήματα και θύρες σε διαθέσιμες υπηρεσίες, και τις υπηρεσίες φιλοξενίας να απαντούν στα αιτήματα. Για αυτό επιλέχθηκε όλα τα υποσυστήματα να βασίζονται σε μικροελεγκτές Atmel AVR8.

ADCS

Το ADCS σταθεροποιεί σε 3 άξονες το σύστημα, με ενεργοποιητές magnetorquers. Η ανίχνευση στάσης και γωνιακής ταχύτητας παρέχεται από μαγνητόμετρα και γυροσκόπια, αντίστοιχα.

FP

Το FP περιέχει μηνύματα για τα υποσυστήματα που ενεργοποιούνται σε συγκεκριμένη χρονική στιγμή. Τα νέα μηνύματα μπορούν να μεταφορτωθούν κατά τη διάρκεια της πτήσης, επιτρέποντας έτσι μια αναδιάταξη του FP. Αυτό συμβαίνει λόγω των πακέτων CSP. Αφού λοιπόν το FP χρησιμοποιείται κυρίως για τη ρύθμιση λεπτομερών πειραμάτων στο μεταγενέστερο τμήμα της αποστολής, ένας χρήστης μπορεί να εγγράψει μηνύματα στο έδαφος, να τα ενεργοποιήσει στο σταθμό εδάφους και να τα φορτώσει στο δορυφόρο. Έτσι πειράματα εκκινούν σε στιγμές όπου ο δορυφόρος δεν επικοινωνεί με έναν επίγειο σταθμό κερδίζοντας χρόνο.

LOG

Ο δορυφόρος έχει ένα κοινό ημερολόγιο- σύστημα καταγραφής, όπου όλα τα υποσυστήματα μπορούν να προσθέσουν συμβάντα. Εκεί αποθηκεύονται και μπορεί να περιλαμβάνουν:
Severity – π.χ. πληροφορίες, προειδοποίηση, σφάλμα.
Χρόνος
Υποσύστημα που έστειλε το μήνυμα
Event, αναγνωριστικό μηνύματος – π.χ. BOOT_COMPLETE
Γραμμή κειμένου μέχρι 73 bytes
Το σύστημα δεν μπορεί να φιλτράρει μόνο τη συμβολοσειρά κειμένου και φυσικά δεν έχει το ρόλο αποθήκης δεδομένων πειράματος.

Σε αυτό το σημείο κλείνοντας αυτή την ενότητα, οφείλεται να καταγραφεί ότι ούτε και αυτός ο cubesat, όπως και ο προηγούμενα περιγεγραμμένος, δεν φαίνεται να ακολουθεί σχεδιαστικά στα υποσυστήματα του, τη διαμόρφωση αυτή που παρουσιάστηκε στο συνήθη, τυπικό cubesat σε προηγούμενο κεφάλαιο.

5.3 Κοινά Υποσυστήματα

Εάν συγκρίνουμε τα υποσυστήματα των δύο cubesats που περιγράφηκαν στις δύο προηγούμενες ενότητες του κεφαλαίου, θα δούμε ότι φαινομενικά, ή καλύτερα ονοματολογικά, υφίστανται κοινά λειτουργικά υποσυστήματα.

Ο πίνακας 2 που ακολουθεί περιγράφει κάθε cubesat με τα λειτουργικά υποσυστήματα του και καταδεικνύει τα κοινά λειτουργικά υποσυστήματα

Lambdasat (Λ-sat)	**AAUSat3**	**Κοινά λειτουργικά υποσυστήματα**
Λειτουργικά υποσυστήματα		
OBDH	**EPS**	✓ **EPS**
EPS	**COM**	✓ **COM**
COM	**FP**	
	LOG	
	ADCS	

Πίνακας 2. Λειτουργικά υποσυστήματα cubesats Lambdasat (Λ-sat) και AAUSat3

Ωστόσο, όπως προαναφέρθηκε, η ύπαρξη κοινών υποσυστημάτων, είναι μάλλον ονομαστική. Όπως έχει περιγραφεί, το υποσύστημα EPS, παρόλο που υπάρχει και στους δύο cubesats, δεν φαίνεται να προσομοιάζει το ένα στο άλλο. Στο μεν Lambdasat (Λ-sat) έχει το ρόλο του παραγωγού της ενέργειας του συστήματος (power board και φωτοβολταϊκά panels), ενώ στον AAUSat3 έχει ένα πιο πολύπλοκο ρόλο, αυτό του ελεγκτή και συντονιστή των υπολοίπων υποσυστημάτων. Αντίστοιχα, στο υποσύστημα COM, στο Lambdasat (Λ-sat), φαίνεται να έχει το ρόλο του υπεύθυνου υποσυστήματος για τις επικοινωνίες του εξωτερικά (σταθμό εδάφους, Iridium), ενώ στον AAUSat3 το υποσύστημα είναι απλά δρομολογητής (transparent routing device) των υπολοίπων υποσυστημάτων ώστε εκείνα να επικοινωνούν απευθείας με το σταθμό εδάφους.

Από τον τρόπο σχεδιασμού και λειτουργίας προκύπτει λοιπόν, πως δεν μπορεί να αποδοθεί χαρακτηρισμός κοινών υποσυστημάτων ανάμεσα στους δύο cubesats. Αυτό βέβαια καταδεικνύει την απουσία κοινών τρωτών σημείων στους δύο cubesats στο επίπεδο των λειτουργικών τους υποσυστημάτων, που να μπορούσαν να οδηγήσουν σε συγκριτική ανάλυση και να καταγραφόταν ένα κοινό υποσύστημα που να έχει περισσότερα τρωτά σημεία από τα υπόλοιπα.

Εντούτοις, ενδιαφέρον θα έχει και η διερεύνηση, στη γενικότερη θεώρηση του συστήματος μικροδορυφόρου (cubesat), ενός κοινού τρωτού υποσυστήματος, που έχει μεν σχέση με τα λειτουργικά υποσυστήματα των cubesats, αλλά δεν αποτελεί, δε, άλλο ένα λειτουργικό υποσύστημα αυτών. Η συζήτηση αφορά στο σταθμό εδάφους ο οποίος οφείλεται να ελεγχθεί από άποψη τρωτότητας. Ο έλεγχος αυτός θα λάβει χώρα ταυτόχρονα με τη διερεύνηση των λειτουργικών υποσυστημάτων, καθώς πολλές τρωτότητες διαφαίνεται να είναι κοινές και οφείλεται να καταγραφεί σε ποιο υποσύστημα θα πρέπει να αντιστοιχούν.

Περισσότερη ανάλυση για τα ανωτέρω θα σημειωθεί στην επόμενη ενότητα.

5.4 Τρωτότητες

Κατά το σχεδιασμό του κάθε συστήματος, λήφθηκαν υπόψη συγκεκριμένες επιθυμητές λειτουργίες για αυτό. Δόθηκε κυρίως βαρύτητα στις επικοινωνίες (Lambdasat) και στην ενέργεια (AAUSat3).

Ωστόσο, από την πλευρά της ασφάλειας και κυβερνοασφάλειας θεωρείται απαραίτητο να ελεγχθούν όλα τα υποσυστήματα και να μην περιοριστεί η διερεύνηση για ύπαρξη τρωτοτήτων μόνο σε αυτά που σχετίζονται άμεσα με τις παραπάνω λειτουργίες.

EPS Lambdasat (Λ-sat)

Το υποσύστημα αυτό, όπως έχει προαναφερθεί, αποτελείται από τα φωτοβολταϊκά panels και το power board. Τα φωτοβαλταϊκά panels, σύμφωνα με τους Sibeauda και Puilletb (2015)[57], λόγω της επιφανείας τους, μπορούν να βληθούν από τροχιακά «σκουπίδια» (orbital debris). Η βλάβη μπορεί να είναι ανεκτή όταν είναι απευθείας, αλλά μπορεί να είναι και σημαντική όταν τα «σκουπίδια» χτυπήσουν διπλανό στόχο λόγω του εξοστρακισμού, αφού μπορεί να προκληθεί απώλεια στην παραγωγή ενέργειας που επηρεάζει άμεσα το power board, ενώ και συνολικά τον cubesat στην ευρύτερη λειτουργία του.

Έχοντας αυτό υπόψη, και γνωρίζοντας ότι το 2007, η Κίνα κατέρριψε ένα δικό της δορυφόρο στο πλαίσιο δοκιμών ενός ASAT, μπορούμε να υποθέσουμε ότι, εάν ο στόχος της κατάρριψης ήταν ένα σύστημα που είχε σταλεί ως σε αναμονή σε τροχιά (long duration orbital interceptors) όπως επισημαίνει ο Rooker, (2008)[58], ώστε να πλήξει επιθυμητούς στόχους στον επιθυμητό χρόνο, θα μπορούσε η «υποτιθέμενη» κατάρριψή του στο πλαίσιο δοκιμών και η δημιουργία από αυτήν τροχιακών «σκουπιδιών» (orbital debris), να αποτελεί πραγματική επίθεση στον Λ-sat. Όμως και με το απλούστερο σενάριο της κατάρριψης ενός αληθούς δορυφόρου, πάλι με το πρόσχημα των δοκιμών ενός ASAT, τα «σκουπίδια» (orbital debris), μπορούν να

[57] Sibeauda J-M, Puilletb C., 2015, Effects of Debris Cloud Interaction with Satellites Critical Equipments - Experiments and Modeling -, The 13th Hypervelocity Impact Symposium, Procedia Engineering, 103, 561 – 568, Elsevier Ltd

[58] Rooker J. W., 2008, Satellite Vulnerabilities, EWS Contemporary Issue Paper, United States Marine Corps,Command and Staff College, Marine Corps Combat Development,Marine Corps University

αποτελέσουν μέσο επίθεσης στον Λ-sat. Εφόσον λοιπόν, ληφθούν υπόψη και τα αποτελέσματα των ερευνών των Sibeauda και Puilletb, το σενάριο προκύπτει διττό και μπορεί να αναδείξει την τρωτότητα αυτή από πιθανή έως δυνατή με συνέπειες μη μόνιμης βλάβης έως μόνιμης βλάβης.

Αντίστοιχα, ολική καταστροφή μπορεί να συμβεί με μια επίθεση από οπλικό σύστημα υψηλής ισχύος EMP (electromagnetic pulse) όπου σύμφωνα με τους GUO, ZHANG και ZHANG (2016)[59], θα καταστραφεί και το power board του υποσυστήματος λόγω αύξησης της θερμοκρασίας, όπως δηλαδή θα συμβεί με όλα τα υποσυστήματα.

Οι άλλες δύο κατηγορίες μέσων επίθεσης (Electronics και Cyber), δε διαφαίνεται με τη διάταξη του Λ-sat να έχουν άμεση συνέπεια στο EPS.

OBDH Lambdasat (Λ-sat)

Στο υποσύστημα αυτό αντιστοιχούν ο κύριος υπολογιστής, υπεύθυνος για όλες τις λειτουργίες του δορυφόρου, για την επεξεργασία των εντολών που του δίνονται και για τη μετάδοσή τους στα υπόλοιπα υποσυστήματα. Είναι ουσιαστικά το «μυαλό» του συστήματος και ως εκ τούτου, το πλέον σημαντικό υποσύστημα για προστασία από επιθέσεις και κυβερνοεπιθέσεις. Εάν λάβουμε υπόψη το προηγούμενο σενάριο για τα «σκουπίδια» (orbital debris), εδώ εντοπίζουμε ότι λόγω της κατασκευής του σκελετού του Λ-sat, το υποσύστημα είναι προστατευμένο και η οποιαδήποτε «επίθεση» με «σκουπίδια» δε θα προκαλέσει άμεσες και σημαντικές βλάβες. Ωστόσο, εάν τα «σκουπίδια» είναι ικανού μεγέθους (FAS's Panel on Weapons in Space, 2004)[60], τότε είναι ευνόητο πως όλο το σύστημα Λ-sat θα διατρέχει κίνδυνο και όχι μόνο ένα μεμονωμένο υποσύστημα. Με άλλα λόγια, τρωτότητα απέναντι σε συνήθη kinetic physical μέσα επίθεσης δεν διαφαίνεται για το υποσύστημα αυτό.

[59] GUO Li-wen1, ZHANG Zhan-yue, ZHANG Zhe1, 2016, Vulnerability Analysis of Satellites in Strong Electromagnetic Environment, 4th National Conference on Electrical, Electronics and Computer Engineering (NCEECE 2015), Atlantis Press
[60] FAS's Panel on Weapons in Space, 2004, Ensuring America's Space Security Report of the FAS Panel on Weapons in Space, Federation of American Scientists

Αντίθετα, λαμβάνουν χώρα ακριβώς οι ίδιες συνέπειες στην περίπτωση επίθεσης με υψηλής ισχύος non-kinetic physical μέσα, δηλαδή λόγω αύξησης της θερμοκρασίας στο σύστημα από επίθεση υψηλής ισχύος EMP επέρχεται πλήρης καταστροφή.

Στο επίπεδο των electronics ως μέσα επίθεσης, κάθε προσπάθεια jamming ή spoofing, μπορεί να δημιουργήσει σοβαρές δυσλειτουργίες στο υποσύστημα, που μπορεί να προκαλέσουν ακόμη και την καταστροφή του συστήματος, καθώς είτε δε θα λαμβάνει για παράδειγμα νέες οδηγίες για διόρθωση θέση (jamming) ή θα λαμβάνει για παράδειγμα νέες οδηγίες για οποιαδήποτε τροποποίηση στον τρόπο λειτουργίας του, ενώ στην πραγματικότητα δε θα έχει συμβεί κάτι τέτοιο (spoofing), καθώς θα έχει αλλαχθεί το σήμα κατά τη διάρκεια κάλυψης της απόστασης ανάμεσα στο σταθμό εδάφους και το cubesat, το επονομαζόμενο δηλαδή και hijacking (author unknown, date unknown[61]). Για την τρωτότητα αυτή, η ευθύνη κανονικά βαρύνει εξίσου και τον εκάστοτε σταθμό εδάφους, καθώς μπορεί ανά πάσα στιγμή να πραγματοποιηθεί η επίθεση η οποία να μην γίνει αντιληπτή, γιατί μπορεί να εκδηλώνεται σταδιακά ώστε να επιτεύχθει ο στόχος (Wilgenbusch και Heisig (2013)[62]).

Εντούτοις, η τρωτότητα αυτή, στην περίπτωση του Λ-sat, μπορεί να θεωρηθεί ότι καλύπτεται σε ένα βαθμό με το σχεδιασμό για διάστημα ανοχής τριών σφαλμάτων που έχει δοθεί. Άρα εφόσον οι τυχόν επιθέσεις είναι περιστασιακές, το σύστημα θα μπορεί να ανακτήσει πιθανόν την πρωτέρα κατάστασή του, ή έστω να επανέλθει σε μια κανονικότητα μέσω της ανθεκτικότητάς του.

Σε σχέση τώρα με τυχόν κυβερνοεπιθέσεις στο λογισμικό του υποσυστήματος, μπορεί να λάβει κάποιος υπόψη το παράδειγμα του Santamarta (2018)[63], όπου με μελέτη των δεδομένων που κατάφερε να συλλέξει, κατόρθωσε να σπάσει τον κώδικα που χρησιμοποιούν για τη χρήση internet στα αεροπλάνα και να παρέμβει σε αυτόν. Εάν τώρα υποθέσουμε ότι κάποιος επιθυμούσε να κάνει το ίδιο με τον κώδικα του κύριου

[61] Global SatShow - Satellite Conference & Exhibition
http://globalsatshow.com/port/Telecommunications/cyber-attacks-a-major-challenge-faced-by-the-telecommunications-satellites
[62] Wilgenbusch R. C., Heisig A., 2013, Command and Control Vulnerabilities to Communications Jamming , JFQ, issue 69, 2nd quarter, ndupress.ndu.edu
[63] Santamarta R., 2018, \WHITE PAPER\Last Call for SATCOM Security, IOActive, Inc.

υπολογιστή και να παρέμβει στις λειτουργίες του Λ-Sat, τότε μπορεί να θεωρηθεί ότι αντίστοιχα θα υπήρχε επιτυχία. Σε καμιά περίπτωση φυσικά δε σημαίνει ότι ο κώδικας έχει σφάλματα ή δεν είναι σωστά γραμμένος. Τουναντίον, αυτό που αναδεικνύεται είναι το ότι ανεξαρτήτως εάν ένα σύστημα χρησιμοποιεί ένα λογισμικό cots ή ένα custom made σε ανοιχτό κώδικα ή ένα custom made με συγκεκριμένες παραδοχές, πάντα θα υπάρξει κάποιος που εφόσον προσπαθήσει να τον προσπελάσει θα το καταφέρει. Δυστυχώς όσο και εάν φαντάζει υποθετικό αυτό, είναι η πραγματικότητα, καθώς πρέπει να ληφθεί υπόψη ότι τα λογισμικά αυτά, δεν επιδέχονται αναβάθμισης από τη στιγμή που ξεκινήσουν την αποστολή τους και φυσικά από τη στιγμή που σχεδιάζονται τίθενται σε λειτουργία μετά από ένα ή δύο έτη. Αυτό σημαίνει ότι κάποιος που θα θέλει να προκαλέσει βλάβη στο σύστημα μέσω εκμετάλλευσης της τρωτότητας αυτής, πιθανότατα θα το επιτύχει, αφού θα έχει την πολυτέλεια να αναζητήσει για τουλάχιστον ένα με δύο έτη πληροφορίες για το πώς θα το καταφέρει. Σε κάθε περίπτωση, η τρωτότητα αυτή κατατάσσεται στις σημαντικές, αφού επηρεάζει την όλη λειτουργία του συστήματος, μιας και όλες οι λειτουργίες εξαρτώνται από το εν λόγω υποσύστημα.

COM Lambdasat (Λ-sat)

Το εν λόγω υποσύστημα είναι υπεύθυνο, όπως προαναφέρθηκε για τις κεραίες, το ραδιοφάρο και την επικοινωνία με τον αστερισμό του Iridium.

Ως προς τα kinetic physical μέσα, είναι ευνόητο πως και εδώ η τρωτότητα είναι εμφανής. Η χρησιμοποιούμενη κεραία λήψης και μετάδοσης με την τριπλή της διάταξη είναι εύκολο να βληθεί από «σκουπίδια» (orbital debris) που θα προέρχονται από τη χρήση ενός ASAT.

Ομοίως, τα cots που χρησιμοποιούνται, ήτοι ο ραδιοφάρος και το short burst data μοντεμ επικοινωνίας, πέρα από την κεραία, η οποία θα κάνει πιθανότατα coupling στην περίπτωση χρήσης ενός non-kinetic physical μέσου υψηλής ισχύος (EMP), πιθανότατα θα καταστραφούν λόγω αύξησης της θερμοκρασίας που θα δημιουργηθεί.

Σε σχέση με τα electronics, αυτό που οφείλεται να σημειωθεί είναι ότι το εύρος της κεραίας έχει καθοριστικό ρόλο στην τρωτότητα του υποσυστήματος. Εάν δεν είναι ειδικά στοχευμένο, αλλά έχει μια γενικότερη κάλυψη, ώστε να πετυχαίνει ευρύτερη διασύνδεση, τότε πιθανότατα να είναι πιο εκτεθειμένο σε κίνδυνο. Στην περίπτωση του Λ-sat, η τριπλή διάταξη για καλύτερη διασύνδεση με το σταθμό εδάφους αλλά και με τα πλοία, αντιστοιχεί σε αύξηση της επιτυχούς επίθεσης.

Εάν τώρα, ληφθεί υπόψη και ότι σύμφωνα με τον Rooker (2008)[64] το 2003, ένα σήμα από την Κούβα κατάφερε να πετύχει uplink jamming σε μια μετάδοση σήματος (πληροφορίας) μέσω δορυφόρου (όχι στρατιωτικού) τηλεπικοινωνιών που είχε προορισμό το Ιραν και ότι αυτό επετεύχθει γνωρίζοντας την ακριβή συχνότητα, έχοντας μια καλά κατευθυνόμενη κεραία και αρκετή ισχύ για να ξεπεράσει την πηγή του σήματος, τότε στην περίπτωση του Λ-sat, όπου η συχνότητα είχε δοθεί σε όλους τους ραδιοερασιτέχνες για να κάνουν ping και να λαμβάνουν πληροφορίες από αυτόν, γίνεται εύκολα αντιληπτό ότι η τρωτότητα μπορεί να θεωρηθεί κρίσιμη.

Αντίστοιχη τρωτότητα προκύπτει και στην περίπτωση που χρησιμποποιηθεί η μέθοδος spoofing, ειδικά εάν είναι παρατεταμένης διάρκειας και συνδυαστεί με hijacking, αφού αυτό είναι εφικτό κατά τη μετάδοση του σήματος μέσω του constellation, αφού για αυτό χρησιμοποιείται το μοντεμ (είδος cots), του οποίου τα specifications είναι εύκολο να βρεθούν και να καταστρωθεί από κάποιον που το επιθυμεί σχέδια προσπελασιμότητάς του. Ομοίως ισχύει και για το ραδιοφάρο.

Επίσης, στην περίπτωση κυβερνοεπίθεσης, το υποσύστημα θεωρείται τρωτό, αφού μπορεί να λάβει οποιαδήποτε εντολή από το σταθμό εδάφους, ο οποίος είναι θεωρητικά, αλλά και πρακτικά πιο ευάλωτος, λόγω της χρήσης του διαδικτύου και των υπολοίπων κοινών λειτουργικών λογισμικών.

[64] Rooker J. W., 2008, Satellite Vulnerabilities, EWS Contemporary Issue Paper, United States Marine Corps,Command and Staff College, Marine Corps Combat Development,Marine Corps University

Σύμφωνα με τον Bichler (2015)[65] τώρα, τα συχνότερα σενάρια κυβερνοεπιθέσεων και ανάδειξης τρωτοτήτων σε σταθμούς εδάφους είναι τα cross-site scripting, τα cross-site request forgery και τα "drive-by" hacking. Αυτά τα σενάρια βρίσκονται και στη λίστα των 10 πρώτων τρωτοτήτων σύμφωνα με το Open Web Application Security Project. Κοινώς, είναι τα σενάρια όπου ο «εισβολέας» παίρνει τον έλεγχο της οθόνης (και άρα του Η/Υ συστήματος) με χρήση Trojan, με συνέπεια να μπορεί να παρακολουθεί και να στέλνει οτιδήποτε επιθυμεί στο μικροδορυφόρο. Φυσικά, η τρωτότητα ισχύει και για το σταθμό εδάφους του Λ-sat, με ισχυρό αντίκτυπο στην όλη αποστολή.

Περνόντας πλέον στα υποσυστήματα του AAUSat3, θα θεωρηθεί για ευνόητους λόγους ότι τα non-kinetic physical υψηλής ισχύος μέσα (EMP) έχουν όμοιες επιπτώσεις σε όλα τα υποσυστήματα και σε αυτό το cubesat, όπως στο Λ-sat.

EPS AAUSat3

Σημαντικό θεωρείται να υπεθμιστεί ότι το EPS του συγκεκριμένου cubesat είναι υπεύθυνο για την έναρξη της λειτουργίας του, οφείλει να είναι λειτουργικό συνέχεια και μεταβιβάζει την εντολή στα υπόλοιπα ότι μπορούν να ενεργοποιούνται ή να μπαίνουν σε κατάσταση ύπνου. Υποστηρίζεται από ενσωματωμένα φωτοβολταϊκά panels επιφανείας, μπαταρία και ρυθμισμένο διανομέα ισχύος. Το υποσύστημα αυτό μεταφέρει ενέργεια σε όλα τα άλλα υποσυστήματα, και αυτό το επιτυγχάνει ρυθμιζόμενα μέσω μεμονωμένων, ατομικών καναλιών. Αυτά παρακολουθούνται και τίθενται σε λειτουργία ή βγαίνουν εκτός λειτουργίας από το ίδιο το EPS. Έχει επίσης ένα υψηλής ενέργειας σημειακού εντοπισμού (Maximum Power Point Tracking - MPPT) φορτιστή ηλιακής συστοιχίας. Το υποσύστημα βασίζεται σε ένα 8-bit AVR MCU. Κατά την επιχειρησιακή του λειτουργία, το υποσύστημα χειρίζεται τη φόρτιση και την εκφόρτιση των μπαταριών και παρακολουθεί την ομαλή λειτουργία και την υγεία του cubesat.

[65] Bichler S.F., Maj, USAF, 2015, Mitigating Cyber Security Risk in Satellite Ground Systems, Air Command and Staff College, Air University, Muir S. Fairchild Research Information Center, Digital colletcion

Όπως προκύπτει, τα καθήκοντα αυτού του υποσυστήματος είναι αρκετά και αυτό το κάνει το πιο σημαντικό υποσύστημα του συγκεκριμένου cubesat. Αυτό όμως δημιουργεί και περισσότερες ανάγκες διασφάλισης, καθώς η ύπαρξη τρωτοτήτων σε αυτό μπορεί να αποβεί μοιραία για όλο το σύστημα

Όσον αφορά τα «σκουπίδια», κάνοντας χρήση του ίδιου σεναρίου όπως και στο Λ-sat, λόγω των φωτοβολταϊκών panels, είναι προφανές ότι ισχύουν τα ίδια αποτελέσματα.

Σχετικά με τα σενάρια jamming και spoofing με συνδυασμό με hijacking, προκύπτουν τα ακόλουθα. Εφόσον η επαφή με το δταθμό εδάφους είναι ελεύθερη και δεν παρεμβάλεται το υποσύστημα COM, καθίσταται σαφές ότι οποιαδήποτε παρεμβολή σήματος, κατά τη διάρκεια της επικοινωνίας, μπορεί να αποβεί μοιραία. Επίσης, η οποιαδήποτε τροποποίηση εντολών, η οποία θα καταγράφεται ως αληθής και στο υποσύστημα LOG του AAUSat3, ενώ στην ουσία θα είναι αποτέλεσμα spoofing, δύναται να αποδειχθεί και αυτή καταστροφική.

Η ύπαρξη υποσυστημάτων εντός του υποσυστήματος EPS, με κυριότερο το PCU που συντονίζει τα υπόλοιπα μέσω του MCU που διαθέτει (hardware και λογισμικό), και η ταυτόχρονη ελεύθερη επικοινωνία με το σταθμό εδάφους των υποσυστημάτων, όπως προαναφέρθηκε, μπορεί να θεωρηθεί ως ένα ακόμη τρωτό σημείο για το υποσύστημα EPS.

Το Δεκέμβριο του 2018, η NASA ανακοίνωσε ότι είχε ένα σοβαρό κενό ασφαλείας σε υπολογιστή. Δεν ανέφερε πόσες επιθέσεις έγιναν ή πόση ζημιά έγινε, απλά σημειώθηκε ότι «μάλλον δεν υπήρξε πρόβλημα σε καμιά αποστολή της» καθώς και ότι «το κενό αφορά σε υπαλλήλους της και μάλιστα ακόμη και σε εκείνους που εργάζονταν στην Υπηρεσία το 2006 και πλέον όχι». Τι θα γινόταν όμως εάν το χτύπημα δεν γινόταν αντιληπτό και το υποσύστημα EPS του δορυφόρου ερχόταν σε επαφή με προσβεβλημένο υπολογιστή στο σταθμό εδάφους; (υποθέτοντας φυσικά ότι ο δορυφόρος επικοινωνούσε με το συγκεκριμένο σταθμό της υπηρεσίας). Ο δορυφόρος και ιδιαίτερα το κύριο λειτουργικό του υποσύστημα που λειτουργεί

ακατάπαυστα και δεν πέφτει ποτέ σε default mode, θα πραγματοποιούσε, χωρίς κάποιο άλλο ενδιάμεσο, άμεση επαφή με πιθανή μόνιμη βλάβη ή έως και ολική καταστροφή του, σε περίπτωση που η εντολή που θα του δινόταν από το κακόβουλο λογισμικό θα ήταν να επαναπρογραμματίσει τις διαδικασίες του υποσυστήματος του PCU, εντολή που μπορεί να δοθεί από το σταθμό εδάφους, με τιμές εκτός των ορίων λειτουργίας.

COM AAUSat3

Όπως έχει περιγραφεί ο AAUSat3, στο υποσύστημα αυτό, χρησιμοποιεί κυρίως cots, για να μπορέσει η κεραία του, η οποία είναι στενής ζώνης υψηλής απόδοσης, να λάβει ή να αποστείλει πληροφορία, με παράλληλη λειτουργία λογισμικού ανοικτού κώδικα. Αναφέρεται ξανά, ότι το CSP επιτρέπει στους προγραμματιστές υποσυστημάτων να χρησιμοποιήσουν επικοινωνία socket-like ανάμεσα στα υποσυστήματα με την ανάθεση διευθύνσεων σε υποσυστήματα και θύρες σε διαθέσιμες υπηρεσίες, και τις υπηρεσίες φιλοξενίας να απαντούν στα αιτήματα.

Από τα ανωτέρω, προκύπτουν τα ακόλουθα. Όπως και στην περίπτωση του Λ-sat η έκθεση της κεραίας, η οποία σημειωτέον, και σε αυτόν τον cubesat, είναι μια για όλες τις χρήσεις, σε «σκουπίδια» (orbital debris), θα προκαλέσει βλάβη, εφόσον το μέγεθος των «σκουπιδιών» είναι τέτοιο που να μπορεί να προκαλέσει ζημιά.

Σε σχέση με τα electronic μέσα (jamming και spoofing), αλλά και τα cyber, είναι προφανές ότι υπάρχουν αρκετά τρωτά σημεία για να καταφέρουν βλάβη στο σύστημα. Ίσως η κωδικοποίηση που λαμβάνει χώρα κατά την αποστολή και λήψη πληροφοριών με το σταθμό εδάφους να δημιουργεί ένα ανάχωμα στην όποια επίθεση, όμως με δεδομένο ότι όλα τα μέρη που αποτελούν το υποσύστημα είναι cots και το λογισμικό είναι με χρήση ανοικτού κώδικα, δίνεται η δυνατότητα σε οποιοδήποτε «εισβολέα» να μελετήσει τα specs και τον κώδικα και να δράσει αναλόγως.

FP AAUSat3

Υπενθυμίζεται ότι με το FP ένας χρήστης μπορεί να εγγράψει μηνύματα στο έδαφος, να τα ενεργοποιήσει στο σταθμό εδάφους και να τα φορτώσει στο δορυφόρο για να

ενεργοποιηθούν σε δεύτερο χρόνο και να πραγματοποιηθούν τα πειράματα σε στιγμές όπου ο δορυφόρος δεν επικοινωνεί με έναν επίγειο σταθμό.

Όπως γίνεται αντιληπτό, η έκθεση σε «σκουπίδια» (orbital debris), δεν επιφέρει προβλήματα στο υποσύστημα αυτό, αφού δεν έχει εκτεθειμένα μέρη.

Ομοίως, δε διαφαίνεται να δημιουργούνται προβλήματα από jamming ή τουλάχιστον, εάν δημιουργούνται, μπορούν να θεωρηθούν μικρού μεγέθους και σημασίας.

Δεν μπορεί να σημειωθεί το ίδιο και για το spoofing. Ειδικά σε συνδυασμό με hijacking. Από μόνο του το υποσύστημα έχει ένα ρόλο αναμονής και ενεργοποίησης σε δεύτερο χρόνο. Αυτό, προφανώς διευκολύνει την όποια αποστολή διαφορετικών εντολών από αυτές που αποστέλλονται από το σταθμό εδάφους, εφόοσν υφίσταται τέτοιου είδους επίθεση, οι οποίες δεν μπορούν να ελεγχθούν και να διορθωθούν. Το ίδιο ισχύει και για τα cyber μέσα.

LOG AAUSat3

Στο υποσύστημα αυτό διαφαίνεται να υφίσταται μόνο μια τρωτότητα, όπως αυτή έχει αναφερθεί νωρίτερα, ήτοι η χρήση υψηλής ισχύος non-kinetic physical μέσου.

ADCS AAUSat3

Έχοντας υπόψη ότι το υποσύστημα αυτό αποτελείται από ενεργοποιητές magnetorquers, μαγνητόμετρα και γυροσκόπια, μπορούν να σημειωθούν τα ακόλουθα.

Η έκθεση σε «σκουπίδια» (orbital debris), δεν φαίνεται να επιφέρει προβλήματα στο υποσύστημα.

Δεν μπορεί να σημειωθεί το ίδιο για το jamming, το spoofing καθώς και για τα cyber μέσα. Σε περίπτωση τέτοιας επίθεσης, πιθανότατα δε θα μπορέσει να ληφθεί εντολή αλλαγής θέσης με πιθανό αποτέλεσμα ακόμη και τη σύγκρουση σε επόμενο χρόνο με

άλλο δορυφορικό ή μικροδορυφορικό σύστημα. Κρίνονται λοιπόν σημαντικής ισχύος επιθέσεις και η τρωτότητα αυτή οφείλει να παρακολουθηθεί και να αντιμετωπιστεί.

Οι τρωτότητες στα δύο συστήματα cubesats, μπορούν να είναι αρκετές, ειδικά όταν εκ των υστέρων ελέγχει κάποιος τα συστήματα. Στην περίπτωση των δύο αυτών cubesats, θεωρείται ότι κάθε υποσύστημα μπορεί να είναι σε κίνδυνο, με δεδομένο ότι δεν είχε πραγματοποιηθεί κανένας έλεγχος για την ασφάλεια και την κυβερνοασφάλεια τους. Σκεπτόμενος κάποιος με τη μέθοδο root cause, θα μπορούσε να υποστηρίξει ότι εκεί είναι και η πηγή της βλάβης, εφόσον αυτή προκληθεί. Η απουσία μέριμνας για ασφάλεια και κυβερνοασφάλεια. Διαφαίνεται, ωστόσο, ότι τα σημεία τρωτότητας κατανέμονται στα λειτουργικά υποσυστήματα όπως προαναφέρθηκαν.

Συνοψίζοντας, σχηματικά τα παραπάνω φαίνονται στον πίνακα 3 που ακολουθεί

Cubesat	Υποσύστημα	Ύπαρξη τρωτότητας		Αιτία	Πιθανότητα πραγματοποίησης σεναρίου				Αποτελέσματα Συνέπειες			Ιεράρχηση			
		Ναι	Όχι		α	β	γ	δ	I	II	III	1	2	3	4
					Δυνατό (possible)	Πιθανό (probable)	Απίθανο (improbable)	Αδύνατο (impossible)	Μη μόνιμη βλάβη	Μόνιμη βλάβη	Ολική καταστροφή	Υψηλή σημαντικότητα	Λιγότερο υψηλής σημαντικότητας	Χαμηλής σημαντικότητας	Καθόλου σημαντική
Λ-sat	**EPS**			Asat – orbital debris	α				I			**3**			
Λ-sat	**EPS**			Asat – orbital debris με εξοστρακισμό		β				II		**1**			
Λ-sat	**EPS**			EMP			γ				III		**2**		
Λ-sat	**EPS**			Electronics											
Λ-sat	**EPS**			Cyber											
Λ-sat	**OBDH**			Asat											
Λ-sat	**OBDH**			EMP			γ				III		**2**		
Λ-sat	**OBDH**			Jamming	α				I				**2**		

Λ-sat	**OBDH**		Jamming (Intense)	γ	III	**2**
Λ-sat	**OBDH**		Hijacking – Spoofing	α	I	**1**
Λ-sat	**OBDH**		Hijacking – Spoofing (Intense)	γ	III	**1**
Λ-sat	**OBDH**		Cyber	α	II III	**1**
Λ-sat	**COM**		Asat	β	II	**2**
Λ-sat	**COM**		EMP	γ	III	**3**
Λ-sat	**COM**		Jamming (Intense)	β	I	**1**
Λ-sat	**COM**		Hijacking – Spoofing (Intense)	α	II III	**1**
Λ-sat	**COM**		Cyber	α	II III	**1**
AAUSat3	**EPS**		Asat – orbital debris	α	I	**3**
AAUSat3	**EPS**		Asat – orbital debris με εξοστρακισμό	β	II	**1**
AAUSat3	**EPS**		EMP	γ	III	**2**
AAUSat3	**EPS**		Jamming	α	II	**1**
AAUSat3	**EPS**		Jamming (Intense)	β	I	**1**

AAUSat3	**EPS**		Hijacking – Spoofing	α	II	III	**1**
AAUSat3	**EPS**		Hijacking – Spoofing (Intense)	α	II	III	**1**
AAUSat3	**EPS**		Cyber	α	II	III	**1**
AAUSat3	**COM**		Asat	β	II		**2**
AAUSat3	**COM**		EMP	γ	III		**3**
AAUSat3	**COM**		Jamming (Intense)	β	I		**1**
AAUSat3	**COM**		Hijacking – Spoofing (Intense)	α	II	III	**1**
AAUSat3	**COM**		Cyber	α	II	III	**1**
AAUSat3	**FP**		Asat				
AAUSat3	**FP**		EMP	γ	III		**3**
AAUSat3	**FP**		Jamming	β	I		**4**
AAUSat3	**FP**		Hijacking – Spoofing (Intense)	α	III		**1**
AAUSat3	**FP**		Cyber	α	III		**1**
AAUSat3	**LOG**		Asat				
AAUSat3	**LOG**		EMP	γ	III		**3**

AAUSat3	**LOG**		Jamming (Intense)				
AAUSat3	**LOG**		Hijacking – Spoofing (Intense)				
AAUSat3	**LOG**		Cyber				
AAUSat3	**ADCS**		Asat				
AAUSat3	**ADCS**		EMP	γ	III		**3**
AAUSat3	**ADCS**		Jamming	β	II	III	**1**
AAUSat3	**ADCS**		Spoofing	β	II	III	**1**
AAUSat3	**ADCS**		Cyber	β	II	III	**1**
Λ-sat & AAUSat3	**GROUND CONTROL**		Asat	α	II	III	**1**
Λ-sat & AAUSat3	**GROUND CONTROL**		EMP	α	II	III	**1**
Λ-sat & AAUSat3	**GROUND CONTROL**		Jamming (Intense)	α	II	III	**1**
Λ-sat & AAUSat3	**GROUND CONTROL**		Hijacking – Spoofing (Intense)	α	II	III	**1**
Λ-sat & AAUSat3	**GROUND CONTROL**		Cyber	α	II	III	**1**

Πίνακας 3. Τρωτότητες σε λειτουργικά υποσυστήματα cubesats Lambdasat (Λ-sat) και AAUSat3

6. Εντοπισμός τρωτοτήτων ασφάλειας και κυβερνοασφάλειας υποσυστήματος φορτίου (payload)

Αντίστοιχη καταγραφή των payloads των δύο cubesats, θα πραγματοποιηθεί παρακάτω. Εδώ θα πρέπει να αποδεχτούμε τις ερευνητικές υποθέσεις ύπαρξης τρωτοτήτων ασφάλειας και κυβερνοασφάλειας στην αποστολή και λήψη σήματος του payload καθώς και της σημαντικότητας των τρωτοτήτων. Τα προκύπτοντα ερωτήματα που θα πρέπει να απαντηθούν είναι τα ακόλουθα:

- Υπάρχουν τρωτότητες ασφάλειας και κυβερνοασφάλειας στην αποστολή και λήψη σήματος του payload.
- Οι κίνδυνοι που προκύπτουν από τις τρωτότητες μπορούν να κατηγοριοποιηθούν σε σημαντικούς ή μη.
- Θεωρείται σημαντικότερη η ασφάλεια μετάδοσης της πληροφορίας ή η ασφάλεια του μικροδορυφόρου.

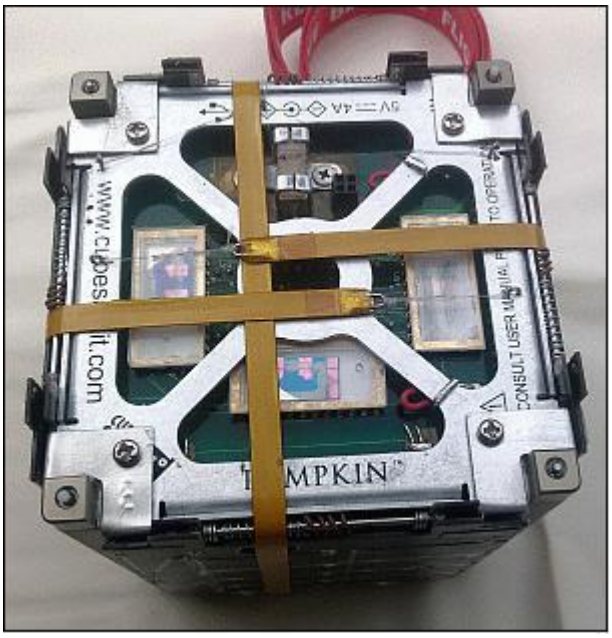
Εντούτοις, χωρίς να μειώνεται η σημαντικότητα, κάθε άλλο, των τρωτοτήτων που μπορεί να υπάρχουν στη λειτουργία των payloads, το ζήτημα πλέον έγκειται στο τελευταίο ερώτημα που θα πρέπει να απαντηθεί, καθώς ο όποιος σχεδιασμός αεροδιαστημικών εφαρμογών και ιδιαίτερα μικροδορυφόρων και cubesats, θα πρέπει να βαδίζει αντίστοιχα.

6.1 Περιγραφή φορτίου μικροδορυφόρου (payload) Lambdasat (Λ-sat)

Το payload του Lambdasat (Λ-sat) αποτελείται από δύο είδη.

Το πρώτο είναι μια συσκευή δέκτης αυτόματου εντοπισμού πλοίων (AIS) που σκοπό έχει τη λήψη σημάτων AIS από τα εμπορικά πλοία για να μπορέσει να υπάρξει καλύτερη επίβλεψη αυτών, ειδικά όταν αυτά πλέουν σε περιοχές που είναι αυξημένες οι πιθανότητες πειρατείας ή άλλων έκνομων ενεργειών. Με το AIS θα γίνεται επικοινωνία με την πλατφόρμα του Iridium η οποία θα μεταδίδει και θα συλλέγει τα δεδομένα AIS που συλλέγονται από το έδαφος.

Το δεύτερο είναι φέτες (τεμάχια) γραφενίου GFET (Graphene Field-Effect Transistor). Με επικοινωνία μέσω της Stensat θα γίνεται downlink στα πειραματικά δεδομένα του γραφενίου. Τα δεδομένα θα αφορούν στην επίδραση της ακτινοβολίας στη δομή κρυστάλλου δεσμού-γραφενίου, τις επιδράσεις στην ηλεκτρονική απόδοση και κινητικότητα, την επίδραση στο υπόστρωμα και τη διηλεκτρική διεπαφή και την επικάλυψη των αποτελεσμάτων σκέδασης παρουσία ακτινοβολίας.



Εικόνα 3: Το γραφένιο στον LambdaSat (Λ-sat)

(image credit: NASA, Periklis Papadopoulos)[66]

[66] https://directory.eoportal.org/web/eoportal/satellite-missions/L/LAMBDASAT#sensors

6.2 Περιγραφή φορτίου μικροδορυφόρου (payload) AAUSat3

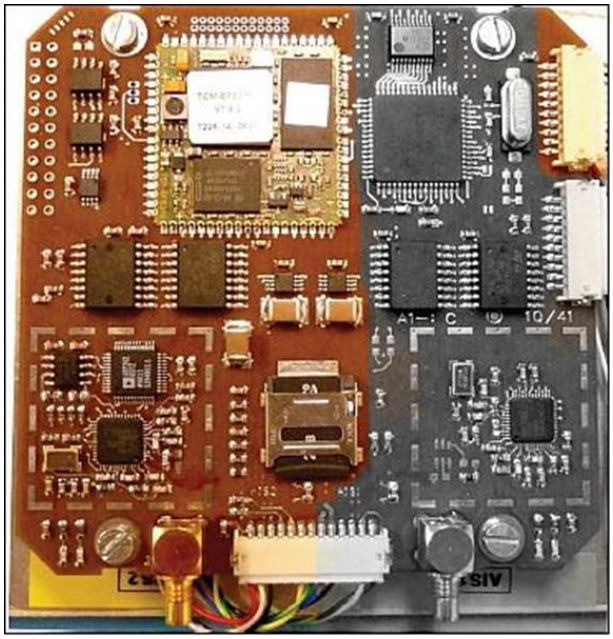
Το payload του δορυφόρου είναι δύο συστήματα AIS, διακριτά μεταξύ τους τόσο σε επίπεδο κατασκευής δέκτη, όσο και μεθόδου αποδιαμόρφωσης.

Το πρώτο (AIS1) που είναι και το κύριο, αποδιαμορφώνει τα σήματα με ένα εμπορικό radio frontend και με σειριακή έξοδο αποκωδικοποιεί τα μηνύματα AIS.
Το AIS1 είναι hardware δέκτης που βασίζεται στο Analog Devices ADF 7021 ραδιοπομποδέκτη. Συνδέεται με SPI (Serial Peripheral Interface) σε ένα Atmel AVR μικροελεγκτή που επεξεργάζεται και αποκωδικοποιεί τα δεδομένα. Τα ληφθέντα μηνύματα αποκωδικοποιούνται και τόσο με σωστό, όσο και με λανθασμένο FCS (Frame Check Sequence), αποθηκεύονται για περαιτέρω ανάλυση σε δεύτερο χρόνο.

Το AIS1 περιλαμβάνει
• LNA (Low Noise Amplifier)
- Around +15dB
- Includes SAW filter
• Radio chip
- Analog Devices ADF 7021
- Advantage: SPI compatible bitstream output.

Το δεύτερο (AIS 2), λειτουργεί με λογισμικό, με τυχαία έξοδο ενδιάμεσης συχνότητας και αποθηκεύει για περαιτέρω επεξεργασία σε δεύτερο χρόνο. Το πρόβλημα όμως είναι ότι μοιράζονται μια κοινή κεραία VHF και ένα χαμηλού θορύβου ενισχυτή LNA.

Το AIS2 έχει σχεδιαστεί ως SDR (Software Defined Radio) σύστημα με βάση το DSP module της Bluetechnix. Το module βρίσκεται σε ένα Blackfin 16 bit fixed point DSP (Digital Signal Processor) με RAM/Flash για βασικές λειτουργίες. Η λήψη AIS γίνεται με ένα radio frontend και ένα ADC (Analog to Digital Converter) ρυθμίζοντας την IF (Intermediate Frequency) και αποδιαμορφώνει σε λογισμικό στο DSP. Επιπλέον, έχει μια SD (Secure Digital) κάρτα μνήμης για επιπλέον χωρητικότητα σε μνήμη.



Εικόνα 4: Το ολοκληρωμένο SDR του AIS2 (image credit: AAU)[67]

Το AIS2 περιλαμβάνει

• LNA (Low Noise Amplifier)

- Around +15dB

- Includes SAW filter

• RF front-end

- Analog Devices ADF 7020

- Advantage: I/Q at 200 kHz IF

• ADC (Analog Digital Converter)

- Analog Devices AD 7262

- Capable of 1 Msample/s.

• AIS sensitivity better than -114 dBm.

Η κεραία λήψης για σήματα AIS είναι μονή διπολική με κατεύθυνση τη Γη

[67] https://directory.eoportal.org/web/eoportal/satellite-missions/a/aausat3

6.3 Τρωτότητες

Όπως αναφέρθηκε στην πρώτη ενότητα του παρόντος κεφαλαίου, η όλη σημασία της ανάλυσης αυτής, έγκειται ουσιαστικά στην μετάδοση της πληροφορίας, το οποίο μεταφράζεται κατά τον παρακάτω σχολιασμό, ως το κατά πόσο οι τρωτότητες στα payloads που πιθανά θα προκύψουν από τη διερεύνηση, αποτελούν σημαντικούς ή όχι παράγοντες για τη μετάδοση της πληροφορίας και όχι τόσο ως προς την ύπαρξη του cubesat. Άρα δε θα ελεγχθούν για τρωτότητες που μπορεί να υπάρχουν σε σχέση με physical kinetic και non-physical kinetic μέσα απειλής, αφού εφόσον αυτά εφαρμοστούν, όπως αναλύθηκε στο προηγούμενο κεφάλαιο, θα έχουν ήδη βλάψει όλο τον cubesat, συνεπαγόμενα δηλαδή και τα payloads.

Ο σχεδιασμός του Lambdasat (Λ-sat), όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο, περιλαμβάνει την επικοινωνία με constellation και με την πλατφόρμα του Iridium, με μία αντένα. Το γεγονός ότι δεν έχει προβλεφθεί δεύτερο σύστημα κεραίας, λήψης – μετάδοσης δηλαδή, που να αφορά μόνο το payload καθιστά τη βασική πληροφορία ως σε κρίσιμη κατάσταση. Επίσης, σε αυτό το δυναμικό ενδεχόμενο παίζει ρόλο και η αποστολή του σήματος από και προς το σταθμό εδάφους αλλά και από και προς το πλοίο . Εάν για παράδειγμα έχει γίνει μια επίθεση σε αυτά, με μέθοδο jamming ή spoofing ή ακόμη και με παρατεταμένο spoofing σε συνδυασμό με hijacking (που μπορεί να θεωρηθεί κυβερνοεπίθεση), τότε το σήμα είτε δε θα μεταδίδεται ή θα μεταδίδεται λανθασμένο. Αυτό μπορεί να οδηγήσει σε λανθασμένα συμπεράσματα κατά την ανάλυση της πληροφορίας. Με άλλα λόγια, το σύστημα θα είναι τρωτό, όχι ως σύστημα μικροδορυφόρος, αλλά ως σύστημα μετάδοσης πληροφορίας. Ως εκ τούτου, διαφαίνεται να βρίσκεται σε κατάσταση επικινδυνότητας και η πληροφορία που μεταφέρεται, το σήμα δηλαδή AIS, όχι μόνο από παράγοντες που μπορούν να πλήξουν αυτό καθ’ αυτό το σύστημα cubesat αλλά να το βλάψουν ως προς την αξιοπιστία του, την ποιότητα και τη βασιμότητα δηλαδή της πληροφορίας που μεταφέρει. Σε κάθε περίπτωση βλάβη επιτυγχάνεται.

Από την άλλη, το γεγονός ότι η μετάδοση πληροφορίας, στην περίπτωση του γραφενίου, θα γινόταν με ένα σύστημα που κατά κύριο λόγο εξυπηρετεί τους

ραδιοερασιτέχνες παγκοσμίως στο να προβαίνουν σε pings σε δορυφόρους που επιθυμούν, θεωρείται πιθανό ζήτημα διερεύνησης για θέματα ασφάλειας και κυβερνοασφάλειας. Ανεξάρτητα εάν είναι δηλωμένη η ταυτότητα των ραδιοερασιτεχνών προκαλείται μια γκρίζα περιοχή γύρω από το ποιος ή γιατί επιχειρεί επαφή με τον cubesat, ειδικά όταν το payload λειτουργεί και για θέματα ασφάλειας ναυσιπλοΐας (AIS).

Για την περίπτωση του AAUSat3, το γεγονός ότι το payload λειτουργεί δύο ίδια συστήματα, τα οποία εργάζονται ταυτόχρονα και λαμβάνουν σήματα με διαφορετικό τρόπο, δημιουργεί μια αίσθηση μείωσης κινδύνου. Εφόσον δεν είχαν κοινή κεραία λήψης φυσικά, καθώς οποιαδήποτε επίθεση ή κυβερνοεπίθεση θα πλήξει και τα δύο συστήματα, ακυρώνοντας έτσι τη δυνατότητα διάσωσης και διάδοσης της πραγματικής πληροφορίας. Κατά τα άλλα ισχύουν τα ίδια με τις τρωτότητες του Λ-sat, περί spoofing, jamming και hijacking.

Συνοψίζοντας, σχηματικά τα παραπάνω φαίνονται στον πίνακα 4 που ακολουθεί

Cubesat	Payload	Ύπαρξη τρωτότητας		Αιτία	Πιθανότητα πραγματοποίησης σεναρίου				Αποτελέσματα Συνέπειες			Ιεράρχηση			
		Ναι	Όχι		α	β	γ	δ	I	II	III	1	2	3	4
					Δυνατό (possible)	Πιθανό (probable)	Απίθανο (improbable)	Αδύνατο (impossible)	Μη μόνιμη βλάβη	Μόνιμη βλάβη	Ολική καταστροφή	Υψηλή επιπτωση	Λιγότερο σημαντικό	Χαμηλής σημαντικότητας	Καθόλου σημαντική
Λ-sat	**Graphene**			Μετάδοση πληροφορίας με σύστημα ραδιοερασιτεχνών (ping στον cubesat)			γ		I			**3**			
Λ-sat	**AIS**			Communication μέσω Iridium και constellation για τα αποτελέσματα με μία κεραία		β			I			**3**			
Λ-sat	**Ship**			Jamming στη μετάδοση πληροφορίας	α				I			**1**			
Λ-sat	**Ship**			Spoofing στη μετάδοση πληροφορίας (εφόσον έχει διάρκεια) Hijacking (Cyber)	α					II		**1**			
Λ-sat	**GROUND CONTROL**			Jamming στη μετάδοση πληροφορίας	α				I			**1**			
Λ-sat	**GROUND CONTROL**			Spoofing στη μετάδοση πληροφορίας	α					II		**1**			

			(εφόσον έχει διάρκεια) Hijacking (Cyber)			
AAUSat3	**AIS 1**		Κοινή κεραία λήψης και αποστολής πληροφορίας με AIS 2	α	II	**1**
AAUSat3	**AIS 2**		Κοινή κεραία λήψης και αποστολής πληροφορίας με AIS 1	α	II	**1**
AAUSat3	**Ship**		Jamming στη μετάδοση πληροφορίας	α	I	**1**
AAUSat3	**Ship**		Spoofing στη μετάδοση πληροφορίας (εφόσον έχει διάρκεια) Hijacking (Cyber)	α	II	**1**
AAUSat3	**GROUND CONTROL**		Jamming στη μετάδοση πληροφορίας	α	I	**1**
AAUSat3	**GROUND CONTROL**		Spoofing στη μετάδοση πληροφορίας (εφόσον έχει διάρκεια) Hijacking (Cyber)	α	II	**1**

Πίνακας 4. Τρωτότητες σε payload cubesats Lambdasat (Λ-sat) και AAUSat3

Το ερώτημα που μένει να απαντηθεί πλέον είναι ποια είναι πιο σημαντική, η ασφάλεια και κυβερνοασφάλεια της μετάδοσης της πληροφορίας ή η ασφάλεια και κυβερνοασφάλεια του μικροδορυφόρου.

Σε αυτό το ερώτημα, μια καλή τοποθέτηση μπορεί να θεωρηθεί ο συνδυασμός των δύο. Είναι τόσο συνιφασμένη η ασφάλεια και κυβερνοασφάλεια της μετάδοσης της πληροφορίας με αυτή της ασφάλειας και κυβερνοασφάλειας του μικροδορυφόρου που μπορεί να θεωρηθεί ένα. Ασφάλεια και κυβερνοασφάλεια στη μετάδοση της πληροφορίας δεν μπορεί να υπάρξει εάν δεν υφίσταται ασφαλής και κυβερνοασφαλής μικροδορυφόρος που θα τη λάβει και θα τη μεταβιβάσει. Αντίστοιχα, εάν δεν είναι καθόλα διασφαλισμένη η μετάδοση της πληροφορίας, δεν μπορεί να θεωρηθεί καθόλα ασφαλές το σύστημα του μικροδορυφόρου, αφού οποιαδήποτε τρωτότητα στην μετάδοση της πληροφορίας μπορεί να προκαλέσει βλάβη και σε αυτόν.

7. Συμπεράσματα – Προτάσεις

7.1 Συμπεράσματα

Η παρούσα έρευνα πραγματοποιήθηκε στο πλαίσιο ολοκλήρωσης του ΠΜΣ «Νέες Τεχνολογίες στη Ναυτιλία και τις Μεταφορές» του Τμήματος "Ναυτιλίας και Επιχειρηματικών Υπηρεσιών" του Πανεπιστημίου Αιγαίου και του Τμήματος "Μηχανικών Βιομηχανικής Σχεδίασης και Παραγωγής" (πρώην "Τμήμα Αυτοματισμού Τ.Ε.") του Πανεπιστημίου Δυτικής Αττικής (πρώην Ανώτατου Εκπαιδευτικού Ιδρύματος Πειραιά ΤΤ), καθώς αποτελεί την τελική εργασία.

Πιο συγκεκριμένα προτάθηκε ως συνδεόμενη με την τρίτη κατεύθυνση «Σχεδιασμός και Λειτουργία Αεροδιαστημικών Συστημάτων και εφαρμογές στη Ναυτιλία», και σκοπό είχε την ανάδειξη των θεμάτων ασφάλειας και κυβερνοασφάλειας στις αεροδιαστημικές εφαρμογές και δη αυτές που σχετίζονται με τη ναυτιλία.

Για την παρούσα εργασία επιλέχθηκαν τυχαία δύο μικροδορυφόροι μεγέθους cubesat, προκειμένου να καταγραφούν τα συστήματά τους και να ελεγχθεί εάν υφίστανται τρωτά σημεία σε αυτούς.

Σε πρώτο στάδιο πραγματοποιήθηκε μια εισαγωγή στις έννοιες πληροφορία, μικροδορυφόρος, ασφάλεια και κυβερνοασφάλεια και τρωτότητα και ακολούθησε καταγραφή των υποσυστημάτων των δύο μικροδορυφόρων προκειμένου να απαντηθούν ερωτήματα, όπως εάν υφίστανται τρωτότητες σε αυτά.

Από την εργασία αναδείχθηκε το πολλά υποσχόμενο μέλλον στη χρήση μικροδορυφόρων. Εφόσον όμως ληφθεί υπόψη η αναγκαιότητα δημιουργίας περιβάλλοντος ασφάλειας και κυβερνοασφάλειας, προκειμένου να αξιοποιηθούν πλήρως οι δυνατότητες που δίνονται.

Όπως προκύπτει από τη σύνοψη των αποτελεσμάτων στους πίνακες 3 και 4, η σημαντικότητα κατά την ιεράρχηση των τρωτοτήτων, δεν συσχετίζεται πάντα με την κρισιμότητα της βλάβης. Για παράδειγμα, παρόλο που θα προκύψει ολική

καταστροφή από επίθεση με EMP και ουσιαστικά δεν τίθεται θέμα τρωτότητας συγκεκριμένου υποσυστήματος, αλλά τίθεται υπό συζήτηση η θωράκιση της συνολικής ασφάλειας του cubesat, με την χαμηλή πιθανότητα μιας τέτοιας πράξης, η βαθμολογία της τρωτότητας κατατάσσεται χαμηλή.

Επίσης, όπως προκύπτει, οι τρωτότητες που προέρχονται από τους σταθμούς εδάφους, ή/και τα πλοία που δέχονται ή αποστέλλουν πληροφορία μέσω των μικροδορυφορικών συστημάτων, κρίνονται ως πιο σημαντικές από όλες τις υπόλοιπες. Αυτό, αποδεικνύει την αναγκαιότητα αυξημένης ασφάλειας και κυβερνοασφάλειας κατά τη λειτουργία των δομών αυτών, καθώς από την ευκολία προσβασιμότητάς τους και μόνο, καθίστανται πιο εύκολοι στόχοι για κάθε είδους απειλή.

Θα πρέπει να λαμβάνεται μέριμνα για τη διάσωση και τη διάδοση της πλήρους και αληθούς πληροφορίας. Οφείλεται λοιπόν να λαμβάνεται μέριμνα για τον τρόπο μετάδοσης αυτής, πιθανόν με ύπαρξη κεραίας ειδικά για το payload

Σε κάθε περίπτωση όμως αυτό δεν μπορεί να μειώσει τη σημαντικότητα που πρέπει να δοθεί στην ασφάλεια και κυβερνοασφάλεια των υποσυστημάτων των μικροδορυφορικών συστημάτων επί του συνόλου τους.

Επίσης, σε αντιπαραβολή με αντίστοιχη εργασία περί της σημαντικότητας των απειλών και των τρωτοτήτων, αλλά και των συνεπειών των επιθέσεων[68], προκύπτει ότι υφίστανται παρόμοια αποτελέσματα, γεγονός που καταδεικνύει το βάσιμο της έρευνας.

Σύμφωνα με όλα τα παραπάνω, συμπεραίνεται ότι ο χώρος του διαστήματος, παρόλο που είναι τεχνολογικά πιο εξελιγμένος από άλλους, δεν είχε ως κύριο μέλημα, μέχρι πρόσφατα, την ασφάλεια και την κυβερνοασφάλεια.

[68] Moranta S., Pavesi G., Perrichon L., Plattard S., Sarret M., 2018, Security in Outer Space: Rising Stakes for Europe, ESPI Report 64, European Space Policy Institute (ESPI)

Οι δυσκολίες στη μετάδοση της πληροφορίας, αποτελούσαν το μεγαλύτερο «στοίχημα» που έπρεπε να κερδηθεί και με τον τρόπο αυτό δεν εξελίχθηκε το θέμα της ασφάλειας και της κυβερνοασφάλειας. Αυτό το «στοίχημα» ουσιαστικά παραμένει κυρίαρχο, ωστόσο, οι εξελίξεις στην τεχνολογία, οι δυνατότητες χρήσης έτοιμων εφαρμογών και η ελαχιστοποίηση του μεγέθους των δορυφορικών συστημάτων, σε συνδυασμό κυρίως με την ελάττωση του κόστους παραγωγής, οδηγούν ολοένα και περισσότερο κόσμο να ασχοληθεί με τις αεροδιαστημικές εφαρμογές. Αυτό συνεπακόλουθα οδηγεί και στην ανάγκη προφύλαξης των συστημάτων αυτών, καθώς ο χώρος μοιάζει ευάλωτος σε απειλές και κακόβουλες πράξεις.

Η αναγκαιότητα λοιπόν αυξάνεται ολοένα και περισσότερο, ένταξης μέριμνας για ασφάλεια και κυβερνοασφάλεια στο στάδιο του σχεδιασμού ενός μικροδορυφόρου.

7.2 Προτάσεις

Θα πρέπει να λαμβάνεται υπόψη, ότι ένα οποιοδήποτε τέτοιο μικροδορυφορικό σύστημα, σχεδιάζεται και δημιουργείται σήμερα και πρόκειται να λειτουργήσει, στην καλύτερη των περιπτώσεων μετά από ένα με δύο έτη. Από μόνο του αυτό το στοιχείο καταδεικνύει ότι κανένα σύστημα δεν μπορεί να μην έχει τρωτότητες. Κυριότερη πρόταση κρίνεται λοιπόν, η συνέχιση των ερευνών σε επίπεδο ανάλυσης μικροδορυφορικών συστημάτων, με τη χρήση κατάλληλων μεθόδων. Η υιοθέτηση δηλαδή, μεθόδων εντοπισμού τρωτοτήτων, ακόμη και αντισυμβατικών, που όπως φαίνεται κερδίζουν έδαφος σε πολλούς άλλους τομείς,[69] π.χ. τρομοκρατία, αντιμετώπιση φυσικών καταστροφών κ.α., θα πρέπει να αναδειχθεί και στο χώρο του διαστήματος.

Η μετάδοση της πληροφορίας θα πρέπει ορθά να συνεχίσει να κυριαρχεί ως μέλημα στο σχεδιασμό των μικροδορυφορικών συστημάτων, όμως πλέον θα πρέπει να γίνεται σε συνδυασμό με τα αποτελέσματα των ερευνών που θα πραγματοποιούνται κατά το στάδιο της υλοποίησης τέτοιων projects, όπως δηλαδή αναφέρθηκε μόλις πιο πάνω, με χρήση κατάλληλων μεθόδων εντοπισμού τρωτοτήτων.

Επίσης και η εκπαίδευση σε θέματα ασφάλειας και κυβερνοασφάλειας θεωρείται εξίσου σημαντική. Η εκπαίδευση[70] θα επιφέρει τροποποίηση του τρόπου σκέψης και θα δημιουργηθεί το πλαίσιο προκειμένου να θεωρείται δεδομένη η εξασφάλιση του συστήματος μικροδορυφόρος από κακόβουλες πράξεις.

Επιπλέον, η ερευνητική κοινότητα μπορεί να οδηγήσει σε κατάλληλες εφαρμογές που θα ενισχύουν την ασφάλεια και κυβερνοασφάλεια. [71]

[69] Oughton E.J., Ralph D., Leverett E., Pant R., Thacker S., Hall J.W., Copic J., Ruffle S., Tuveson M., 2017, Stochastic Counterfactual Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks, Working Paper No. 03, Cambridge Judge Business School, University of Cambridge

[70] Sigholm J., Falco G., Viswanathan A.,2019, Enhancing Cybersecurity Education through High-Fidelity Live Exercises (HiFLiX), The Hawaii International Conference on System Sciences

[71] Falco G., 2018, The Vacuum of Space Cybersecurity, AIAA SPACE and Astronautics Forum and Exposition

Επίσης, τα κράτη μπορούν να θεσπίσουν μέσω του ITU το κανονιστικό πλαίσιο στο οποίο θα κινείται όποιος ενδιαφέρεται να στείλει ένα μικροδορυφόρο σε τροχιά, καθώς η ενημέρωση της συχνότητας εκπομπής δεν φαίνεται να είναι αρκετή για να αποσοβήσει την οποιαδήποτε απειλή.[72]

Οι χώρες, μπορούν να θέσουν όρους στη δυνατότητα εκτόξευσης δορυφορικών συστημάτων στο διάστημα.

Επιπρόσθετα, η συνεργασία των εταιρειών του κλάδου, οι οποίες παρέχουν τα μέρη που δημιουργούν ένα μικροδορυφόρο, οφείλουν να επενδύσουν στη ασφάλεια και την κυβερνοασφάλεια. [73]

Οι εταιρείες που ασχολούνται στο χώρο της ασφάλειας σε συνεργασία με τους διεθνείς οργανισμούς και τα κράτη, μπορούν να δημιουργήσουν το πλαίσιο εκείνο ώστε να ελαττωθούν οι πιθανότητες, συστήματα που κατασκευάζονται για την άμυνα και την ασφάλεια, να καταλήγουν να γίνονται μέσα για επιθέσεις και κυβερνοεπιθέσεις στο διάστημα.

Συναφώς οι νέες τεχνολογίες στη μετάδοση πληροφοριών[74] και η δημιουργία νέων δικτύων μεταφοράς δεδομένων, εφόσον ληφθεί υπόψη η ανάγκη προστασίας από κυβερνο-επιθέσεις, μπορούν να βοηθήσουν το χώρο του διαστήματος, ώστε οι χρήστες να είναι σίγουροι για την ασφάλειά τους.

Όλα αυτά κρίνονται ως βασικά στοιχεία για να υπάρξει ενδυνάμωση των δορυφορικών συστημάτων. Πραγματική ενδυνάμωση.

[72] Falco G., 2018, Cybersecurity Principles for Space Systems, Journal of Aerospace Information Systems, American Institute of Aeronautics and Astronautics,Inc.
[73] Falco G., 2018, Job One for Space Force: Space Asset Cybersecurity, Cyber Security Project, Belfer Center for Science and International Affairs, Harvard Kennedy School
[74] Neumann S.P., Joshi S.K., Fink M., Scheidl T., Blach R., Scharlemann C., Abouagaga S., Bambery D., Kerstel E., Barthelemy M., Ursin R., 2018, Q3Sat: quantum communications uplink to a 3U CubeSat—feasibility & design, EPJ Quantum Technology, Springer Open Journal

8. Βιβλιογραφία

Ελληνική

- Αισχύλου, Αγαμέμνων, Στίχοι 263-304, Αποσπάσματα, Μετάφραση Ρούσσου Τ., Κάκτος, 1992
- Ζορκάδης Β. (2002), Θεωρία Πληροφορίας και Κωδικοποίησης, Πάτρα, ΕΑΠ, https://eclass.uop.gr/modules/document/file.php/TST244/Θεωρία Πληροφορίας και Κωδικοποίησης.pdf
- Ινστιτούτο Νεοελληνικών Σπουδών (Ίδρυμα Μανόλη Τριανταφυλλίδη) (1998), Λεξικό της κοινής νεοελληνικής, http://www.greek-language.gr/greekLang/modern_greek/tools/lexica/triantafyllides/search.html?lq=πληροφορία&dq=
- Υπουργείο Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, (2018), Εθνική Στρατηγική Κυβερνοασφάλειας, 3η Αναθεώρηση

Ξενόγλωσση

- Addaim A., Kherras A., Zantou El B., (2010) Design of Low-cost Telecommunications CubeSat-class Spacecraft, In Thawar T. Arif (Ed.)Aerospace Technologies Advancements, InTech
- Agasid E. κ.συν. (2015), Small Spacecraft Technology State of the Art, Mission Design Division Ames Research Center, Moffett Field, NASA, California
- Amandine Denis κ.συν. (2015), QB50 System Requirements and Recommendations, Issue 7, VKI
- Andrieu J., El haouzian C.N., 2010, Design and Development of a QOS Policy for AAUSAT3 Communication Protocol, AAUSAT3 Project, Department of Electronics, Networks & Distributed Systems, Aalborg University
- Bichler S.F., Maj, USAF, 2015, Mitigating Cyber Security Risk in Satellite Ground Systems, Air Command and Staff College, Air University, Muir S. Fairchild Research Information Center, Digital colletcion

- Bonyan H. (2010), Looking into Future - Systems Engineering of Microsatellites, In Thawar T. Arif (Ed.) Aerospace Technologies Advancements, InTech
- Cambridge University Press (2019), Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/information#dataset-cald4
- Chatfield A.T., Reddick C.G., 2018, Crowdsourced cybersecurity innovation: The case of the Pentagon's vulnerability reward program, Information Polity: The International Journal of Government & Democracy in the Information Age, Vol. 23, Issue 2, p177-194, IOS Press
- Chin J. κ.συν., (2017), CubeSat 101: Basic Concepts and Processes for First-Time CubeSat Developers, Revision, NASA CubeSat Launch Initiative
- Elbert B.R. (2008), Introduction to Satellite Communication, Third Edition, ARTECH HOUSE INC
- Ercan C., Kale İ., 2017, The role of space in the security and defence policy of Turkey. A change in outlook: Security in space versus security from space, Space Policy, 42, 17–25, Elsevier Ltd.
- Falco G., 2018, Cybersecurity Principles for Space Systems, Journal of Aerospace Information Systems, American Institute of Aeronautics and Astronautics,Inc.
- Falco G., 2018, Job One for Space Force: Space Asset Cybersecurity, Cyber Security Project, Belfer Center for Science and International Affairs, Harvard Kennedy School
- Falco G., 2018, The Vacuum of Space Cybersecurity, AIAA SPACE and Astronautics Forum and Exposition
- FAS's Panel on Weapons in Space, 2004, Ensuring America's Space Security Report of the FAS Panel on Weapons in Space, Federation of American Scientists
- Global SatShow - Satellite Conference & Exhibition
- Greene J., Stellman A., 2014, Head First PMP, Third Edition, O'Reilly Media, Inc.
- Greiman V. A., 2013, Megaproject Management Lessons on Risk and Project Management from the Big Dig, John Wiley & Sons, Inc., Project Management Institute, Inc.
- GUO Li-wen1, ZHANG Zhan-yue, ZHANG Zhe1, 2016, Vulnerability Analysis of Satellites in Strong Electromagnetic Environment, 4th National Conference on Electrical, Electronics and Computer Engineering (NCEECE 2015), Atlantis Press

- Harrison T., Johnson K., Roberts T.G., 2018, Space Threat Assessment 2018, Center for Strategic and International Studies
- HM Government, (2014), National Space Security Policy
- http://globalsatshow.com/port/Telecommunications/cyber-attacks-a-major-challenge-faced-by-the-telecommunications-satellites
- http://lambdasat.com/
- http://www.space.aau.dk/aausat3/index.php
- https://airtable.com/shrafcwXODMMKeRgU/tbldJoOBP5wlNOJQY
- https://directory.eoportal.org/web/eoportal/home
- https://directory.eoportal.org/web/eoportal/satellite-missions/a/aausat3
- https://directory.eoportal.org/web/eoportal/satellite-missions/L/LAMBDASAT
- https://directory.eoportal.org/web/eoportal/satellite-missions/L/LAMBDASAT#sensors
- https://www.cisco.com/c/en/us/products/security/what-is-pen-testing.html
- https://www.incapsula.com/web-application-security/penetration-testing.html
- https://www.nanosats.eu/#database
- https://www.secureauth.com/products/penetration-testing
- Ippolito L.J. Jr. (2017), Satellite Communications Systems Engineering; Atmospheric Effects, Satellite Link Design and System Performance, Second Edition, JohnWiley & Sons Ltd
- Livingstone D., Lewis P., (2016), "Space, the Final Frontier for Cybersecurity?", London, The Royal Institute of International Affairs Chatham House
- Logan T., (2018), The US must secure its supply chain in the face of anti-satellite weapons, C4ISRNET, https://www.c4isrnet.com/opinion/2018/05/16/the-us-must-secure-its-supply-chain-in-the-face-of-anti-satellite-weapons/
- Madden A.D., October 2000, A definition of information, Aslib Proceedings, Vol 52, No.9, (343-349)
- Madry S., Martinez P., Laufer R. (2018), Innovative Design, Manufacturing and Testing of Small Satellites, Springer Praxis Books, Springer International Publishing AG, part of Springer Nature

- Mantzouris G., Papadopoulos P., Nikitakos N., Manso M., Bordetsky A., Sarris Z., Markarian G., Kourousis K., 2015, Picosatellites for Maritime Security Applications – the Lambdasat Case, Journal of Aerospace Technology and Management, Vol.7, No 4, pp.490-503
- Maral G. & Bousquet M. (2009), Satellite Communications Systems; Systems, Techniques and Technology, Fifth Edition, John Wiley & Sons Ltd
- Moranta S., Pavesi G., Perrichon L., Plattard S., Sarret M., 2018, Security in Outer Space: Rising Stakes for Europe, ESPI Report 64, European Space Policy Institute (ESPI)
- Neumann S.P., Joshi S.K., Fink M., Scheidl T., Blach R., Scharlemann C., Abouagaga S., Bambery D., Kerstel E., Barthelemy M., Ursin R., 2018, Q3Sat: quantum communications uplink to a 3U CubeSat—feasibility & design, EPJ Quantum Technology, Springer Open Journal
- Oughton E.J., Ralph D., Leverett E., Pant R., Thacker S., Hall J.W., Copic J., Ruffle S., Tuveson M., 2017, Stochastic Counterfactual Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks, Working Paper No. 03, Cambridge Judge Business School, University of Cambridge
- Oxford University Press, (2019), Oxford Dictionaries, https://en.oxforddictionaries.com/definition/information; https://public.oed.com/blog/word-stories-information/#
- Pindják P., 2016, A Stronger EU in Cosmos: Embracing the Concept of Space Security, INCAS Bulletin, Volume 8, Issue 3, pp. 91 – 97
- Rooker J. W., 2008, Satellite Vulnerabilities, EWS Contemporary Issue Paper, United States Marine Corps,Command and Staff College, Marine Corps Combat Development,Marine Corps University
- Santamarta R., 2018, \WHITE PAPER\Last Call for SATCOM Security, IOActive, Inc.
- Shaikh S.A. (2017), Future of the Sea: Cyber Security, UK Government Office for Science, Crown

- Sibeauda J-M, Puilletb C., 2015, Effects of Debris Cloud Interaction with Satellites Critical Equipments - Experiments and Modeling -, The 13th Hypervelocity Impact Symposium, Procedia Engineering, 103, 561 – 568, Elsevier Ltd
- Sigholm J., Falco G., Viswanathan A., 2019, Enhancing Cybersecurity Education through High-Fidelity Live Exercises (HiFLiX), The Hawaii International Conference on System Sciences
- Thompson M.A., Ryan M.J., Slay J. and McLucas A.C., 2016, Harmonized taxonomies for security and resilience, Information Security Journal: A Global Perspective, Vol. 25, Nos. 1–3, 54–67, Taylor & Francis
- Wilgenbusch R. C., Heisig A., 2013, Command and Control Vulnerabilities to Communications Jamming , JFQ, issue 69, 2nd quarter, ndupress.ndu.edu
- Woo G., Maynard T., Seria J., 2017, Reimagining history: Counterfactual risk analysis, Emerging Risk Report 2017, Understanding risk, Emerging Risk Report 2017, Lloyd's-RMS

Περαιτέρω μελέτη

- Baronienė L., Žirgutis V., 2017, Cybersecurity Facets: Counterfactual Impact Evaluation of Measure "Procesas LT" in enterprises of the IT sector, Journal of Security and Sustainability Issues, Volume 6 Number 3
- Baylon C., Lewis P., Asbeck F., Baseley-Walker B., Catalano C., Demidov O., Johnson-Freese J., Jolly C., Joubert V., Livingstone D., Pasco X., Rajagopalan P.R., Suzuki K., Wang G., 2014, Challenges at the Intersection of Cyber Security and Space Security Country and International Institution Perspectives, Research Paper, Chatham House, The Royal Institute of International Affairs
- Brumbaugh Gamble K., Lightsey E.G., 2015, Decision Analysis Applied to Small Satellite Risk Management, American Institute of Aeronautics and Astronautics, Journal of Spacecraft and Rockets
- Cisco, 2016, Midyear Cybersecurity Report
- Cisco, 2018, Annual Cybersecurity Report
- Constantinou A.C., Yet B., Fenton N., Neil M., Marsh W., 2015, Artificial Intelligence in Medicine, Pre-Publication Draft, Artificial Intelligence in Medicine

- Das K.S., Kant K., Zhang N., 2012, Handbook on Securing Cyber-Physical Critical Infrastructure, Elsevier-Morgan Kaufmann
- Donaldson E.S., Siegel G.S., Williams K.C., Aslam A., 2015, Enterprise Cybersecurity-How to Build a Successful Cyberdefense Program Against Advanced Threats, Apress
- Hakim S., Albert G., Shiftan Y., 2016, Securing Transportation Systems, John Wiley & Sons
- Holt J.T., Schell H.B., 2013, Hackers and Hacking A Reference Handbook, ABC-CLIO, LLC
- Jabbour K., Poisson J., 2016, Cyber Risk Assessment in Distributed Information Systems, The Cyber Defense Review, Vol. 1, No. 1, pp. 91-112, Army Cyber Institute
- Johnson C., 2016, Why We Cannot (Yet) Ensure the Cyber-Security of Safety-Critical Systems, Safety-Critical Systems Club
- Loukas G., 2015, Cyber-Physical Attacks - A Growing Invisible Threat, Elsevier-Book Aid
- Mehdi B., Azizol A., Ramlan M., Norwati M., Nur I.U., 2013, Features Selection for IDS in Encrypted Traffic using Genetic Algorithm, Proceedings of the 4th International Conference on Computing and Informatics, ICOCI 2013, Universiti Utara Malaysia (http://www.uum.edu.my), Paper No.038
- Nayak M., 2017, Deterring Aggressive Space Actions with Cube Satellite Proximity Operations, Air & Space Power Journal. Vol. 31 Issue 4, p92-102. 11p.
- Peterson C., Miller S.M., Duettmann A., 2017, Cyber, Nano, and AGI Risks: Decentralized Approaches to Reducing Risks, Foresight Institute
- Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, 2006, European Network and information Security Agency (ENISA)
- Singer P.W., Friedman A., 2014, Cybersecurity and Cyberwar-What Everyone Needs To Know, Oxford University Press
- Thomas R.C., Antkiewicz M., Florer P., Widup S., Woodyard M., 2013, How Bad Is It? A Branching Activity Modelto Estimate the Impact of Information Security

Breaches, Paper accepted by 12th Workshop on the Economics of Information Security; version 2.0

- Vacca J., 2014, Cyber Security And IT Infrastructure Protection, Elsevier-Syngress
- Value of Information Analysis for Interventional and Counterfactual Bayesian Networks in Forensic Medical Sciences
- Voeller J., (Edt), 2014, Cyber Security, John Wiley &Sons
- Woo G., "Counterfactual Disaster Risk Analysis," Variance 10:2, 2018, pp. 279-291
- Woo G., 2017, Reimagining the WannaCry Cyberattack, The RMS Blog https://www.rms.com/blog/2017/11/21/reimagining-the-wannacry-cyberattack/

9. Παραρτήματα

Παράρτημα 1: [PAPER]