ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Cybersecurity space system with AI technology

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Μοχάμεντ Αμπντελκαρίμ

Επιβλέπουσα : Βασιλική Διαμαντοπούλου

Μέλη εξεταστικής επιτροπής: Μαλιάτσος Κωνσταντίνος, Κοκολάκης Σπυρίδων

Σάμος, 2024

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Θα ήθελα εκφράσω τις ευχαριστίες μου στην καθηγήτρια μου, κα. Διαμαντοπούλου Βασιλικής, για τη βοήθεια και τις χρήσιμες ιδέες της, που συνέβαλαν στην βελτίωση της εργασίας.

Ευχαριστώ επίσης τους καθηγητές της σχολής που συνέβαλαν στην απόκτηση των απαραίτητων γνώσεων για την επιτυχή φοίτησή μου και την εκπόνηση της πτυχιακής εργασίας, αλλά κυρίως που ενίσχυσαν την αγάπη μου για τον κλάδο της Πληροφορικής, που υπήρχε από τα παιδικά μου χρόνια.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου και τους φίλους μου που μου συμπαραστάθηκαν και με βοήθησαν σε αυτήν την ακαδημαϊκή μου πορεία. Τους ευχαριστώ που στάθηκαν δίπλα μου όλα αυτά τα χρόνια και για την υπομονή και εμπιστοσύνη που υπέδειξαν.

© 2024
του
Μοχάμεντ Αμπντελκαρίμ
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή

Λίστα Σχημάτων

Λίστα Πινάκων

Ακρωνύμια

AI	Artificial Intelligence
ARPANET	Advanced Research Projects Agency Network
IoT	Internet of Things
Tor	The onion router
IP	Internet Protocol
ΤΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών
CSF	Cybersecurity Framework
CIA	Confidentiality, Integrity and Availability
DDoS	Distributed Denial of Service
SQL	Structured Query Language
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NLP	Natural Language Processing
NLG	Natural Language Generator
NLU	Natural Language Understanding
ML	Machine Learning
EO	Earth Observation
TCP	Transmission Control Protocol
GPS	Global Positioning System
SDLP	Space Data Link Protocols
WAN	Wide Area Network
SSL	Secure Sockets Layer
ADS-B	Automatic Dependent Surveillance-Broadcast
UAV	Unmanned Aerial Vehicles
NASA	National Aeronautics and Space Administration
JPL	Jet Propulsion Laboratory
EMP	Electromagnetic Pulse
ASAT	Anti Satellite Attacks
ITU	International Telecommunications Union
COTS	Commercial of the shelf
PCB	Printed Circuit Board
IT	Information Technology
CDER	Cyber Defense Engineering and Research

AT&T	*American Telephone and Telegraph*
DSN	Deep Space Network
DTN	Digital Twin Network
API	Application Programming Interface
SCADA	Supervisory Control and Data Acquisition
ERP	Enterprise Resource Planning
AES	Advanced Encryption Standard
NIST	National Institute of Standards and Technology
DES	Data Encryption Standard
TLS	Transport Layer Security
WPA	Wi-Fi Protected Access
PKI	Public Key Infrastructure
Cas	Certification Authorities
Ras	Registration Authorities
HTTPS	HyperText Transfer Protocol Secure
ACL	Access Control Lists
IDPS	Intrusion Detection and Prevention Systems
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
DSS	Data Security Standard
MFA	Multi Factor Authentication
VPN	Virtual Private Networks
SMTP	Simple Mail Transfer Protocol
IMAP	Internet Message Access Protocol
POP	Point of Presence
VRRP	Virtual Router Redundancy Protocol
SIEM	Security Information and Event Management
OWASP	Open Web Application Security Project
CSRF	Cross-Site Request Forgery
ZAP	Zed Attack Proxy
ISAC	Information Sharing and Analysis Center
CII	Critical Information Infrastructure
PIPL	Personal Information Protection Law

CIIPP	Critical Information Infrastructure Protection Program
FSTEC	Federal Service for Technical and Export Control
NIS	Network and Information Systems
NCSC	National Cyber Security Centre
SPD	Space Policy Directive
CISA	Cybersecurity and Infrastructure Security Agency Act
NIA	National Intelligence Agency
NSA	National Security Agency
USSPACECOM	United States Space Command
COPUOS	Committee on the Peaceful Uses of Outer Space
MAC	Media Access Control
ICAO	International Civil Aviation Organization
ESA	European Space Agency
JAXA	Japan Aerospace Exploration Agency
CSA	Canadian Space Agency
ISS	International Space Station
CNSA	China National Space Administration
NEPA	National Environmental Policy Act.
FAA	Federal Aviation Administration
NOAA	National Oceanic and Atmospheric Administration
FCC	Federal Communications Commission

Περίληψη

Η έρευνα αυτή αναδεικνύει τη σημασία της κυβερνοασφάλειας στα διαστημικά συστήματα με τη χρήση της τεχνητής νοημοσύνης. Πρώτα απ΄όλα εξετάζονται οι προκλήσεις και οι κίνδυνοι που αντιμετωπίζουν τα διαστημικά συστήματα από κυβερνοεπιθέσεις και παρουσιάζονται προτεινόμενες τεχνολογικές λύσεις για την ανίχνευση και την αντιμετώπισή τους. Επιπλέον αναλύονται οι ανάγκες για διεθνή συνεργασία και ανάπτυξη ενοποιημένων προτύπων και κανονισμών, καθώς και η σημασία της συνεχούς εκπαίδευσης των επαγγελματιών του κλάδου. Η μελλοντική έρευνα θα πρέπει να επικεντρωθεί στην ανάπτυξη προηγμένων αλγορίθμων ανίχνευσης εισβολών, συστημάτων πρόβλεψης απειλών και τεχνολογιών για την προστασία των δορυφόρων. Επίσης, υπογραμμίζεται η ανάγκη για ενίσχυση της διεθνούς συνεργασίας και η δημιουργία κοινών πρωτοκόλλων ασφαλείας, ώστε να διασφαλιστεί η παγκόσμια ασφάλεια και η ανθεκτικότητα των διαστημικών συστημάτων.

Λέξεις Κλειδιά: *Κυβερνοασφάλεια , Τεχνητή Νοημοσύνη , Πολιτική Ασφαλείας , Κυβερνοχώρος , Διαστημικά Συστήματα*

Abstract

This research highlights the importance of cybersecurity in space systems using artificial intelligence. First, it examines the challenges and risks faced by space systems from cyber-attacks and presents proposed technological solutions for their detection and mitigation Furthermore, the need for international cooperation and the development of unified standards and regulations, as well as the importance of continuous education and training of professionals in the field are analyzed. Future research should focus on developing advanced intrusion detection algorithms, threat prediction systems, and technologies for satellite protection. Additionally, the study emphasizes the need to enhance international collaboration and create common security protocols to ensure global security and resilience of space systems.

Keywords: *Artificial Intelligence, Cybersecurity, Security Policy, Cyberspace, Space Systems*

1

Εισαγωγή

Η σύγχρονη εποχή χαρακτηρίζεται από έναν έντονο ρυθμό εξέλιξης στους τομείς της τεχνολογίας και της διαστημικής εξερεύνησης. Η τεχνητή νοημοσύνη, ειδικότερα, έχει εδραιωθεί στο προσκήνιο της τεχνολογικής προόδου, ανοίγοντας νέους ορίζοντες για την ανθρώπινη φαντασία και παράλληλα διευρύνοντας το πεδίο των εφικτών επιστημονικών και τεχνολογικών επιτευγμάτων. Η συνδυαστική χρήση της τεχνητής νοημοσύνης με διαστημικά συστήματα έχει ανοίξει ένα νέο κεφάλαιο στην ανθρώπινη εξερεύνηση, το οποίο παρουσιάζει τόσο προκλήσεις όσο και ευκαιρίες. Η ολοένα αυξανόμενη εξάρτησή των ανθρώπων από δορυφορικά και διαστημικά συστήματα έχει κάνει πιο επιτακτική την ανάγκη για τη λήψη αυστηρών μέτρων ασφαλείας. Τα δορυφορικά συστήματα που είναι ουσιαστικά τα μάτια και τα αυτιά μας στο διάστημα, πρέπει να λειτουργούν χωρίς παρεμβάσεις ή απειλές από κυβερνοεπιθέσεις, οι οποίες θα μπορούσαν να επηρεάσουν κρίσιμες λειτουργίες όπως την παγκόσμια πλοήγηση, την επικοινωνία και την παρακολούθηση του περιβάλλοντος. Αυτή η νέα διάσταση της διαστημικής εξερεύνησης φέρνει μαζί της καινούργιες προκλήσεις στο πεδίο της κυβερνοασφάλειας. Οι πτυχές της τεχνητής νοημοσύνης, παρά τις θετικές τους επιπτώσεις, ενσωματώνουν και σημαντικούς κινδύνους όταν χρησιμοποιούνται σε περιβάλλοντα όπου η ασφάλεια είναι διακυβευμένη. Η αύξηση της ευφυΐας των συστημάτων δημιουργεί επιπλέον ευπάθειες και απαιτεί εξειδικευμένα μέτρα προστασίας που θα ανταποκρίνονται σε πιο εξελιγμένες και εξειδικευμένες απειλές. Στο πλαίσιο αυτό, η ανάλυση της κυβερνοασφάλειας καθίσταται ζήτημα ζωτικής σημασίας. Απαιτείται μια συνολική και συστηματική προσέγγιση που θα περιλαμβάνει τόσο την κατανόηση των δυνητικών απειλών όσο και την ανάπτυξη αντιμετρήσεων που θα εγγυώνται την ασφάλεια και την ακεραιότητα των διαστημικών λειτουργιών. Μόνο με μια ολοκληρωμένη και προετοιμασμένη στρατηγική θα είναι σε θέση ο σύγχρονος άνθρωπος να προστατεύσει τα διαστημικά συστήματά μας από τις πολύπλοκες απειλές της νέας εποχής και να συνεχίσει την ανάπτυξη των τεχνολογικών μας δυνατοτήτων με ασφάλεια και εμπιστοσύνη. Η παρούσα εργασία επιδιώκει να παρουσιάσει μια εκτενή και κατατοπιστική ανάλυση των

κινδύνων και των προκλήσεων που ανακύπτουν στο συγκεκριμένο τομέα, όπως επίσης και των τρόπων μέσω των οποίων οι σύγχρονες τεχνολογίες AI θα μπορούσαν να συμβάλλουν στην ασφάλεια και τη βελτίωση των διαστημικών λειτουργιών.

1.1 Σκοπός – Αντικείμενο Διπλωματικής

Ο σκοπός της παρούσας διπλωματικής είναι να αναλύσει την σχέση μεταξύ της κυβερνοασφάλειας και των διαστημικών συστημάτων που χρησιμοποιούν τεχνολογία AI. Συγκεκριμένα εστιάζει στην ανάδειξη των κινδύνων και προκλήσεων που αντιμετωπίζουν αυτά τα διαστημικά συστήματα, καθώς και στην εξέταση των τεχνικών προσεγγίσεων για την αντιμετώπιση και πρόληψη αυτών των κινδύνων. Επιπλέον μέσα από την ανάλυση αυτής της σχέσης, η διπλωματική αποσκοπεί στο να παράσχει κατευθυντήριες αρχές και προτάσεις για την ανάπτυξη ασφαλών και αξιόπιστων διαστημικών συστημάτων που χρησιμοποιούν τεχνολογία AI. Ο στόχος είναι να δοθεί έμφαση στην ενίσχυση της ασφάλειας αυτών των συστημάτων μέσω της εφαρμογής κατάλληλων μέτρων προστασίας και της ανάπτυξης προληπτικών στρατηγικών. Έτσι, η διπλωματική αυτή αναλύει τη συνολική δομή της ασφάλειας στον τομέα των διαστημικών συστημάτων που εφαρμόζουν τεχνολογία AI και παρέχει οδηγίες για τη βελτίωση της ασφάλειας και την αντιμετώπιση των προκλήσεων που αντιμετωπίζουν αυτά τα συστήματα.

1.2 Δομή Διπλωματικής

Το περιεχόμενο της διπλωματικής διαρθρώνεται ως εξής:

Στο 1ο κεφάλαιο γίνεται εισαγωγή στο θέμα της διπλωματικής εργασίας , περιγράφεται το αντικείμενό της και γίνεται και ανάλυση της δομής της. Στο 2ο κεφάλαιο παρέχεται μια επισκόπηση των βασικών εννοιών που σχετίζονται με την κυβερνοασφάλεια, τα διαστημικά συστήματα και την τεχνητή νοημοσύνη. Στο 3ο κεφάλαιο γίνεται ανάλυση των κινδύνων και των ευπαθειών που σχετίζονται με τις κυβερνοεπιθέσεις εναντίον διαστημικών συστημάτων που χρησιμοποιούν τεχνητή νοημοσύνη. Στο 4ο κεφάλαιο αναφέρονται οι λόγοι που τα διαστημικά συστήματα είναι ευάλωτα σε κυβερνοεπιθέσεις, καθώς και περιστατικά προηγούμενων επιθέσεων και τρέχουσες ευπάθειες. Στο 5ο κεφάλαιο εξετάζονται τα τεχνικά μέτρα για την αντιμετώπιση κυβερνοεπιθέσεων κατά των διαστημικών συστημάτων, συμπεριλαμβανομένης της αρχιτεκτονικής ασφαλείας, της κρυπτογράφησης, και των συστημάτων ανίχνευσης και πρόληψης εισβολών και αρκετά άλλα. Στο 6ο κεφάλαιο γίνεται ανάλυση και μελέτη των υφιστάμενων ελλείψεων σε προτύπων καθώς και των νομοθετικών μηχανισμών για την κυβερνοασφάλεια στον τομέα του διαστήματος. Στο 7ο κεφάλαιο παρουσιάζονται τα συμπεράσματα της έρευνας και γίνεται αναδρομική επισκόπηση των βασικών ευρημάτων και προτεινόμενων μελλοντικών ερευνητικών κατευθύνσεων Τέλος στο 8ο που είναι και το τελευταίο κεφάλαιο παρατίθενται οι πηγές και η βιβλιογραφία που χρησιμοποιήθηκαν κατά την εκπόνηση της διπλωματικής εργασίας.

1.3 Μεθοδολογία

Η παρούσα διπλωματική εργασία ακολουθεί τη μεθοδολογία της βιβλιογραφικής έρευνας για την ανάλυση και τη διερεύνηση των βασικών θεμάτων που αφορούν την κυβερνοασφάλεια στα διαστημικά συστήματα με χρήση τεχνητής νοημοσύνης. Η διαδικασία της έρευνας ξεκίνησε με τη συγκέντρωση πληροφοριών από αξιόπιστες πηγές, όπως έγκριτα επιστημονικά περιοδικά, συνέδρια και αναφορές από οργανισμούς που ασχολούνται με την ασφάλεια στον κυβερνοχώρο και τις διαστημικές τεχνολογίες. Στη συνέχεια, τα ευρήματα από τις πηγές κατηγοριοποιήθηκαν ανάλογα με τις θεματικές ενότητες της εργασίας, οι οποίες περιλαμβάνουν την ανάλυση των κυβερνοαπειλών και ευπαθειών σε διαστημικά συστήματα, την εφαρμογή της τεχνητής νοημοσύνης για την ανίχνευση και πρόληψη των επιθέσεων, καθώς και τις διεθνείς πολιτικές και κανονισμούς για την κυβερνοασφάλεια στο διάστημα. Επιπλέον, χρησιμοποιήθηκαν διάφορες τεχνικές ανάλυσης των δεδομένων για να προσδιοριστούν οι υπάρχουσες τάσεις και τα κενά στην έρευνα σχετικά με την προστασία των διαστημικών συστημάτων. Η μελέτη επικεντρώθηκε στην αναγνώριση προτεινόμενων λύσεων και τεχνολογικών καινοτομιών για την ενίσχυση της κυβερνοασφάλειας στον τομέα αυτό. Τέλος, έγινε μια κριτική ανάλυση των προκλήσεων που αντιμετωπίζουν τα διαστημικά συστήματα σε συνδυασμό με τη χρήση της τεχνητής νοημοσύνης, καθώς και των μελλοντικών προοπτικών στον τομέα της έρευνας και της ανάπτυξης. Η μεθοδολογία αυτή προσφέρει μια ολοκληρωμένη εικόνα της βιβλιογραφίας, προσδιορίζοντας τα κύρια σημεία όπου οι σύγχρονες τεχνολογίες, όπως η τεχνητή νοημοσύνη, μπορούν να εφαρμοστούν για την ενίσχυση της ασφάλειας των διαστημικών συστημάτων.

1.4 Ερευνητικά Ερωτήματα

1. Ποιοι είναι οι βασικοί κίνδυνοι κυβερνοασφάλειας και προκλήσεις που αντιμετωπίζουν τα διαστημικά συστήματα τα οποία χρησιμοποιούν τεχνητή νοημοσύνη;

2. Ποιες είναι οι ευπάθειες που εντοπίζονται στα διαστημικά συστήματα ως προς την κυβερνοασφάλεια και πώς μπορούν να γίνουν αντικείμενο εκμετάλλευσης αυτές οι ευπάθειες από κυβερνοεπιθέσεις;

3. Ποιες είναι οι τεχνικές προσεγγίσεις και οι λύσεις που μπορούν να αξιοποιηθούν για την αντιμετώπιση και πρόληψη των κυβερνοεπιθέσεων κατά των διαστημικών συστημάτων;

4. Ποιες είναι οι ελλείψεις στα υφιστάμενα πρότυπα και νομοθετικά πλαίσια που αφορούν την κυβερνοασφάλεια στον τομέα του διαστήματος;

5. Ποιες είναι οι προτεινόμενες βελτιώσεις ή αλλαγές στα πρότυπα και τις νομοθεσίες για την κυβερνοασφάλεια στον τομέα του διαστήματος;

6. Πώς η ενσωμάτωση τεχνητής νοημοσύνης μπορεί να βελτιώσει τις δυνατότητες ανίχνευσης και πρόληψης των κυβερνοεπιθέσεων σε διαστημικά συστήματα;

7. Ποιες είναι οι προκλήσεις που προκύπτουν από τη χρήση τεχνητής νοημοσύνης στα διαστημικά συστήματα όσον αφορά την κυβερνοασφάλεια;

8. Ποιες είναι οι προτεινόμενες τεχνολογικές καινοτομίες για την προστασία των δορυφόρων και άλλων διαστημικών συστημάτων από κυβερνοεπιθέσεις;

9. Ποιος είναι ο ρόλος της διεθνούς συνεργασίας και της ανάπτυξης κοινών πρωτοκόλλων ασφαλείας στην αντιμετώπιση των απειλών κυβερνοασφάλειας στα διαστημικά συστήματα;

10. Πώς μπορεί να βελτιωθεί η εκπαίδευση και η ευαισθητοποίηση των επαγγελματιών του κλάδου όσον αφορά την κυβερνοασφάλεια στα διαστημικά συστήματα;

2

Θεωρητικό Υπόβαθρο

2.1 Ορισμοί

Το κεφάλαιο που ακολουθεί προσφέρει μία εισαγωγική διερεύνηση στις βασικές έννοιες που αναγνωρίζονται ως βασικοί πυλώνες του κυβερνοχώρου και της κυβερνοασφάλειας, προσδιορίζοντας τη σημασία και το ρόλο τους στο πλαίσιο ενός συστήματος ασφάλειας που ενσωματώνει την προηγμένη τεχνολογία της AI.

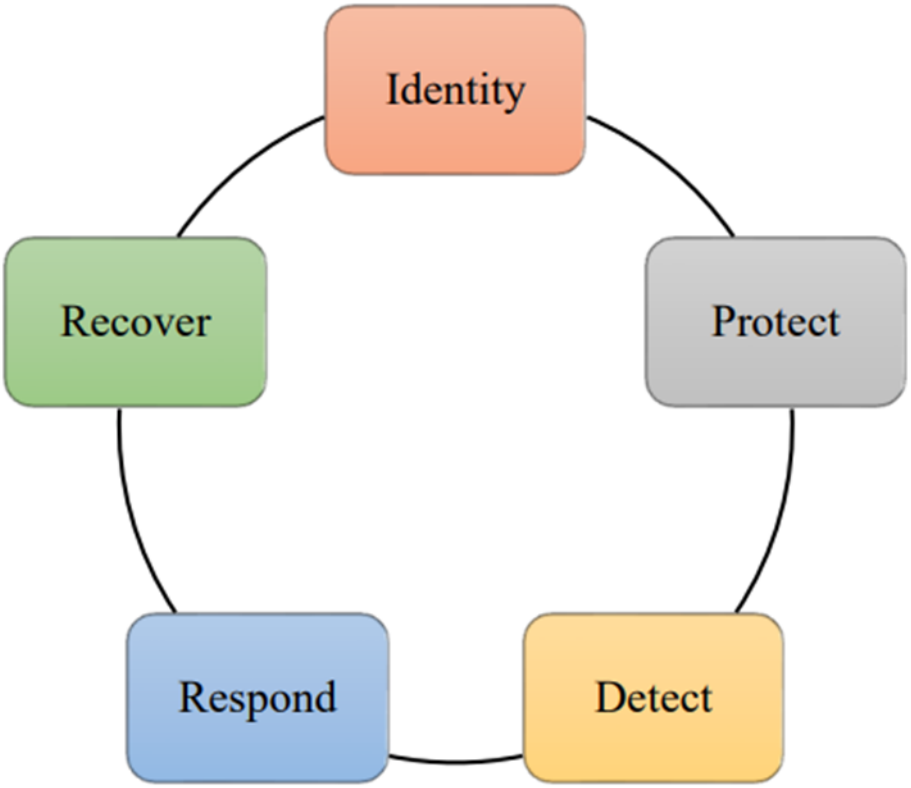
2.1.1 Κυβερνοχώρος

Ο κυβερνοχώρος αναφέρεται στο εικονικό περιβάλλον όπου πληροφορίες και δεδομένα μεταφέρονται, αποθηκεύονται και γίνονται αντικείμενο επεξεργασίας μέσω δικτύων υπολογιστών και άλλων ηλεκτρονικών μέσων. Αυτό το περιβάλλον είναι παντού και διαρκώς επεκτείνεται καθώς νέες τεχνολογίες και δίκτυα ενσωματώνονται στην καθημερινή ζωή. Ο κυβερνοχώρος ορίζεται ως το σύνολο των ψηφιακών δικτύων, υποδομών και ηλεκτρονικών συστημάτων που επιτρέπουν την ανταλλαγή, την επεξεργασία και την αποθήκευση πληροφοριών. Έτσι αποτελεί ένα σημαντικό μέρος της ζωής μας, αφού επηρεάζει από τις απλές καθημερινές συνήθειες μέχρι και την οικονομία της χώρας και δίνει τη δυνατότητα στον άνθρωπο για την επεξεργασία πληροφοριών, καθώς και την χρήση τους ως εκπαιδευτικό και ψυχαγωγικό περιεχόμενο. Παρόλα αυτά κάποια προβλήματα όπως η παραβίαση της ιδιωτικότητας καθώς και οικονομικής φύσεως εγκλήματα μέσω διαδικτύου παραμένουν και ενισχύονται μέσω της εξέλιξης της τεχνολογίας. Με την ενσωμάτωση της AI, ο κυβερνοχώρος βιώνει μετασχηματισμούς που οδηγούν σε αυτοματοποιημένες και αυτόνομες λειτουργίες, διευρύνοντας έτσι τα πεδία εφαρμογής και τις δυνατότητες ασφάλειας, αλλά και τις προκλήσεις που συναντούν τα συστήματα αυτά. Η ανάγκη για προηγμένες τεχνικές κρυπτογράφησης, καθώς και για εξελιγμένα συστήματα ανίχνευσης και αντιμετώπισης κυβερνοεπιθέσεων, έχει γίνει πιο αναγκαία από ποτέ [43].

Η ιστορία του κυβερνοχώρου ξεκινά από τις πρώιμες μέρες του ψηφιακού υπολογισμού, με τη δημιουργία της ARPANET το 1969. Πρόκειται για το πρώτο δίκτυο που χρησιμοποίησε την τεχνολογία packet switching για να διευκολύνει την επικοινωνία μεταξύ διαφορετικών υπολογιστών. Από αυτό το αρχικό στάδιο, ο κυβερνοχώρος εξελίχθηκε σε ένα παγκόσμιο δίκτυο που συνδέει δισεκατομμύρια συσκευές και υποδομές, από κινητά τηλέφωνα και προσωπικούς

υπολογιστές έως υπερυπολογιστές και cloud servers. Η διαδρομή από ένα ακαδημαϊκό και στρατιωτικό εργαλείο σε έναν κρίσιμο παράγοντα της παγκόσμιας οικονομίας και καθημερινότητας δείχνει την τεράστια αύξηση στη σημασία του κυβερνοχώρου. Σημαντικά γεγονότα συνέβαλαν περαιτέρω στην εξέλιξη αυτού του χώρου, όπως η εμφάνιση του World Wide Web το 1989-1990, που άλλαξε ριζικά τον τρόπο ανταλλαγής πληροφοριών, καθιστώντας τον κυβερνοχώρο πιο προσβάσιμο και διαδεδομένο. Το 1988, ο Morris Worm, ο πρώτος μεγάλης κλίμακας ιός, υπογράμμισε την ανάγκη για καλύτερα μέτρα ασφαλείας. Η εμπορική χρήση του διαδικτύου στα μέσα της δεκαετίας του 90 ανέδειξε νέες επιχειρηματικές και επικοινωνιακές δυνατότητες, ενώ η αύξηση του κυβερνοεγκλήματος και των τεχνικών κυβερνοπολέμου κατά τη δεκαετία του 2000 επιβεβαίωσε την ανάγκη για προηγμένες τεχνολογίες και στρατηγικές ασφαλείας. Αυτά τα περιστατικά έδειξαν ότι η ασφάλεια των πληροφοριών και των ψηφιακών δικτύων είναι κρίσιμη για την προστασία των οργανισμών και των ατόμων σε όλο τον κόσμο [20].

Το κυριότερο χαρακτηριστικό του κυβερνοχώρου είναι η ψηφιακή του φύση και η δυνατότητα ασύνδετης και ταυτόχρονης πρόσβασης από οπουδήποτε στον κόσμο. Αυτό το χαρακτηριστικό επιτρέπει ευελιξία αλλά δημιουργεί και νέες ευπάθειες ασφαλείας. Στην ουσία πρόκειται για αδιάκοπη σύνδεση και ψηφιακή παρουσία που επεκτείνεται πέρα από τα συνοριακά και γεωγραφικά όρια. Αυτή η ψηφιακή διασυνδεσιμότητα επιτρέπει την ταχεία και σχεδόν ανεξέλεγκτη διάδοση πληροφοριών, διευκολύνοντας την παγκόσμια επικοινωνία και την πληροφοριακή ανταλλαγή. Ωστόσο, το γεγονός αυτό αυτόματα εμφανίζει και σημαντικές προκλήσεις όπως την αυξημένη ευπάθεια σε κυβερνοεπιθέσεις και την δυσκολία στην εφαρμογή εθνικών νομοθεσιών σε έναν ανεξάρτητο από σύνορα ψηφιακό χώρο. Επιπλέον ξεχωρίζει η ανωνυμία, η ψηφιακή διάσπαση καθώς και η διαρκής και ασταμάτητη εξέλιξη. Η ανωνυμία στον κυβερνοχώρο παρέχει τη δυνατότητα στους χρήστες να κρύβουν ή να αλλάζουν την ταυτότητά τους μέσω ψευδωνύμων, ανώνυμων δικτύων όπως το Tor, και ειδικού λογισμικού για την απόκρυψη της IP διεύθυνσης. Αυτή η δυνατότητα ανωνυμίας μπορεί να επιτρέψει την ελεύθερη έκφραση και την προστασία από τον κίνδυνο πολιτικής δίωξης, αλλά ταυτόχρονα διευκολύνει την παραβατικότητα και το κυβερνοέγκλημα. Ανώνυμες δραστηριότητες μπορεί να περιλαμβάνουν τη διακίνηση παράνομου υλικού, την εκτέλεση κυβερνοεπιθέσεων και την παραβίαση δεδομένων χωρίς το φόβο αναγνώρισης. Η ψηφιακή διάσπαση αναφέρεται στις διαφορές που υπάρχουν μεταξύ ατόμων, νοικοκυριών, επιχειρήσεων και γεωγραφικών περιοχών σε επίπεδο πρόσβασης στις σύγχρονες ΤΠΕ και το διαδίκτυο. Επιπροσθέτως η ψηφιακή διάσπαση επηρεάζει την εκπαίδευση, την υγεία, την απασχόληση, και τη δημοκρατία, καθώς άτομα χωρίς πρόσβαση δεν μπορούν να εκμεταλλευτούν τις ίδιες ευκαιρίες. Ο κυβερνοχώρος βρίσκεται σε μια διαρκή και ταχύτατη εξέλιξη, με την εμφάνιση νέων τεχνολογιών όπως τεχνητή νοημοσύνη, μηχανική μάθηση, big data analytics, και Internet of Things (IoT) να αλλάζουν δραματικά το τοπίο. Αυτή η διαρκής τεχνολογική ανάπτυξη φέρνει νέες ευκαιρίες για καινοτομία και ανάπτυξη αλλά και σημαντικές προκλήσεις στην κυβερνοασφάλεια, καθώς οι απειλές εξελίσσονται το ίδιο γρήγορα με τις τεχνολογίες που προσπαθούν να προστατεύσουν.



Σχήμα 1 : Πλαίσιο Κυβερνοασφάλειας του Ινστιτούτου Εθνικών Προτύπων και Τεχνολογίας [18].

Η παραπάνω εικόνα δείχνει το Πλαίσιο Κυβερνοασφάλειας (CSF) του Ινστιτούτου Εθνικών Προτύπων και Τεχνολογίας (NIST), το οποίο βασίζεται σε μια στρατηγική διαχείρισης κινδύνου κυβερνοασφάλειας που μπορεί να προσαρμοστεί για διάφορους τομείς. Δημιουργεί μια κοινή γλώσσα και προσέγγιση που οι οργανισμοί μπορούν να χρησιμοποιήσουν σύμφωνα με τους πόρους και τις επιχειρηματικές τους ανάγκες. Το CSF διαθέτει πέντε λειτουργίες: αναγνώριση, προστασία, ανίχνευση, αντίδραση και ανάκτηση. Οι λειτουργίες παρουσιάζονται σε κυκλική διάταξη για να επισημανθεί ότι η κυβερνοασφάλεια είναι μια διαρκής και ατελείωτη διαδικασία, η οποία επιτρέπει σε μια επιχείρηση να αντιμετωπίσει τον κόσμο των επαναλαμβανόμενων κυβερνοαπειλών [18].

2.1.2 Διαστημική Κυβερνοασφάλεια

Η κυβερνοασφάλεια αναφέρεται στο σύνολο τεχνολογιών, διαδικασιών και πρακτικών που είναι σχεδιασμένες για την προστασία των δικτύων, των υπολογιστών, των προγραμμάτων και των δεδομένων από επιθέσεις, βλάβες ή μη εξουσιοδοτημένη πρόσβαση. Η κυβερνοασφάλεια είναι επίσης γνωστή για την ικανότητά της να προστατεύει την πληροφορία και τα συστήματα από κυβερνοεγκληματίες που επιδιώκουν να κερδίσουν πρόσβαση, να αλλοιώσουν ή να καταστρέψουν ευαίσθητα δεδομένα, να κλέψουν πνευματική ιδιοκτησία, ή να διαταράξουν τις κανονικές επιχειρηματικές διαδικασίες. Η σημασία του κυβερνοχώρου καθιστά την ασφάλεια στον

κυβερνοχώρο επίκαιρο ζήτημα, ωστόσο δεν είναι σαφές σε όλους τι αντιπροσωπεύει η κυβερνοασφάλεια. Με βάση τη βιβλιογραφία που εξετάστηκε, φαίνεται ότι λίγη έρευνα έχει γίνει για το τι θέματα μελετώνται στα ιδρύματα τριτοβάθμιας εκπαίδευσης για την κυβερνοασφάλεια [30].

Αρκετές μελέτες στην επιστημονική βιβλιογραφία διαπιστώνουν ότι η κυβερνοασφάλεια είναι διεπιστημονική και περιέχει έννοιες από διάφορα πεδία π.χ. διαχείριση επιχειρήσεων, μελέτες συμπεριφοράς και τεχνική και μηχανική λογισμικού. Το πρώτο μέρος «cyber» χρησιμοποιείται ως πρόθεμα αναφερόμενο γενικά στον ψηφιακό κόσμο . Προέρχεται από τη λέξη «cybernetics», η οποία είναι η μελέτη των υπολογιστών και των συστημάτων αυτοματισμού και επικοινωνιών. Χρησιμοποιείται παράλληλα με την έννοια του κυβερνοχώρου, όντας ένας εικονικός και άυλος χώρος που υπάρχει με τη συγχώνευση μιας ποικιλίας ηλεκτρονικών συστημάτων και δικτύων επικοινωνίας σε έναν ηλεκτρονικό χώρο που δεν αποτελεί μέρος του γνωστού και ορατού και του φυσικού. Το δεύτερο μέρος της είναι η λέξη «security» που το ορίζει ως ασφαλές και προστατευμένο από κινδύνους και απειλές . Γενικά καταλήγουμε ότι ως κυβερνοασφάλεια ορίζουμε την οργάνωση και συλλογή πόρων, διαδικασιών και δομών που χρησιμοποιούνται για προστασία του κυβερνοχώρου και των συστημάτων που υποστηρίζουν τον κυβερνοχώρο από περιστατικά που παραβιάζουν τα δικαιώματα ιδιοκτησίας. Ένα συμπέρασμα που μπορεί να εξαχθεί και κάνει το όλο ζήτημα να αποκτήσει περισσότερη σημασία είναι ότι δεν είναι δυνατός ο διαχωρισμός μεταξύ του φυσικού και του εικονικού ή των ψηφιακών στοιχείων της κυβερνοασφάλειας, καθώς τα γεγονότα στον κυβερνοχώρο μπορεί να έχουν φυσικές συνέπειες και απτές επιπτώσεις ακόμη αν και ο κυβερνοχώρος από μόνος του είναι άυλος.

Η διαστημική κυβερνοασφάλεια, αν και αποτελεί έναν σχετικά νέο τομέα, αναδεικνύεται σε κρίσιμο παράγοντα για τη διασφάλιση των διαστημικών συστημάτων και δικτύων από ψηφιακές επιθέσεις. Οι τεχνολογίες που χρησιμοποιούνται σε δορυφόρους, διαστημικά οχήματα, καθώς και οι επίγειοι σταθμοί επικοινωνίας, είναι ευάλωτες σε κυβερνοεπιθέσεις που μπορούν να προκαλέσουν σημαντικές ζημίες, τόσο σε επίπεδο δεδομένων όσο και σε φυσικά συστήματα. Οι επιθέσεις στον τομέα του διαστήματος μπορούν να οδηγήσουν σε παγκόσμιες διαταραχές, καθώς οι δορυφόροι χρησιμοποιούνται για μια πληθώρα εφαρμογών, όπως το παγκόσμιο σύστημα εντοπισμού θέσης (GPS), που είναι κρίσιμο για τη ναυτιλία, τις στρατιωτικές επιχειρήσεις και την καθημερινή μετακίνηση. Μια επίθεση που παραποιεί ή εμποδίζει τα σήματα GPS μπορεί να έχει εκτεταμένες επιπτώσεις στην παγκόσμια οικονομία και ασφάλεια. Επίσης, τα συστήματα τηλεπικοινωνιών εξαρτώνται σε μεγάλο βαθμό από δορυφορικές επικοινωνίες για τη μετάδοση δεδομένων, την τηλεόραση, και τις στρατιωτικές εφαρμογές. Η παρεμβολή σε αυτές τις επικοινωνίες θα μπορούσε να προκαλέσει μεγάλες διακοπές. Επιπλέον, οι δορυφόροι χρησιμοποιούνται για τη συλλογή δεδομένων για την παρακολούθηση του κλίματος και των καιρικών φαινομένων. Μια κυβερνοεπίθεση που διαταράσσει αυτά τα συστήματα θα μπορούσε να έχει σοβαρές επιπτώσεις στην πρόβλεψη ακραίων καιρικών φαινομένων.

Οι κύριες προκλήσεις της διαστημικής κυβερνοασφάλειας περιλαμβάνουν τη συνδεσιμότητα και την απόσταση, καθώς οι διαστημικές υποδομές λειτουργούν σε μεγάλες αποστάσεις από τη Γη, κάτι που σημαίνει ότι η πρόσβαση για επιδιόρθωση, συντήρηση ή άμεση αντίδραση σε επιθέσεις είναι εξαιρετικά περιορισμένη. Επίσης, λόγω της απομακρυσμένης φύσης των διαστημικών συστημάτων, οι αναβαθμίσεις λογισμικού είναι δύσκολες. Μια ευπάθεια ασφαλείας που παραμένει ανεπίλυτη μπορεί να παραμείνει για μεγάλα χρονικά διαστήματα. Επιπλέον, η μετάδοση δεδομένων

από και προς το διάστημα απαιτεί ισχυρή κρυπτογράφηση για την προστασία από πιθανές υποκλοπές ή αλλοιώσεις. Εκτός από τις κυβερνοεπιθέσεις, τα διαστημικά συστήματα είναι ευάλωτα και σε φυσικές επιθέσεις, όπως η καταστροφή δορυφόρων μέσω εχθρικών διαστημικών αποστολών ή συστημάτων αντιδορυφορικών όπλων (ASAT).

Οι βασικές στρατηγικές για τη διαστημική κυβερνοασφάλεια περιλαμβάνουν την ανάπτυξη ανθεκτικών συστημάτων, ώστε να αντέχουν και να συνεχίζουν τη λειτουργία τους ακόμα και μετά από μια επίθεση. Αυτό μπορεί να περιλαμβάνει την ύπαρξη συστημάτων ασφαλείας που θα επαναφέρουν τη λειτουργία του συστήματος ή θα αποκλείσουν τη ζημιά. Επίσης, η ενσωμάτωση τεχνητής νοημοσύνης μπορεί να χρησιμοποιηθεί για την ανίχνευση ανωμαλιών σε πραγματικό χρόνο και την αυτόματη ενεργοποίηση αμυντικών μέτρων. Παράλληλα, είναι απαραίτητη η ανάπτυξη διεθνών πολιτικών και κανονισμών για τη διαστημική κυβερνοασφάλεια, δεδομένου ότι ο διαστημικός τομέας είναι παγκόσμια υπόθεση και όχι μεμονωμένη υπόθεση κάποιας χώρας.

Καθώς κλείνει αυτό το κεφάλαιο για τον κυβερνοχώρο και την κυβερνοασφάλεια, είναι σαφές ότι η δυναμική του κυβερνοχώρου αποτελεί έναν θεμελιώδη παράγοντα στη σύγχρονη κοινωνία και οικονομία. Οι συνεχείς τεχνολογικές αλλαγές και η ολοένα αυξανόμενη εξάρτηση από ψηφιακά συστήματα καθιστούν την κυβερνοασφάλεια απαραίτητη, όχι μόνο για την προστασία δεδομένων και υποδομών, αλλά και για τη διασφάλιση της δημοκρατίας και των θεμελιωδών ανθρωπίνων δικαιωμάτων. Η ενσωμάτωση προηγμένης τεχνολογίας όπως η τεχνητή νοημοσύνη προσφέρει νέες λύσεις και αυξάνει την αποτελεσματικότητα των αμυντικών μέτρων, αλλά ταυτόχρονα αναδεικνύει την ανάγκη για ενίσχυση της νομικής και ηθικής ρύθμισης. Καθώς ο κυβερνοχώρος συνεχίζει να εξελίσσεται, οι προκλήσεις που αντιμετωπίζει ο άνθρωπος θα γίνονται περισσότερο περίπλοκες και οι λύσεις που απαιτούνται θα πρέπει να είναι πιο καινοτόμες και ευέλικτες, διασφαλίζοντας έτσι την ομαλή και ασφαλή λειτουργία της ψηφιακής μας εποχής .Η τεχνολογία διαδραματίζει κεντρικό ρόλο στην προστασία του διαστήματος. Η εφαρμογή της τεχνητής νοημοσύνης και της μηχανικής μάθησης παρέχει νέες δυνατότητες στην κυβερνοασφάλεια στο διάστημα, βοηθώντας στην πρόβλεψη πιθανών επιθέσεων και στην ταχύτερη ανταπόκριση σε κυβερνοαπειλές. Παράλληλα, η τεχνολογία blockchain μπορεί να προσφέρει νέους τρόπους για την ασφαλή αποθήκευση και διαχείριση δεδομένων, εξαλείφοντας την πιθανότητα υποκλοπής ή αλλοίωσης δεδομένων από εξωτερικές πηγές. Εν κατακλείδι, η διαστημική κυβερνοασφάλεια αποτελεί έναν τομέα που απαιτεί συνεχείς επενδύσεις, έρευνα και διεθνή συνεργασία. Η προστασία των διαστημικών υποδομών δεν αφορά μόνο την ασφάλεια των επικοινωνιών, αλλά έχει εκτεταμένες επιπτώσεις στην παγκόσμια οικονομία και την ασφάλεια. Καθώς το διάστημα συνεχίζει να εξελίσσεται σε έναν σημαντικό τομέα για την ανθρωπότητα, η διασφάλιση της ψηφιακής του ακεραιότητας είναι κρίσιμη [12].

2.1.3 Μέτρα Προστασίας

Η κυβερνοασφάλεια σε συστήματα διαστημικής τεχνολογίας με τη χρήση τεχνητής νοημοσύνης είναι σημαντική για την προστασία των συστημάτων από ενδεχόμενες κυβερνοεπιθέσεις. Μέτρα προστασίας, όπως η ανίχνευση απειλών, η ενίσχυση της ευπάθειας και η διαχείριση των επικινδυνοτήτων, είναι σημαντικά για τη διασφάλιση της ασφάλειας των συστημάτων. Επιπλέον, η εκπαίδευση του προσωπικού και η ευαισθητοποίηση για τις κυβερνοεπιθέσεις συμβάλλουν στη δημιουργία ενός ικανού προσωπικού. Με τη σωστή εφαρμογή αυτών των μέτρων, τα συστήματα διαστημικής τεχνολογίας μπορούν να προστατευθούν αποτελεσματικά από κυβερνοεπιθέσεις και να λειτουργήσουν με ασφάλεια και αποτελεσματικότητα [3].

2.1.3.1 Απειλή

Μια απειλή είναι μια ενέργεια που εκμεταλλεύεται τις αδυναμίες ασφαλείας σε ένα σύστημα και έχει αρνητικές επιπτώσεις σε αυτό. Οι απειλές μπορούν να προέρχονται από δύο κύριες πηγές: από ανθρώπους και από τη φύση . Φυσικές απειλές, όπως σεισμοί, τυφώνες, πλημμύρες και πυρκαγιές μπορούν να προκαλέσουν σοβαρές ζημιές στα υπολογιστικά συστήματα. Λίγα μέτρα προστασίας μπορούν να εφαρμοστούν εναντίον φυσικών καταστροφών, και κανείς δεν μπορεί να τις εμποδίσει από το να συμβούν . Οι ανθρώπινες απειλές είναι αυτές που προκαλούνται από ανθρώπους, όπως κακόβουλες απειλές που αποτελούνται από εσωτερικές (κάποιος έχει εξουσιοδοτημένη πρόσβαση) ή εξωτερικές απειλές (άτομα ή οργανισμοί που εργάζονται εκτός του δικτύου) που αποσκοπούν στο να βλάψουν και να διαταράξουν ένα σύστημα. Σε ότι αφορά τις κυβερνοεπιθέσεις σε συστήματα διαστημικής τεχνολογίας έχουμε να κάνουμε με δύο είδη απειλών, τις εσωτερικές και τις εξωτερικές. Οι εσωτερικές απειλές προέρχονται από άτομα με εξουσιοδοτημένη πρόσβαση στα συστήματα και δίκτυα της οργάνωσης και μπορούν να περιλαμβάνουν διαρροή πληροφοριών, σαμποτάζ, κακόβουλο κώδικα, κακή διαχείριση πληροφοριών ή κατά λάθος διαγραφή ή αλλαγή δεδομένων. Από την άλλη πλευρά, οι εξωτερικές απειλές προέρχονται από άτομα ή οργανισμούς χωρίς εξουσιοδοτημένη πρόσβαση και περιλαμβάνουν διακοπές υπηρεσιών (DDoS), κυβερνοκατασκοπεία, ransomware και phising ή άλλες τακτικές απάτης μέσω του ηλεκτρονικού ταχυδρομείου και των μέσων κοινωνικής δικτύωσης. Η πρόληψη και αντιμετώπιση των απειλών απαιτεί εξειδικευμένες στρατηγικές και συνεχή προσαρμογή των μέτρων ασφαλείας για τη διατήρηση της ασφάλειας δικτύων και συστημάτων [5].

2.1.3.2 Επιθέσεις

Οι κυβερνοεπιθέσεις εξελίσσονται συνεχώς, καθώς οι επιτιθέμενοι αναπτύσσουν νέες μεθόδους για να παρακάμψουν τα αμυντικά μέτρα και να εκμεταλλευτούν τις ευπάθειες στα συστήματα. Αυτές οι ενέργειες έχουν ως στόχο να διαταράξουν, να παραβιάσουν, ή ακόμη και να καταστρέψουν την κανονική λειτουργία των ψηφιακών υποδομών. Οι επιτιθέμενοι μπορεί να διαφέρουν σε κίνητρα, δυνατότητες και μεθόδους, ποικίλλοντας από μεμονωμένους χάκερς έως οργανωμένα εγκληματικά δίκτυα και κυβερνητικές οντότητες. Το κόστος της επίθεσης για τους

επιτιθέμενους συχνά σχετίζεται με την αναγκαία εμπειρία, τους πόρους και την προσπάθεια που απαιτείται για να ξεπεράσουν τα αμυντικά συστήματα. Από τα παραπάνω καταλαβαίνουμε ότι, η αυξανόμενη διαθεσιμότητα εργαλείων και τεχνικών στο σκοτεινό διαδίκτυο έχει μειώσει το κόστος εισόδου για νέους εγκληματίες, καθιστώντας τις κυβερνοεπιθέσεις πιο προσιτές και διαδεδομένες. Η κυβερνοασφάλεια, ως απάντηση σε αυτή την απειλή, πρέπει να είναι δυναμική και συνεχώς εξελισσόμενη. Η ανάπτυξη περιεκτικών στρατηγικών ασφαλείας που συμπεριλαμβάνουν τεχνολογικά, διαδικαστικά και ανθρώπινα στοιχεία είναι ουσιώδης για την προστασία των συστημάτων. Οι οργανισμοί πρέπει να επενδύουν στην εκπαίδευση των υπαλλήλων τους, τη διαρκή ενημέρωση και βελτίωση των συστημάτων ασφαλείας και την εφαρμογή πολιτικών που μειώνουν τον κίνδυνο εκμετάλλευσης ευπαθειών. Μέσα από αυτές τις διαρκείς προσπάθειες, είναι δυνατόν να δημιουργηθεί ένα πιο ασφαλές και ανθεκτικό ψηφιακό περιβάλλον [2].

2.1.3.3 Ευπάθειες

Οι ευπάθειες είναι αδυναμίες σε ένα σύστημα ή στον σχεδιασμό του που επιτρέπουν σε έναν εισβολέα να εκτελέσει εντολές, να έχει πρόσβαση σε μη εξουσιοδοτημένα δεδομένα και/ή να διεξάγει επιθέσεις άρνησης υπηρεσιών. Μπορούν να βρεθούν σε διάφορους τομείς των συστημάτων. Μπορεί να είναι αδυναμίες στο υλικό ή το λογισμικό του συστήματος, αδυναμίες στις πολιτικές και τις διαδικασίες που χρησιμοποιούνται στα συστήματα και αδυναμίες των ίδιων των χρηστών του συστήματος. Εντοπίζονται λόγω συμβατότητας και αλληλεπίδρασης του υλικού και επίσης της προσπάθειας που απαιτείται για να διορθωθούν. Ειδικότερα οι ευπάθειες λογισμικού μπορούν να βρεθούν σε λειτουργικά συστήματα, λογισμικό εφαρμογών και λογισμικό ελέγχου όπως πρωτόκολλα επικοινωνίας και οδηγοί συσκευών. Υπάρχει μια σειρά παραγόντων που οδηγούν σε ελαττώματα στον σχεδιασμό λογισμικού, συμπεριλαμβανομένων ανθρώπινων παραγόντων και πολυπλοκότητας λογισμικού. Τεχνικές ευπάθειες συνήθως συμβαίνουν λόγω ανθρώπινων αδυναμιών. Αυτές περιλαμβάνουν είτε λάθη στον κώδικα που δείχνουν σε ελλιπή εκπαίδευση προσωπικού είτε αμέλεια συντήρησης και ενημέρωσης λογισμικού. Σε ότι αφορά την πολυπλοκότητα του λογισμικού γνωρίζουμε ότι τα τεχνολογικά συστήματα αναπτύσσονται ολοένα και ταχύτερα άρα αυτόματα αυξάνεται η πολυπλοκότητα και έτσι ανεβαίνει και η πιθανότητα για λάθη. Αυτά για να αντιμετωπιστούν θα πρέπει να εφαρμοστεί αυστηρότερη ανίχνευση και αξιολόγηση έτσι ώστε να πραγματοποιηθεί έγκαιρος εντοπισμός και ταχύτατη διόρθωση των ευπαθειών πριν κάποιος τις εκμεταλλευτεί. Συνεπώς όλα τα παραπάνω συνδυαστικά οδηγούν σε αυξημένες ανάγκες εκπαίδευσης και κατάρτισης μέσω διαδικασιών [4].

2.1.3.4 Εκτίμηση και Διαχείριση Κινδύνων

Η εκτίμηση και τη διαχείριση κινδύνων έχει ως στόχο την αναγνώριση και αξιολόγηση των δυνητικών κινδύνων καθώς και την οργάνωση δράσεων για την μείωσή τους. Η διαδικασία αξιολόγησης και διαχείρισης κινδύνου είναι κρίσιμη για τη διασφάλιση της ασφάλειας και της ανθεκτικότητας ενός οργανισμού στον ψηφιακό κόσμο. Αυτή η κατηγορία εστιάζει στην ταυτοποίηση, την καταγραφή και την ανάλυση των πιθανών απειλών και των ευπαθειών που μπορεί να επηρεάσουν τον οργανισμό, καθώς και στην εφαρμογή των απαραίτητων μέτρων για την προστασία και την ανθεκτικότητα. Πρώτο βήμα στη διαδικασία είναι η ταυτοποίηση των κινδύνων. Αυτό περιλαμβάνει τη συλλογή και ανάλυση δεδομένων για τις υπάρχουσες απειλές στον κυβερνοχώρο, την εκτίμηση των εσωτερικών ευπαθειών του συστήματος και την εξέταση των

πιθανών εξωτερικών απειλών. Μετά την ταυτοποίηση των κινδύνων, ακολουθεί η ανάλυση για το πώς αυτοί οι κίνδυνοι μπορεί να επηρεάσουν τον οργανισμό. Εκτιμάται η πιθανότητα εμφάνισης κάθε κινδύνου και οι πιθανές επιπτώσεις τους, ώστε να καθοριστεί η σοβαρότητα του κινδύνου. Η επόμενη φάση είναι η ανάπτυξη και εφαρμογή στρατηγικών για τη μείωση ή εξουδετέρωση των επικρατέστερων κινδύνων. Αυτό περιλαμβάνει την εφαρμογή τεχνολογικών λύσεων, τη βελτίωση των διαδικασιών και την εκπαίδευση του προσωπικού. Επίσης σημαντικό είναι ο σχεδιασμός και η εφαρμογή αποτελεσματικών σχεδίων αντίδρασης για την αντιμετώπιση τυχόν περιστατικών που μπορεί να συμβούν. Αυτά τα σχέδια διασφαλίζουν ότι οι επιπτώσεις θα ελαχιστοποιηθούν και ότι ο οργανισμός μπορεί να ανακάμψει γρήγορα. Τέλος, η διαδικασία αξιολόγησης και διαχείρισης κινδύνου απαιτεί συνεχή επανεξέταση και ενημέρωση, καθώς οι κυβερνοαπειλές είναι δυναμικές και εξελίσσονται συνεχώς. Οι τακτικές αναθεωρήσεις εξασφαλίζουν ότι οι στρατηγικές και τα μέτρα παραμένουν επίκαιρα και αποτελεσματικά στο κόσμο της συνεχούς ψηφιακής μεταβολής [10].

2.1.4 Πολιτική Ασφαλείας

Οι πολιτικές είναι πλαίσια ανάπτυξης που δημιουργούνται από τους κύριους υπεύθυνους και του ανώτερους διευθυντές ενός οργανισμού και πρέπει να τηρούνται αυστηρά, ακόμα και σε δύσκολες καταστάσεις. Πρόσφατα, πολλές επιχειρήσεις, οργανισμοί, πρωτοβουλίες ή ακόμα κα χώρες δημιουργούν και ακολουθούν πολιτικές για να καθοδηγήσουν τις δραστηριότητές τους Αυτά τα έγγραφα λειτουργούν ως οδηγός για το πώς πρέπει να ενεργήσουν σε διάφορε καταστάσεις, ανεξαρτήτως εάν είναι καλές ή κακές, αναμενόμενες ή απρόβλεπτες. Η επιτυχία μια πρωτοβουλίας εξαρτάται από τους στόχους που τίθενται και τις μεθόδους που χρησιμοποιούνται για να τους επιτύχουν. Μια λειτουργική πολιτική και στρατηγική κυβερνοασφάλειας θα διευκόλυνε τη μείωση της πιθανότητας επιτυχούς κυβερνοεπίθεσης σε εθνικό επίπεδο. Θα παρέχει στη χώρα τη δυνατότητα να προλαμβάνει τέτοιες επιθέσεις και να αντιμετωπίζει γρήγορα τις επιπτώσεις τους σε περίπτωση που συμβούν. Επιπλέον, θα αντιπροσωπεύει τη διεθνή ισότητα προωθώντας τη συνεργασία μεταξύ των χωρών σε θέματα ασφάλειας και ανάπτυξης. Η ανάπτυξη και εφαρμογή πολιτικών κυβερνοασφάλειας μπορεί να κατανοηθεί μέσα από μία ιστορική αναδρομή, η οποία καταδεικνύει τη σημασία και την εξέλιξη αυτών των πολιτικών στον κόσμο της ψηφιακής τεχνολογίας και του διαδικτύου. Τη δεκαετία του 1970, με τη δημιουργία των πρώτων δικτυακών συστημάτων, όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο, το ARPANET, ξεκίνησε η ανάγκη για την εξασφάλιση της ασφάλειας των δεδομένων. Οι επιστήμονες και οι μηχανικοί άρχισαν να συνειδητοποιούν ότι η προστασία των διαδικτυακών συστημάτων έπρεπε να είναι προτεραιότητα για να προληφθούν παραβιάσεις και καταστροφές. Με την εμφάνιση των πρώτων ιών και κακόβουλου λογισμικού τη δεκαετία του 1980, οι οργανισμοί άρχισαν να υιοθετούν τις πρώτες επίσημες πολιτικές κυβερνοασφάλειας. Η ανάγκη για συστηματική προσέγγιση στην ασφάλεια έγινε επιτακτική, καθώς οι απειλές εξελίσσονταν και έγιναν πιο πολύπλοκες. Καθώς το Διαδίκτυο έγινε πιο προσβάσιμο στις αρχές του 1990, η ανάγκη για πιο ανεπτυγμένες και ολοκληρωμένες πολιτικές κυβερνοασφάλειας έγινε ακόμα πιο έκδηλη. Η ευρεία χρήση του διαδικτύου εισήγαγε νέους κινδύνους και απειλές, απαιτώντας πιο σύνθετα μέτρα ασφαλείας και διαχείρισης πληροφοριών. Πρότυπα όπως το ISO/IEC 27001 καθιερώθηκαν για να παρέχουν ένα συνεκτικό πλαίσιο προστασίας δεδομένων και διαδικτυακής ασφάλειας παγκοσμίως. Σήμερα, η κυβερνοασφάλεια αποτελεί μία διαρκή πρόκληση καθώς η τεχνολογία εξελίσσεται ταχύτατα. Η ανάπτυξη του cloud computing, του big data και του Internet of Things (IoT) έχει πολλαπλασιάσει τις πιθανές επιφάνειες επίθεσης, καθιστώντας απαραίτητη την ενημέρωση και εξέλιξη των πολιτικών κυβερνοασφάλειας [8].

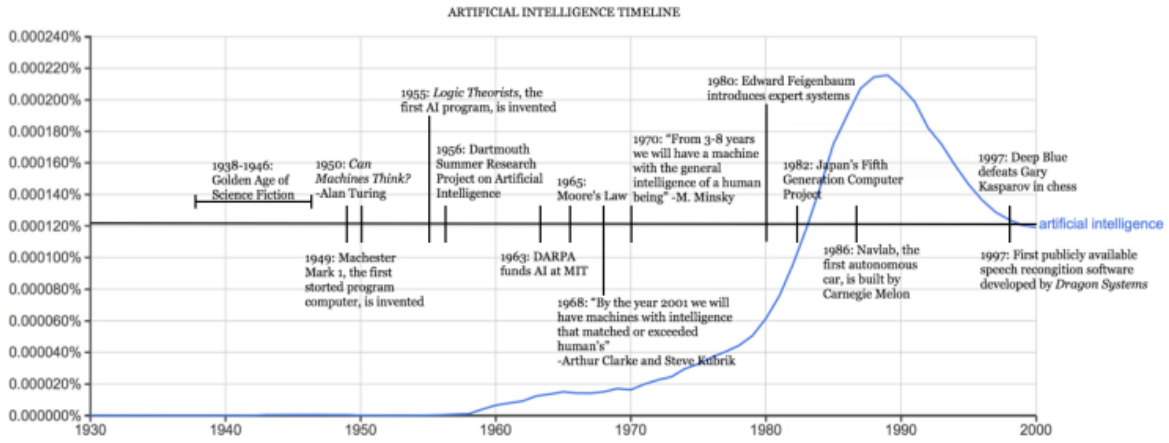
2.1.5 Τεχνητή Νοημοσύνη

Η τεχνητή νοημοσύνη (AI) αντιπροσωπεύει την επιστήμη και την μηχανική της δημιουργίας έξυπνων μηχανών, ιδιαίτερα έξυπνων προγραμμάτων υπολογιστών. Είναι ένας τομέας της τεχνολογίας που στοχεύει στη μίμηση των ανθρωπίνων εγκεφαλικών λειτουργιών μέσω της μηχανικής μάθησης, της βαθιάς μάθησης, της επεξεργασίας φυσικής γλώσσας και του αυτόματου συλλογισμού. Επιπλέον η AI έχει εφαρμογές από την αυτοματοποιημένη ρομποτική έως την ανάλυση δεδομένων και από την επιστήμη των δεδομένων έως τα έξυπνα οικιακά συστήματα και επομένως έχει τη δυνατότητα να μετασχηματίσει πολλές βιομηχανίες και να προσφέρει νέες, επαναστατικές λύσεις σε παλιά προβλήματα [23].

Η τεχνητή νοημοσύνη μπορεί να θεωρηθεί ως ένα ευρύ θεματικό πλαίσιο. Ο σκοπός της είναι να επιτρέπει στους υπολογιστές να μιμούνται την ανθρώπινη σκέψη, να προσομοιώνουν ανθρώπινες δραστηριότητες και να επιλύουν προβλήματα ταχύτερα και αποδοτικότερα από ότι μπορούν να τα επιλύσουν οι άνθρωποι. Διάφορες εργασίες, όπως η δημιουργική σκέψη, η σχεδίαση, η μετακίνηση, η ομιλία, η αναγνώριση αντικειμένων και ήχων, οι κοινωνικές και επιχειρηματικές συναλλαγές, μπορούν να εκτελούνται εκμεταλλευόμενες την τεχνητή νοημοσύνη. Για την εκτέλεση εργασιών, μπορούν να χρησιμοποιηθούν διάφορες μέθοδοι, όπως οι μέθοδοι βασισμένες σε ενδείξεις, η επεξεργασία φυσικής γλώσσας (NLP), η ανάλυση κειμένου, τα συστήματα συστάσεων, η μηχανική μάθηση και η βαθιά μάθηση. Οι παραπάνω μέθοδοι μπορούν επίσης να χρησιμοποιηθούν για την επίλυση προβλημάτων στην κυβερνοασφάλεια.

Η μηχανική μάθηση είναι ένας υποκλάδος της τεχνητής νοημοσύνης που επικεντρώνεται στην ανάπτυξη αλγορίθμων οι οποίοι μπορούν να μαθαίνουν αλλά και να κάνουν προβλέψεις επί των δεδομένων. Αυτό επιτυγχάνεται χωρίς να προγραμματίζονται ρητά για μια συγκεκριμένη εργασία, παράγοντας μοντέλα που μπορούν να προσαρμοστούν και να βελτιωθούν με την πρόσληψη νέων δεδομένων [7].

Η τεχνητή νοημοσύνη έχει αναδειχθεί ως ένα από τα πιο σημαντικά εργαλεία στη σύγχρονη τεχνολογία. Μέσω της χρήσης προηγμένων αλγορίθμων και μηχανικής μάθησης, η τεχνητή νοημοσύνη επιτρέπει στις συσκευές και τους υπολογιστικούς μηχανισμούς να αναλαμβάνουν πολύπλοκες εργασίες με ακρίβεια και ταχύτητα. Από την υποστήριξη στη λήψη αποφάσεων στην ανάλυση δεδομένων και την αυτόματη παραγωγή περιεχομένου, η τεχνητή νοημοσύνη έχει επηρεάσει τον τρόπο λειτουργίας των οργανισμών και της κοινωνίας.



Σχήμα 2 : Διαγραμματική ιστορική εξέλιξη της τεχνητής νοημοσύνης [1].

Από το παραπάνω χρονοδιάγραμμα της τεχνητής νοημοσύνης παρατηρούμε μια συνεχή και επίμονη πρόοδο στην έρευνα και ανάπτυξη από τις πρώιμες μέρες της AI έως σήμερα. Η AI έχει συνδυαστεί με άλλες τεχνολογίες, όπως την ρομποτική και τα συστήματα αυτοματοποίησης, επεκτείνοντας τις δυνατότητές της. Επιπλέον η AI έχει αποδειχθεί καθοριστική στον εντοπισμό κυβερνοαπειλών και στην προσαρμοστική άμυνα, παρέχοντας την ικανότητα να ανταποκρίνεται γρήγορα και αποτελεσματικά στις εξελισσόμενες τακτικές επίθεσης. Έτσι η άνθιση της AI έχει φέρει μαζί της νέες ηθικές και ασφαλιστικές διαστάσεις, επισημαίνοντας την ανάγκη για ρύθμιση και διαχείριση των τεχνολογικών κινδύνων. Από το 2000 και μετά, η τεχνητή νοημοσύνη έχει αναπτυχθεί πολύ γρήγορα. Αυτό οφείλεται σε πολλά δεδομένα που έχουμε στη διάθεσή μας, στην αύξηση της ισχύος των υπολογιστών και στις βελτιώσεις στους αλγόριθμους. Η τεχνητή νοημοσύνη χρησιμοποιείται σε πολλά πολλές εφαρμογές, όπως η αναγνώριση φωνής και εικόνας, η αυτόνομη οδήγηση και η προσωποποιημένη ιατρική [1].

Τα συστήματα AI πλέον δεν περιορίζονται στην εκτέλεση στατικών εργασιών, αλλά μπορούν να αλληλοεπιδρούν με το περιβάλλον, να μαθαίνουν από την εμπειρία και να προβλέπουν και να προσαρμόζονται σε μεταβαλλόμενες συνθήκες. Η δυνατότητα αυτή των συστημάτων AI να προσαρμόζονται και να βελτιώνονται με την πάροδο του χρόνου αντιπροσωπεύει μια σημαντική αλλαγή παραδείγματος στην ανάπτυξη και την εφαρμογή της τεχνολογίας.

Η Τεχνητή Νοημοσύνη περιλαμβάνει επίσης τη Γεννήτρια Φυσικής Γλώσσας (NLG), η οποία αναφέρεται στη δημιουργία πληροφοριών κειμένου από δεδομένα. Είναι μια διαδικασία κατά την οποία τα δεδομένα πρέπει να ερμηνευθούν κατάλληλα. Λειτουργεί διερμηνεύοντας κειμενικά δεδομένα και παρουσιάζοντας τα αποτελέσματα με τη μορφή φυσικής γλώσσας. Αυτοί οι τύποι εργαλείων χρησιμοποιούνται κατά την επεξεργασία μεγάλων δομημένων και μη δομημένων συνόλων δεδομένων. Το αποτέλεσμα της επεξεργασίας NLG είναι ένα κείμενο φυσικής γλώσσας, το οποίο δημιουργείται από τον συνδυασμό δεδομένων που συλλέχθηκαν και της εισόδου που παράχθηκε από τον χρήστη. Η Φυσική Γλωσσική Επεξεργασία αποτελεί την αντίστροφη διαδικασία της Φυσικής Γλωσσικής Κατανόησης (NLU). Κατά τη διαδικασία της NLU, το σύστημα αποφασίζει πώς να απεικονίσει τα εισερχόμενα δεδομένα, ενώ η NLP παράγει δεδομένα από μια είσοδο φυσικής γλώσσας [9].

Τα τελευταία χρόνια παρατηρείται αυξημένη χρήση τεχνολογιών Μηχανικής Μάθησης και Τεχνητής Νοημοσύνης για εφαρμογές Παρακολούθησης της Γης (ΕΟ).Η εκθετική αύξηση των δεδομένων που συλλέγονται από δορυφόρους απαιτεί τη χρήση τεχνολογιών για μια γρήγορη και ακριβή ανάλυση. Ένα παράδειγμα αυτής της χρήσης είναι το (Φ-Sat-1), ο πρώτος ευρωπαϊκός δορυφόρος που χρησιμοποιεί τεχνητή νοημοσύνη για να στέλνει αποτελεσματικά δεδομένα ΕΟ πίσω στη Γη. Ζούμε τώρα στην εποχή των μεγάλων δεδομένων, μια εποχή στην οποία έχουμε τη δυνατότητα να συλλέγουμε τεράστιες ποσότητες πληροφοριών που είναι υπερβολικά σύνθετες για ένα άτομο να επεξεργαστεί. Η εφαρμογή της τεχνητής νοημοσύνης σε αυτόν τον τομέα ήδη έχει φέρει θετικά αποτελέσματα σε διάφορους κλάδους όπως η τεχνολογία, οι τραπεζικές συναλλαγές, το μάρκετινγκ και ο χώρος της ψυχαγωγίας. Έχουμε δει ότι ακόμα κι αν οι αλγόριθμοι δεν βελτιωθούν πολύ, τα μεγάλα δεδομένα και οι τεράστιοι υπολογιστικοί πόροι απλά επιτρέπουν στην τεχνητή νοημοσύνη να μαθαίνει μέσω brute force.Ο όρος brute force αναφέρεται σε μια μέθοδο επίλυσης προβλημάτων ή αναζήτησης λύσεων που βασίζεται στη δοκιμή όλων των πιθανών εναλλακτικών, χωρίς να χρησιμοποιείται κάποιος εξειδικευμένος αλγόριθμος για να βρεθεί η λύση με λιγότερο κόστος σε χρόνο και πόρους συνδυαστικά .Η εφαρμογή αλγορίθμων brute force είναι συχνά αποτελεσματική για μικρά προβλήματα, αλλά μπορεί να είναι απαγορευτικά ακριβή ή ανεφάρμοστη για προβλήματα μεγάλης κλίμακας λόγω της τεράστιας πολυπλοκότητας όταν αυξάνεται ο αριθμός των πιθανών επιλογών. Συνίσταται να γίνεται χρήση brute force όταν έχουμε περιορισμένο αριθμό εναλλακτικών ο οποίος είναι και γνωστός [11].

Υπάρχουν επίσης ενδείξεις ότι ο νόμος του Moore επιβραδύνεται ελαφρώς, αλλά η αύξηση στα δεδομένα σίγουρα δεν έχει χάσει ορμή. Οι επιτυχίες στην επιστήμη υπολογιστών, τα μαθηματικά ή τη νευροεπιστήμη λειτουργούν ως πιθανές λύσεις μέσω της κορύφωσης του νόμου του Moore. Ο νόμος του Moore αναφέρεται στην παρατήρηση που έκανε ο συνιδρυτής της Intel, Gordon Moore, το 1965, σύμφωνα με τον οποίο ο αριθμός των transistors σε έναν ενσωματωμένο κύκλωμα ή μικροτσίπ διπλασιάζεται περίπου κάθε δύο χρόνια. Αυτή η τάση έχει οδηγήσει σε συνεχή βελτίωση της υπολογιστικής ισχύος και της απόδοσης των υπολογιστών σε διάφορες εφαρμογές, και έχει θεωρηθεί ως η κινητήρια δύναμη για την επίτευξη της τεχνολογικής προόδου. Ωστόσο, κατά την πάροδο του χρόνου, οι φυσικοί περιορισμοί και οι τεχνολογικές προκλήσεις έχουν αρχίσει να επιβραδύνουν αυτήν την τάση, καθώς η επίτευξη υψηλότερων επιπέδων ολοκλήρωσης στα μικροτσίπς γίνεται πιο δύσκολη.

Η επίδραση της τεχνητής νοημοσύνης στην κυβερνοασφάλεια και τον κυβερνοχώρο είναι τεράστια και πολυδιάστατη, καθώς το AI έχει τη δυνατότητα να ενισχύσει τις αμυντικές ικανότητες των ψηφιακών συστημάτων, αλλά και να επιτρέπει πιο προηγμένες μορφές επιθέσεων. Έτσι στην ουσία έχουμε σημαντικά πλεονεκτήματα μέσω των οποίων η τεχνητή νοημοσύνη μπορεί και ενισχύει το πεδίο της Κυβερνοασφάλειας. Το βασικότερο από αυτά είναι η αυτοματοποίηση και η ανίχνευση των απειλών. Συγκεκριμένα η τεχνητή νοημοσύνη μπορεί να αυτοματοποιήσει την ανίχνευση και ανταπόκριση σε κυβερνοαπειλές. Συστήματα που χρησιμοποιούν AI μπορούν να αναλύουν εκατομμύρια σημεία δεδομένων και να αναγνωρίζουν ανωμαλίες ή πρότυπα που συνδέονται με κακόβουλη δράση, όπως η χρήση ransomware ή άλλων τύπων malware. Αυτή η δυνατότητα επιτρέπει την ταχύτερη και πιο αποτελεσματική αντίδραση σε απειλές, μειώνοντας τον χρόνο ανάκαμψης και τις ζημιές. Επιπλέον μέσω της μηχανικής μάθησης και άλλων μορφών AI, τα συστήματα κυβερνοασφάλειας μπορούν να εξελίσσονται και να προσαρμόζονται στην εναλλαγή των τακτικών επίθεσης. Αυτό σημαίνει ότι τα συστήματα δεν αντιδρούν απλά στις απειλές, αλλά

προετοιμάζονται για πιθανές μελλοντικές επιθέσεις. Μάλιστα μελετούν συνεχώς τις απειλές και μαθαίνουν από αυτές έτσι ώστε να βρίσκονται πάντα σε ετοιμότητα, ακόμα και όταν φαινομενικά δεν υπάρχει κίνδυνος. Αυτή η προσαρμοστικότητα μας δείχνει ότι τα συστήματα ασφαλείας μπορούν να προσαρμόσουν τα μέτρα που θα ληφθούν ανάλογα με την πορεία των απειλών σε πραγματικό χρόνο. Με αυτόν τον τρόπο βελτιώνεται και η ανίχνευση των πιθανών κινδύνων και η αντίδρασή των συστημάτων αυτών [6].

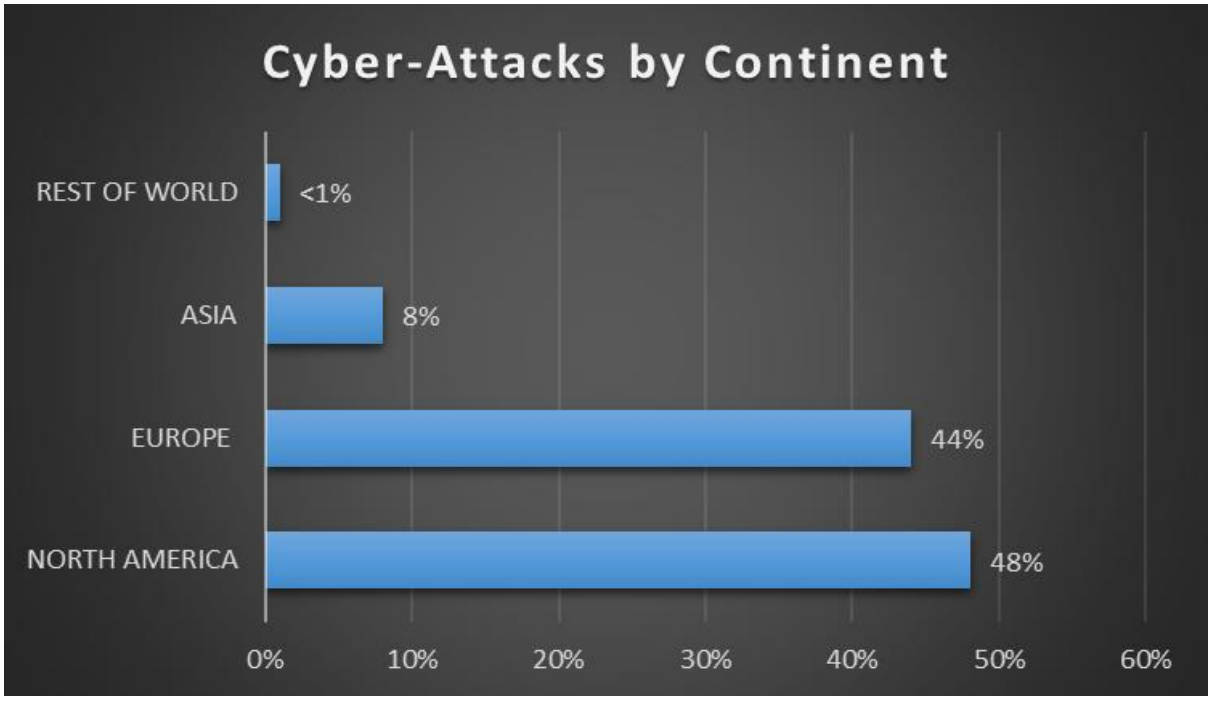
Καθώς εξετάζουμε την πορεία της τεχνητής νοημοσύνης στον χρόνο είναι σαφές ότι δεν είναι πλέον ένα απλό τεχνολογικό εργαλείο, αλλά ένας παράγοντας που επαναπροσδιορίζει τον τρόπο με τον οποίο γίνεται η αλληλεπίδραση με τον κόσμο γύρω μας. Μέσω της τεχνητής νοημοσύνης παρέχεται η δυνατότητα για επεξεργασία μαζικών δεδομένων έτσι ώστε να ανοίξει ευκολότερα ένας νέος δρόμος καινοτομίας μέσω της καταπολέμησης των εμποδίων που υπήρχαν στο παρελθόν. Αυτή η ανάπτυξη της τεχνητής νοημοσύνης οδηγεί στην ένταξή της και σε τομείς όπως η κυβερνοασφάλεια , η υγεία και η βιομηχανία αλλά ταυτόχρονα αυτό δημιουργεί και την ανάγκη μιας ισορροπίας στη διαχείρισή της. Αυτή η ανάγκη για διαχείριση στο μέλλον θα οδηγήσει σε ακόμα μεγαλύτερες αναζητήσεις μεταξύ ισορροπίας και καινοτομίας.

3

Κυβερνοεπιθέσεις του Διαστημικού Συστήματος

3.1 Κίνδυνοι και ευπάθειες

Ένα από τα σημαντικότερα χαρακτηριστικά των δεδομένων από δορυφόρους είναι ότι πρέπει να μετατραπούν σε κατανοητές πληροφορίες. Απαραίτητη προϋπόθεση για να γίνει αυτό είναι η χρησιμοποίηση συγκεκριμένων μεθόδων τεχνητής νοημοσύνης. Η τεχνητή νοημοσύνη αναφέρεται σε διάφορες τεχνικές, όπως η μηχανική μάθηση, που χρησιμοποιούνται για την επεξεργασία δεδομένων από τους δορυφόρους. Αυτό είναι σημαντικό για να μπορούμε να κατανοήσουμε καλύτερα τις φυσικές παραμέτρους. Η τεχνητή νοημοσύνη έχει διάφορες εφαρμογές, όπως η μηχανική μάθηση και η βαθιά μάθηση, οι οποίες χρησιμοποιούνται κυρίως για την ταξινόμηση εικόνων ή την ανίχνευση αντικειμένων. Η αποτελεσματική χρήση δεδομένων από τον δορυφόρο μπορεί να απαιτήσει μεθόδους τεχνητής νοημοσύνης που συνδυάζουν μαθηματικά μοντέλα για την τροχιά του δορυφόρου, τη φυσική εκπομπή και διάδοση ηλεκτρομαγνητικών κυμάτων, την επεξεργασία σήματος, τη μηχανική μάθηση ή την αναπαράσταση γνώσης.



Σχήμα 3: Cyber-Attacks by Continent.

Το παραπάνω διάγραμμα δείχνει την κατανομή των κυβερνοεπιθέσεων κατά Ήπειρο. Οι κυβερνοεπιθέσεις στην Βόρεια Αμερική είναι οι πιο συχνές, αντιπροσωπεύοντας το 48% των συνολικών επιθέσεων. Ακολουθεί η Ευρώπη με το 44%, ενώ η Ασία βρίσκεται αρκετά πίσω με μόλις 8%. Τέλος, οι υπόλοιπες περιοχές του κόσμου συμμετέχουν λιγότερο από το 1% στις συνολικές κυβερνοεπιθέσεις. Αυτή η κατανομή υποδεικνύει ότι οι κυβερνοεπιθέσεις είναι κυρίως ένα φαινόμενο που επηρεάζει τις πιο ανεπτυγμένες περιοχές, όπου υπάρχει μεγαλύτερη εξάρτηση από την τεχνολογία και τις ψηφιακές υποδομές. Οι επιθέσεις γενικά και ανά Ήπειρο θα αναλυθούν παρακάτω [13].

3.1.1 Κυβερνοκίνδυνοι κατά των Διαστημικών Συστημάτων με Τεχνητή Νοημοσύνη

Η πρόβλεψη μιας κυβερνοεπίθεσης δεν είναι εύκολη ή αξιόπιστη. Ο κίνδυνος στον τομέα της κυβερνοασφάλειας ορίζεται από τις απειλές, τις ευπάθειες και τις επιπτώσεις, σε συνδυασμό με τα πιθανά μέτρα προστασίας. Για να αντιμετωπίσουμε τους κυβερνοκινδύνους στα διαστημικά συστήματα με τεχνητή νοημοσύνη, μπορούμε να υιοθετήσουμε διάφορα μέτρα ασφαλείας και τεχνολογικές λύσεις. Ένα σημαντικό μέτρο είναι η χρήση ασφαλών πρωτοκόλλων επικοινωνίας και κρυπτογραφίας για την προστασία της μετάδοσης δεδομένων μεταξύ των διαστημικών συστημάτων και των εδαφικών σταθμών ελέγχου. Επιπλέον, η χρήση συστημάτων ανίχνευσης εισβολών μπορεί να βοηθήσει στην παρακολούθηση της κυκλοφορίας δεδομένων και την ανίχνευση μη εξουσιοδοτημένης πρόσβασης ή ύποπτων δραστηριοτήτων. Επίσης, η υιοθέτηση μέτρων πολυπαραγοντικής ταυτοποίησης είναι σε θέση να διασφαλίσει ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε κρίσιμα συστήματα και δεδομένα. Με αυτούς τους τρόπους, ενισχύουμε την ανθεκτικότητα των διαστημικών συστημάτων με τεχνητή νοημοσύνη ενάντια στους κυβερνοκινδύνους και διασφαλίζουμε την ακεραιότητα και τη διαθεσιμότητα των κρίσιμων δεδομένων και λειτουργιών διαστημικών αποστολών [14].

Η χρήση της τεχνητής νοημοσύνης προσφέρει πολλά πλεονεκτήματα, αλλά ελλοχεύει και ορισμένους κινδύνους. Ανάμεσα σε αυτούς τους κινδύνους είναι η έλλειψη παρακολούθησης της εφαρμογής, οι παραβιάσεις του απορρήτου των δεδομένων και οι προκατειλημμένοι αλγόριθμοι. Η έλλειψη παρακολούθησης και αξιολόγησης των αλγορίθμων μπορεί να οδηγήσει σε λανθασμένες αποφάσεις και επιθέσεις, ενώ οι παραβιάσεις του απορρήτου δεδομένων θέτουν σε κίνδυνο την ασφάλεια και την εμπιστευτικότητα των πληροφοριών, δημιουργώντας νομικά και ηθικά προβλήματα. Επιπλέον, οι αλγόριθμοι μπορεί να περιέχουν ενσωματωμένες προκαταλήψεις, επηρεάζοντας τη λήψη αποφάσεων και καθιστώντας δύσκολη την κατανόηση και την προστασία των περίπλοκων αλγορίθμων από επιθέσεις.

Η γνώση και η κατανόηση των νομικών πλαισίων και οι προσπάθειες διεθνούς συνεργασίας είναι ουσιαστικές για την αντιμετώπιση των κυβερνοκινδύνων στη διαστημική εξερεύνηση. Οι νομικές προϋποθέσεις και οι συμφωνίες μεταξύ των χωρών μπορούν να καθορίσουν κοινά πρότυπα και κανονισμούς για την προστασία των διαστημικών συστημάτων από κυβερνοεπιθέσεις. Η διεθνής συνεργασία μπορεί να προωθήσει την ανταλλαγή πληροφοριών, την ανάπτυξη κοινών προγραμμάτων εκπαίδευσης και τη διαμόρφωση βέλτιστων πρακτικών για την ασφάλεια στο διάστημα. Μέσω αυτών των πρωτοβουλιών, μπορούμε να ενισχύσουμε την ασφάλεια και τη

σταθερότητα των διαστημικών εξερευνήσεων και να διασφαλίσουμε την αδιάκοπη πρόοδο στην εξερεύνηση του διαστήματος για όλη την ανθρωπότητα .

3.1.2 Ευπάθειες σε Κυβερνοεπιθέσεις με Χρήση Τεχνητής Νοημοσύνης

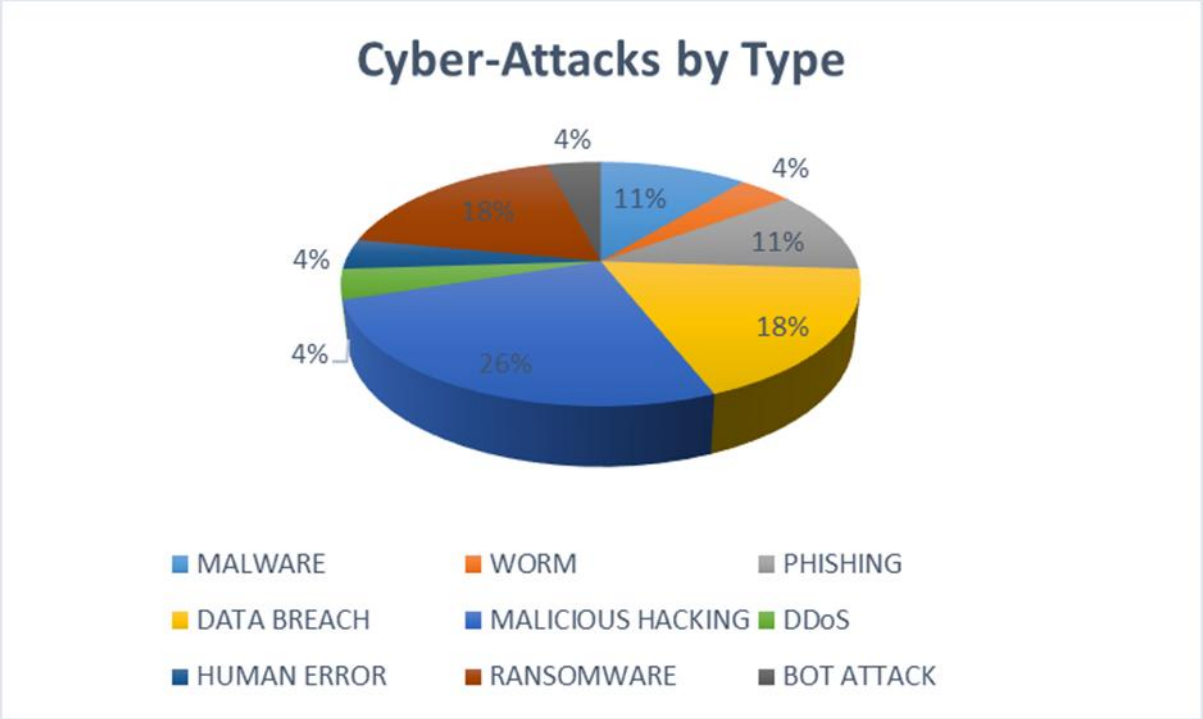
Η τεχνητή νοημοσύνη, και ιδιαίτερα η αδύναμη τεχνητή νοημοσύνη, αποτελεί μια ευάλωτη τεχνολογία στον κυβερνοχώρο. Τα συστήματα της τεχνητής νοημοσύνης δεν είναι μόνο ενσωματωμένα με τις παραδοσιακές μορφές κυβερνοευπαθειών, ιδιαίτερα εκείνες που χρησιμοποιούν μηχανική μάθηση, αλλά εξαρτώνται επίσης από τον τρόπο λειτουργίας και μάθησης της τεχνητής νοημοσύνης. Τα σφάλματα που υπάρχουν μπορεί να αυξηθούν με πρόσθετα, μη επιδιορθώσιμα σφάλματα, κάνοντας το σύστημα που χρησιμοποιεί την τεχνητή νοημοσύνη πιο ευάλωτο σε επιθέσεις.

Οι επιθέσεις για την εκμετάλλευση ευπαθειών των συστημάτων τεχνητής νοημοσύνης έχουν ήδη εξαπλωθεί στο διάστημα από πολλά κράτη και οργανισμούς. Η χρήση αλγορίθμων μηχανικής μάθησης μπορεί να βοηθήσει στην αναγνώριση και την προστασία ενάντια σε κυβερνοευπάθειες και απειλές αυτοματοποιώντας την ανίχνευση μιας επίθεσης και την αντίδρασή της. Από την άλλη πλευρά, οι επιθέσεις με τη χρήση τεχνητής νοημοσύνης μπορούν να καταστήσουν δυσκολότερο τον αποκλεισμό ή την προστασία από κυβερνοεπιθέσεις επιτρέποντας την άμεση προσαρμογή του κακόβουλου λογισμικού. Στον τομέα της κυβερνοασφάλειας της τεχνητής νοημοσύνης, η ευπάθεια αναφέρεται σε μια αδυναμία σε υλικό, λογισμικό ή διαδικασίες. Από την άλλη πλευρά, ο κίνδυνος αναφέρεται στη δυνατότητα απώλειας, ζημίας ή καταστροφής περιουσιακών στοιχείων. Από την εκτέλεση αποστολής μέχρι την ανάλυση δεδομένων, τα συστήματα τεχνητής νοημοσύνης έχουν ακόμα σημαντικούς περιορισμούς και ευπάθειες, ιδιαίτερα όσον αφορά την προβλεψιμότητα, την επαλήθευση και την αξιοπιστία. Τόσο τα συστήματα τεχνητής νοημοσύνης όσο και τα συστήματα που ενισχύονται με την τεχνητή νοημοσύνη που εφαρμόζονται σε διαφορετικά περιβάλλοντα στο διάστημα μπορούν να επιτεθούν. Οι επιθέσεις με τη χρήση τεχνητής νοημοσύνης γίνονται πιο αποτελεσματικές λόγω των περιορισμών στους βασικούς αλγορίθμους της τεχνητής νοημοσύνης που δεν μπορούν να διορθωθούν αυτή τη στιγμή. Συνεπώς, διαφέρουν από τις συμβατικές κυβερνοεπιθέσεις που προκαλούνται από "σφάλματα" ή ανθρώπινα λάθη στους κώδικες. Μια επίθεση μπορεί να στοχεύσει στην ασφάλεια του αλγορίθμου εκπαίδευσης. Από την άλλη πλευρά, οι αδυναμίες στην πλατφόρμα στην οποία λειτουργεί το σύστημα τεχνητής νοημοσύνης μπορεί να επηρεάσουν την αξιοπιστία των αποτελεσμάτων.

Τέλος η τεχνητή νοημοσύνη και ιδιαίτερα η αδύναμη τεχνητή νοημοσύνη, είναι ευάλωτη σε κυβερνοεπιθέσεις. Τα συστήματα τεχνητής νοημοσύνης περιλαμβάνουν παραδοσιακές κυβερνοευπάθειες και επιπλέον εξαρτώνται και από τον τρόπο που λειτουργούν και μαθαίνουν. Οι επιθέσεις σε αυτά τα συστήματα έχουν ήδη πραγματοποιηθεί από διάφορα κράτη και οργανισμούς. Αν και η χρήση αλγορίθμων μηχανικής μάθησης μπορεί να βοηθήσει στην ανίχνευση και προστασία από κυβερνοαπειλές, μπορεί επίσης να κάνει και πιο δύσκολη την αποτροπή κυβερνοεπιθέσεων. Η ασφάλεια του αλγορίθμου εκπαίδευσης και οι αδυναμίες στην πλατφόρμα λειτουργίας επηρεάζουν την αξιοπιστία των αποτελεσμάτων. Επομένως, οι κυβερνοεπιθέσεις σε συστήματα τεχνητής νοημοσύνης είναι πιο αποτελεσματικές λόγω των περιορισμών στους αλγορίθμους και της δυσκολίας αποκλεισμού των επιθέσεων [14].

3.2 Επιθέσεις σε Διαστημικά Συστήματα

Τα δορυφορικά συστήματα έχουν ήδη δεχθεί επιθέσεις από κράτη και εγκληματικές οργανώσεις. Οι πιο γνωστές επιθέσεις στρέφονται εναντίον κυβερνητικών και εταιρικών δορυφορικών συστημάτων. Αυτές οι επιθέσεις αποδεικνύουν ότι ακόμα και τα διαστημικά έργα με μεγάλο προϋπολογισμό δεν διαθέτουν την κατάλληλη κυβερνοασφάλεια για να αντιμετωπίσουν τους χάκερς.



Σχήμα 4: Cyber-Attacks by Type.

Το παραπάνω διάγραμμα απεικονίζει την κατανομή των κυβερνοεπιθέσεων ανά τύπο. Η πιο συνηθισμένη μορφή επίθεσης είναι το Malware, που αντιπροσωπεύει το 26% των συνολικών επιθέσεων. Ακολουθούν η Ransomware και τα Data Breaches με 18% ενώ το Malicious Hacking και το Phishing μοιράζονται την τρίτη θέση με 11% το καθένα. Οι Worm, τα Human Error, DDoS και Bot Attacks αντιπροσωπεύουν το 4% η καθεμία.. Αυτό το διάγραμμα υποδεικνύει την ποικιλομορφία των κυβερνοαπειλών και την ανάγκη για πολλαπλές στρατηγικές ασφάλειας για την αντιμετώπισή τους όπως θα αναλυθούν και παρακάτω.

3.2.1 Επιθέσεις στις Δορυφορικές Επικοινωνίες IP

Μερικές από τις πιο ενδιαφέρουσες επιθέσεις κατά δορυφόρων μέχρι σήμερα είχαν να κάνουν με το ενδιαφέρον των χάκερς για την κατάρρευση του διαστημικού συστήματος, αλλά και με την τεχνολογία που διευκολύνεται από αυτό. Το λογισμικό ασφαλείας Kaspersky Labs αποκάλυψε ότι η ομάδα κυβερνοκατασκόπων με έδρα τη Ρωσία, Turla, εισήλθε παράνομα σε πάροχο δορυφορικού διαδικτύου για να κρύψει κυβερνοκατασκοπικές επιχειρήσεις εναντίον χωρών από τις ΗΠΑ.

Χρησιμοποιώντας μια κεραία, η Turla μπορούσε να εντοπίζει τις διευθύνσεις IP από τους χρήστες του διαδικτύου δορυφόρων και στη συνέχεια να ξεκινάει μια σύνδεση TCP/IP από την κλεμμένη διεύθυνση IP. Η Turla μπορεί να αποφύγει τις κακόβουλες επιχειρήσεις εκμεταλλευόμενη την κλεμμένη διεύθυνση IP του δορυφόρου. Η επίθεση δεν είναι εύκολα ανιχνεύσιμη εξαρτάται από το εάν ο χάκερ και ο νόμιμος χρήστης χρησιμοποιούν την ίδια διεύθυνση IP ταυτόχρονα. Επειδή τόσο το θύμα όσο και οι μηχανές του επιτιθέμενου θα έχουν την ίδια διεύθυνση IP, η επίθεση θα είναι αόρατη και απίθανο να εντοπιστεί από συστήματα ανίχνευσης διείσδυσης [15].

Οι τεχνικές των κυβερνοεπιθέσεων περιλαμβάνουν αρκετές διαφορετικές προσεγγίσεις, όπως η απόσπαση σήματος, η κατάληψη ελέγχου, data corruption, επιθέσεις απόρριψης υπηρεσίας (DDoS) και οι επιθέσεις σε Πρωτόκολλο Διαδικτύου (IP) δορυφόρου. Η προστασία από την απόσπαση σήματος είναι ιδιαίτερα σημαντική στους τηλεπικοινωνιακούς δορυφόρους. Χρησιμοποιώντας μια κεραία που συνδέεται σε έναν υπολογιστή, ο επιτιθέμενος μπορεί να εντοπίσει ένα κενό επικοινωνίας μεταξύ πομπού και δέκτη και να εκμεταλλευτεί το διαθέσιμο εύρος ζώνης. Με αυτόν τον τρόπο, το αντικείμενο θα χρησιμοποιηθεί για τη μετάδοση κακόβουλων πληροφοριών, ακόμη και αν ο πραγματικός κίνδυνος προέρχεται από πιθανές παρεμβολές στην επικοινωνία ή απόρριψη των υπηρεσιών. Μια άλλη ευπάθεια σχετίζεται με το σύνδεσμο Διέλευσης και Ελέγχου (C2) που ανακτά δεδομένα από τα υποσυστήματα.

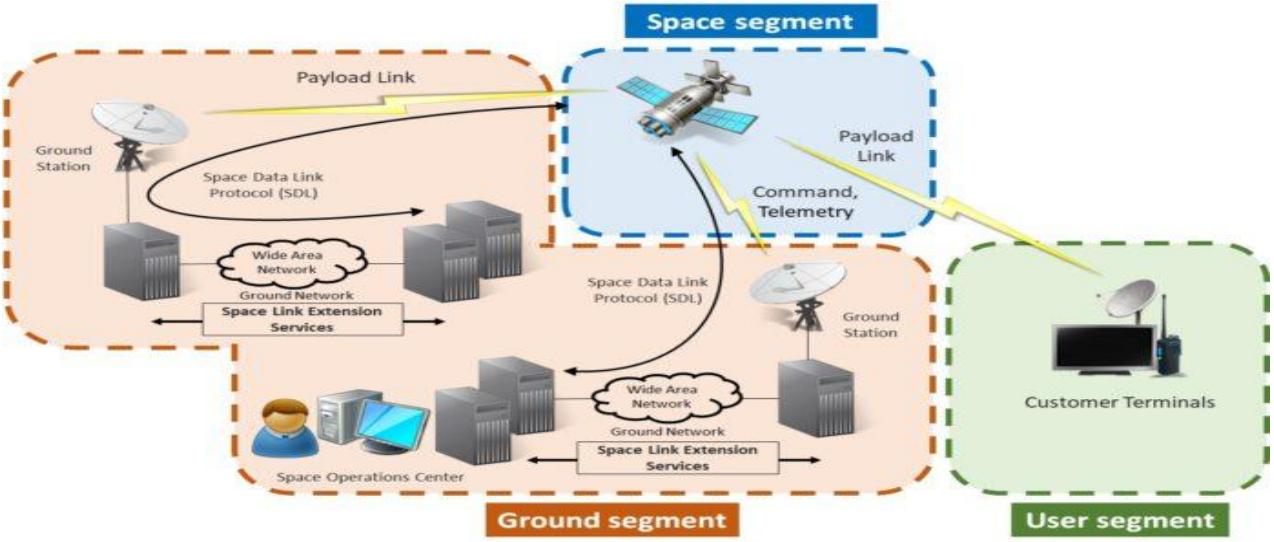
Ο σύνδεσμος διέλευσης και ελέγχου (Command and Control Link - C2 Link) είναι ένα κρίσιμο τμήμα των διαστημικών συστημάτων που χρησιμοποιείται για τη διαχείριση και τον έλεγχο δορυφόρων και άλλων διαστημικών σκαφών. Ο σύνδεσμος αυτός επιτρέπει τη μετάδοση εντολών από τους επίγειους σταθμούς προς το διαστημικό σκάφος και την αποστολή δεδομένων από το διαστημικό σκάφος προς τη Γη. Ο C2 Link διασφαλίζει ότι οι χειριστές μπορούν να ελέγχουν τη λειτουργία του δορυφόρου, να προσαρμόζουν την πορεία του, να ενεργοποιούν και να απενεργοποιούν συστήματα και να λαμβάνουν κρίσιμα δεδομένα και αναφορές κατάστασης.

Μια εισβολή στο σύνδεσμο C2 ενός επιχειρησιακού δορυφόρου μπορεί να καταστήσει δυνατή την ανάληψη του ελέγχου του δορυφόρου από τον επιτιθέμενο. Αυτό θα μπορούσε να οδηγήσει σε μη επιθυμητή αλλαγή της τροχιάς ή της θέσης με συνέπεια την απενεργοποίηση των οπτικών μέσων σε έναν δορυφόρο οπτικής παρακολούθησης. Ένας εισβολέας στο σύνδεσμο C2 μπορεί επίσης να αναλάβει τον έλεγχο ολόκληρου του επικοινωνιακού υποσυστήματος του δορυφόρου, με αποτέλεσμα την παρακολούθηση δεδομένων από τον ανώνυμο χρήστη ή τη διαφθορά τους. Μια επίθεση απόρριψης υπηρεσιών προς το έδαφος και το σύνδεσμο C2 μπορεί να μπλοκάρει τον έλεγχο των λειτουργιών του δορυφόρου και τη συλλογή δεδομένων. Οι ομάδες χάκερ μπορούν επίσης να εντοπίσουν διευθύνσεις IP από δορυφόρους που παρέχουν σύνδεση στο διαδίκτυο και στη συνέχεια να προβούν σε σύνδεση TCP/IP από μια κλεμμένη διεύθυνση IP.

Τέλος , ανεξάρτητα από το πόσο αόρατες μπορούν να είναι οι κυβερνοεπιθέσεις με βάση το διάστημα, μπορούν να προκαλέσουν σοβαρές ζημιές στις λειτουργίες του τελικού χρήστη. Ένας επιτιθέμενος μπορεί να παρακολουθεί πακέτα από τον χρήστη του δορυφόρου ή να εισάγει δεδομένα στο σύστημα χρήστη που συνδέεται με την IP διεύθυνση. Η λανθασμένη εισαγωγή δεδομένων σε ένα στοιχείο του υποσταθμού μπορεί να προκαλέσει μια επίθεση, προκαλώντας ζημιά και διακοπή λειτουργίας στο δίκτυο.

3.2.2 Επιθέσεις στους Δορυφόρους GPS

Μια άλλη κυβερνοεπίθεση βασίστηκε σε δορυφορικά συστήματα GPS, τα οποία βασίζονται σε δορυφόρους για να τριγωνοποιήσουν συγκεκριμένες θέσεις στη Γη. Η εισαγωγή θορύβου στο φάσμα του δέκτη του δορυφόρου GPS μπορεί να προκαλέσει την αποτυχία ενός δέκτη GPS στη Γη να παρέχει ανάγνωση. Αυτή είναι μια τεχνική που αποκαλείται jamming. Η Ρωσία έχει εγκαταστήσει jammers GPS σε πάνω από 250.000 κινητά τηλεφωνικά κέντρα για να διακόψει την καθοδήγηση εισερχομένων πυραύλων από τις ΗΠΑ. Ενώ οι επιθέσεις jamming GPS έχουν χρησιμοποιηθεί στο παρελθόν και δεν θεωρούνται απαραίτητα κυβερνοεπιθέσεις, το GPS spoofing είναι μια κυβερνοεπίθεση λόγω της παραπλάνησης του σήματος GPS. Το GPS spoofing είναι πολύ πιο επικίνδυνο από το jamming, καθώς στην ουσία παραπληροφορεί το GPS και το κάνει να πιστεύει ότι λειτουργεί σωστά. Η εμπιστοσύνη στη συσκευή δεν καταρρέει για ένα spoof, το οποίο



Σχήμα 5:Αρχιτεκτονική δορυφορικού συστήματος [15].

Η παραπάνω εικόνα μας δείχνει το μοντέλο 3-τμημάτων ενός συστήματος δορυφορικών επικοινωνιών

Τμήμα διαστήματος:

- Δορυφόρος: Το κεντρικό στοιχείο του τμήματος διαστήματος που επικοινωνεί τόσο με το τμήμα εδάφους όσο και με το τμήμα χρηστών.
- Σύνδεσμος Φορτίου: Το κανάλι επικοινωνίας μεταξύ του δορυφόρου και των επίγειων σταθμών στο τμήμα εδάφους.
- Εντολές, Τηλεμετρία: Τα κανάλια που χρησιμοποιούνται για την αποστολή εντολών στον δορυφόρο και την παραλαβή τηλεμετρικών δεδομένων από αυτόν.

Τμήμα Εδάφους:

- Επίγειος Σταθμός: Εγκαταστάσεις εξοπλισμένες με κεραίες και άλλο εξοπλισμό για την επικοινωνία με τον δορυφόρο.
- Πρωτόκολλο Σύνδεσης Δεδομένων Διαστήματος (SDLP): Πρωτόκολλα που χρησιμοποιούνται για την επικοινωνία μεταξύ του δορυφόρου και των επίγειων σταθμών.
- Ευρείας Περιοχής Δίκτυο (WAN): Η δικτυακή υποδομή που συνδέει διάφορα στοιχεία του τμήματος εδάφους.
- Υπηρεσίες Επέκτασης Διαστημικής Σύνδεσης: Υπηρεσίες που διευκολύνουν την επέκταση της επικοινωνίας διαστημικής σύνδεσης μέσω επίγειων δικτύων.
- Κέντρο Λειτουργίας Διαστήματος: Το κεντρικό κέντρο όπου διαχειρίζονται οι λειτουργίες που σχετίζονται με τον δορυφόρο, συμπεριλαμβανομένης της επεξεργασίας δεδομένων και του ελέγχου εντολών.

Τμήμα Χρηστών

- Τερματικά Πελατών: Οι τελικές συσκευές των χρηστών που είναι εξοπλισμένες για να λαμβάνουν δεδομένα από τον δορυφόρο.
- Επίγειος Σταθμός: Μέρος του τμήματος χρηστών, αυτοί οι σταθμοί διευκολύνουν την λήψη και αποστολή δεδομένων μεταξύ των τερματικών πελατών και του δορυφόρου.

Το jamming περιλαμβάνει τη χρήση μιας συσκευής για τη διακοπή ενός στοχευμένου ραδιοσυχνοτικού σήματος μέσω παρεμβολής. Οι σύνδεσμοι δεδομένων είναι γενικώς ευάλωτοι και το jamming χρησιμοποιείται σε μεγάλη συχνότητα. Αυτό σημαίνει ότι κάποιος μπορεί να χρησιμοποιήσει ένα ειδικό μηχάνημα για να διακόψει το σήμα που χρησιμοποιείται για την επικοινωνία. Αρκετές εταιρείες έχουν αναπτύξει εξοπλισμό για να αντιμετωπίσουν αυτά τα προβλήματα, αλλά πρέπει να λάβουν υπόψη τους ότι υπάρχει ακόμα κίνδυνος. Ακόμα και αν οι κατασκευαστές έχουν προβλέψει αυτά τα προβλήματα, μπορεί ακόμα να συμβούν. Ένα απλό παράδειγμα είναι η παρεμβολή σε ένα drone με αποτέλεσμα να χαθεί η επικοινωνία για λίγο και να καταλήξει σε μια απαγορευμένη περιοχή. Αυτά τα προβλήματα δείχνουν ότι υπάρχουν ακόμα κενά στην ασφάλεια που πρέπει να διορθωθούν. Άλλη μια παρόμοια περίπτωση που μπορεί να συμβεί είναι να πέσει ένα drone και να προκαλέσει τραυματισμό σε ανθρώπους. Αυτές οι επιθέσεις τύπου jamming συνέβησαν το 2016 στη Νότια Κορέα με θύτη τη γείτονα χώρα Βόρεια Κορέα. Το jamming μπορεί να πάρει πολλές μορφές και να στοχεύει διαφορετικά συστήματα. Μπορεί να επηρεάσει δορυφορικά σήματα, στρατιωτικές επικοινωνίες, συστήματα πλοήγησης όπως το GPS και συστήματα ελέγχου drones. Για παράδειγμα, τα συστήματα GPS είναι συχνός στόχος, διότι η διακοπή τους μπορεί να προκαλέσει σοβαρά προβλήματα στην πλοήγηση και τον συντονισμό. Στον στρατιωτικό τομέα, το jamming μπορεί να χρησιμοποιηθεί για να αποτρέψει τις επικοινωνίες του εχθρού, να διακόψει τη λειτουργία των drones ή να παραπλανήσει τα όπλα καθοδηγούμενα από GPS [17].Οι συσκευές jamming ποικίλλουν σε μέγεθος και ισχύ. Μερικές είναι μικρές και φορητές, κατάλληλες για χρήση σε τοπικό επίπεδο, ενώ άλλες είναι μεγαλύτερες και ισχυρότερες, ικανές να

διακόψουν σήματα σε μεγαλύτερες αποστάσεις. Η χρήση τέτοιων συσκευών είναι παράνομη σε πολλές χώρες, καθώς μπορεί να προκαλέσει σοβαρές διαταραχές στην καθημερινή ζωή, από τις επικοινωνίες έκτακτης ανάγκης μέχρι τις καθημερινές επαγγελματικές δραστηριότητες. Γενικά στη λειτουργία της μια τέτοια συσκευή διαθέτει προστασία τύπου SSL έτσι ώστε κανένας να μη μπορεί να αποκτήσει πρόσβαση σε αυτή είτε για να την εκμεταλλευτεί είτε για να την αχρηστέψει. Συνήθως εκπέμπουν σήμα μέχρι -75dBm το οποίο δίνει εύρος παρεμβολής μέχρι 20 μέτρα. Οι μπαταρίες τους κρατάνε μέχρι 1 ώρα λειτουργίας και καλύπτουν τα διαφορετικά εύρη λειτουργίας ανάλογα την Ήπειρο [19].

Για την αντιμετώπιση του jamming, οι εταιρείες και οι κυβερνήσεις αναπτύσσουν τεχνολογίες και στρατηγικές ανθεκτικές σε τέτοιες επιθέσεις. Αυτές περιλαμβάνουν την ανάπτυξη αντί-jamming τεχνολογιών που μπορούν να ανιχνεύουν και να μετριάζουν τις επιπτώσεις του jamming. Οι στρατιωτικές εφαρμογές συχνά χρησιμοποιούν συστήματα επικοινωνίας ειδικά διαμορφωμένα για την αποφυγή του jamming μέσω προσαρμοστικών φίλτρων, ειδικών διαμορφώσεων σήματος και εξελιγμένη κρυπτογράφηση για την προστασία των δεδομένων. Η ανάπτυξη και η εφαρμογή ανθεκτικών τεχνολογιών είναι κρίσιμη για την προστασία από αυτές τις επιθέσεις. Παρά τα μέτρα που λαμβάνονται, η συνεχής εξέλιξη των τεχνολογιών jamming απαιτεί συνεχή επιτήρηση και καινοτομία στην κυβερνοασφάλεια [21].

Το spoofing είναι μια μορφή επίθεσης όπου ένας κοντινός πομπός ραδιοφωνικών κυμάτων στέλνει παραποιημένες πληροφορίες, όπως λανθασμένες συντεταγμένες GPS, στον δέκτη για να τον εξαπατήσει. Το spoofing είναι ευρέως διαδεδομένο στις συνδέσεις GPS και μπορεί να επηρεάσει επίσης συνδέσεις ADS-B το διαδίκτυο και άλλα συστήματα πλοήγησης. Συχνά συνδέεται με το jamming του GPS και έχει προκαλέσει πολλά προβλήματα κυβερνοασφαλείας για τα UAV (unmanned aerial vehicles), καθώς πολλά από αυτά βασίζονται σε αυτές τις πληροφορίες για την πλοήγησή τους. Παρόλο που το spoofing δεν περιορίζεται αποκλειστικά στο GPS, μπορεί εύκολα να εκμεταλλευτεί το ενσωματωμένο σύστημα σταθεροποίησης ή το αυτόματο σχέδιο πτήσης ενός UAV, δίνοντάς του την εντύπωση ότι βρίσκεται σε μια μη επιθυμητή θέση ή ταξιδεύει σε μια μη επιθυμητή κατεύθυνση. Αυτό μπορεί να οδηγήσει σε σοβαρά προβλήματα, καθώς το UAV μπορεί να πρέπει να διορθώσει την πορεία του, συχνά με επικίνδυνες συνέπειες. Το spoofing GPS έχει προκαλέσει σοβαρά προβλήματα ασφαλείας σε πολλά UAV, καθώς πολλά βασίζονται σε αυτές τις πληροφορίες για να πλοηγηθούν. Το spoofing δεν περιορίζεται μόνο σε στρατιωτικές εφαρμογές. Στον εμπορικό τομέα, έχουν υπάρξει αναφορές για spoofing σε εμπορικά πλοία, όπου παραποιημένες πληροφορίες GPS έχουν οδηγήσει σε λανθασμένη πλοήγηση και επικίνδυνες καταστάσεις. Οι επιθέσεις spoofing μπορούν επίσης να επηρεάσουν τους χρήστες κινητών τηλεφώνων, καθώς πολλές εφαρμογές βασίζονται στις πληροφορίες GPS για την παροχή υπηρεσιών. Για την αντιμετώπιση του spoofing, αναπτύσσονται τεχνολογίες και στρατηγικές ανθεκτικές σε αυτές τις επιθέσεις. Αυτές περιλαμβάνουν τη χρήση ενισχυμένων δεκτών GPS που μπορούν να ανιχνεύουν και να απορρίπτουν επεξεργασμένα σήματα, την εφαρμογή συστημάτων ανίχνευσης spoofing που μπορούν να εντοπίζουν ανωμαλίες στις πληροφορίες πλοήγησης και την ανάπτυξη πρωτοκόλλων ασφάλειας που ενισχύουν την ανθεκτικότητα των συστημάτων πλοήγησης. Άρα το spoofing αποτελεί μια σοβαρή απειλή για την ασφάλεια των επικοινωνιών και της πλοήγησης. Η ανάπτυξη και εφαρμογή ανθεκτικών τεχνολογιών και στρατηγικών είναι κρίσιμη για την προστασία από αυτές τις επιθέσεις. Παρά τα μέτρα που λαμβάνονται, η συνεχής εξέλιξη των τεχνολογιών spoofing απαιτεί συνεχή επιτήρηση και καινοτομία στην κυβερνοασφάλεια.

Υπάρχουν πολλοί τρόποι για να γίνει spoofing σε ένα δορυφορικό σύστημα GPS. Ένας μηχανισμός είναι η αποδυνάμωση του δέκτη του δορυφόρου και η τροποποίηση του σήματος εξόδου από τον δορυφόρο. Μια άλλη ευκαιρία για το spoofing του δορυφορικού συστήματος GPS είναι μέσω μιας επίθεσης εισαγωγής ψευδών δεδομένων, όπου ένας εχθρός χρησιμοποιεί ένα προσομοιωτή σήματος GPS ή χρησιμοποιεί έναν ορισμένο από λογισμικό spoofer. Οι spoofer ορισμένοι από το λογισμικό είναι πιο αξιόπιστοι. Δουλεύουν εισάγοντας ένα δύσκολα ανιχνεύσιμο ψεύτικο σήμα πίσω από το πραγματικό σήμα. Σταδιακά, η ισχύς του ψεύτικου σήματος αυξάνεται μέχρι το σημείο που ο δέκτης νομίζει ότι το ψεύτικο σήμα είναι πραγματικά το πραγματικό σήμα. Ένα σύστημα που μπορεί να εκτελέσει μια επίθεση spoof με ορισμένο από λογισμικό κοστίζει περίπου 1.000-2.000 δολάρια ΗΠΑ για να κατασκευαστεί. [38]

Το 2017, η Αμερικανική Διοίκηση Ναυτιλίας ανέφερε την πρώτη επίθεση spoofing GPS σε πάνω από 20 πλοία στη Μαύρη Θάλασσα. Η αλληλογραφία μεταξύ ενός από τα επηρεασμένα πλοία και του κέντρου ελέγχου τους αντικατοπτρίζει ότι κατά τη διάρκεια της επίθεσης, η θέση GPS που εμφανιζόταν στο εργαλείο πλοήγησής τους έδειχνε μερικές φορές "χαμένη θέση GPS". Σε μια στιγμή κατά τη διάρκεια της επίθεσης, η παραποιημένη τοποθεσία έδειχνε ότι το πλοίο βρισκόταν κοντά στο αεροδρόμιο του Γκελέντζικ, αλλά στην πραγματικότητα βρισκόταν 25 ναυτικά μίλια μακριά από την αναφερόμενη θέση [39].

Σύμφωνα με μια μη κερδοσκοπική οργάνωση με το όνομα Ανθεκτική Πλοήγηση και Χρονολογία, η οποία παρακολουθεί περιστατικά GPS, οι αναφορές περί spoofing δεν είναι ασυνήθιστες στα ρωσικά ύδατα. Είναι ευρέως διαδεδομένο το σενάριο ότι μια άλλη επίθεση αυτού του τύπου χρησιμοποιήθηκε από τους Ιρανούς για να αιχμαλωτίσουν ένα αμερικανικό drone το Δεκέμβριο του 2011. Τον Σεπτέμβριο του 2011, οι Ιρανοί δήλωσαν ότι είχαν κατακτήσει μια νέα τεχνική για να χρησιμοποιήσουν το GPS spoofing. Αυτή η τεχνική επιδείχθηκε όταν κατάφεραν να αιχμαλωτίσουν ένα αμερικανικό drone RQ-170 Sentinel, ανακατασκευάζοντας τις συντεταγμένες του σήματος GPS για να κάνουν το drone να προσγειωθεί στο Ιράν αντί για τη βάση του στο Αφγανιστάν. Η αμερικανική στρατιωτική αεροπορία απέδωσε την αιχμαλωσία του drone σε βλάβη, αλλά δεν μπόρεσε να εξηγήσει πώς οι Ιρανοί έλαβαν το drone ανέπαφο [40].

3.2.3 Επιθέσεις στους Δημόσιους Δορυφόρους

Υπάρχουν πολλές περιπτώσεις κυβερνητικών διαδικτυακών επιθέσεων σε διαστημικά συστήματα που διαχειρίζεται η κυβέρνηση των ΗΠΑ. Στις 7 Οκτωβρίου 2007 και στις 23 Ιουλίου 2008, ένα δορυφορικό σύστημα παρατήρησης της Γης, το οποίο διαχειρίζονταν η NASA και το Κέντρο Γεωλογικής Έρευνας των ΗΠΑ, δέχτηκε παρεμβολή για "12 ή περισσότερα λεπτά". Η Επιτροπή Οικονομικής και Στρατιωτικής Ασφάλειας ΗΠΑ επιβεβαίωσε το 2011, αρκετά χρόνια μετά την επίθεση, ότι ο παρεμβαίνων δεν κατάφερε να εκτελέσει όλα τα βήματα για τον έλεγχο και του δορυφόρου. Στις 20 Ιουνίου 2008 και 22 Οκτωβρίου 2008, ο Terra EOS AM-1, ένας δορυφόρος παρατήρησης της Γης που διαχειρίζεται από τη NASA, παρεμβλήθηκε για 2 και 9 λεπτά και τις δύο περιπτώσεις, οι χάκερς κατάφεραν να αποκτήσουν έλεγχο και των δορυφόρων, αλλά δεν εξέδωσαν εντολές. Αυτές οι επιθέσεις αποδίδονται στην Κίνα και οι επιθέσεις ενδέχεται να είχαν ως στόχο την καταστρατήγηση της εικόνας των δορυφορικών εικόνων, τη μείωση της μετάδοσης των εικόνων ή την εξαγωγή εικόνων [26].

Ένα άλλο παράδειγμα κυβερνητικής διαστημικής παραβίασης ήταν το 2011, όταν χάκερς απέκτησαν πλήρη λειτουργικό έλεγχο επί του Εργαστηρίου Κινητικής Προώθησης (JPL) της NASA. Αυτό επιτεύχθηκε με την κλοπή πάνω από 150 χρήστες της NASA .Οι χάκερς που είχαν πρόσβαση στα συστήματα του Εργαστηρίου Κινητικής Προώθησης της NASA μπορούσαν να κάνουν τα εξής: (1) να αλλάξουν, να αντιγράψουν ή να διαγράψουν σημαντικά αρχεία, (2) να προσθέσουν, να τροποποιήσουν ή να διαγράψουν λογαριασμούς χρηστών για κρίσιμα συστήματα του Εργαστηρίου Κινητικής Προώθησης, (3) να ανεβάσουν εργαλεία χάκερ για να κλέψουν λογαριασμούς χρήστη και να επηρεάσουν άλλα συστήματα της NASA, και (4) να αλλάξουν τα καταγραφικά συστήματα για να κρύψουν τις δραστηριότητές τους. Δεν είναι σαφές ποια συγκεκριμένη ζημιά μπορεί να έχει προκληθεί κατά τη διάρκεια του χρόνου που οι χάκερς είχαν τον λειτουργικό έλεγχο, αλλά το εύρος της πιθανής ζημιάς από αυτήν την επίθεση είναι προβληματικό [27].

Αυτά τα παραδείγματα αποτελούν μια μικρή δειγματοληψία ανάμεσα σε πολλές άλλες αναφερόμενες κυβερνητικές επιθέσεις κατά διαστημικών πόρων. Πέρα από τις πραγματικές κυβερνητικές επιθέσεις, υπάρχουν πειραματικά σενάρια και επιδεικτικές επιθέσεις σε διαστημικούς πόρους που έχουν αναφερθεί σε διάφορες αναφορές [29,31].

Οι επιπτώσεις των κυβερνοεπιθέσεων σε δημόσιους δορυφόρους είναι πολλές και σοβαρές γιατί δεν επηρεάζουν μόνο την ασφάλεια και την αξιοπιστία των διαστημικών συστημάτων αλλά και την εθνική ασφάλεια , την οικονομία και σε συνδυασμό αυτών και την κοινωνία. Όπως είδαμε και παραπάνω με τον ίδιο τρόπο επηρεάζουν και στρατιωτικές και πολιτικές επιχειρήσεις. Οι προκλήσεις για την αντιμετώπιση αυτών των επιθέσεων είναι εξίσου μεγάλες. Οι κυβερνήσεις και οι οργανισμοί πρέπει να επενδύσουν σε προηγμένα συστήματα κυβερνοασφάλειας και να αναπτύξουν ανθεκτικές τεχνολογίες για την προστασία των διαστημικών συστημάτων. Αυτό περιλαμβάνει την ενίσχυση της κρυπτογράφησης, την εφαρμογή πολυπαραγοντικής ταυτοποίησης και την ανάπτυξη συστημάτων ανίχνευσης και απόκρισης σε πραγματικό χρόνο για την αντιμετώπιση των απειλών. Η διεθνής συνεργασία είναι επίσης κρίσιμη, καθώς οι δορυφόροι συχνά εξυπηρετούν παγκόσμιες ανάγκες και οι επιθέσεις σε αυτούς μπορούν να έχουν διεθνείς συνέπειες. Η ανταλλαγή πληροφοριών, η ανάπτυξη κοινών προτύπων ασφαλείας και η διεξαγωγή κοινών ασκήσεων μπορούν να συμβάλλουν στην αποτελεσματική αντιμετώπιση των κυβερνοαπειλών στους διαστημικούς πόρους.

Με την αυξανόμενη εξάρτηση από τα διαστημικά συστήματα, η προστασία τους καθίσταται ολοένα και πιο κρίσιμη. Οι κυβερνήσεις, οι διαστημικές υπηρεσίες και οι ιδιωτικές εταιρείες πρέπει να συνεργαστούν για την ενίσχυση της ασφάλειας των διαστημικών υποδομών και την εξασφάλιση της συνεχούς λειτουργίας τους προς όφελος της κοινωνίας και της οικονομίας.

3.2.4 Επιθέσεις σε Διαστημικά Συστήματα Εδάφους

Η ασφάλεια των διαστημικών συστημάτων εδάφους αποτελεί κρίσιμο παράγοντα για την αποτελεσματική λειτουργία και προστασία των διαστημικών αποστολών. Τα συστήματα αυτά περιλαμβάνουν τους επίγειους σταθμούς ελέγχου, τα δίκτυα επικοινωνιών και τους διαχειριστικούς υπολογιστές που υποστηρίζουν τις λειτουργίες των διαστημικών σκαφών. Οι επιθέσεις σε αυτά τα συστήματα μπορούν να έχουν σοβαρές συνέπειες, όπως απώλεια δεδομένων, διακοπή λειτουργιών

και καταστροφή κρίσιμων υποδομών. Παρακάτω ακολουθούν οι βασικές κατηγορίες επιθέσεων που μπορούν να στοχεύσουν τα διαστημικά συστήματα εδάφους.

Οι επίγειοι σταθμοί ελέγχου είναι υπεύθυνοι για την παρακολούθηση και τον έλεγχο των δορυφόρων και άλλων διαστημικών σκαφών. Οι επιθέσεις σε αυτούς τους σταθμούς μπορούν να περιλαμβάνουν παρεμβολές σημάτων (jamming), όπου οι επιτιθέμενοι χρησιμοποιούν εξοπλισμό για να παρεμβάλουν στα σήματα επικοινωνίας μεταξύ του επίγειου σταθμού και του διαστημικού σκάφους, προκαλώντας διακοπές στη μετάδοση δεδομένων ή απώλεια ελέγχου. Επίσης, μπορούν να πραγματοποιηθούν κακόβουλες αναλήψεις ελέγχου (hijacking) μέσω επιθέσεων phishing ή εκμεταλλευόμενοι ευπάθειες στο λογισμικό, αποκτώντας πρόσβαση στα συστήματα ελέγχου και εκτελώντας μη εξουσιοδοτημένες εντολές. Επιπλέον, είναι δυνατές οι επιθέσεις τύπου man-in-the-middle, όπου οι επιτιθέμενοι παρεμβαίνουν μεταξύ του επίγειου σταθμού και του δορυφόρου, υποκλέπτοντας και τροποποιώντας τα δεδομένα επικοινωνίας [22].

Τα δίκτυα επικοινωνιών που συνδέουν τους επίγειους σταθμούς με τους δορυφόρους και τα άλλα διαστημικά σκάφη αποτελούν κρίσιμο σημείο για επιθέσεις. Οι επιθέσεις DDoS (Distributed Denial of Service) στοχεύουν στην υπερφόρτωση των δικτύων με υπερβολικό αριθμό αιτημάτων, προκαλώντας διακοπές στην επικοινωνία και την υπηρεσία. Παράλληλα, οι παραβιάσεις δεδομένων εκμεταλλεύονται ευπάθειες στα δίκτυα για να αποκτήσουν πρόσβαση σε εμπιστευτικά δεδομένα που μεταδίδονται μεταξύ του επίγειου σταθμού και του δορυφόρου [24].

Οι διαχειριστικοί υπολογιστές που υποστηρίζουν τις λειτουργίες των διαστημικών συστημάτων είναι επίσης στόχος επιθέσεων. Οι επιτιθέμενοι μπορούν να εισαγάγουν κακόβουλο λογισμικό (malware) στους διαχειριστικούς υπολογιστές, προκαλώντας απώλεια δεδομένων ή βλάβες στα συστήματα. Επίσης, με τη χρήση ransomware, οι επιτιθέμενοι μπορούν να κρυπτογραφήσουν τα δεδομένα των διαχειριστικών υπολογιστών και να απαιτήσουν λύτρα για την αποκατάστασή τους. Οι εσωτερικές απειλές (insider threats) από εργαζόμενους που έχουν πρόσβαση στα συστήματα, είτε λόγω λάθους είτε λόγω κακόβουλης πρόθεσης, μπορούν να προκαλέσουν σημαντικές ζημιές [25].

Η φυσική πρόσβαση σε εγκαταστάσεις των επίγειων σταθμών και των δικτύων μπορεί να επιτρέψει στους επιτιθέμενους να πραγματοποιήσουν καταστροφικές ενέργειες. Οι επιθέσεις σαμποτάζ περιλαμβάνουν τη φυσική βλάβη στις υποδομές των σταθμών ελέγχου, όπως καταστροφή εξοπλισμού ή κοπή καλωδίων επικοινωνίας. Επίσης, η φυσική κλοπή δεδομένων είναι δυνατή μέσω της πρόσβασης σε υπολογιστές ή συσκευές αποθήκευσης, επιτρέποντας την κλοπή εμπιστευτικών δεδομένων.

Η κοινωνική μηχανική αποτελεί σημαντική απειλή για τα διαστημικά συστήματα εδάφους, καθώς εκμεταλλεύεται την ανθρώπινη αδυναμία. Μέσω απατηλών μηνυμάτων ηλεκτρονικού ταχυδρομείου ή άλλων μορφών επικοινωνίας (phishing), οι επιτιθέμενοι μπορούν να παραπλανήσουν το προσωπικό και να αποκτήσουν πρόσβαση σε κρίσιμα συστήματα. Οι επιθέσεις εξαπάτησης (pretexting) περιλαμβάνουν την προσποίηση εξουσιοδοτημένων χρηστών ή τεχνικών, αποκτώντας έτσι πρόσβαση σε ευαίσθητες πληροφορίες ή συστήματα [28].

Αν και οι επιθέσεις αυτές δεν στοχεύουν άμεσα στα συστήματα εδάφους, οι αντί-δορυφορικές επιθέσεις (ASAT) και οι ηλεκτρομαγνητικές επιθέσεις (EMP) μπορούν να προκαλέσουν σοβαρές συνέπειες. Οι αντί-δορυφορικές επιθέσεις μπορούν να απενεργοποιήσουν πολλές δυνατότητες ενός δορυφόρου καθώς ακόμα και να τον καταστρέψουν, επηρεάζοντας την επικοινωνία και τον έλεγχο

από τη Γη. Οι ηλεκτρομαγνητικές επιθέσεις μπορούν να προκαλέσουν εκτεταμένες ζημιές στις ηλεκτρονικές συσκευές των επίγειων σταθμών[32].

Η προστασία των διαστημικών συστημάτων εδάφους από τις παραπάνω επιθέσεις απαιτεί μια σύνθετη προσέγγιση στην ασφάλεια. Αυτή περιλαμβάνει την εφαρμογή ισχυρών μέτρων κυβερνοασφάλειας, την εκπαίδευση του προσωπικού, την υιοθέτηση φυσικών μέτρων προστασίας και την ανάπτυξη στρατηγικών ανίχνευσης και απόκρισης σε περιστατικά. Η συνεχής αξιολόγηση και βελτίωση των πρακτικών ασφάλειας είναι απαραίτητη για την αντιμετώπιση των συνεχώς εξελισσόμενων απειλών.

4

Ευπάθειες και Επιθέσεις στα Διαστημικά Συστήματα

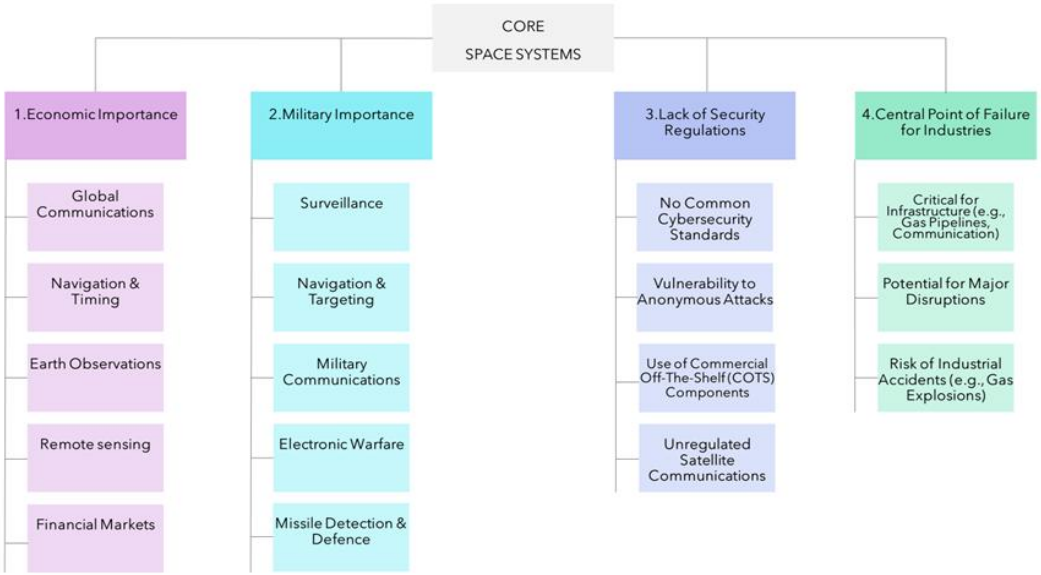
4.1 Λόγοι που τα διαστημικά συστήματα αποτελούν στόχο επίθεσης

Τα διαστημικά συστήματα είναι κρίσιμα για την υποστήριξη της παγκόσμιας οικονομίας και της στρατιωτικής παρουσίας, και αποτελούν ένα κεντρικό σημείο αποτυχίας για πολλές βιομηχανίες. Οι κυβερνοεπιθέσεις από διακριτικούς χάκερ έχουν ως στόχο να περιορίσουν την ανίχνευσή τους και να μεγιστοποιήσουν την ζημιά που προκαλούν.

Οι δορυφόροι και τα συστήματα ελέγχου εδάφους που υποστηρίζουν τις υποδομές αποτελούν ένα κεντρικό σημείο αποτυχίας για το εμπόριο και άλλες βιομηχανίες. Χωρίς τα διαστημικά συστήματα, πολλές βιομηχανίες δεν μπορούν να λειτουργήσουν αποτελεσματικά. Για παράδειγμα, οι εταιρείες διανομής φυσικού αερίου βασίζονται σε δορυφόρους για τις επικοινωνίες από απομακρυσμένους αγωγούς, ώστε να κατανοήσουν την κατάσταση των συστημάτων τους. Οι χάκερ που παραβιάζουν έναν δορυφόρο επικοινωνιών μπορούν να προκαλέσουν εκρήξεις αγωγών αν μπλοκάρουν τις κλήσεις συντήρησης από αυτούς τους απομακρυσμένους αγωγούς προς το κέντρο εντολών του διανομέα φυσικού αερίου. Υπάρχουν διάφοροι τρόποι επίθεσης για να ανασταλεί η λειτουργία ενός διαστημικού συστήματος, δύο εκ των οποίων είναι ο κατασκευαστής του εξοπλισμού διαστημικών συστημάτων και ο διαχειριστής ή η εταιρεία διαχείρισης των διαστημικών συστημάτων . Τα διαστημικά συστήματα, όπως οι δορυφόροι και τα συστήματα ελέγχου τους, είναι συνήθως περίπλοκα εξοπλισμένα με συστήματα επικοινωνίας .Παρ' όλα αυτά, τα πρότυπα κυβερνοασφάλειας για τα διαστημικά συστήματα δεν ρυθμίζονται από κάποιον επίσημο φορέα, και η έλλειψη κανονισμών σημαίνει ότι οι δορυφόροι δεν έχουν κοινά πρότυπα κυβερνοασφάλειας και μπορεί να χρησιμοποιηθούν για κυβερνοεπιθέσεις με ατιμωρησία ή ανωνυμία. Αυτό είναι διαφορετικό από άλλες βιομηχανίες, όπως τα ηλεκτρικά συστήματα. Η Διεθνής Ένωση Τηλεπικοινωνιών (ITU), ένας οργανισμός των Ηνωμένων Εθνών, ρυθμίζει τις συχνότητες των δορυφορικών επικοινωνιών για να αποτρέψει τις παρεμβολές και καταγράφει τις τροχιές των δορυφόρων, αλλά πέρα από αυτά τα θέματα, υπάρχουν λίγα πρότυπα. Αυτή τη στιγμή, δεν υπάρχουν φορείς που να περιορίζουν τη χρήση των δορυφόρων και δεν υπάρχει κάποιος οργανισμός που να παρακολουθεί τη χρήση των δορυφόρων. Λόγω αυτού του κενού, είναι πιθανό κάποιοι δορυφόροι να χρησιμοποιούνται ως βάση για κυβερνοεπιχειρήσεις ή για άλλους κακόβουλους σκοπούς[33].

Ορισμένα συστήματα απαιτούν πολλούς κατασκευαστές με διάφορες ειδικότητες για να αναπτύξουν πολλαπλές τεχνολογίες και έναν ενσωματωτή συστημάτων για να συνδυάσει όλα τα εξαρτήματα ώστε να λειτουργούν ως ένα. Οι πολλαπλοί προμηθευτές παρέχουν διάφορα σημεία πρόσβασης για έναν χάκερ ώστε να αποκτήσει πρόσβαση σε έναν δορυφόρο. Κάθε επιπλέον προμηθευτής παρέχει μια επιπλέον ευκαιρία να παραβιαστεί ένας δορυφόρος. Για αυτά τα πολύπλοκα συστήματα, θα υποθέταμε ότι υπάρχουν αυστηρά πρωτόκολλα ασφαλείας. Ωστόσο, δεν είναι όλοι οι δορυφόροι τόσο εξελιγμένοι. Μια πρόσφατη τάση περιλαμβάνει την εκτόξευση χαμηλού κόστους δορυφόρων που χρησιμοποιούν τεχνολογία εμπορικών προϊόντων (COTS). Λαμβάνοντας υπόψη τη φύση των COTS, είναι πιθανό τα εξαρτήματα, όπως λειτουργικά συστήματα ανοιχτού κώδικα γεμάτα με ευπάθειες ασφαλείας, να είναι κεντρικά για τη λειτουργία αυτών των δορυφόρων. Υπάρχουν σημαντικές ανησυχίες για την ασφάλεια αυτών των συστημάτων επειδή: 1) η ευρεία διανομή αυτών των προϊόντων σημαίνει ότι πολλοί άνθρωποι έχουν πρόσβαση στις συσκευές, έτσι ένας χάκερ μπορεί να αναλύσει εκτενώς τη συσκευή για ευπάθειες, και 2) τα προϊόντα COTS χρειάζεται να διατηρούνται ενεργά και να αναβαθμίζονται με ενημερώσεις ασφαλείας που συχνά δεν εφαρμόζονται από τους χρήστες. Κυβερνητικοί οργανισμοί είναι γνωστό ότι μισθώνουν εύρος ζώνης σε εμπορικούς δορυφόρους, και κάνοντας το αυτό θα μπορούσαν να εισάγουν ευπάθειες στο οικοσύστημα πληροφορικής του στρατού. Παρόλο που είναι απίθανο αυτό να είναι η πρώτη επιλογή ενός επιτιθέμενου για να απενεργοποιήσει έναν δορυφόρο, θα μπορούσε ακόμη και να είναι δυνατό για έναν κακόβουλο οργανισμό να χακάρει έναν μικρό δορυφόρο με πρόωση και να τον κατευθύνει να συγκρουστεί με άλλους δορυφόρους[34].

Τα διαστημικά συστήματα είναι ελκυστικοί στόχοι λόγω της ικανότητάς τους να λειτουργούν ως κεντρικό σημείο αποτυχίας για μεγάλα συστήματα, της έλλειψης κανονισμών ασφάλειας και της μεγάλης επιφάνειας επίθεσης που παρέχουν. Λαμβάνοντας υπόψη ότι τόσο μεγάλο μέρος της κρίσιμης υποδομής των ΗΠΑ εξαρτάται από τα διαστημικά συστήματα, θα ήταν λογικό για τους χάκερ να προσπαθήσουν να παραβιάσουν την κρίσιμη υποδομή μέσω αυτού του μέσου. Τα διαστημικά συστήματα δεν χρειάζονται ουσιαστικά διαφορετικά συστήματα ασφάλειας από άλλα κρίσιμα συστήματα· ωστόσο, χρειάζονται ιδιαίτερη προσοχή για την ασφάλεια, επειδή συχνά παραβλέπονται. Επιπλέον η ευθύνη της κυβερνοασφάλειας για τα διαστημικά συστήματα είναι εξαιρετικά περίπλοκη σε σύγκριση με άλλες βιομηχανίες, γεγονός που αφήνει περιθώρια για ασάφεια σχετικά με το ποιος πρέπει να ασφαλίσει αυτά τα ζωτικά συστήματα και πώς πρέπει να ασφαλιστούν [35].



Σχήμα 6: Βασικοί λόγοι για τη σημασία διαστημικών συστημάτων.

Η παραπάνω εικόνα παρουσιάζει τα βασικά διαστημικά συστήματα και τα χωρίζει σε τέσσερις κατηγορίες. Η πρώτη είναι η οικονομική σημασία, που δείχνει πώς τα διαστημικά συστήματα υποστηρίζουν παγκόσμιες επικοινωνίες, πλοήγηση, παρατηρήσεις της Γης, τηλεπισκόπηση και χρηματοοικονομικές αγορές. Η δεύτερη αφορά τη στρατιωτική σημασία, με έμφαση σε επιτήρηση, πλοήγηση, στρατιωτικές επικοινωνίες και άμυνα πυραύλων. Η τρίτη κατηγορία αναδεικνύει την έλλειψη κανονισμών ασφάλειας, επισημαίνοντας κινδύνους όπως η ευπάθεια σε ανώνυμες επιθέσεις και η χρήση μη ρυθμισμένων δορυφορικών επικοινωνιών. Τέλος, η τέταρτη κατηγορία αναφέρεται στο ότι τα διαστημικά συστήματα είναι κεντρικά σημεία για κρίσιμες υποδομές, με την αποτυχία τους να μπορεί να προκαλέσει μεγάλες διαταραχές ή βιομηχανικά ατυχήματα.

4.2 Περιστατικά και Επιθέσεις σε Διαστημικά Συστήματα

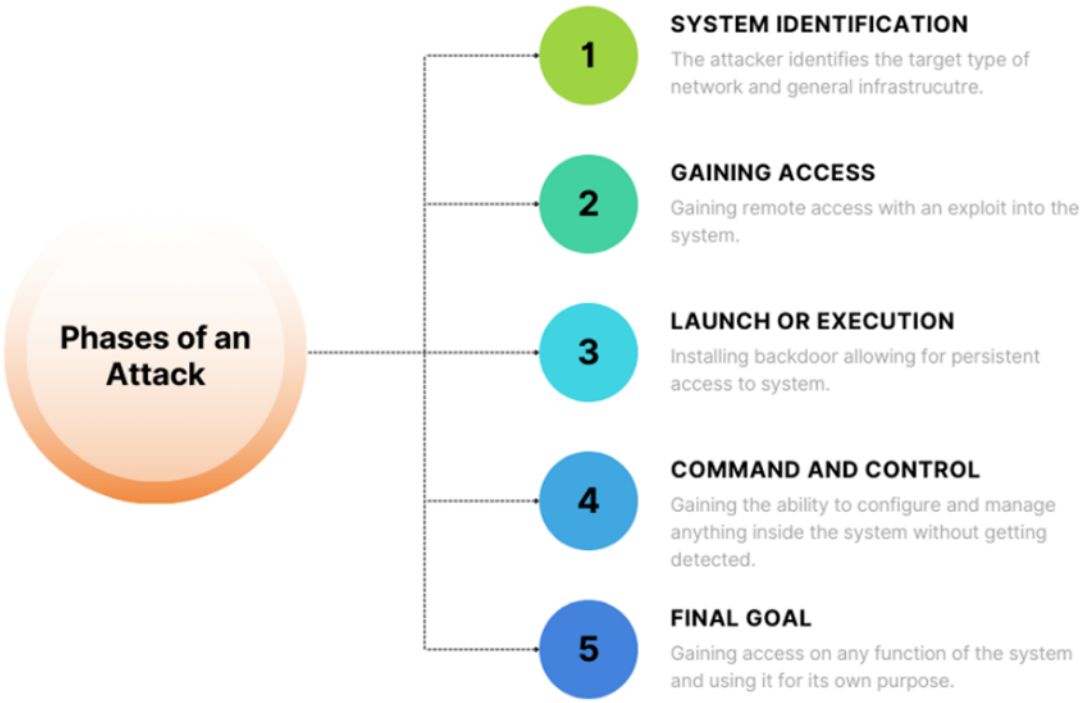
Τα διαστημικά περιουσιακά στοιχεία έχουν ήδη παραβιαστεί από κράτη και εγκληματικές οργανώσεις. Οι πιο γνωστές επιθέσεις έγιναν εναντίον κυβερνητικών και εταιρικών διαστημικών περιουσιακών στοιχείων. Αυτές οι επιθέσεις δείχνουν ότι ακόμη και καλά χρηματοδοτούμενα διαστημικά έργα δεν διαθέτουν την κατάλληλη κυβερνοασφάλεια για να αμυνθούν απέναντι στους χάκερ.

Ανάμεσα στις πιο ενδιαφέρουσες επιθέσεις που έχουν γίνει μέχρι τώρα σε δορυφόρους, δεν ήταν τόσο το ενδιαφέρον των χάκερ να παραβιάσουν το διαστημικό σύστημα, αλλά την τεχνολογία που υποστηριζόταν από αυτό. Η Kaspersky Labs ανακάλυψε ότι η ρωσική ομάδα κυβερνοκατασκοπείας, Turla, χάκαρε έναν πάροχο δορυφορικού ίντερνετ για να κρύψει τις επιχειρήσεις κατασκοπείας της εναντίον χωρών, από τις ΗΠΑ μέχρι το πρώην Ανατολικό Μπλοκ. Χρησιμοποιώντας μια κεραία εδάφους, η ομάδα Turla μπορούσε να ανιχνεύσει IP διευθύνσεις από χρήστες δορυφορικού ίντερνετ και στη συνέχεια να ξεκινήσει μια σύνδεση TCP/IP από τη κλεμμένη IP διεύθυνση. Η Turla μπορεί να καλύψει τις κακόβουλες ενέργειές της χρησιμοποιώντας τη κλεμμένη δορυφορική IP διεύθυνση. Η επίθεση δεν ανιχνεύεται εύκολα επειδή η επιχείρηση κατασκοπείας δεν χρειάζεται να επηρεάσει αντιληπτά την απόδοση του αθώου χρήστη· εξαρτάται

από το αν ο χάκερ και ο νόμιμος χρήστης χρησιμοποιούν ταυτόχρονα την ίδια IP διεύθυνση. Επειδή τόσο ο υπολογιστής του θύματος όσο και του επιτιθέμενου θα έχουν την ίδια IP διεύθυνση, η επίθεση θα είναι αθόρυβη και είναι απίθανο να εντοπιστεί από τα συστήματα ανίχνευσης εισβολών.

Ανεξάρτητα από το πόσο αόρατες μπορούν να είναι οι κυβερνοεπιθέσεις που βασίζονται στο διάστημα, μπορούν να προκαλέσουν σοβαρές ζημιές στις λειτουργίες του τελικού χρήστη. Οι χάκερ χρησιμοποιούν την τεχνική της Turla για να στοχεύσουν σε έναν απομακρυσμένο ηλεκτρικό υποσταθμό. Ένας επιτιθέμενος μπορεί να παρεμβάλει πακέτα επικοινωνίας από την IP διεύθυνση του θύματος ή να εισάγει δεδομένα στο σύστημα χρήστη που συνδέεται με την IP διεύθυνση. Μια τέτοια παρεμβολή δεδομένων σε ένα αυτόνομο drone μπορεί να οδηγήσει στην αναστροφή του συστήματος ή ακόμη και στην πτώση του αεροσκάφους [36].

Μια άλλη κυβερνοεπίθεση που βασίστηκε στο διάστημα έθεσε σε κίνδυνο τα συστήματα GPS, τα οποία εξαρτώνται από δορυφόρους για να τριγωνίσουν συγκεκριμένες θέσεις στη Γη. Η εισαγωγή θορύβου στο φάσμα λήψης του δορυφόρου GPS μπορεί να προκαλέσει την αποτυχία ενός δέκτη GPS στη Γη να παρέχει ανάγνωση. Αυτή είναι μια τεχνική γνωστή ως παρεμβολή σήματος. Οι επιθέσεις παρεμβολής GPS έχουν χρησιμοποιηθεί στο παρελθόν και δεν θεωρούνται απαραίτητα κυβερνοεπιθέσεις, η παραπληροφόρηση GPS είναι κυβερνοεπίθεση λόγω της διαστρέβλωσης του σήματος GPS. Η παραπληροφόρηση GPS είναι πολύ πιο επικίνδυνη από την παρεμβολή επειδή φαίνεται ότι το GPS λειτουργεί όπως αναμένεται.



Σχήμα 7: Φάσεις επίθεσης σε ένα πληροφοριακό σύστημα.

Η παραπάνω εικόνα παρουσιάζει τις φάσεις μιας επίθεσης σε ένα πληροφοριακό σύστημα. Αρχικά, ο επιτιθέμενος προσδιορίζει τον τύπο του δικτύου-στόχου και τη γενική του υποδομή. Στη συνέχεια, αποκτά απομακρυσμένη πρόσβαση στο σύστημα μέσω εκμετάλλευσης μιας ευπάθειας. Μετά την απόκτηση πρόσβασης, εγκαθιστά μια "πίσω πόρτα" (backdoor) που επιτρέπει συνεχή πρόσβαση στο σύστημα. Ακολούθως, αποκτά τη δυνατότητα να διαμορφώσει και να διαχειριστεί οτιδήποτε εντός του συστήματος χωρίς να ανιχνευτεί. Τέλος, ο επιτιθέμενος αποκτά πρόσβαση σε οποιαδήποτε λειτουργία του συστήματος και τη χρησιμοποιεί για τους δικούς του σκοπούς.

Υπάρχουν πολλοί τρόποι για να παραπλανηθεί ένας δορυφόρος GPS. Ένας μηχανισμός για να το πετύχει κάποιος αυτό είναι να τον δέκτη του δορυφόρου και να αλλάξει το σήμα εξόδου από τον δορυφόρο. Μια άλλη ευκαιρία είναι μέσω μιας επίθεσης εισαγωγής ψευδών δεδομένων, όπου ένας αντίπαλος χρησιμοποιεί έναν προσομοιωτή σήματος GPS ή χρησιμοποιεί έναν προγραμματιζόμενο σήματος που ορίζεται από λογισμικό. Οι προγραμματιζόμενοι σήματος που ορίζονται από λογισμικό είναι πιο αξιόπιστοι. Συγκεκριμένα λειτουργούν εισάγοντας ένα ψεύτικο σήμα που είναι μόλις ανιχνεύσιμο πίσω από το πραγματικό σήμα. Σταδιακά, η ισχύς του ψεύτικου σήματος αυξάνεται μέχρι που ο δέκτης νομίζει ότι το ψεύτικο σήμα είναι το πραγματικό. Οι επιθέσεις χρησιμοποιώντας παραπλάνηση με εξομοιωτή σήματος δεν είναι απλώς θεωρητικές ή πραγματοποιούνται σε εργαστήριο.

Αυτά τα περιστατικά αντιπροσωπεύουν ένα μικρό δείγμα από πολλές άλλες αναφερόμενες κυβερνοεπιθέσεις σε διαστημικά συστήματα. Πέρα από τις πραγματικές κυβερνοεπιθέσεις και επιδείξεις επιθέσεων σε διαστημικά συστήματα έχουν αναφερθεί σε διάφορες αναφορές.

4.3 Απειλές και Προκλήσεις Κυβερνοασφάλειας για Διαστημικά Συστήματα

Αρχικά, τα διαστημικά μέσα, όπως και όλη η άλλη τεχνολογία, ήταν αναλογικές συσκευές. Αυτά τα συστήματα δεν παρουσίαζαν τις ίδιες ευκαιρίες για χάκινγκ επειδή δεν είχαν λογισμικό με ευπάθειες κώδικα και την ικανότητα απομακρυσμένης πρόσβασης στο σύστημα. Καθώς η τεχνολογία προχωρούσε στην ψηφιακή εποχή, τα διαστημικά μέσα μετατράπηκαν επίσης σε ψηφιακά.

Όπως τα περισσότερα συστήματα εκείνης της εποχής, η κυβερνοασφάλεια γενικά δεν θεωρούνταν και σίγουρα δεν ήταν προτεραιότητα. Για παράδειγμα, όταν δημιουργήθηκε το TCP/IP, η ασφάλεια του πρωτοκόλλου δεν θεωρήθηκε πρόβλημα. Ακόμη και όταν απαιτούνταν και λαμβανόταν υπόψη η ασφάλεια, οι κατασκευαστές δεν έπαιρναν την κυβερνοασφάλεια σοβαρά. Ένα παράδειγμα που δείχνει αυτό το πρόβλημα είναι η δορυφορική συστοιχία Iridium, η οποία παρείχε δυνατότητες GPS στο Πεντάγωνο. Όταν δημιουργήθηκε η συστοιχία, δεν αναπτύχθηκαν ειδικές παράμετροι κυβερνοασφάλειας επειδή οι μηχανικοί πίστευαν ότι η τεχνολογία ήταν πολύ προηγμένη για να την παραβιάσει ένας χάκερ [37]. Αυτή η αφέλεια δεν ήταν μοναδική στους δημιουργούς της συστοιχίας Iridium, καθώς η ασφάλεια δεν θεωρούνταν ανησυχία για δεκαετίες μέχρι τις αρχές της δεκαετίας του 2000 για πολλές βιομηχανίες. Για παράδειγμα, οι χειριστές και οι κατασκευαστές συστημάτων βιομηχανικού ελέγχου αναφέρουν τα ιδιόκτητα πρωτόκολλα στα συστήματά τους και επιμένουν ότι το πρωτόκολλο θα ήταν πολύ περίπλοκο και ασαφές για να παραβιαστεί [41] . Όσον αφορά την κυβερνοασφάλεια, τα διαστημικά μέσα δεν ήταν διαφορετικά από τα ψηφιακά μέσα στη Γη.

Καθώς οι κατασκευαστές και οι διαχειριστές διακομιστών δεδομένων άρχισαν να δίνουν σημασία στην ασφάλεια στις αρχές της δεκαετίας του 2000, μετά τις δημοσιοποιημένες κυβερνοεπιθέσεις που επηρέασαν τις επιχειρήσεις τους, τα διαστημικά μέσα άρχισαν να μένουν πίσω. Παρά το γεγονός ότι οι περισσότερες βιομηχανίες υιοθέτησαν τυπικά σχήματα κρυπτογράφησης για την αποθήκευση και τη μεταφορά δεδομένων τη δεκαετία του '90 [42], οι σχεδιαστές και οι κατασκευαστές διαστημικής τεχνολογίας φαίνεται να αντιστέκονταν στην κίνηση προς την ασφάλεια [44]. Μπορούμε να υποθέσουμε ότι αυτή η αντίσταση μπορεί να οφείλεται σε χαμηλότερα περιθώρια κέρδους για τα διαστημικά συστήματα σε σύγκριση με τα εμπορικά προϊόντα ή τα αμυντικά συστήματα. Επίσης, κάποιες τεχνικές ασφάλειας, όπως η κρυπτογράφηση, απαιτούν περισσότερη επεξεργαστική ισχύ για να λειτουργήσουν. Σε πολλά διαστημικά συστήματα, η επεξεργαστική ισχύς και το εύρος ζώνης είναι πολύτιμοι πόροι και άλλες λειτουργίες δίνουν προτεραιότητα.

Μερική καθυστέρηση που σχετίζεται με την ασφάλεια των διαστημικών μέσων μπορεί να εξηγηθεί από την πολυπλοκότητα της αλυσίδας εφοδιασμού και του οικοσυστήματος προμηθευτών για τα μεγάλα εταιρικά, κυβερνητικά και στρατιωτικά χρηματοδοτούμενα συστήματα. Τα εξειδικευμένα μέρη που χρειάζονται για τα διαστημικά μέσα δεν κατασκευάζονται όλα από έναν κατασκευαστή. Στην πραγματικότητα, για να διατηρηθούν τα κόστη χαμηλά, η NASA και άλλοι αναπτυξιακοί φορείς διαστημικής τεχνολογίας αγοράζουν εξαρτήματα από καταλόγους εγκεκριμένων προμηθευτών σε όλο τον κόσμο [45]. Η διαδικασία έγκρισης αυτών των προμηθευτών δεν περιλαμβάνει απαραίτητα συγκεκριμένα πρότυπα ελέγχου ασφάλειας στον κυβερνοχώρο, αλλά αφορά τον φυσικό ποιοτικό έλεγχο. Όταν η NASA αγοράζει ένα μέρος από έναν προμηθευτή, έχει ελάχιστο έλεγχο σχετικά με το ποιος τεχνικός ανέπτυξε την πλακέτα τυπωμένου κυκλώματος (PCB) ή ποιος μηχανικός λογισμικού έγραψε τον κώδικα για ένα συγκεκριμένο εξάρτημα. Αυτή η έλλειψη πληροφοριών εισάγει σημαντικό κίνδυνο για την κυβερνοασφάλεια. Επιπλέον, εκτός από την ευπάθεια των προμηθευτών σε όλη την αλυσίδα εφοδιασμού του συστήματος, οι οργανισμοί διαστημικών μέσων γενικά συνεργάζονται με διάφορα ερευνητικά κέντρα που μπορεί να διαθέτουν ευπάθειες. Οι συνεργασίες μεταξύ πολλών εταίρων επιδεινώνουν τα πιθανά προβλήματα ασφάλειας.

Τέλος, ο θεσμικός σχεδιασμός των οργανισμών διαστημικών συστημάτων προκαλεί προκλήσεις ασφάλειας. Για να ασφαλιστεί σωστά ένα σύστημα, είναι σημαντικό να κατανοήσουμε πώς λειτουργεί το σύστημα και τις διάφορες ευκαιρίες που μπορεί να έχει ένας χάκερ να διαταράξει το μέσο. Επειδή αυτή είναι η πραγματικότητα, οι ειδικοί στην ασφάλεια που είναι γνώστες στη διαχείριση δεδομένων, στους διακομιστές και στα εσωτερικά δίκτυα για παραδοσιακή IT υποδομή πιθανόν δεν είναι οι ίδιοι ειδικοί που κατανοούν πλήρως ένα εξειδικευμένο δορυφορικό ή επίγειο σύστημα ελέγχου για ένα διαστημικό μέσο βαθέως διαστήματος. Παρ' όλα αυτά, οι περισσότερες ομάδες ασφαλείας των οργανισμών διαστημικών συστημάτων δεν είναι δομημένες για να ξεχωρίζουν την εσωτερική IT υποδομή από τα εξειδικευμένα διαστημικά συστήματα. Αυτό θα μπορούσε να αφήσει τα διαστημικά μέσα ευάλωτα επειδή οι ειδικοί που κατανοούν τη λειτουργία τους δεν ασχολούνται με την ασφάλειά τους. Επίσης, λόγω των ευρέων αρμοδιοτήτων της ομάδας ασφαλείας—που καλύπτουν τόσο την IT υποδομή όσο και τα διαστημικά μέσα—οι ειδικοί στην ασφάλεια είναι διασκορπισμένοι.

4.4 Εξελίξεις στην Ασφάλεια των Διαστημικών Συστημάτων

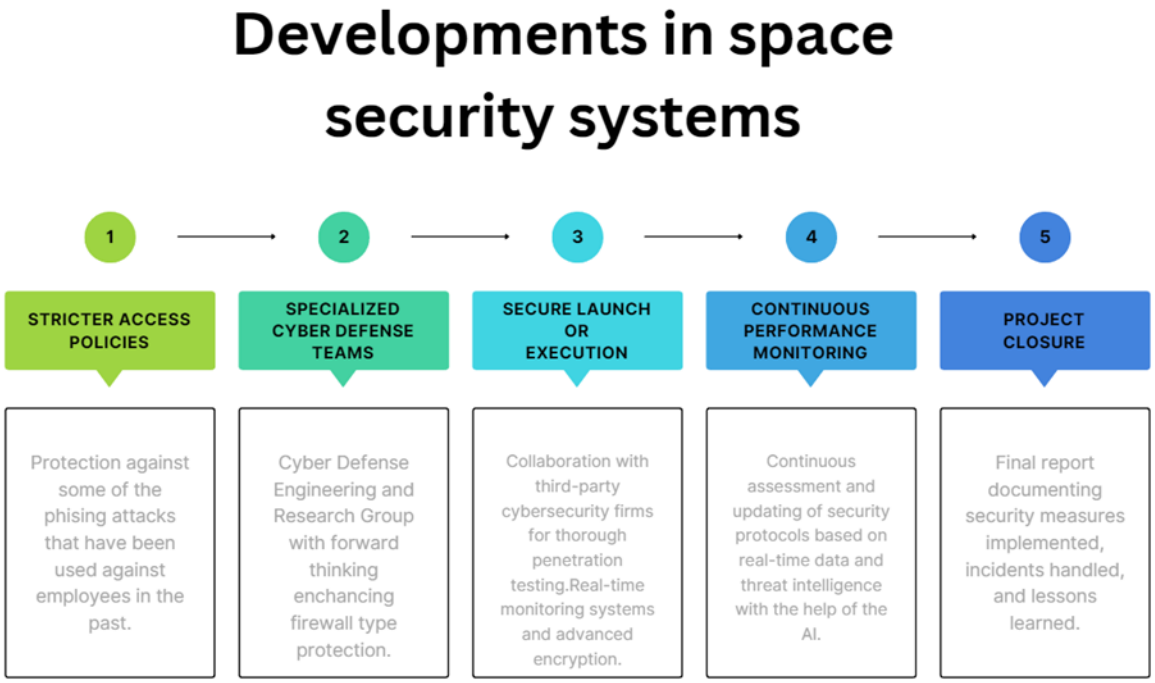
Στον τομέα της διαστημικής βιομηχανίας, υπάρχει αυξημένη ανάγκη για προσοχή σε θέματα κυβερνοασφάλειας. Ωστόσο, οι πιθανές αντιδράσεις σε τέτοιου είδους απειλές είναι πολλές. Ένας έλεγχος της NASA το οικονομικό έτος 2015 αποκάλυψε την ανάγκη αναθεώρησης των προτύπων και πρωτοκόλλων κυβερνοασφάλειας της NASA. Ο έλεγχος ανέφερε αρκετές επιθέσεις σε διαστημικά μέσα της NASA, οι οποίες δεν είχαν δημοσιοποιηθεί, ως τον κύριο λόγο για την έκκληση για μεταρρύθμιση .Η NASA έχει λάβει αρκετά μέτρα για τη βελτίωση της ασφάλειας γύρω από τα διαστημικά μέσα και έτσι υπάρχουν σημαντικές ευκαιρίες για βελτίωση. Πρώτον, η NASA έχει αρχίσει να εφαρμόζει αυστηρότερες πολιτικές ελέγχου πρόσβασης στους παρόχους και τους μηχανικούς της. Αυτό θα βοηθήσει στην προστασία από μερικές επιθέσεις phishing που έχουν χρησιμοποιηθεί στο παρελθόν εναντίον των υπαλλήλων της NASA, οι οποίες κλέβουν διαπιστευτήρια και πρόσβαση σε πολύτιμη πνευματική ιδιοκτησία [46].

Δεύτερον, η NASA έχει δημιουργήσει ομάδες στα κέντρα ανάπτυξης διαστημικών μέσων της, που εργάζονται ειδικά για την ασφάλεια των συστημάτων των αποστολών της. Προηγουμένως, το Γραφείο του Γενικού Διευθυντή Πληροφοριών ήταν υπεύθυνο για όλη την κυβερνοασφάλεια της NASA. Ωστόσο, οι ομάδες του δεν μπορούσαν να επικεντρώσουν πλήρως την προσοχή τους τόσο στην ασφάλεια της υποδομής των διακομιστών των εργαστηρίων της NASA όσο και στα συστήματα των αποστολών, αντίστοιχα. Για να αντιμετωπίσει αυτή την πρόκληση, το Εργαστήριο Αεριώθησης (JPL) της NASA δημιούργησε την Ομάδα Μηχανικής και Έρευνας Κυβερνοάμυνας (CDER). Ο στόχος του CDER είναι να αντιμετωπίσει συγκεκριμένα τα συστήματα των αποστολών (όπως το Mars Science Lab ή το Europa Lander), τα οποία συχνά έχουν μοναδικές απαιτήσεις κυβερνοασφάλειας σε σχέση με τους παραδοσιακούς διακομιστές με προστασία firewall. Η ανάπτυξη εξειδικευμένων ομάδων με μοναδική εξειδίκευση στα συστήματα αποστολών επιτρέπει προσαρμοσμένη ανάλυση και προστασία για αυτά τα διαστημικά μέσα με τρόπους που οι ομάδες ασφάλειας που προστατεύουν διακομιστές και δεδομένα δεν θα μπορούσαν. Κάποια από τη δουλειά του CDER στοχεύει στην ανάπτυξη εργαλείων και μεθοδολογιών που εφαρμόζονται σε πολλαπλά συστήματα αποστολών για να μειώσουν το κόστος και τις λειτουργίες ασφαλείας. [47]

Τέλος, η NASA έχει αρχίσει να κρυπτογραφεί τα δεδομένα τόσο κατά την αποθήκευση όσο και κατά τη μεταφορά τους. Πρόσφατα, στα τέλη του 2016, η AT&T κρυπτογράφησε το DSN της NASA, το οποίο αποτελεί τη βάση της επικοινωνιακής υποδομής για τεχνολογίες όπως το Mars Rover. Σύμφωνα με τις προηγούμενες εξηγήσεις για το γιατί τα διαστημικά μέσα υστερούν στην κυβερνοασφάλεια, η AT&T κρυπτογράφησε το DSN μόνο μετά την εμφάνιση μιας αναφοράς στο διαδίκτυο για το πώς να χακάρεις το Mars Rover. Η κρυπτογράφηση παρέχει ιδιωτικές επικοινωνίες που είναι ορατές μόνο σε όσους έχουν το κρυπτογραφικό κλειδί. Αυτή η κρυπτογράφηση θα γίνει η πρώτη γραμμή άμυνας κατά των χάκερ που σκοπεύουν να καταλάβουν το DSN ή να παρακολουθήσουν τις επικοινωνίες που στέλνονται μέσω αυτού του δισεκατομμυρίων δολαρίων μακρινής επικοινωνιακής δικτύου.

Η ομάδα CDER της NASA JPL συνεργάζεται επίσης με ερευνητές του πανεπιστημίου MIT για να πραγματοποιήσουν δοκιμές διείσδυσης στο λογισμικό των συστημάτων αποστολών. Αυξάνοντας τη συνεργασία με την ευρύτερη ερευνητική κοινότητα στον τομέα της ασφάλειας, θα βελτιωθεί σημαντικά η ασφάλεια των συστημάτων αποστολών για διαστημικά μέσα. Η CDER ξεκίνησε να δημιουργεί μια κουλτούρα ασφάλειας με ένα διασκεδαστικό παιχνίδι που ονομάζεται

Donuts. Όταν ένα μέλος της ομάδας CDER αφήνει τον υπολογιστή του ξεκλείδωτο, ένας άλλος συνεργάτης της CDER στέλνει ένα email από τον ξεκλείδωτο υπολογιστή με θέμα "Donuts". Αν σταλεί αυτό το μήνυμα, ο χρήστης του παραβιασμένου υπολογιστή πρέπει να αγοράσει Donuts για την ομάδα. Οι ομάδες παρακολουθούν πόσα Donuts χρωστάει κάθε μέλος της ομάδας, ενθαρρύνοντας έτσι τους συνεργάτες να κλειδώνουν τις μηχανές τους όταν απομακρύνονται. Στην αρχή, η ομάδα έπαιρνε καθημερινά τα μερίδιά της σε Donuts, αλλά καθώς η ευαισθητοποίηση για την ασφάλεια αυξήθηκε, τα ντόνατς σταμάτησαν να έρχονται. Αυτό το παιχνίδι έχει επεκταθεί και σε άλλες ομάδες στο JPL, βοηθώντας έτσι να δημιουργηθεί μια κουλτούρα συνεχούς ευαισθητοποίησης για την ασφάλεια.[47]



Σχήμα 8: Developments in space security systems.

Το παραπάνω σχήμα παρουσιάζει τις εξελίξεις στα συστήματα ασφάλειας του διαστήματος, περιγράφοντας μια διαδικασία που ξεκινά με την εφαρμογή αυστηρότερων πολιτικών πρόσβασης για την προστασία από επιθέσεις phishing. Ακολουθεί η δημιουργία εξειδικευμένων ομάδων κυβερνοάμυνας που ενισχύουν την προστασία των συστημάτων με προχωρημένες τεχνολογίες. Στη συνέχεια, διασφαλίζεται η ασφαλής εκκίνηση ή εκτέλεση μέσω συνεργασίας με εξωτερικές εταιρείες κυβερνοασφάλειας για δοκιμές διείσδυσης και προηγμένη κρυπτογράφηση. Ακολουθεί η συνεχής παρακολούθηση της απόδοσης και η αναβάθμιση των πρωτοκόλλων ασφαλείας με τη βοήθεια τεχνητής νοημοσύνης. Τέλος, ολοκληρώνεται η διαδικασία με την τεκμηρίωση των μέτρων ασφαλείας, των περιστατικών και των διδαγμάτων που αντλήθηκαν.

Όπως και η NASA, η ιδιωτική βιομηχανία διαστημικών συστημάτων βελτιώνει αυτή τη στιγμή την ασφάλειά της αλλά είναι αδύνατο να αξιολογηθούν πολλές εταιρείες του ιδιωτικού τομέα που δεν είναι διαφανείς σχετικά με τις προσπάθειές τους για την κυβερνοασφάλεια .Ερευνητές ασφάλειας εντοπίζουν συνεχώς κενά σε διάφορα συστήματα δικτύων δορυφόρων και ζητούν από την υπεύθυνη εταιρεία να διορθώσει τις ευπάθειες. Δυστυχώς, αυτές οι ειδοποιήσεις για ευπάθειες

συχνά αγνοούνται λόγω έλλειψης πόρων από τους κατασκευαστές για την αντιμετώπιση των προβλημάτων. Οι πολυπλοκότητες του κύκλου ζωής και οι συναφείς ερωτήσεις ευθύνης που συζητήθηκαν νωρίτερα περιπλέκουν περαιτέρω τη διόρθωση των ευπαθειών. Εάν αγνοηθούν, οι χάκερς συνήθως ακολουθούν διαδικασίες υπεύθυνης αναφοράς και δημοσιοποιούν την ευπάθεια μετά από μια περίοδο χρόνου αφού ειδοποιήσουν τον κατασκευαστή. Με την ανακοίνωση της απειλής δημόσια, οι χάκερς σκοπεύουν να συγκεντρώσουν μεγάλη προσοχή στο πρόβλημα και να αναγκάσουν τον κατασκευαστή να διορθώσει το ζήτημα. Αυτό συνέβη με τους ιδιοκτήτες των δορυφόρων Iridium που ισχυρίστηκαν ότι τα συστήματά τους ήταν εξαιρετικά δύσκολο να χακαριστούν. Μόνο αφού ο χάκερς ανακοίνωσαν τις ευπάθειες και ντρόπιασαν την εταιρεία, η Iridium έλαβε μέτρα για να βελτιώσει την ασφάλεια του δικτύου επικοινωνιών της [48].

Σε αντίθεση με τους δορυφόρους GPS που μπορούν να ανιχνευθούν και να ελεγχθούν για ευπάθειες χωρίς άμεση πρόσβαση στο διαστημικό σύστημα, η ασφάλεια άλλων διαστημικών συστημάτων της ιδιωτικής βιομηχανίας είναι ένα θέμα που ελέγχεται δύσκολα και συνεπώς δεν μπορεί να ελεγχθεί από την κοινότητα ασφάλειας. Για παράδειγμα, η SpaceX, η Virgin Galactic και άλλοι προγραμματιστές, ιδιοκτήτες και διαχειριστές διαστημικών συστημάτων δεν καθιστούν την τεχνολογία τους άμεσα διαθέσιμη για έλεγχο από ερευνητές ασφάλειας. Αυτό πιθανότατα συμβαίνει επειδή ανησυχούν ότι ο ευαίσθητος κώδικας ή οι πληροφορίες τους θα πέσουν στα χέρια ανταγωνιστών. Ένας άλλος λόγος είναι ότι οι ιδιωτικοί προγραμματιστές διαστημικών συστημάτων ανησυχούν για το τι θα βρουν οι ερευνητές ασφάλειας και φοβούνται ότι αν αυτό δημοσιοποιηθεί, μπορεί να καταστρέψει τις εταιρείες τους. Επιπλέον, δεν υπάρχει κάποια υποχρέωση για αποκάλυψη ή αναφορά σχετικά με τις διαδικασίες δοκιμών κυβερνοασφάλειας από αυτές τις εταιρείες και αυτό έχει ως αποτέλεσμα να είναι δύσκολο για την κοινότητα ασφάλειας να αξιολογήσει την κυβερνοασφάλεια αυτών των διαστημικών συστημάτων. Το θέμα της ευθύνης αποκάλυψης ευπαθειών και ο κίνδυνος απελευθέρωσης της τεχνολογίας για δοκιμές είναι σημαντικός, και αυτό αποτελεί μεγάλο εμπόδιο για τη διαφάνεια σχετικά με την ασφάλεια των διαστημικών συστημάτων [49].

Παρά τις προσπάθειες τόσο των δημόσιων όσο και των ιδιωτικών οργανισμών για την ενίσχυση της κυβερνοασφάλειας στα διαστημικά συστήματα, εξακολουθούν να υπάρχουν σημαντικά κενά που πρέπει να καλυφθούν. Η NASA, μέσω του έργου της JPL, έχει κάνει σημαντικά βήματα προς τη δημιουργία μιας κουλτούρας ασφάλειας για την αντιμετώπιση των ευπαθειών. Ωστόσο, τα διαστημικά συστήματα της ιδιωτικής βιομηχανίας συχνά παραμένουν δύσκολα προσβάσιμα για έλεγχο ασφαλείας, καθιστώντας δύσκολη την αξιολόγηση και βελτίωση της ασφάλειας αυτών των συστημάτων. Είναι απαραίτητο να ενισχυθούν οι προσπάθειες για τη βελτίωση της κυβερνοασφάλειας, να κλείσουν τα υφιστάμενα κενά και να επιτευχθεί μεγαλύτερη διαφάνεια και συνεργασία μεταξύ των διαστημικών οργανισμών και της ευρύτερης κοινότητας ασφάλειας.

5

Τεχνικά Μέτρα Καταπολέμησης

Η συνεχής αύξηση των κυβερνοεπιθέσεων καθιστά αναγκαία την εφαρμογή αποτελεσματικών τεχνικών μέτρων για την προστασία των πληροφοριακών συστημάτων και δεδομένων. Τα τεχνικά μέτρα καταπολέμησης των κυβερνοαπειλών περιλαμβάνουν μια σειρά από πρακτικές και τεχνολογίες που στοχεύουν στην ενίσχυση της ασφάλειας και στην αποτροπή κακόβουλων δραστηριοτήτων. Ενδεικτικά μεταξύ των βασικών τεχνικών μέτρων είναι η χρήση ισχυρών firewall, η εφαρμογή ενημερώσεων λογισμικού, η εγκατάσταση λογισμικού antivirus, η χρήση συστημάτων ανίχνευσης και αποτροπής εισβολών (IDS/IPS) και η κρυπτογράφηση δεδομένων. Αυτά τα μέτρα είναι κρίσιμα για την προστασία από ποικίλες απειλές, όπως malware, phishing, και ransomware, εξασφαλίζοντας την ακεραιότητα, την εμπιστευτικότητα και τη διαθεσιμότητα των συστημάτων.

5.1 Αρχιτεκτονική ενός Δικτύου Digital Twin

Το Digital Twin Network είναι μια προηγμένη έννοια όπου δημιουργείται μια εικονική αναπαράσταση, ή "ψηφιακός δίδυμος" ενός φυσικού δικτύου για να προσομοιώνει, να παρακολουθεί, να αναλύει και να βελτιστοποιεί το πραγματικό του αντίστοιχο. Αυτή η ψηφιακή αναπαράσταση περιλαμβάνει όλες τις πτυχές του φυσικού δικτύου, όπως συσκευές, συνδέσεις, διαμορφώσεις, πρότυπα κυκλοφορίας και λειτουργικά δεδομένα.

Η αρχιτεκτονική ενός Δικτύου Digital Twin (Ψηφιακού Διδύμου) αποτελείται από διάφορα δομικά στοιχεία και τεχνολογίες που συνεργάζονται για τη δημιουργία και τη συντήρηση ενός ακριβούς ψηφιακού αντιγράφου ενός φυσικού συστήματος. Η αναπαράσταση αυτή χρησιμοποιείται για την ανάλυση, την προσομοίωση, τη βελτιστοποίηση και την πρόβλεψη της συμπεριφοράς του συστήματος στον πραγματικό κόσμο [50]. Η αρχιτεκτονική ενός Δικτύου Digital Twin περιλαμβάνει τα εξής βασικά στοιχεία:

1. **Αισθητήρες και Συστήματα Συλλογής Δεδομένων**

Οι αισθητήρες και τα συστήματα συλλογής δεδομένων τοποθετούνται στο φυσικό σύστημα για τη συνεχή παρακολούθηση και τη συλλογή δεδομένων. Αυτά τα δεδομένα μπορεί να περιλαμβάνουν πληροφορίες για θερμοκρασία, πίεση, ταχύτητα, κατανάλωση ενέργειας και άλλες κρίσιμες

παραμέτρους λειτουργίας. Οι αισθητήρες συνδέονται στο Διαδίκτυο των Πραγμάτων (IoT) για τη μετάδοση δεδομένων σε πραγματικό χρόνο.

2. Πλατφόρμες IoT και Middleware

Οι πλατφόρμες IoT και τα middleware είναι υπεύθυνες για τη συλλογή, την επεξεργασία και τη διαχείριση των δεδομένων που προέρχονται από τους αισθητήρες. Παρέχουν τις απαραίτητες διεπαφές και APIs για την επικοινωνία μεταξύ των φυσικών συσκευών και του ψηφιακού διδύμου. Επίσης, εξασφαλίζουν την ασφάλεια και την αξιοπιστία των δεδομένων.

3. Μοντέλα Δεδομένων και Ανάλυση

Τα δεδομένα που συλλέγονται από τους αισθητήρες χρησιμοποιούνται για τη δημιουργία μοντέλων που αναπαριστούν τη συμπεριφορά του φυσικού συστήματος. Τα μοντέλα αυτά μπορεί να είναι στατιστικά, φυσικά, ή βασισμένα στη μηχανική μάθηση. Η ανάλυση των δεδομένων επιτρέπει την εξαγωγή χρήσιμων πληροφοριών και την ανίχνευση ανωμαλιών, καθώς και την πρόβλεψη μελλοντικών καταστάσεων.

4. Εικονικά Περιβάλλοντα και Προσομοίωση

Το ψηφιακό δίδυμο αναπτύσσεται μέσα σε ένα εικονικό περιβάλλον όπου μπορεί να γίνουν προσομοιώσεις και πειράματα. Αυτά τα εικονικά περιβάλλοντα επιτρέπουν την εκτέλεση δοκιμών και την αξιολόγηση διαφόρων σεναρίων χωρίς να επηρεάζεται το φυσικό σύστημα. Τα εργαλεία προσομοίωσης χρησιμοποιούνται για τη δοκιμή των αντιδράσεων του συστήματος σε διαφορετικές συνθήκες.

5. Ενοποίηση μέσω Συστημάτων Διαχείρισης και Υποστήριξης Λήψης Αποφάσεων

Η ενσωμάτωση του ψηφιακού διδύμου με συστήματα διαχείρισης, όπως τα SCADA και ERP επιτρέπει τη χρήση των πληροφοριών που προέρχονται από το δίδυμο για τη λήψη αποφάσεων. Η υποστήριξη λήψης αποφάσεων βοηθά στη βελτιστοποίηση των διαδικασιών και τη βελτίωση της απόδοσης του συστήματος.

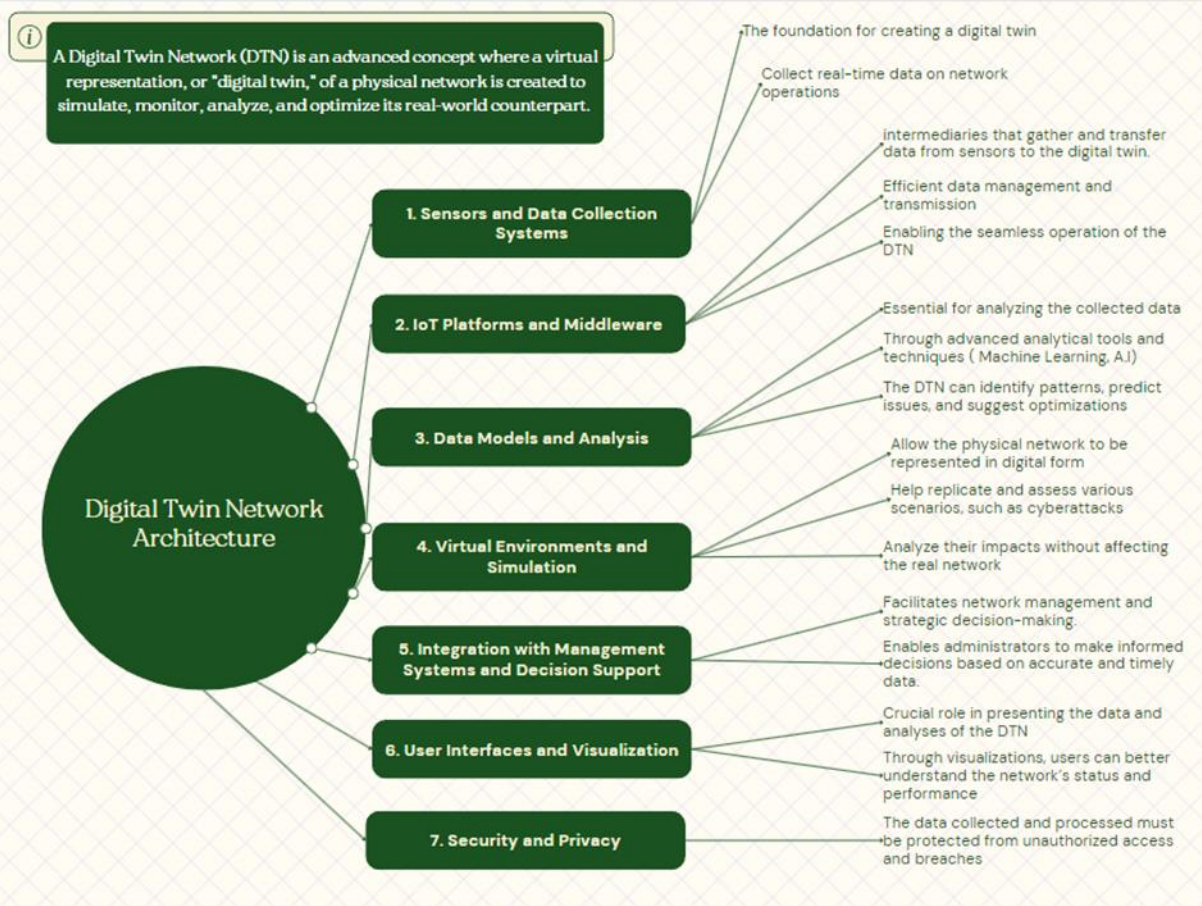
6. **Διεπαφές Χρήστη και Οπτικοποίηση**

Οι διεπαφές χρήστη και τα εργαλεία οπτικοποίησης παρέχουν στους χρήστες πρόσβαση στο ψηφιακό δίδυμο και στις πληροφορίες που προέρχονται από αυτό. Αυτές οι διεπαφές επιτρέπουν την εύκολη κατανόηση των δεδομένων μέσω γραφημάτων, διαγραμμάτων και άλλων οπτικών αναπαραστάσεων. Η οπτικοποίηση βοηθά στη λήψη ταχύτερων και πιο ενημερωμένων αποφάσεων.

7. Ασφάλεια και Ιδιωτικότητα

Η ασφάλεια και η ιδιωτικότητα των δεδομένων αποτελούν κρίσιμες πτυχές της αρχιτεκτονικής του Δικτύου Digital Twin. Η προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση και επιθέσεις είναι ζωτικής σημασίας για τη διασφάλιση της ακεραιότητας και της εμπιστευτικότητας των πληροφοριών. Τα μέτρα ασφαλείας περιλαμβάνουν την κρυπτογράφηση, τον έλεγχο πρόσβασης και την παρακολούθηση δικτύου.

Από τα παραπάνω καταλαβαίνουμε ότι η αρχιτεκτονική ενός Δικτύου Digital Twin είναι μια πολυσύνθετη δομή που απαιτεί τη συνεργασία πολλών τεχνολογιών και συστημάτων. Από τη συλλογή και την ανάλυση δεδομένων μέχρι την προσομοίωση και τη λήψη αποφάσεων, κάθε στοιχείο παίζει καθοριστικό ρόλο στη δημιουργία ενός ακριβούς και χρήσιμου ψηφιακού διδύμου. Αυτή η αρχιτεκτονική επιτρέπει τη βελτιστοποίηση των διαδικασιών και την πρόβλεψη των μελλοντικών αναγκών, προσφέροντας σημαντικά οφέλη για τις επιχειρήσεις και τις βιομηχανίες.



Σχήμα 9: Αρχιτεκτονική Digital Twin Network.

Το παραπάνω σχήμα παρουσιάζει την αρχιτεκτονική ενός Δικτύου Ψηφιακών Διδύμων, που είναι μια προηγμένη έννοια όπου δημιουργείται μια ψηφιακή αναπαράσταση ενός φυσικού δικτύου για να προσομοιώσει, παρακολουθήσει, αναλύσει και βελτιστοποιήσει το πραγματικό του αντίστοιχο. Η αρχιτεκτονική ενός Δικτύου Ψηφιακών Διδύμων περιλαμβάνει διάφορα βασικά στοιχεία. Τα συστήματα αισθητήρων και συλλογής δεδομένων συλλέγουν δεδομένα σε πραγματικό χρόνο για τις λειτουργίες του δικτύου. Οι πλατφόρμες IoT και middleware λειτουργούν ως ενδιάμεσοι, συγκεντρώνοντας και μεταφέροντας δεδομένα από τους αισθητήρες στο ψηφιακό δίδυμο, εξασφαλίζοντας αποδοτική διαχείριση και μετάδοση δεδομένων. Τα μοντέλα δεδομένων και η ανάλυση είναι απαραίτητα για την ανάλυση των συλλεγόμενων δεδομένων μέσω προχωρημένων εργαλείων ανάλυσης και τεχνικών, όπως η μηχανική μάθηση και η τεχνητή νοημοσύνη. Το DTN μπορεί να εντοπίζει μοτίβα, να προβλέπει προβλήματα και να προτείνει βελτιώσεις. Τα εικονικά περιβάλλοντα και η προσομοίωση επιτρέπουν την αναπαράσταση του φυσικού δικτύου σε ψηφιακή μορφή, βοηθώντας στην προσομοίωση και αξιολόγηση διαφόρων σεναρίων, όπως οι κυβερνοεπιθέσεις, χωρίς να επηρεάζονται τα πραγματικά δίκτυα. Η ενσωμάτωση με συστήματα διαχείρισης και υποστήριξης αποφάσεων την κατάσταση και την απόδοση του δικτύου. Τέλος, η ασφάλεια και η ιδιωτικότητα των δεδομένων που συλλέγονται και επεξεργάζονται πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και παραβιάσεις.

Αυτή η αρχιτεκτονική επιτρέπει την αποτελεσματική διαχείριση και βελτιστοποίηση των δικτύων, προσφέροντας δυνατότητες προσομοίωσης, ανάλυσης και προστασίας σε πραγματικό χρόνο.

Το Digital Twin διευκολύνει τη διαχείριση του δικτύου και τη λήψη στρατηγικών αποφάσεων, επιτρέποντας στους διαχειριστές να λαμβάνουν ενημερωμένες αποφάσεις βάσει ακριβών και έγκαιρων δεδομένων. Οι διεπαφές χρηστών και η οπτικοποίηση είναι κρίσιμες για την παρουσίαση των δεδομένων και των αναλύσεων του DTN, μέσω των οποίων οι χρήστες μπορούν να κατανοήσουν καλύτερα

5.2 Δημιουργία blocks του Δικτύου Digital Twin

Η δημιουργία των blocks του Δικτύου Digital Twin αποτελεί μια θεμελιώδη διαδικασία για την ανάπτυξη ενός ολοκληρωμένου και λειτουργικού ψηφιακού διδύμου. Κάθε block αντιπροσωπεύει μια συγκεκριμένη λειτουργία ή στοιχείο του συστήματος και η συνεργασία όλων των blocks διασφαλίζει την αποτελεσματικότητα και την ακρίβεια του ψηφιακού διδύμου. Παρακάτω περιγράφονται τα κύρια blocks που αποτελούν το Δίκτυο Digital Twin καθώς και οι λειτουργίες τους:

1. Data Acquisition Block

Το block συλλογής δεδομένων είναι υπεύθυνο για τη συνεχή παρακολούθηση και συλλογή δεδομένων από το φυσικό σύστημα. Περιλαμβάνει αισθητήρες και συσκευές IoT που μετρούν παραμέτρους όπως θερμοκρασία, πίεση, υγρασία, ταχύτητα, κατανάλωση ενέργειας κ.ά. Τα δεδομένα αυτά μεταδίδονται σε πραγματικό χρόνο σε ένα κεντρικό σύστημα για περαιτέρω επεξεργασία.

2. Data Processing and Storage Block

Αυτό το block είναι υπεύθυνο για την επεξεργασία, την αποθήκευση και τη διαχείριση των δεδομένων που συλλέγονται από το φυσικό σύστημα. Χρησιμοποιεί τεχνολογίες big data και cloud computing για την αποθήκευση μεγάλων ποσοτήτων δεδομένων και την επεξεργασία τους σε πραγματικό χρόνο. Περιλαμβάνει βάσεις δεδομένων, εργαλεία επεξεργασίας δεδομένων και πλατφόρμες cloud.

3. Data Integration and Management Block

Το block ενσωμάτωσης και διαχείρισης δεδομένων εξασφαλίζει την ομαλή ροή και ενοποίηση των δεδομένων από διάφορες πηγές. Παρέχει τα APIs και τις διεπαφές για τη σύνδεση διαφορετικών συστημάτων και την ενοποίηση των δεδομένων. Επίσης, διασφαλίζει την ποιότητα, την ακρίβεια και την ασφάλεια των δεδομένων μέσω μηχανισμών διαχείρισης δεδομένων.

4. Modeling and Simulation Block

Αυτό το block δημιουργεί και διαχειρίζεται τα μοντέλα που αναπαριστούν το φυσικό σύστημα. Χρησιμοποιεί τεχνικές προσομοίωσης και ανάλυσης για την κατανόηση της συμπεριφοράς του συστήματος και την πρόβλεψη μελλοντικών καταστάσεων. Τα μοντέλα μπορεί να είναι φυσικά, στατιστικά ή βασισμένα στη μηχανική μάθηση, και χρησιμοποιούνται για την εκτέλεση πειραμάτων και την αξιολόγηση διαφόρων σεναρίων.

5. Visualization and User Interface Block

Το block οπτικοποίησης και διεπαφής χρήστη παρέχει τα εργαλεία για την παρουσίαση των δεδομένων και των αποτελεσμάτων της προσομοίωσης στους χρήστες. Χρησιμοποιεί γραφήματα, διαγράμματα και άλλες μορφές οπτικής αναπαράστασης για να διευκολύνει την κατανόηση των πληροφοριών. Επίσης, προσφέρει τις διεπαφές μέσω των οποίων οι χρήστες μπορούν να αλληλοεπιδρούν με το ψηφιακό δίδυμο και να λαμβάνουν αποφάσεις.

6. Analytics and Decision Support Block

Αυτό το block παρέχει τις δυνατότητες ανάλυσης των δεδομένων και υποστήριξης λήψης αποφάσεων. Χρησιμοποιεί αλγορίθμους ανάλυσης δεδομένων, μηχανικής μάθησης και τεχνητής νοημοσύνης για την εξαγωγή χρήσιμων πληροφοριών και την υποστήριξη των αποφάσεων. Τα αποτελέσματα της ανάλυσης βοηθούν στη βελτιστοποίηση των διαδικασιών και τη βελτίωση της απόδοσης του συστήματος.

7. Security and Privacy Block

Το block ασφάλειας και ιδιωτικότητας διασφαλίζει την προστασία των δεδομένων και των συστημάτων από μη εξουσιοδοτημένη πρόσβαση και επιθέσεις. Περιλαμβάνει μέτρα ασφαλείας όπως η κρυπτογράφηση, ο έλεγχος πρόσβασης, η ανίχνευση και η πρόληψη απειλών, καθώς και μηχανισμούς για τη διατήρηση της ιδιωτικότητας των δεδομένων.

8. Communication and Networking Block

Αυτό το block διαχειρίζεται την επικοινωνία μεταξύ των διαφορετικών στοιχείων του Δικτύου Digital Twin. Χρησιμοποιεί τεχνολογίες δικτύωσης για τη διασφάλιση της αξιόπιστης και γρήγορης μεταφοράς δεδομένων μεταξύ των συσκευών IoT, των συστημάτων επεξεργασίας και αποθήκευσης δεδομένων, και των εργαλείων ανάλυσης και οπτικοποίησης.

Μελετώντας τη δημιουργία των blocks του Δικτύου Digital Twin γίνεται σαφές ότι είναι μια διαδικασία που απαιτεί την προσεκτική ενσωμάτωση και συνεργασία πολλών διαφορετικών τεχνολογιών και συστημάτων. Κάθε block παίζει έναν κρίσιμο ρόλο στη συνολική λειτουργία και απόδοση του ψηφιακού διδύμου, εξασφαλίζοντας την ακριβή αναπαράσταση και βελτιστοποίηση του φυσικού συστήματος. Η επιτυχής υλοποίηση αυτών των blocks επιτρέπει στις επιχειρήσεις και τις βιομηχανίες να αξιοποιήσουν τα πλεονεκτήματα του ψηφιακού διδύμου για τη βελτίωση της απόδοσης, την εξοικονόμηση πόρων και την επίτευξη στρατηγικών στόχων [51].

5.3 Κρυπτογράφηση και Ταυτοποίηση (AES & PKI)

Ο AES είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης που έχει καθιερωθεί ως το πρότυπο κρυπτογράφησης για την ασφάλεια των δεδομένων από το NIST των ΗΠΑ. Ο AES

επιλέχθηκε το 2001, αντικαθιστώντας τον παλαιότερο Data Encryption Standard (DES), λόγω της μεγαλύτερης ασφάλειας και αποδοτικότητάς του [52].

Ο AES είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης, που σημαίνει ότι χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων. Το κλειδί πρέπει να παραμένει εμπιστευτικό μεταξύ των μερών που επικοινωνούν. Ο αλγόριθμος υποστηρίζει κλειδιά μεγέθους 128, 192 και 256 bit, με μεγαλύτερα κλειδιά να προσφέρουν υψηλότερο επίπεδο ασφάλειας αλλά να απαιτούν περισσότερους πόρους για την επεξεργασία. Η δομή του AES βασίζεται σε επαναλήψεις, με τον αριθμό των επαναλήψεων να εξαρτάται από το μέγεθος του κλειδιού: 10 γύροι για κλειδιά 128 bit, 12 γύροι για κλειδιά 192 bit και 14 γύροι για κλειδιά 256 bit. Κάθε γύρος αποτελείται από μια σειρά λειτουργιών: SubBytes, ShiftRows, MixColumns(εκτός του τελευταίου γύρου) και AddRoundKey [53].

- **SubBytes:**

Αυτή η λειτουργία αντικαθιστά κάθε byte του μπλοκ δεδομένων με ένα άλλο byte σύμφωνα με έναν σταθερό πίνακα αντικατάστασης, γνωστό ως S-box. Ο S-box σχεδιάστηκε για να έχει ισχυρές μη γραμμικές ιδιότητες, γεγονός που συμβάλλει στην ασφάλεια του αλγορίθμου.

- **ShiftRows:**

Σε αυτή τη φάση, τα bytes σε κάθε σειρά του πίνακα δεδομένων μετατοπίζονται κυκλικά προς τα αριστερά. Ο αριθμός των θέσεων που μετατοπίζεται κάθε σειρά εξαρτάται από τη θέση της σειράς. Η πρώτη σειρά δεν μετατοπίζεται, η δεύτερη σειρά μετατοπίζεται κατά μία θέση, η τρίτη κατά δύο θέσεις και η τέταρτη κατά τρεις θέσεις. Αυτή η λειτουργία δημιουργεί διάδοση των δεδομένων.

- **MixColumns:**

Αυτή η λειτουργία εφαρμόζει μια γραμμική μετατροπή σε κάθε στήλη του πίνακα δεδομένων. Τα bytes κάθε στήλης αναμειγνύονται χρησιμοποιώντας έναν συγκεκριμένο μαθηματικό τύπο που περιλαμβάνει πολλαπλασιασμό και πρόσθεση σε ένα πεπερασμένο σώμα (Galois Field). Αυτή η φάση συμβάλλει επίσης στη διάδοση των δεδομένων. Σημειώνεται ότι η λειτουργία MixColumns δεν εκτελείται στον τελευταίο γύρο του αλγορίθμου.

- **AddRoundKey:**

Σε αυτή τη φάση, κάθε byte του μπλοκ δεδομένων συνδυάζεται με το αντίστοιχο byte του κλειδιού του γύρου χρησιμοποιώντας τη λειτουργία XOR (αποκλειστικό Ή). Το κλειδί του γύρου είναι ένα υποκλειδί που προκύπτει από το αρχικό κλειδί μέσω μιας διαδικασίας που ονομάζεται Key Expansion (επέκταση κλειδιού) [53].

Ο AES θεωρείται εξαιρετικά ασφαλής αλγόριθμος και χρησιμοποιείται ευρέως σε πολλές εφαρμογές, συμπεριλαμβανομένων των στρατιωτικών και κυβερνητικών υπηρεσιών. Μέχρι σήμερα, δεν έχει βρεθεί κάποιος πρακτικός τρόπος διάσπασης του AES με συμβατικά μέσα. Είναι σχεδιασμένος για αποδοτικότητα τόσο σε λογισμικό όσο και σε υλικό και χρησιμοποιείται ευρέως σε πολλές πλατφόρμες, από μικρές συσκευές μέχρι μεγάλες υπολογιστικές υποδομές. Επιπλέον χρησιμοποιείται για την ασφάλεια δικτύων, κρυπτογραφώντας δεδομένα που μεταδίδονται μέσω δικτύων, όπως το SSL/TLS για ασφαλείς συνδέσεις στο διαδίκτυο τα οποία θα αναφερθούν παρακάτω. Επίσης, προστατεύει δεδομένα που αποθηκεύονται σε δίσκους και άλλα αποθηκευτικά μέσα, όπως το BitLocker στα Windows. Επιπλέον, ενσωματώνεται σε διάφορα πρωτόκολλα ασφαλείας για την προστασία της επικοινωνίας, όπως το WPA2 για ασύρματα δίκτυα. Τέλος ο AES συνεχίζει να αποτελεί τη βάση για την ασφάλεια των πληροφοριακών συστημάτων και θεωρείται ένα από τα πιο αξιόπιστα και ασφαλή πρότυπα κρυπτογράφησης που υπάρχουν σήμερα.

Η Υποδομή Δημόσιου Κλειδιού PKI από την άλλη πλευρά είναι ένα σύστημα που επιτρέπει την ασφαλή ανταλλαγή πληροφοριών στο διαδίκτυο μέσω της χρήσης κρυπτογραφίας δημόσιου κλειδιού. Το PKI υποστηρίζει την ταυτοποίηση των χρηστών και των συσκευών, την εξασφάλιση της ακεραιότητας των δεδομένων και την παροχή εμπιστευτικότητας στις επικοινωνίες. Η βασική ιδέα πίσω από το PKI είναι η χρήση δύο κλειδιών: ενός δημόσιου και ενός ιδιωτικού κλειδιού. Το δημόσιο κλειδί διανέμεται ελεύθερα και χρησιμοποιείται για την κρυπτογράφηση των δεδομένων ή για την επαλήθευση της ψηφιακής υπογραφής. Το ιδιωτικό κλειδί διατηρείται εμπιστευτικό και χρησιμοποιείται για την αποκρυπτογράφηση των δεδομένων ή για τη δημιουργία της ψηφιακής υπογραφής.

Τα ψηφιακά πιστοποιητικά αποτελούν ηλεκτρονικά έγγραφα που συνδέουν ένα δημόσιο κλειδί με την ταυτότητα του κατόχου του. Εκδίδονται από αξιόπιστες αρχές πιστοποίησης CAs. Ένα τυπικό ψηφιακό πιστοποιητικό περιλαμβάνει το δημόσιο κλειδί του κατόχου, τα στοιχεία ταυτοποίησης του κατόχου, την υπογραφή της αρχής πιστοποίησης και την περίοδο ισχύος του πιστοποιητικού. Οι CAs είναι υπεύθυνες για την έκδοση, τη διαχείριση και την ανάκληση των ψηφιακών πιστοποιητικών, παίζοντας τον ρόλο του αξιόπιστου τρίτου μέρους που επικυρώνει την ταυτότητα των χρηστών και των συσκευών. Οι αρχές καταχώρησης (Registration Authorities - RAs) είναι υπεύθυνες για την επαλήθευση της ταυτότητας των αιτούντων πριν την έκδοση του ψηφιακού πιστοποιητικού από την CA, λειτουργώντας ως ενδιάμεσοι μεταξύ των χρηστών και της CA. Το PKI περιλαμβάνει μηχανισμούς για τη δημιουργία, την αποθήκευση, τη διανομή και την ανάκληση των κλειδιών. Η ασφαλής διαχείριση των κλειδιών είναι κρίσιμη για την ακεραιότητα και την εμπιστευτικότητα των επικοινωνιών. Επιπλέον χρησιμοποιείται για την κρυπτογράφηση των δεδομένων, εξασφαλίζοντας ότι μόνο οι εξουσιοδοτημένοι παραλήπτες μπορούν να τα αποκρυπτογραφήσουν. Οι ψηφιακές υπογραφές διασφαλίζουν την αυθεντικότητα και την ακεραιότητα των μηνυμάτων και των εγγράφων. Χρησιμοποιώντας το ιδιωτικό κλειδί, ο αποστολέας μπορεί να υπογράψει ψηφιακά ένα μήνυμα, το οποίο μπορεί να επαληθευτεί από τον παραλήπτη με το δημόσιο κλειδί του αποστολέα. Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται για την επαλήθευση της ταυτότητας των χρηστών και των συσκευών, διασφαλίζοντας ότι μόνο εξουσιοδοτημένα μέρη έχουν πρόσβαση σε ευαίσθητες πληροφορίες και πόρους. Το PKI υποστηρίζει την ασφαλή ανταλλαγή πληροφοριών μέσω πρωτοκόλλων όπως το SSL/TLS, το οποίο χρησιμοποιείται για την ασφαλή επικοινωνία στο διαδίκτυο, όπως σε ιστοσελίδες HTTPS. Μέσω της ταυτοποίησης και της επαλήθευσης των χρηστών, το PKI βοηθά στη διαχείριση των

δικαιωμάτων πρόσβασης σε συστήματα και δεδομένα, ενισχύοντας την πολιτική ασφάλειας ενός οργανισμού [54].

Οι παρακάτω δύο πίνακες περιγράφουν τα χαρακτηριστικά και τις ιδιότητες δύο διαφορετικών μεθόδων κρυπτογράφησης: της Συμμετρικής Κρυπτογράφησης με Αλγόριθμο AES (Advanced Encryption Standard) και της Ασύμμετρης Κρυπτογράφησης με χρήση PKI (Public Key Infrastructure). Συνολικά περιγράφονται τα μειονεκτήματα, οι χρήσεις και η βασικές τους λειτουργίες. Η σύγκριση γίνεται μέσω:

- Ταχύτητας
- Κόστους
- Τύπου
- Μεγέθους κλειδιού
- Ασφάλειας
- Χρήσης
- Υιοθέτησης

CATEGORY	**STATUS**	**ANALYSIS**
SPEED	FAST	Modern processors often include dedicated instructions for AES encryption and decryption (such as Intel's AES-NI - AES New Instructions). These instructions accelerate the AES algorithm, allowing for extremely fast encryption and decryption processes with minimal CPU overhead.
COST	LOW	The algorithm requires minimal computational resources, making it efficient for devices with limited processing power and energy resources, such as mobile devices and embedded systems. Also, the low latency of AES makes it ideal for real-time applications where quick data encryption and decryption are critical, such as in video streaming, online gaming, and secure communications.

TYPE	SYMMETRIC	Symmetric encryption uses the same key for both encryption and decryption, which means that both the sender and the receiver must have access to the same secret key. This contrasts with asymmetric encryption, which uses a pair of public and private keys.
KEY SIZE	128, 192, 256 bits	The different key sizes provide varying levels of security and performance. While all three key sizes offer strong security, a larger key size generally provides higher security but may slightly reduce performance due to increased computational requirements.
SECURITY	HIGH	The high security level of AES is due to its robust algorithm, which has been extensively analyzed and tested by cryptographic experts. It is resistant to all known practical attacks, including brute-force attacks, making it a reliable choice for securing sensitive data.
USES	WIDELY USED	Bulk Data Encryption: Encrypting large amounts of data efficiently. Secure Communications: Protecting data in transit over networks. File Encryption: Safeguarding data stored on disks or in the cloud. Wireless Network Security: Securing wireless communications, such as in WPA2 (Wi-Fi Protected Access II).

ADOPTION	WIDELY ADOPTED	AES was established as a standard by NIST (National Institute of Standards and Technology) in 2001, and it has since become the encryption standard used globally. Its wide adoption across various industries and applications underscores its reliability and trustworthiness.

Πίνακας 1 : Πίνακας ανάλυσης δυνατοτήτων AES.

CATEGORY	**STATUS**	**ANALYSIS**
SPEED	Moderate	PKI encryption and decryption processes are generally slower than symmetric encryption methods like AES due to the computational complexity involved in handling public and private keys.
COST	Higher	The cost is higher compared to symmetric encryption due to the need for managing public and private keys, certificates, and the supporting infrastructure.
TYPE	Asymmetric	PKI uses a pair of keys: a public key and a private key. The public key is used for encryption, while the private key is used for decryption. This key pair ensures secure communication without sharing private keys.
KEY SIZE	2048-4096 bits	The larger key sizes provide enhanced security but also require more computational power and resources for encryption and decryption processes.

SECURITY	Very High	PKI provides a high level of security using asymmetric encryption and digital certificates. It is resistant to many forms of cryptographic attacks, making it suitable for securing sensitive communications.
USES	Widely Used	Digital Signatures: Verifying the authenticity and integrity of digital messages and documents. Secure Communications: Protecting data in transit over the internet, such as in HTTPS. Email Security: Ensuring secure email communications through encryption and digital signatures. Authentication: Validating identities in various systems, including user authentication and software code signing.
ADOPTION	Widely Adopted	PKI is widely adopted in various industries, especially for secure communications, e-commerce, government applications, and secure email systems. Its adoption is supported by international standards and regulatory requirements.

Πίνακας 2 : Πίνακας ανάλυσης δυνατοτήτων PKI.

Ο συνδυασμός κρυπτογράφησης AES και υποδομής PKI παρέχει ένα ισχυρό πλαίσιο προστασίας ενάντια σε ποικίλες κυβερνοαπειλές. Το AES προσφέρει ισχυρή κρυπτογράφηση των δεδομένων, εξασφαλίζοντας την εμπιστευτικότητα και την ακεραιότητα, ενώ το PKI προσφέρει μηχανισμούς ταυτοποίησης και επαλήθευσης, εξασφαλίζοντας ότι οι επικοινωνίες είναι ασφαλείς και ότι μόνο εξουσιοδοτημένα μέρη έχουν πρόσβαση στις πληροφορίες. Αυτά τα τεχνικά μέτρα συνεργάζονται για να παρέχουν μια ολοκληρωμένη λύση ασφάλειας πληροφοριών.

5.4 Διαίρεση Δικτύου (ACL)

Η διαίρεση δικτύου με τη χρήση λιστών ελέγχου πρόσβασης ACL είναι μια μέθοδος διαχείρισης και προστασίας δικτύων υπολογιστών. Οι ACL χρησιμοποιούνται για τον έλεγχο της κίνησης των δεδομένων στο δίκτυο, επιτρέποντας ή απορρίπτοντας συγκεκριμένα πακέτα δεδομένων βάσει προκαθορισμένων κανόνων. Αυτή η διαδικασία είναι κρίσιμη για την ασφάλεια και την αποτελεσματική λειτουργία των δικτύων.

Η διαίρεση δικτύου μέσω ACL πραγματοποιείται με τους εξής τρόπους:

• Καθορισμός Κανόνων: Οι ACL αποτελούνται από μια σειρά κανόνων που καθορίζουν ποιοι τύποι κίνησης επιτρέπονται ή απορρίπτονται. Κάθε κανόνας περιλαμβάνει πληροφορίες όπως η διεύθυνση IP πηγής, η διεύθυνση IP προορισμού, οι θύρες και το πρωτόκολλο επικοινωνίας. Οι κανόνες μπορούν να είναι αρκετά συγκεκριμένοι ή γενικοί, ανάλογα με τις ανάγκες του δικτύου.

• Εφαρμογή σε Διεπαφές Δικτύου: Οι ACL εφαρμόζονται σε συγκεκριμένες διεπαφές δικτύου (network interfaces), όπως οι θύρες δρομολογητών ή οι διακόπτες δικτύου. Μπορούν να εφαρμοστούν είτε στην είσοδο (inbound) είτε στην έξοδο (outbound) των πακέτων δεδομένων, ελέγχοντας την κίνηση που εισέρχεται ή εξέρχεται από το δίκτυο.

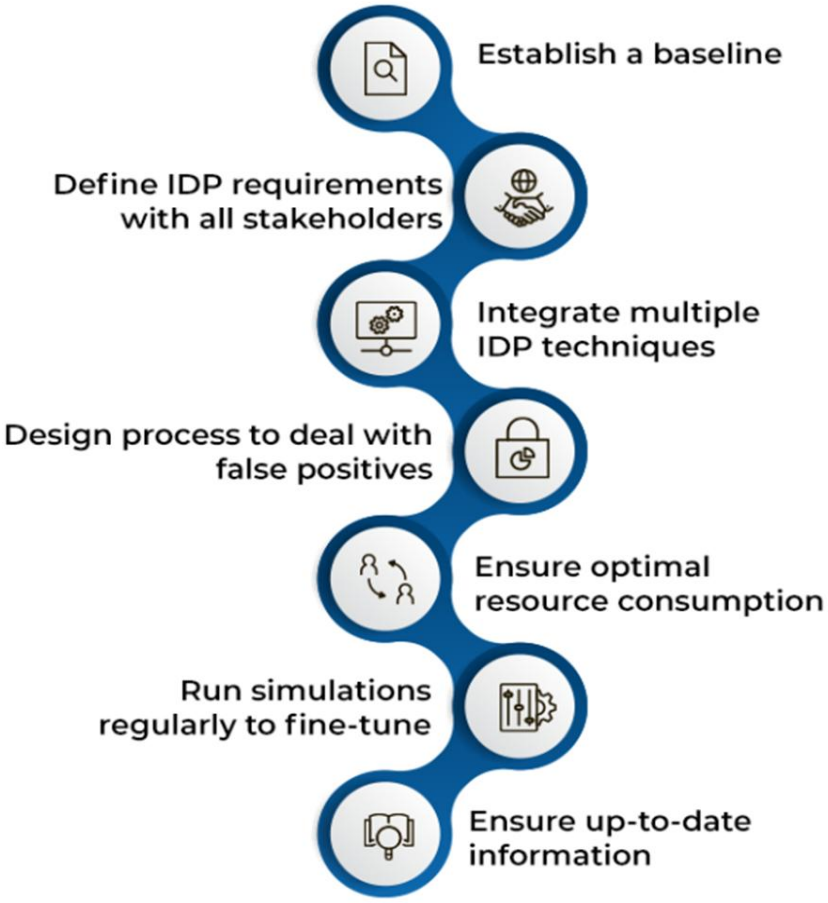
• Εκτέλεση Ελέγχων: Όταν ένα πακέτο δεδομένων εισέρχεται ή εξέρχεται από μια διεπαφή όπου εφαρμόζεται ACL, το πακέτο εξετάζεται βάσει των κανόνων της λίστας. Αν το πακέτο πληροί τους κανόνες, επιτρέπεται να συνεχίσει την πορεία του. Αν όχι, απορρίπτεται. Αυτή η διαδικασία εκτέλεσης ελέγχων είναι συνεχής και διασφαλίζει ότι μόνο οι επιτρεπόμενες κινήσεις επιτρέπονται στο δίκτυο.

Οι ACL παρέχουν διάφορα πλεονεκτήματα, όπως η βελτιωμένη ασφάλεια, καθώς επιτρέπουν μόνο εξουσιοδοτημένη κίνηση, και ο περιορισμός της πρόσβασης σε ευαίσθητα μέρη του δικτύου. Επίσης, οι ACL μπορούν να βοηθήσουν στη βελτίωση της απόδοσης του δικτύου, μειώνοντας την ανεπιθύμητη κίνηση. Παρά τα πλεονεκτήματά τους, οι ACL έχουν και περιορισμούς. Η διαχείριση μεγάλου αριθμού κανόνων μπορεί να γίνει περίπλοκη και χρονοβόρα. Επίσης, οι ACL δεν παρέχουν προστασία από όλες τις απειλές, όπως οι επιθέσεις που βασίζονται σε ανάλυση περιεχομένου πακέτων (deep packet inspection) ή οι επιθέσεις DDoS [55].

5.5 Συστήματα Ανίχνευσης και Πρόληψης Εισβολών (IDPS)

Τα Συστήματα Ανίχνευσης και Πρόληψης Εισβολών IDPS είναι κρίσιμα εργαλεία για την ασφάλεια των δικτύων και των συστημάτων πληροφορικής. Τα IDPS συνδυάζουν λειτουργίες ανίχνευσης και πρόληψης εισβολών, προσφέροντας μια ολοκληρωμένη προσέγγιση για την προστασία των πληροφοριακών συστημάτων από κακόβουλες δραστηριότητες. Η ανίχνευση εισβολών μπορεί να είναι δικτυακής βάσης (Network-based IDPS - NIDPS), που ελέγχει την κυκλοφορία δικτύου σε πραγματικό χρόνο για να εντοπίζει ύποπτες δραστηριότητες, ή βάσης υπολογιστή (Host-based IDPS - HIDPS), που ελέγχει τη δραστηριότητα σε συγκεκριμένους υπολογιστές ή διακομιστές, παρακολουθώντας αρχεία καταγραφής (logs), την ακεραιότητα των αρχείων και τις διαδικασίες του συστήματος. Η πρόληψη εισβολών επεμβαίνει ενεργά για να αποτρέψει την επιτυχή εκτέλεση κακόβουλων δραστηριοτήτων, μπλοκάροντας ύποπτες συνδέσεις δικτύου ή τερματίζοντας

επικίνδυνες διαδικασίες σε έναν κεντρικό υπολογιστή. Τα IDPS διαθέτουν εργαλεία ανάλυσης για τη διερεύνηση περιστατικών ασφάλειας και την ανάλυση της συμπεριφοράς των απειλών. Προσφέρουν αναφορές και ειδοποιήσεις στους διαχειριστές ασφάλειας για γρήγορη ανταπόκριση. Χρησιμοποιούν βάσεις δεδομένων με υπογραφές γνωστών επιθέσεων και τεχνικών, οι οποίες ανανεώνονται τακτικά για να παραμένουν ενημερωμένα με τις τελευταίες απειλές. Προηγμένα IDPS χρησιμοποιούν τεχνικές εκμάθησης μηχανής για την αναγνώριση νέων και αγνώστων απειλών, ενώ η ανάλυση συμπεριφοράς επιτρέπει την ανίχνευση ανωμαλιών που μπορεί να υποδηλώνουν μια εισβολή. Επίσης παρέχουν ένα επιπλέον επίπεδο ασφάλειας, ανιχνεύοντας και αποτρέποντας επιθέσεις που μπορεί να παρακάμψουν άλλες μορφές προστασίας. Προσφέρουν ειδοποιήσεις και αναφορές σε πραγματικό χρόνο, επιτρέποντας γρήγορη ανταπόκριση στις απειλές. Είναι εξίσου σημαντικό ότι βοηθούν τους οργανισμούς να συμμορφώνονται με κανονισμούς ασφάλειας δεδομένων, όπως το GDPR, το HIPAA και το PCI-DSS, παρέχοντας αποδείξεις παρακολούθησης και ανίχνευσης απειλών. Επιπλέον παρέχουν προστασία τόσο από εξωτερικές επιθέσεις όσο και από εσωτερικές απειλές, όπως κακόβουλους υπαλλήλους ή ακούσια σφάλματα χρήστη. Ωστόσο, αυτά τα συστήματα μπορεί να δημιουργήσουν ψευδώς θετικά (false positives), όπου κανονική δραστηριότητα ανιχνεύεται ως κακόβουλη, και ψευδώς αρνητικά (false negatives), όπου κακόβουλη δραστηριότητα δεν ανιχνεύεται. Η διαχείριση και η ρύθμιση των IDPS μπορεί να είναι πολύπλοκη και απαιτεί εξειδικευμένη γνώση και πόρους. Σε μεγάλα δίκτυα, η χρήση τους μπορεί να επηρεάσει την απόδοση του συστήματος, ιδιαίτερα αν η ανίχνευση γίνεται σε πραγματικό χρόνο [56].



Σχήμα 10: Διαδικασία IDPS [57].

Στο παραπάνω σχήμα παρουσιάζεται η διαδικασία εγκατάστασης και βελτιστοποίησης ενός Συστήματος Ανίχνευσης και Πρόληψης Εισβολών (IDPS) με τα εξής βήματα [57]:

- Καθορισμό των κανονικών επιπέδων δραστηριότητας στο δίκτυο ή στο σύστημα, έτσι ώστε να υπάρχει ένα σημείο αναφοράς για την ανίχνευση ανωμαλιών.
- Όλοι οι ενδιαφερόμενοι καθορίζουν τις συγκεκριμένες ανάγκες και απαιτήσεις του συστήματος IDPS, εξασφαλίζοντας ότι όλοι έχουν συμφωνήσει στους στόχους και τις προσδοκίες.
- Χρήση διαφορετικών τεχνικών και μεθόδων ανίχνευσης και πρόληψης για να καλύπτονται καλύτερα οι ποικίλες απειλές και τρωτά σημεία.
- Ο σχεδιασμός μιας διαδικασίας για την αντιμετώπιση ψευδών θετικών ανιχνεύσεων είναι κρίσιμος για να μην καταναλώνονται πόροι και να μην υπάρχει άσκοπη ανησυχία λόγω λανθασμένων συναγερμών.
- Διασφαλίζεται ότι το σύστημα IDPS δεν υπερφορτώνει τους πόρους του συστήματος, αλλά λειτουργεί αποτελεσματικά χωρίς να επηρεάζει την απόδοση.
- Οι τακτικές προσομοιώσεις επιτρέπουν τη συνεχή βελτιστοποίηση του συστήματος, διασφαλίζοντας ότι μπορεί να ανιχνεύει και να προλαμβάνει νέες και εξελισσόμενες απειλές.
- Διασφαλίζεται ότι το σύστημα IDPS παραμένει ενημερωμένο με τις τελευταίες απειλές και τεχνικές ανίχνευσης, μέσω τακτικών αναβαθμίσεων και ανανεώσεων των βάσεων δεδομένων .

5.6 Ασφαλής Διαμόρφωση Διαχείρισης

Η ασφαλής διαμόρφωση διαχείρισης είναι ένα σημαντικό πεδίο της κυβερνοασφάλειας που αφορά την προστασία των διαστημικών συστημάτων από ευπάθειες και επιθέσεις. Περιλαμβάνει την εφαρμογή συγκεκριμένων πρακτικών και πολιτικών για τη διασφάλιση ότι τα διαχειριστικά περιβάλλοντα και τα συστήματα ελέγχου είναι σωστά διαμορφωμένα, ασφαλή και ανθεκτικά σε κακόβουλες ενέργειες.

Επιπλέον περιλαμβάνει την εφαρμογή πολιτικών ασφαλείας, όπως τις πολιτικές κωδικών πρόσβασης και τις πολιτικές πρόσβασης. Χρησιμοποιούνται ισχυροί, μοναδικοί κωδικοί πρόσβασης που ανανεώνονται περιοδικά, ενώ εφαρμόζεται η αρχή του ελάχιστου δικαιώματος (least privilege) ώστε οι χρήστες να έχουν πρόσβαση μόνο στις πληροφορίες και τα συστήματα που είναι απαραίτητα για την εργασία τους.

Η διαμόρφωση συστήματος περιλαμβάνει την ενίσχυση του συστήματος, την αφαίρεση ή απενεργοποίηση μη απαραίτητων υπηρεσιών και εφαρμογών για τη μείωση της επιφάνειας επίθεσης και τη διατήρηση των συστημάτων και λογισμικών ενημερωμένων με τις τελευταίες εκδόσεις και κώδικες ασφαλείας. Επίσης, χρησιμοποιούνται ασφαλείς προεπιλεγμένες ρυθμίσεις στις συσκευές και τα συστήματα.

Η διαχείριση διαχειριστικών λογαριασμών περιλαμβάνει την ισχυρή ταυτοποίηση και πιστοποίηση, όπως η χρήση πολυπαραγοντικής ταυτοποίησης (MFA) για πρόσβαση στους

διαχειριστικούς λογαριασμούς. Η καταγραφή και παρακολούθηση των διαχειριστικών ενεργειών είναι επίσης σημαντική για την ανίχνευση ασυνήθιστων δραστηριοτήτων.

Η ασφαλής διαχείριση απομακρυσμένης πρόσβασης περιλαμβάνει τη χρήση κρυπτογραφημένων συνδέσεων, όπως το SSH και το VPN, για την ασφαλή απομακρυσμένη πρόσβαση, καθώς και τον περιορισμό του αριθμού των ατόμων που έχουν απομακρυσμένη πρόσβαση και τον περιορισμό της πρόσβασης σε συγκεκριμένες IP διευθύνσεις.

Ο συνεχής έλεγχος και η αξιολόγηση περιλαμβάνουν τη διεξαγωγή τακτικών ελέγχων και δοκιμών διείσδυσης για την αξιολόγηση της ασφάλειας των συστημάτων, καθώς και τη χρήση εργαλείων ανίχνευσης ευπαθειών και διορθωτικών ενεργειών για την αντιμετώπιση των εντοπισμένων αδυναμιών.

Τα διαστημικά συστήματα αντιμετωπίζουν μοναδικές προκλήσεις λόγω της φύσης τους, όπως η περιορισμένη φυσική πρόσβαση, οι μεγάλες χρονικές καθυστερήσεις και το περιβάλλον υψηλής ακτινοβολίας. Για την αντιμετώπιση αυτών των προκλήσεων, απαιτούνται αυστηρές κρυπτογραφικές πρακτικές, αυτόματες ενημερώσεις και εφαρμογή patches, επαναλαμβανόμενες δοκιμές ανθεκτικότητας και δυναμική διαχείριση πρόσβασης. Η ασφαλής διαμόρφωση διαχείρισης αποτελεί ουσιαστικό στοιχείο για την προστασία των διαστημικών συστημάτων από ευπάθειες και επιθέσεις. Με την εφαρμογή αυστηρών πολιτικών, τη χρήση προηγμένων τεχνολογιών ασφαλείας και τη συνεχή παρακολούθηση και αξιολόγηση, είναι δυνατή η δημιουργία ενός ασφαλούς και ανθεκτικού περιβάλλοντος διαχείρισης [58].

5.7 Ασφαλή Πρωτόκολλα Επικοινωνίας (TLS / SSL)

Τα ασφαλή πρωτόκολλα επικοινωνίας, όπως το TLS (Transport Layer Security) και το SSL (Secure Sockets Layer), παίζουν κρίσιμο ρόλο στην προστασία των δεδομένων κατά τη μεταφορά τους μέσω δικτύων, ιδιαίτερα στο διαδίκτυο. Αυτά τα πρωτόκολλα εξασφαλίζουν ότι οι επικοινωνίες είναι κρυπτογραφημένες και προστατεύουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων.

Το TLS είναι ο διάδοχος του SSL και έχει εξελιχθεί για να προσφέρει αυξημένα επίπεδα ασφάλειας. Η βασική λειτουργία του TLS είναι η παροχή κρυπτογράφησης στις επικοινωνίες μεταξύ διακομιστών και πελατών, όπως οι συνδέσεις μεταξύ ενός προγράμματος περιήγησης και ενός διακομιστή ιστού. Το TLS χρησιμοποιεί μια σειρά από κρυπτογραφικά πρωτόκολλα και αλγόριθμους για να επιτύχει αυτή την προστασία [59].

Η διαδικασία επικοινωνίας μέσω TLS περιλαμβάνει τα εξής στάδια:

- Στο στάδιο του handshake, ο πελάτης και ο διακομιστής διαπραγματεύονται τις παραμέτρους ασφαλείας που θα χρησιμοποιήσουν για τη σύνδεση, όπως η έκδοση του πρωτοκόλλου TLS και οι αλγόριθμοι κρυπτογράφησης. Ο διακομιστής αποστέλλει το ψηφιακό του πιστοποιητικό, το οποίο περιέχει το δημόσιο κλειδί του.
- Ο πελάτης επαληθεύει το πιστοποιητικό του διακομιστή και χρησιμοποιεί το δημόσιο κλειδί του διακομιστή για να κρυπτογραφήσει ένα τυχαίο μυστικό (pre-master secret). Αυτό το μυστικό αποστέλλεται στον διακομιστή και χρησιμοποιείται για τη δημιουργία του συμμετρικού κλειδιού κρυπτογράφησης.

- Το pre-master secret χρησιμοποιείται και από τα δύο μέρη για τη δημιουργία συμμετρικών κλειδιών κρυπτογράφησης, τα οποία θα χρησιμοποιηθούν για την κρυπτογράφηση των δεδομένων κατά τη διάρκεια της συνεδρίας.
- Μετά την ολοκλήρωση του handshake, τα δεδομένα που ανταλλάσσονται μεταξύ του πελάτη και του διακομιστή κρυπτογραφούνται με τα συμμετρικά κλειδιά, εξασφαλίζοντας την εμπιστευτικότητα και την ακεραιότητά τους.

Το SSL είναι ο προκάτοχος του TLS και αρχικά αναπτύχθηκε από την Netscape. Παρόλο που το TLS έχει αντικαταστήσει το SSL λόγω των βελτιώσεων στην ασφάλεια και την απόδοση, οι όροι συχνά χρησιμοποιούνται εναλλακτικά. Οι εκδόσεις του SSL, όπως το SSL 2.0 και το SSL 3.0, έχουν αποσυρθεί λόγω σοβαρών ευπαθειών και δεν πρέπει να χρησιμοποιούνται σε σύγχρονες εφαρμογές. Η χρήση ασφαλών πρωτοκόλλων επικοινωνίας, όπως το TLS, προσφέρει σημαντικά πλεονεκτήματα για την ασφάλεια των δεδομένων. Η κρυπτογράφηση δεδομένων εξασφαλίζει ότι τα δεδομένα που μεταφέρονται μεταξύ των μερών είναι κρυπτογραφημένα και δεν μπορούν να διαβαστούν από τρίτους. Μέσω της χρήσης ψηφιακών πιστοποιητικών, τα πρωτόκολλα TLS και SSL επαληθεύουν την ταυτότητα των μερών που συμμετέχουν στην επικοινωνία, αποφεύγοντας επιθέσεις τύπου man-in-the-middle. Τα πρωτόκολλα περιλαμβάνουν μηχανισμούς για την ανίχνευση αλλαγών στα δεδομένα που μεταφέρονται, εξασφαλίζοντας την ακεραιότητά τους. Μάλιστα το TLS είναι ευρέως αποδεκτό και υποστηρίζεται από όλους τους σημαντικούς browser και διακομιστές ιστού, καθιστώντας το μια αξιόπιστη λύση για ασφαλείς επικοινωνίες στο διαδίκτυο. Τα πρωτόκολλα TLS και SSL χρησιμοποιούνται ευρέως σε πολλές εφαρμογές και υπηρεσίες. Οι ιστότοποι που χρησιμοποιούν HTTPS προστατεύουν τις επικοινωνίες μεταξύ του browser και του διακομιστή. Τα πρωτόκολλα όπως το STARTTLS προσθέτουν ασφάλεια στις συνδέσεις SMTP, IMAP και POP3. Τα VPN χρησιμοποιούν το TLS για την ασφαλή μεταφορά δεδομένων μεταξύ απομακρυσμένων δικτύων. Οι υπηρεσίες Voice over IP συχνά χρησιμοποιούν το TLS για την προστασία των συνομιλιών. Η ενσωμάτωση ασφαλών πρωτοκόλλων επικοινωνίας είναι απαραίτητη για την προστασία των δεδομένων και την εξασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας στις ψηφιακές επικοινωνίες [59].

5.8 Μηχανισμοί Περιττότητας και Ανακατεύθυνσης

Οι μηχανισμοί περιττότητας (redundancy) και ανακατεύθυνσης (failover) αποτελούν βασικά τεχνικά μέτρα για την εξασφάλιση της διαθεσιμότητας και της ασταμάτητης λειτουργίας των συστημάτων, ιδιαίτερα σε κρίσιμα περιβάλλοντα όπως τα διαστημικά συστήματα που μελετάμε. Αυτοί οι μηχανισμοί διασφαλίζουν ότι σε περίπτωση αποτυχίας ενός συστήματος ή μιας συσκευής, υπάρχει ένας εφεδρικός πόρος έτοιμος να αναλάβει τη λειτουργία χωρίς διακοπή της υπηρεσίας. Αποτελούν βασικά τεχνικά μέτρα για την εξασφάλιση της συνεχούς και ασταμάτητης λειτουργίας των συστημάτων, ιδιαίτερα σε κρίσιμα περιβάλλοντα όπως τα διαστημικά συστήματα που μελετάμε. Αυτοί οι μηχανισμοί διασφαλίζουν ότι σε περίπτωση αποτυχίας ενός συστήματος ή μιας συσκευής, υπάρχει ένας εναλλακτικός πόρος έτοιμος να αναλάβει τη λειτουργία χωρίς διακοπή της υπηρεσίας.

Η περιττότητα αναφέρεται στη δημιουργία και διατήρηση εφεδρικών συστημάτων ή συσκευών που μπορούν να αντικαταστήσουν άμεσα τα πρωτεύοντα σε περίπτωση βλάβης ή αποτυχίας. Αυτό επιτυγχάνεται μέσω της χρήσης πλεονασματικών στοιχείων, όπως διπλές μονάδες τροφοδοσίας, εφεδρικούς διακομιστές, εναλλακτικές διαδρομές δικτύου και αντιγραφές δεδομένων σε πολλαπλές τοποθεσίες. Για παράδειγμα, σε ένα διαστημικό σύστημα, μπορεί να υπάρχουν πολλαπλές ανεξάρτητες διαδρομές επικοινωνίας ή πολλαπλές εφεδρικές μονάδες ελέγχου για να διασφαλιστεί ότι η αποτυχία μιας μονάδας δεν θα επηρεάσει την συνολική λειτουργία του συστήματος.

Η ανακατεύθυνση περιλαμβάνει τις διαδικασίες και τις τεχνολογίες που χρησιμοποιούνται για την αυτόματη μετάβαση από ένα αποτυχημένο σύστημα σε ένα εφεδρικό. Αυτό περιλαμβάνει την ανίχνευση της αποτυχίας, την ενεργοποίηση του εφεδρικού συστήματος και την ανακατεύθυνση της κυκλοφορίας ή των λειτουργιών χωρίς διακοπή της υπηρεσίας. Στα διαστημικά συστήματα, οι μηχανισμοί ανακατεύθυνσης πρέπει να είναι εξαιρετικά αξιόπιστοι και γρήγοροι λόγω της κρισιμότητας των λειτουργιών που υποστηρίζουν. Η υλοποίηση αυτών των μηχανισμών μπορεί να περιλαμβάνει τη χρήση τεχνολογιών όπως το VRRP για δικτυακές συσκευές ή τεχνολογίες αποθήκευσης που υποστηρίζουν real-time replication και failover.

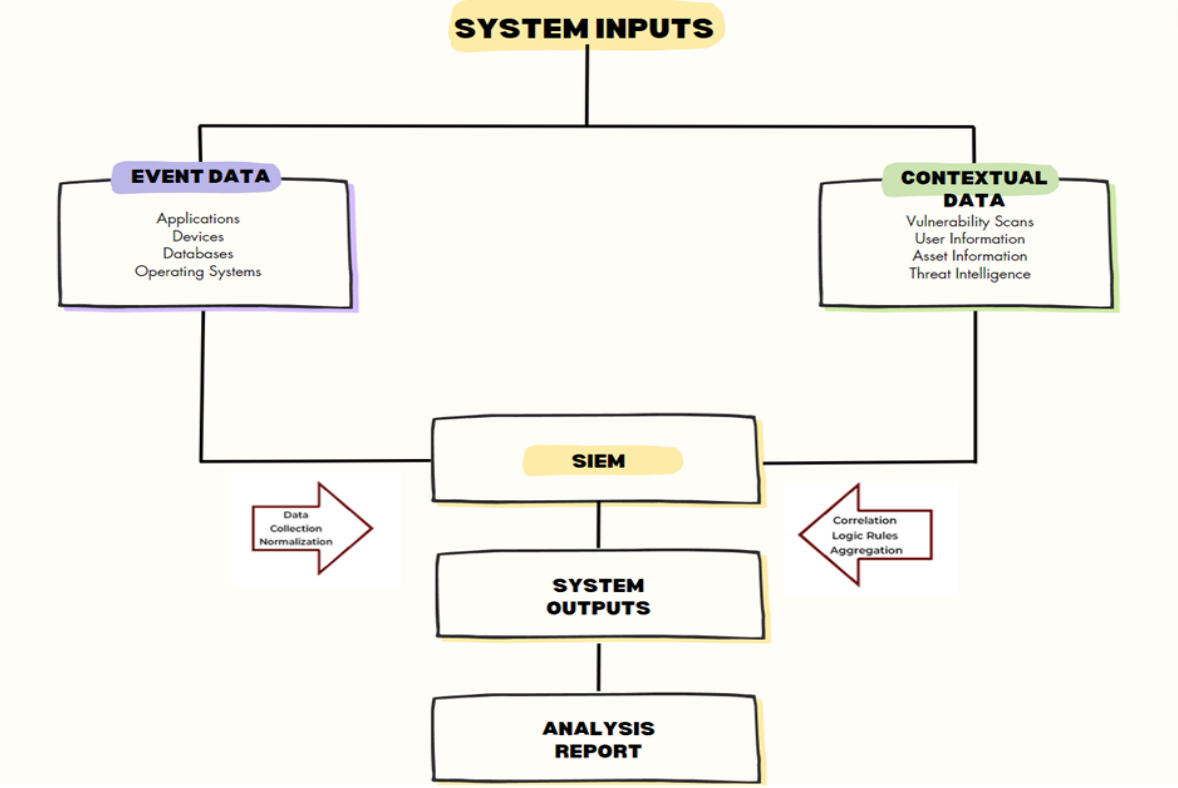
Η συνδυασμένη χρήση μηχανισμών περιττότητας και ανακατεύθυνσης συμβάλλει σημαντικά στη βελτίωση της ανθεκτικότητας και της αξιοπιστίας των συστημάτων. Για παράδειγμα, σε ένα διαστημικό σύστημα παρακολούθησης και ελέγχου, μπορεί να υπάρχουν πολλαπλά συστήματα ελέγχου και επικοινωνίας που λειτουργούν παράλληλα, ενώ ταυτόχρονα εφαρμόζονται πρωτόκολλα ανακατεύθυνσης που εξασφαλίζουν την αυτόματη μετάβαση σε εναλλακτικά συστήματα σε περίπτωση αποτυχίας. Η ανάπτυξη και η διαχείριση τέτοιων μηχανισμών απαιτούν προσεκτικό σχεδιασμό και συνεχείς δοκιμές για να διασφαλιστεί η αποτελεσματικότητά τους. Πρέπει να λαμβάνονται υπόψη παράγοντες όπως η ταχύτητα μετάβασης, η αξιοπιστία των εφεδρικών συστημάτων, και η δυνατότητα ανίχνευσης και αντιμετώπισης αποτυχιών σε πραγματικό χρόνο. Επιπλέον, η συνεχής παρακολούθηση και η τακτική αναβάθμιση αυτών των μηχανισμών είναι απαραίτητες για να αντιμετωπιστούν οι εξελισσόμενες απειλές και οι αλλαγές στις τεχνολογικές απαιτήσεις. Έτσι καταλήγουμε ότι οι μηχανισμοί περιττότητας και ανακατεύθυνσης είναι ουσιαστικά τεχνικά μέτρα για την εξασφάλιση της συνεχούς λειτουργίας και της διαθεσιμότητας των συστημάτων, ιδιαίτερα σε περιβάλλοντα με υψηλές απαιτήσεις όπως τα διαστημικά συστήματα. Η σωστή υλοποίηση και διαχείρισή τους μπορεί να προσφέρει σημαντικά οφέλη, μειώνοντας τους κινδύνους από αποτυχίες και διακοπές και εξασφαλίζοντας την ασταμάτητη παροχή υπηρεσιών [60].

5.9 Συνεχής Παρακολούθηση και Ανταπόκριση σε Περιστατικά (SIEM)

Η συνεχής παρακολούθηση και ανταπόκριση σε περιστατικά είναι ένας θεμελιώδης πυλώνας της κυβερνοασφάλειας, ιδιαίτερα για τα διαστημικά συστήματα, όπου η ασφάλεια και η ακεραιότητα των δεδομένων είναι κρίσιμη. Η εφαρμογή λύσεων SIEM επιτρέπει την ενσωμάτωση, ανάλυση και ανταπόκριση σε απειλές σε πραγματικό χρόνο, παρέχοντας μια ολοκληρωμένη άποψη της ασφάλειας του συστήματος. Η τεχνική SIEM συνδυάζει τη διαχείριση πληροφοριών ασφαλείας σε μία ενιαία πλατφόρμα. Αυτή η πλατφόρμα συλλέγει, αναλύει και συσχετίζει δεδομένα ασφαλείας από διάφορες πηγές σε πραγματικό χρόνο, επιτρέποντας την άμεση ανίχνευση και αντιμετώπιση

περιστατικών ασφαλείας. Η συνεχής παρακολούθηση περιλαμβάνει τη συλλογή και ανάλυση δεδομένων από διαφορετικές πηγές, όπως συσκευές δικτύου, διακομιστές, εφαρμογές και βάσεις δεδομένων. Τα δεδομένα αυτά περιλαμβάνουν καταγραφές συμβάντων, ειδοποιήσεις και ανιχνεύσεις ανωμαλιών. Με τη χρήση προηγμένων αλγορίθμων και τεχνικών μηχανικής μάθησης, μπορεί να εντοπιστεί ανώμαλη δραστηριότητα που ενδέχεται να υποδεικνύει μια απειλή ή μια επίθεση. Η ανταπόκριση σε περιστατικά μέσω SIEM περιλαμβάνει τη διαδικασία ανάλυσης και διαχείρισης των ανιχνευόμενων απειλών. Όταν το σύστημα εντοπίσει μια πιθανή απειλή, μπορεί να δημιουργήσει ειδοποιήσεις για την ομάδα ασφαλείας, να ενεργοποιήσει αυτοματοποιημένες ενέργειες ανταπόκρισης και να καταγράψει λεπτομερώς το περιστατικό για περαιτέρω ανάλυση. Οι αυτοματοποιημένες ενέργειες μπορούν να περιλαμβάνουν τον αποκλεισμό μιας κακόβουλης διεύθυνσης IP, την απομόνωση ενός παραβιασμένου συστήματος ή την ενεργοποίηση διαδικασιών αποκατάστασης [61].

Η υλοποίηση μιας τέτοιας λύσης στα διαστημικά συστήματα είναι ιδιαίτερα σημαντική λόγω των μοναδικών προκλήσεων που αυτά αντιμετωπίζουν, όπως οι μεγάλες αποστάσεις, οι καθυστερήσεις στην επικοινωνία και οι αυξημένες απαιτήσεις ασφαλείας. Η συνεχής παρακολούθηση επιτρέπει την άμεση ανίχνευση και ανταπόκριση σε απειλές, ελαχιστοποιώντας τον χρόνο αντίδρασης και μειώνοντας την πιθανότητα επιτυχίας μιας επίθεσης. Τέλος η αποτελεσματική χρήση του SIEM απαιτεί την προσεκτική επιλογή και παραμετροποίηση των εργαλείων και των συστημάτων που θα παρακολουθούνται. Πρέπει να καθοριστούν σαφείς πολιτικές και διαδικασίες για την παρακολούθηση, την ανάλυση και την ανταπόκριση σε περιστατικά. Επίσης, η συνεχής εκπαίδευση του προσωπικού και η τακτική αναθεώρηση των στρατηγικών ασφαλείας είναι απαραίτητες για τη διατήρηση της αποτελεσματικότητας του συστήματος SIEM.



Σχήμα 11: Διαδικασία λειτουργίας SIEM.

Στο παραπάνω σχήμα παρουσιάζεται η διαδικασία λειτουργίας ενός συστήματος. Αρχικά, συλλέγονται δεδομένα από διάφορες πηγές, όπως εφαρμογές, συσκευές, βάσεις δεδομένων και λειτουργικά συστήματα (Event Data), καθώς και από σαρώσεις ευπαθειών, πληροφορίες χρηστών, περιουσιακών στοιχείων και απειλών (Contextual Data). Αυτά τα δεδομένα εισέρχονται στο σύστημα SIEM, όπου πραγματοποιείται η συλλογή και κανονικοποίησή τους. Το SIEM λειτουργεί ως κεντρικός κόμβος επεξεργασίας, όπου τα δεδομένα αναλύονται μέσω συσχετίσεων, λογικών κανόνων και συσσωρεύσεων. Τα αποτελέσματα αυτής της επεξεργασίας παράγουν αναφορές και άλλες πληροφορίες για ανάλυση. Η τελική αναφορά (Analysis Report) παρέχει ολοκληρωμένη εικόνα της ασφάλειας του συστήματος. Το σχήμα στην ουσία απεικονίζει τη ροή πληροφοριών και τη διαδικασία επεξεργασίας, υπογραμμίζοντας τη σημασία της ενσωμάτωσης ποικίλων πηγών δεδομένων για την αποτελεσματική διαχείριση της ασφάλειας [61].

5.10 Ασφαλείς Πρακτικές Ανάπτυξης Λογισμικού (OWASP)

Οι ασφαλείς πρακτικές ανάπτυξης λογισμικού είναι κρίσιμες για την προστασία των εφαρμογών από επιθέσεις και ευπάθειες. Το OWASP είναι ένας παγκόσμιος οργανισμός που επικεντρώνεται στη βελτίωση της ασφάλειας του λογισμικού. Ο οργανισμός παρέχει οδηγίες και εργαλεία για την ανάπτυξη ασφαλών εφαρμογών. Ακολουθούν μερικές από τις βασικές ασφαλείς πρακτικές ανάπτυξης λογισμικού σύμφωνα με το OWASP:

- Κατανόηση και Εντοπισμός Απειλών και Κινδύνων: Είναι σημαντικό να γίνει κατανόηση των πιθανών απειλών και των κινδύνων που αντιμετωπίζει η εφαρμογή . Η ανάλυση κινδύνων και η εκτίμηση των απειλών μπορούν να βοηθήσουν στον εντοπισμό και την κατάταξη των ευπαθειών που πρέπει να αντιμετωπιστούν.

- Χρήση Ασφαλούς Κωδικοποίησης: Εφαρμογή ασφαλών πρακτικών κωδικοποίησης για να αποτραπούν κοινές ευπάθειες, όπως SQL Injection, XSS (Cross-Site Scripting), και CSRF , με βάση τις οδηγίες του OWASP Secure Coding Practices για να διασφαλίσετε ότι ο κώδικάς σας είναι ασφαλής.

- Επιβεβαίωση και Καθαρισμός Δεδομένων Εισόδου: Πάντα να γίνεται καθαρισμός και επιβεβαίωση των δεδομένων εισόδου από τους χρήστες για την αποτροπή της εισαγωγής κακόβουλων δεδομένων. Αυτό περιλαμβάνει τη χρήση whitelists και τη χρήση έτοιμων βιβλιοθηκών για την επιβεβαίωση των δεδομένων.

- Ασφαλής Διαχείριση Αυθεντικοποίησης και Εξουσιοδότησης: Διασφάλιση ότι οι μηχανισμοί αυθεντικοποίησης και εξουσιοδότησης είναι ισχυροί και ασφαλείς. Να γίνεται χρήση πρακτικών όπως η αποθήκευση κωδικών πρόσβασης με ισχυρούς αλγόριθμους hash και η υλοποίηση μηχανισμών multi-factor authentication (MFA).

- Ασφάλεια στην Επικοινωνία: Χρήση κρυπτογράφησης για την προστασία των δεδομένων κατά τη μεταφορά τους μέσω δικτύων. Χρήση πρωτοκόλλων όπως το TLS

(Transport Layer Security) για τη διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων.

- Καταγραφή και Παρακολούθηση: Εφαρμόζονται μηχανισμοί καταγραφής και παρακολούθησης για να εντοπίζουμε και να αναλύουμε πιθανές επιθέσεις ή παραβιάσεις ασφαλείας. Γίνεται χρήση εργαλείων SIEM για να συλλογή και να ανάλυση δεδομένων καταγραφής.

- Τακτική Ενημέρωση και Επιδιόρθωση Ευπαθειών: Διατήρηση συνεχών ενημερώσεων όλων των βιβλιοθηκών και των εξαρτημάτων με τις τελευταίες επιδιορθώσεις ασφαλείας. Ενσωμάτωση διαδικασιών για την τακτική αναγνώριση και επιδιόρθωση των ευπαθειών στον κώδικα της εφαρμογής μας.

- Εκπαίδευση Ομάδων Ανάπτυξης: Παροχή συνεχούς εκπαίδευσης στις ομάδες ανάπτυξής μας για τις τελευταίες πρακτικές ασφαλείας και τις νέες απειλές. Οι προγραμματιστές πρέπει να είναι ενημερωμένοι για τις αρχές της ασφαλούς ανάπτυξης λογισμικού και τις τεχνικές ανάλυσης ευπαθειών.

- Δοκιμή Ασφαλείας Λογισμικού: Ενσωμάτωση δοκιμών ασφαλείας στη διαδικασία ανάπτυξης λογισμικού μας. Αυτό περιλαμβάνει την εκτέλεση στατικών και δυναμικών αναλύσεων κώδικα, καθώς και τη χρήση εργαλείων όπως τα OWASP ZAP για την αναγνώριση και την αξιολόγηση των ευπαθειών στις εφαρμογές.

- Διαχείριση και Ασφάλεια Συστημάτων Παραγωγής: Τα συστήματα παραγωγής πρέπει να είναι σίγουρο ότι είναι σωστά διαμορφωμένα και ασφαλή. Γίνεται χρήση πρακτικών όπως η ελαχιστοποίηση της επιφάνειας επίθεσης, η εφαρμογή των αρχών ελαχιστοποίησης δικαιωμάτων και η προστασία των διακομιστών με ενημερωμένα τείχη προστασίας και λογισμικά ασφαλείας.

Οι ασφαλείς πρακτικές ανάπτυξης λογισμικού που προτείνει το OWASP βοηθούν τους οργανισμούς να προστατεύσουν τις εφαρμογές τους από ευπάθειες και να εξασφαλίσουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων. Ακολουθώντας αυτές τις πρακτικές, οι προγραμματιστές μπορούν να δημιουργήσουν πιο ασφαλείς και αξιόπιστες εφαρμογές [62].

5.11 Εκπαίδευση και Ευαισθητοποίηση στην Κυβερνοασφάλεια

Η εκπαίδευση και η ευαισθητοποίηση στην κυβερνοασφάλεια είναι θεμελιώδεις πτυχές για τη δημιουργία ενός ασφαλούς περιβάλλοντος σε οποιονδήποτε οργανισμό, ιδιαίτερα στα διαστημικά συστήματα που απαιτούν υψηλό επίπεδο ασφάλειας και προστασίας. Πρώτα απ' όλα η συνεχής εκπαίδευση του προσωπικού και η ευαισθητοποίηση σχετικά με τις απειλές και τις βέλτιστες πρακτικές κυβερνοασφάλειας αποτελούν κρίσιμα τεχνικά μέτρα για την αντιμετώπιση των ευπαθειών και των επιθέσεων. Η εκπαίδευση περιλαμβάνει την παροχή στοχευμένων

εκπαιδευτικών προγραμμάτων που καλύπτουν βασικές και προχωρημένες έννοιες της ασφάλειας πληροφοριών. Αυτά τα προγράμματα μπορεί να περιλαμβάνουν θέματα όπως η διαχείριση κωδικών πρόσβασης, η αναγνώριση phishing επιθέσεων, η ασφαλής χρήση των δικτυακών πόρων και οι διαδικασίες αναφοράς περιστατικών ασφαλείας. Η εκπαίδευση αυτή πρέπει να είναι τακτική και να ανανεώνεται συνεχώς για να καλύπτει τις νέες απειλές και τις τεχνολογικές εξελίξεις. Αξίζει να σημειωθεί ότι η ευαισθητοποίηση στην κυβερνοασφάλεια επικεντρώνεται στην καλλιέργεια μιας κουλτούρας ασφάλειας μέσα στον οργανισμό. Περιλαμβάνει τη συνεχή ενημέρωση του προσωπικού για τις τρέχουσες απειλές, τις νέες μεθόδους επίθεσης και τις βέλτιστες πρακτικές για την αποφυγή τους. Αυτό μπορεί να επιτευχθεί μέσω τακτικών ενημερωτικών δελτίων, σεμιναρίων, διαδικτυακών σεμιναρίων (webinars) και προσομοιώσεων επιθέσεων (όπως phishing campaigns).

Η εφαρμογή προγραμμάτων εκπαίδευσης και ενημέρωσης απαιτεί τη δέσμευση της διοίκησης και την ενσωμάτωσή τους στην ευρύτερη στρατηγική ασφαλείας του οργανισμού. Είναι σημαντικό να δημιουργηθεί ένα περιβάλλον όπου οι εργαζόμενοι αισθάνονται άνετα να αναφέρουν ύποπτες δραστηριότητες και να ζητούν βοήθεια όταν την χρειάζονται. Οι πολιτικές ασφάλειας πρέπει να είναι σαφείς και εύκολα προσβάσιμες, ενώ η εκπαίδευση πρέπει να προσαρμόζεται στις ανάγκες και το επίπεδο γνώσεων των εργαζομένων.

Για τα διαστημικά συστήματα, η εκπαίδευση και η ευαισθητοποίηση έχουν επιπλέον σημασία λόγω της πολυπλοκότητας και της κρισιμότητας των υποδομών που προστατεύουν. Το προσωπικό που εργάζεται σε αυτά τα συστήματα πρέπει να είναι καλά ενημερωμένο για τις ειδικές απειλές που αντιμετωπίζουν, όπως οι κυβερνοεπιθέσεις σε δορυφόρους ή οι προσπάθειες παρεμβολής στις επικοινωνίες. Η εκπαίδευση πρέπει να καλύπτει θέματα όπως η φυσική ασφάλεια των εγκαταστάσεων, η ασφάλεια των επικοινωνιών και η προστασία των ευαίσθητων δεδομένων [63].

5.12 Κοινοποίηση Πληροφοριών με Συνεργατικό Τρόπο (ISAC)

Η κοινοποίηση πληροφοριών με συνεργατικό τρόπο μέσω των Κέντρων Ανάλυσης και Κοινοποίησης Πληροφοριών ISACs αποτελεί ένα κρίσιμο τεχνικό μέτρο για την καταπολέμηση των ευπαθειών και την ενίσχυση της ασφάλειας στα διαστημικά συστήματα. Τα ISACs είναι οργανισμοί που συγκροτούνται για να διευκολύνουν τη συνεργασία και την ανταλλαγή πληροφοριών σχετικά με απειλές, ευπάθειες και βέλτιστες πρακτικές ασφάλειας μεταξύ οργανισμών που δραστηριοποιούνται σε συγκεκριμένους τομείς. Η αποστολή των ISACs είναι να παρέχουν στα μέλη τους έγκαιρη και ακριβή πληροφόρηση σχετικά με τις τρέχουσες και νέες απειλές. Αυτές οι πληροφορίες περιλαμβάνουν δεδομένα για κυβερνοεπιθέσεις, αναλύσεις ευπαθειών, συμβουλές ασφαλείας και στρατηγικές απόκρισης σε περιστατικά. Μέσω της ανταλλαγής αυτών των πληροφοριών, οι οργανισμοί μπορούν να προετοιμαστούν καλύτερα και να αντιδράσουν αποτελεσματικότερα σε επιθέσεις, μειώνοντας τους κινδύνους και ελαχιστοποιώντας τις επιπτώσεις των περιστατικών ασφαλείας. Η συμμετοχή σε ένα ISAC προσφέρει πολλαπλά οφέλη στους οργανισμούς. Πρώτον, παρέχει πρόσβαση σε συλλογική γνώση και εμπειρία, η οποία μπορεί να βελτιώσει σημαντικά την ικανότητα ανίχνευσης και απόκρισης σε απειλές. Δεύτερον, επιτρέπει τη γρήγορη κοινοποίηση πληροφοριών για νέες απειλές και ευπάθειες, δίνοντας τη δυνατότητα στα μέλη να εφαρμόσουν άμεσα μέτρα προστασίας. Τρίτον, ενθαρρύνει τη συνεργασία και την εμπιστοσύνη μεταξύ των μελών, διευκολύνοντας την ανάπτυξη κοινών λύσεων και πρωτοβουλιών για την ασφάλεια. Για τα διαστημικά συστήματα, η συνεργατική προσέγγιση μέσω ISACs είναι ιδιαίτερα σημαντική λόγω της πολυπλοκότητας και της κρισιμότητας των υποδομών

που εμπλέκονται. Οι οργανισμοί που διαχειρίζονται διαστημικά συστήματα πρέπει να αντιμετωπίζουν μοναδικές απειλές, όπως οι κυβερνοεπιθέσεις σε δορυφορικές επικοινωνίες και οι προσπάθειες παρεμβολής στις αποστολές διαστήματος. Μέσω αυτών, αυτοί οι οργανισμοί μπορούν να μοιράζονται πληροφορίες για τις ειδικές απειλές που αντιμετωπίζουν και να αναπτύσσουν κοινές στρατηγικές για την προστασία των διαστημικών υποδομών.

Η λειτουργία τους απαιτεί μια δομημένη προσέγγιση για τη συλλογή, ανάλυση και διανομή πληροφοριών. Περιλαμβάνει τη δημιουργία ασφαλών καναλιών επικοινωνίας για την ανταλλαγή πληροφοριών, την εφαρμογή αυστηρών πρωτοκόλλων για την προστασία των δεδομένων και τη διασφάλιση της εμπιστευτικότητας των κοινοποιήσεων. Επιπλέον, συνεργάζονται στενά με κυβερνητικές αρχές, ρυθμιστικούς φορείς και άλλους σχετικούς οργανισμούς για να ενισχύσουν την ασφάλεια σε εθνικό και διεθνές επίπεδο. Συμπερασματικά, γίνεται αντιληπτό ότι η κοινοποίηση πληροφοριών με συνεργατικό τρόπο μέσω των ISACs είναι ένα ουσιαστικό τεχνικό μέτρο για την ενίσχυση της ασφάλειας στα διαστημικά συστήματα. Η συμμετοχή σε ISACs επιτρέπει στους οργανισμούς να μοιράζονται κρίσιμες πληροφορίες, να βελτιώνουν τη συλλογική τους άμυνα και να ανταποκρίνονται αποτελεσματικά σε απειλές. Μέσω της συνεργασίας και της ανταλλαγής πληροφοριών, οι οργανισμοί μπορούν να προστατεύσουν καλύτερα τις διαστημικές υποδομές και να διασφαλίσουν τη συνεχή λειτουργία και ασφάλεια των συστημάτων τους [64].

6

Έλλειψη Προτύπων/Κανονισμών για την Κυβερνοασφάλεια στο Διάστημα

Η κυβερνοασφάλεια στο διάστημα αποτελεί έναν αυξανόμενα κρίσιμο τομέα, καθώς η εξάρτηση των εθνών από τις διαστημικές τεχνολογίες και υπηρεσίες συνεχίζει να αυξάνεται. Οι διαστημικές υποδομές, όπως οι δορυφόροι, οι επικοινωνίες και τα συστήματα πλοήγησης, είναι ευάλωτες σε κυβερνοεπιθέσεις, που μπορούν να έχουν σοβαρές συνέπειες για την εθνική ασφάλεια, την οικονομία και την καθημερινή ζωή. Παρά την αυξανόμενη σημασία της ασφάλειας των διαστημικών συστημάτων, υπάρχει έλλειψη ενωμένων προτύπων και κανονισμών που να διασφαλίζουν την αποτελεσματική προστασία των διαστημικών υποδομών από κυβερνοαπειλές. Σε αυτό το κεφάλαιο, θα εξετάσουμε τις εθνικές προοπτικές, τους διεθνείς οργανισμούς και κανονισμούς, καθώς και τις προσπάθειες που γίνονται για την ανάπτυξη και εφαρμογή προτύπων και κανονισμών για την κυβερνοασφάλεια στο διάστημα.

6.1 Εθνικές Προοπτικές

Κάθε χώρα αντιμετωπίζει την κυβερνοασφάλεια στο διάστημα με βάση τις εθνικές της ανάγκες, τις τεχνολογικές της δυνατότητες και τις πολιτικές της προτεραιότητες. Οι εθνικές πολιτικές ασφάλειας στο διάστημα ποικίλλουν σημαντικά, ανάλογα με τις διαφορετικές προσεγγίσεις και στρατηγικές που υιοθετούνται για την προστασία των διαστημικών υποδομών και υπηρεσιών από κυβερνοαπειλές. Θα εξετάσουμε τις πολιτικές και κανονισμούς της Κίνας, της Ρωσίας, των Ηνωμένων Πολιτειών και του Ηνωμένου Βασιλείου.

6.1.1 Πολιτικές Πληροφοριών και Ασφάλειας της Κίνας

Η Κίνα έχει επενδύσει σημαντικά στην ανάπτυξη και εφαρμογή πολιτικών και κανονισμών που αφορούν την κυβερνοασφάλεια, ειδικά στον τομέα του διαστήματος. Η χώρα έχει διαμορφώσει ένα ολοκληρωμένο πλαίσιο που καλύπτει την ασφάλεια των πληροφοριών, την προστασία των δεδομένων και την κυβερνοασφάλεια των διαστημικών συστημάτων. Αυτή η προσέγγιση δίνει σημασία στις εθνικές της ανάγκες για αυτονομία και ασφάλεια στις διαστημικές της επιχειρήσεις καθώς και στον έμμεσο σκοπό της να καταστεί παγκόσμιος ηγέτης στον τομέα του διαστήματος.

Ο Νόμος για την Ασφάλεια στον Κυβερνοχώρο (Cybersecurity Law of the People’s Republic of China), που εφαρμόστηκε το 2017, είναι ο βασικός νόμος που ρυθμίζει την κυβερνοασφάλεια

στην Κίνα. Καλύπτει την προστασία των δικτύων, των πληροφοριακών συστημάτων και των δεδομένων, επιβάλλοντας αυστηρές απαιτήσεις για την αποθήκευση και την προστασία των δεδομένων εντός της χώρας. Ο νόμος απαιτεί από τις εταιρείες να εφαρμόζουν μέτρα ασφαλείας για την προστασία των κρίσιμων πληροφοριακών υποδομών CII, που περιλαμβάνουν και τις διαστημικές υποδομές [65].

Ο Νόμος για την Προστασία των Προσωπικών Δεδομένων PIPL, που καθιερώθηκε το 2021, ρυθμίζει τη συλλογή, επεξεργασία και αποθήκευση προσωπικών δεδομένων. Προβλέπει αυστηρά μέτρα ασφαλείας για την προστασία των προσωπικών δεδομένων από κακόβουλες ενέργειες, με ιδιαίτερη σημασία για την κυβερνοασφάλεια, καθώς τα προσωπικά δεδομένα μπορούν να χρησιμοποιηθούν για την προστασία των διαστημικών υποδομών [65].

Οι Κανονισμοί για την Προστασία των Κρίσιμων Πληροφοριακών Υποδομών (Regulations on the Protection of Critical Information Infrastructure), που εκδόθηκαν το 2021, προβλέπουν ειδικά μέτρα για την προστασία των κρίσιμων πληροφοριακών υποδομών. Οι διαστημικές υποδομές θεωρούνται μέρος των κρίσιμων πληροφοριακών υποδομών και υπακούουν σε αυστηρούς κανόνες ασφαλείας [65].

Η Κίνα έχει επίσης ορίσει μια σειρά από εθνικά πρότυπα για την κυβερνοασφάλεια, όπως τα GB/T 22239-2008 και GB/T 25070-2010, που καλύπτουν τη διαχείριση της ασφάλειας πληροφοριακών συστημάτων και την ασφάλεια των δικτύων. Τα πρότυπα αυτά παρέχουν τις κατευθυντήριες γραμμές για την ανάπτυξη και εφαρμογή πολιτικών ασφαλείας σε διάφορους τομείς, συμπεριλαμβανομένου του διαστήματος [65].

Το Πρόγραμμα Κριτικής Πληροφοριακής Υποδομής CIIPP είναι ένα εθνικό πρόγραμμα που στοχεύει στην προστασία των κρίσιμων πληροφοριακών υποδομών μέσω της ενίσχυσης των μέτρων ασφαλείας και της εφαρμογής προοδευτικών τεχνολογιών. Εφαρμόζεται σε όλες τις κρίσιμες υποδομές, συμπεριλαμβανομένων των διαστημικών, για να διασφαλίσει την ανθεκτικότητα και την ασφάλειά τους από κυβερνοαπειλές [65].

Το Κέντρο Κυβερνοασφάλειας και Προστασίας των Δεδομένων (Cybersecurity and Data Protection Center) είναι ένα εθνικό κέντρο που δημιουργήθηκε για την παρακολούθηση και διαχείριση της κυβερνοασφάλειας. Παρέχει υποστήριξη και καθοδήγηση για την εφαρμογή πολιτικών και μέτρων ασφαλείας στις διαστημικές υποδομές [65].

Η Εθνική Στρατηγική Κυβερνοασφάλειας (National Cybersecurity Strategy) περιλαμβάνει οδηγίες και στόχους για την προστασία των διαστημικών υποδομών από κυβερνοαπειλές. Προωθεί τη συνεργασία μεταξύ των διαφόρων κυβερνητικών φορέων, ιδιωτικών εταιρειών και ακαδημαϊκών ιδρυμάτων για την ανάπτυξη καινοτόμων λύσεων κυβερνοασφάλειας [65].

Το Πρόγραμμα Ανάπτυξης Διαστημικής Τεχνολογίας (Space Technology Development Program) είναι ένα πρόγραμμα που στοχεύει στην προώθηση της ανάπτυξης προηγμένων διαστημικών τεχνολογιών. Εστιάζει στην ενσωμάτωση μέτρων κυβερνοασφάλειας στις νέες διαστημικές τεχνολογίες και συστήματα για να διασφαλιστεί η ανθεκτικότητα τους [65].

Συμπερασματικά η Κίνα με τη διαμόρφωση ενός ισχυρού και ολοκληρωμένου πλαισίου για την κυβερνοασφάλεια των διαστημικών της συστημάτων, δείχνει την αποφασιστικότητά της να προστατεύσει τις διαστημικές της υποδομές και να διασφαλίσει την ασφάλεια και ακεραιότητα των διαστημικών της επιχειρήσεων. Οι νομοθετικές πρωτοβουλίες και τα πρότυπα που έχουν δημιουργηθεί αποτελούν θεμέλια για την ανάπτυξη μιας ασφαλούς και ανθεκτικής διαστημικής βιομηχανίας.

6.1.2 Πολιτική Ασφάλειας της Ρωσίας

Η Ρωσία έχει αναπτύξει και εφαρμόζει αυστηρές πολιτικές ασφάλειας που περιλαμβάνουν την προστασία των διαστημικών της υποδομών από κυβερνοαπειλές. Η προσέγγιση της Ρωσίας στην κυβερνοασφάλεια κινείται με βάση την ανάγκη της να προστατεύσει τις διαστημικές της επιχειρήσεις από εξωτερικές απειλές, καθώς και να διατηρήσει την ισχύ της στον τομέα του διαστήματος. Ακολουθούν αναλυτικές πληροφορίες σχετικά με τους νόμους, τα πρότυπα και τις στρατηγικές που εφαρμόζει η Ρωσία για την κυβερνοασφάλεια στο διάστημα.

Η Ομοσπονδιακή Νομοθεσία για την Ασφάλεια των Πληροφοριών (Federal Law on Information Security), που ιδρύθηκε το 1995 και έχει τροποποιηθεί αρκετές φορές, παρέχει το νομικό πλαίσιο για την ασφάλεια των πληροφοριών στη Ρωσία. Ο νόμος αυτός καλύπτει την προστασία των πληροφοριακών συστημάτων και των δικτύων από κυβερνοαπειλές και επιθέσεις, επιβάλλοντας αυστηρές απαιτήσεις για την προστασία των δεδομένων και των κρίσιμων υποδομών [66].

Ο Νόμος για την Ασφάλεια στον Κυβερνοχώρο (Cybersecurity Law) ορίστηκε το 2016 και στοχεύει στην ενίσχυση της προστασίας των κρίσιμων πληροφοριακών υποδομών της Ρωσίας. Ο νόμος περιλαμβάνει μέτρα για την ανίχνευση, την πρόληψη και την αντιμετώπιση κυβερνοεπιθέσεων, καθώς και κατευθυντήριες γραμμές για την εφαρμογή τεχνολογιών ασφαλείας στις κρίσιμες υποδομές, συμπεριλαμβανομένων των διαστημικών συστημάτων [67].

Η Ρωσία έχει δημιουργήσει μια σειρά από εθνικά πρότυπα για την ασφάλεια των πληροφοριών και την κυβερνοασφάλεια, όπως τα GOST R 50922-96 και GOST R 51583-2000, που καλύπτουν τη διαχείριση της ασφάλειας πληροφοριακών συστημάτων και δικτύων. Αυτά τα πρότυπα παρέχουν οδηγίες για την ανάπτυξη και εφαρμογή πολιτικών ασφαλείας σε διάφορους τομείς, περιλαμβανομένου του διαστημικού [68].

Η Κεντρική Υπηρεσία για την Ασφάλεια στον Κυβερνοχώρο FSTEC είναι ο κύριος φορέας που επιβλέπει την εφαρμογή των πολιτικών κυβερνοασφάλειας στη Ρωσία. Η FSTEC παρέχει υποστήριξη και καθοδήγηση για την ανάπτυξη και εφαρμογή μέτρων ασφαλείας στις κρίσιμες πληροφοριακές υποδομές, συμπεριλαμβανομένων των διαστημικών [69].

Η Εθνική Στρατηγική Ασφάλειας του Πληροφοριακού Χώρου (National Security Strategy in the Information Space), που ανακοινώθηκε το 2016, καθορίζει τους στόχους και τις κατευθυντήριες γραμμές για την προστασία των πληροφοριακών υποδομών της Ρωσίας από κυβερνοαπειλές. Η στρατηγική αυτή προωθεί τη συνεργασία μεταξύ των κρατικών φορέων και των ιδιωτικών επιχειρήσεων για την ανάπτυξη και εφαρμογή μέτρων ασφαλείας [70].

Το Πρόγραμμα Ανάπτυξης Διαστημικής Τεχνολογίας (Space Technology Development Program) της Ρωσίας στοχεύει στην ενίσχυση της ασφάλειας των διαστημικών συστημάτων μέσω της ενσωμάτωσης προηγμένων τεχνολογιών ασφαλείας. Το πρόγραμμα αυτό περιλαμβάνει την ανάπτυξη νέων τεχνολογιών και συστημάτων που μπορούν να ανιχνεύσουν και να αποτρέψουν κυβερνοεπιθέσεις στις διαστημικές υποδομές [71].

Η Στρατηγική Κυβερνοασφάλειας της Ρωσίας (Cybersecurity Strategy of Russia), που θεσπίστηκε το 2014, εστιάζει στην ενίσχυση των δυνατοτήτων κυβερνοάμυνας της χώρας. Η στρατηγική αυτή περιλαμβάνει την ανάπτυξη και εφαρμογή προηγμένων τεχνολογιών ασφαλείας, την εκπαίδευση του προσωπικού και την προώθηση της διεθνούς συνεργασίας για την αντιμετώπιση των κυβερνοαπειλών [71].

Οι πολιτικές που εφαρμόζει η Ρωσία, μέσω των νομοθετικών πρωτοβουλιών, των προτύπων και των στρατηγικών της, στοχεύει να διασφαλίσει την ανθεκτικότητα και την ασφάλεια των

διαστημικών της υποδομών από κυβερνοαπειλές. Οι πολιτικές της δείχνουν την ανάγκη της να προστατεύσει τις κρίσιμες πληροφοριακές υποδομές της και να διατηρήσει την ισχύ της στον τομέα του διαστήματος. Με την εφαρμογή αυστηρών μέτρων ασφαλείας και την προώθηση της συνεργασίας, η Ρωσία ενισχύει τη δυνατότητά της να αντιμετωπίζει τις σύγχρονες κυβερνοαπειλές και να προστατεύει τις διαστημικές της επιχειρήσεις.

6.1.3 Πολιτικές Κυβερνοασφάλειας και Διαστημικής Ασφάλειας του Ηνωμένου Βασιλείου

Το Ηνωμένο Βασίλειο διαθέτει ισχυρές πολιτικές και κανονισμούς που αφορούν την κυβερνοασφάλεια και την ασφάλεια των διαστημικών υποδομών του. Η προσέγγιση της χώρας αντικατοπτρίζει την ανάγκη προστασίας των διαστημικών της συστημάτων από κυβερνοαπειλές, καθώς και την προώθηση της συνεργασίας με διεθνείς εταίρους. Ακολουθούν αναλυτικές πληροφορίες σχετικά με τους νόμους, τα πρότυπα και τις στρατηγικές που εφαρμόζει το Ηνωμένο Βασίλειο για την κυβερνοασφάλεια στο διάστημα.

Ο Νόμος για την Προστασία των Δεδομένων 2018 (Data Protection Act 2018) ενσωματώνει τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης στο εθνικό δίκαιο του Ηνωμένου Βασιλείου. Αυτός ο νόμος επιβάλλει αυστηρές απαιτήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα και την ασφάλεια των πληροφοριακών συστημάτων. Ειδικά για τον τομέα του διαστήματος, αυτό σημαίνει ότι οι οργανισμοί που διαχειρίζονται διαστημικά δεδομένα πρέπει να εφαρμόζουν μέτρα για την προστασία τους από κακόβουλες ενέργειες [72].

Ο Νόμος για την Ασφάλεια στον Κυβερνοχώρο 2018 γνωστός και ως NIS Regulations, εφαρμόζεται για την ενίσχυση της ασφάλειας των δικτύων και των πληροφοριακών συστημάτων κρίσιμων υποδομών, συμπεριλαμβανομένων των διαστημικών συστημάτων. Ο νόμος απαιτεί από τους οργανισμούς να εφαρμόζουν μέτρα ασφαλείας, να αναφέρουν περιστατικά ασφαλείας και να διασφαλίζουν την ανθεκτικότητα των συστημάτων τους [73].

Το Εθνικό Κέντρο Κυβερνοασφάλειας NCSC, που ιδρύθηκε το 2016, είναι ο κύριος φορέας που επιβλέπει την εφαρμογή των πολιτικών κυβερνοασφάλειας στο Ηνωμένο Βασίλειο. Το NCSC παρέχει καθοδήγηση, υποστήριξη και συμβουλές για την προστασία των κρίσιμων πληροφοριακών υποδομών, συμπεριλαμβανομένων των διαστημικών. Το κέντρο εργάζεται στενά με κυβερνητικούς φορείς, επιχειρήσεις και ακαδημαϊκούς για την ενίσχυση της κυβερνοασφάλειας [74].

Η Εθνική Στρατηγική Κυβερνοασφάλειας 2016-2021 (National Cyber Security Strategy 2016-2021) καθορίζει τους στόχους για την προστασία των πληροφοριακών υποδομών του Ηνωμένου Βασιλείου από κυβερνοαπειλές. Η στρατηγική αυτή περιλαμβάνει την ανάπτυξη προηγμένων τεχνολογιών ασφαλείας, την προώθηση της συνεργασίας με διεθνείς εταίρους και την ενίσχυση της ανθεκτικότητας των διαστημικών συστημάτων [75].

Το Κέντρο Διαστημικής Ανθεκτικότητας (Space Resilience Centre), που ιδρύθηκε το 2020, επικεντρώνεται στην προστασία των διαστημικών υποδομών από φυσικές και ανθρωπογενείς απειλές, συμπεριλαμβανομένων των κυβερνοεπιθέσεων. Το κέντρο αυτό συνεργάζεται με διεθνείς οργανισμούς και εθνικούς φορείς για την ανάπτυξη και εφαρμογή μέτρων ασφαλείας [76].

Η Εθνική Στρατηγική Διαστήματος 2021 (National Space Strategy 2021) καθορίζει τις φιλοδοξίες του Ηνωμένου Βασιλείου για την ανάπτυξη των διαστημικών του ικανοτήτων. Η στρατηγική αυτή αναγνωρίζει την ανάγκη για ισχυρή κυβερνοασφάλεια και προωθεί την ενσωμάτωση μέτρων ασφαλείας σε όλες τις διαστημικές δραστηριότητες. Η στρατηγική περιλαμβάνει επίσης στόχους για την ανάπτυξη νέων τεχνολογιών και τη βελτίωση της ανθεκτικότητας των διαστημικών συστημάτων [77].

Το Πρόγραμμα Ανθεκτικότητας στον Κυβερνοχώρο (Cyber Resilience Programme) είναι μια πρωτοβουλία που στοχεύει στην ενίσχυση των κρίσιμων υποδομών, συμπεριλαμβανομένων των διαστημικών συστημάτων. Το πρόγραμμα αυτό περιλαμβάνει δράσεις για την ανίχνευση και αντιμετώπιση κυβερνοαπειλών, την εκπαίδευση του προσωπικού και την ανάπτυξη συνεργασιών με διεθνείς εταίρους [78].

Καταλαβαίνουμε ότι το Ηνωμένο Βασίλειο, μέσω των νομοθετικών πρωτοβουλιών, των προτύπων και των στρατηγικών του, στοχεύει στο να διασφαλίσει την ανθεκτικότητα και την ασφάλεια των διαστημικών του υποδομών από κυβερνοαπειλές. Οι πολιτικές του μας δείχνουν την ανάγκη προστασίας των κρίσιμων πληροφοριακών υποδομών και την προώθηση της συνεργασίας με διεθνείς εταίρους για την αντιμετώπιση των σύγχρονων κυβερνοαπειλών. Με την εφαρμογή αυστηρών μέτρων ασφαλείας και την ανάπτυξη καινοτόμων τεχνολογιών, το Ηνωμένο Βασίλειο ενισχύει τη δυνατότητά του να προστατεύει τις διαστημικές του επιχειρήσεις και να διατηρεί την ανθεκτικότητά του σε έναν διαρκώς μεταβαλλόμενο κυβερνοχώρο.

6.1.4 Πολιτική Ασφάλειας του Διαστήματος των Ηνωμένων Πολιτειών

Οι Ηνωμένες Πολιτείες έχουν ορίσει ένα ισχυρό και ολοκληρωμένο πλαίσιο για την κυβερνοασφάλεια των διαστημικών τους υποδομών, αναγνωρίζοντας τη στρατηγική σημασία του διαστήματος για την εθνική ασφάλεια, την οικονομία και την καθημερινή ζωή. Ακολουθούν αναλυτικές πληροφορίες σχετικά με τους νόμους, τα πρότυπα και τις στρατηγικές που εφαρμόζουν οι ΗΠΑ για την κυβερνοασφάλεια στο διάστημα.

Ο Νόμος για τη Διαστημική Πολιτική 2017 SPD-1, που εκδόθηκε από τον Πρόεδρο Ντόναλντ Τραμπ, αναθεωρεί την εθνική στρατηγική για την εξερεύνηση του διαστήματος, τονίζοντας την ανάγκη για συνεργασία μεταξύ των δημόσιων και ιδιωτικών τομέων. Η SPD-1 περιλαμβάνει κατευθυντήριες γραμμές για την προστασία των διαστημικών υποδομών από κυβερνοαπειλές και την ανάπτυξη τεχνολογιών που ενισχύουν την ασφάλεια [79].

Ο Νόμος για την Κυβερνοασφάλεια των Κρίσιμων Υποδομών 2018 - CISA Act ορίστηκε για την ενίσχυση της κυβερνοασφάλειας των κρίσιμων υποδομών των ΗΠΑ, συμπεριλαμβανομένων των διαστημικών συστημάτων. Ο νόμος αυτός δημιούργησε την Υπηρεσία Κυβερνοασφάλειας και Ασφάλειας Υποδομών (CISA), η οποία έχει ως αποστολή την προστασία των κρίσιμων πληροφοριακών υποδομών από κυβερνοαπειλές [80].

Η Εθνική Υπηρεσία Αεροναυπηγικής και Διαστήματος (NASA) εφαρμόζει αυστηρά πρότυπα κυβερνοασφάλειας για την προστασία των διαστημικών της συστημάτων. Η NASA συνεργάζεται με άλλες κυβερνητικές υπηρεσίες, ακαδημαϊκά ιδρύματα και τον ιδιωτικό τομέα για την ανάπτυξη και εφαρμογή τεχνολογιών ασφαλείας που προστατεύουν τις διαστημικές αποστολές και τα δεδομένα.

Η Εθνική Υπηρεσία Πληροφοριών NIA είναι υπεύθυνη για την προστασία των πληροφοριακών συστημάτων που σχετίζονται με την εθνική ασφάλεια. Η NIA παρέχει κατευθυντήριες γραμμές και υποστήριξη για την εφαρμογή μέτρων κυβερνοασφάλειας στις διαστημικές υποδομές [81].

Η Εθνική Υπηρεσία Ασφάλειας NSA έχει σημαντικό ρόλο στην προστασία των διαστημικών υποδομών των ΗΠΑ από κυβερνοαπειλές. Η NSA συνεργάζεται με άλλες κυβερνητικές υπηρεσίες για την ανάπτυξη προηγμένων τεχνολογιών ασφαλείας και την εφαρμογή μέτρων προστασίας [82].

Η Εθνική Στρατηγική για την Κυβερνοασφάλεια 2018 (National Cyber Strategy 2018) καθορίζει τους στόχους και τις κατευθυντήριες γραμμές για την προστασία των πληροφοριακών

υποδομών των ΗΠΑ από κυβερνοαπειλές. Η στρατηγική αυτή περιλαμβάνει δράσεις για την ενίσχυση της ανθεκτικότητας των διαστημικών συστημάτων, την προώθηση της συνεργασίας μεταξύ των δημόσιων και ιδιωτικών τομέων και την ανάπτυξη νέων τεχνολογιών ασφαλείας [83].

Η Εθνική Στρατηγική Διαστήματος 2020 (National Space Strategy 2020) καθορίζει τις φιλοδοξίες των ΗΠΑ για την εξερεύνηση και την εκμετάλλευση του διαστήματος. Η στρατηγική αυτή τονίζει την ανάγκη για ισχυρή κυβερνοασφάλεια και περιλαμβάνει στόχους για την ενσωμάτωση μέτρων ασφαλείας σε όλες τις διαστημικές δραστηριότητες. Επίσης, προωθεί τη συνεργασία με διεθνείς εταίρους για την ανάπτυξη κοινών προτύπων και κανονισμών ασφάλειας [84].

Το Πρόγραμμα Κυβερνοανθεκτικότητας των Διαστημικών Υποδομών (Space Infrastructure Cyber Resilience Program) είναι μια πρωτοβουλία που στοχεύει στην ενίσχυση της ανθεκτικότητας των διαστημικών υποδομών των ΗΠΑ απέναντι σε κυβερνοεπιθέσεις. Το πρόγραμμα περιλαμβάνει δράσεις για την ανίχνευση και αντιμετώπιση κυβερνοαπειλών, την εκπαίδευση του προσωπικού και την ανάπτυξη συνεργασιών με διεθνείς εταίρους [85].

Η Διαστημική Διοίκηση των ΗΠΑ USSPACECOM, που ιδρύθηκε το 2019, έχει ως αποστολή την προστασία των διαστημικών επιχειρήσεων των ΗΠΑ και την ενίσχυση της ανθεκτικότητας των διαστημικών συστημάτων απέναντι σε απειλές. Η USSPACECOM συνεργάζεται στενά με άλλες στρατιωτικές και κυβερνητικές υπηρεσίες για την ανάπτυξη και εφαρμογή στρατηγικών και μέτρων ασφαλείας [86].

6.2 Διεθνείς Οργανισμοί και Κανονισμοί

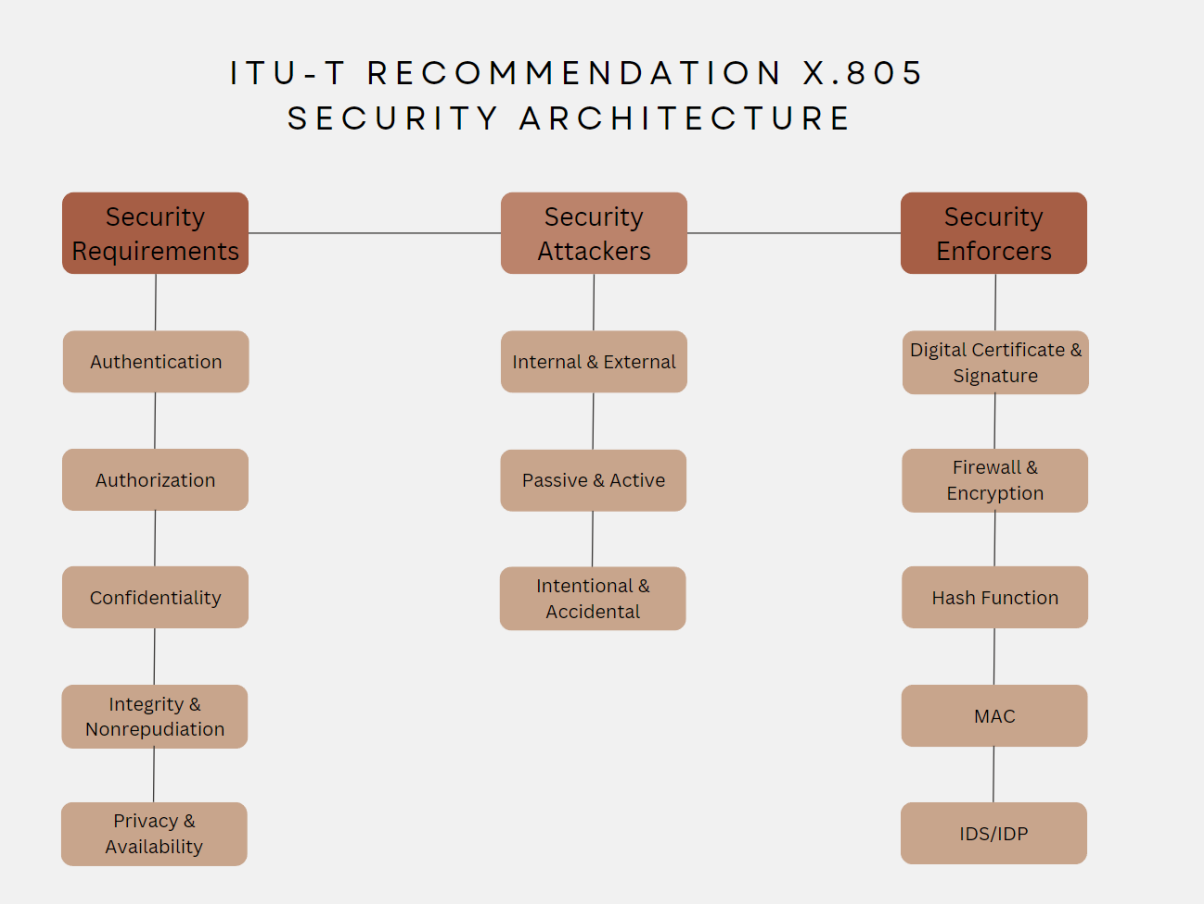
Η έλλειψη προτύπων και κανονισμών για την κυβερνοασφάλεια στο διάστημα απαιτεί συντονισμένες προσπάθειες από διεθνείς οργανισμούς όπως η ITU και η COPUOS. Αυτοί οι οργανισμοί διαδραματίζουν κρίσιμο ρόλο στην ανάπτυξη προτύπων, την προώθηση της διεθνούς συνεργασίας και την ευαισθητοποίηση σχετικά με την ασφάλεια στο διάστημα. Η συνεχής συνεργασία και η ανταλλαγή γνώσεων είναι απαραίτητες για την αντιμετώπιση των προκλήσεων και την εξασφάλιση ενός ασφαλούς και βιώσιμου διαστημικού περιβάλλοντος. Η ITU και η COPUOS, με τις πρωτοβουλίες και τις δράσεις τους, συμβάλλουν σημαντικά στη διαμόρφωση ενός ασφαλούς διαστημικού οικοσυστήματος. Η ανάπτυξη διεθνών προτύπων, η ενίσχυση της διεθνούς συνεργασίας και η προώθηση της εκπαίδευσης και της ενημέρωσης αποτελούν θεμέλια για την επιτυχία των προσπαθειών αυτών. Η διαρκής εξέλιξη των τεχνολογιών και των απειλών καθιστά αναγκαία την προσαρμογή και την αναθεώρηση των κανονισμών, ώστε να διασφαλίζεται η ασφάλεια και η βιωσιμότητα των διαστημικών δραστηριοτήτων σε παγκόσμιο επίπεδο.

6.2.1 Διεθνής Ένωση Τηλεπικοινωνιών (ITU)

Η Διεθνής Ένωση Τηλεπικοινωνιών (ITU) είναι ένας εξειδικευμένος οργανισμός των Ηνωμένων Εθνών που επικεντρώνεται σε θέματα που αφορούν τις πληροφορίες και τις τηλεπικοινωνίες. Ιδρυθείσα το 1865, η ITU παίζει καθοριστικό ρόλο στην ανάπτυξη διεθνών προτύπων για τις τηλεπικοινωνίες και την κυβερνοασφάλεια, ιδιαίτερα όσον αφορά τις δορυφορικές και άλλες διαστημικές επικοινωνίες. Η ITU αναπτύσσει και εκδίδει διεθνή πρότυπα που στοχεύουν στην εξασφάλιση ασφαλούς και αξιόπιστης επικοινωνίας για δορυφορικά και άλλα διαστημικά συστήματα. Αυτά τα πρότυπα περιλαμβάνουν κανονισμούς για την προστασία των δορυφορικών σημάτων από παρεμβολές και κακόβουλες ενέργειες, ενώ διασφαλίζουν ότι τα συστήματα επικοινωνίας μπορούν να συνεργάζονται απρόσκοπτα, παρέχοντας έτσι παγκόσμια συμβατότητα και ασφάλεια. Επίσης συνεργάζεται στενά με κυβερνήσεις, ιδιωτικούς φορείς και άλλους διεθνείς οργανισμούς για την προώθηση της κυβερνοασφάλειας στο διάστημα. Οργανώνει συνεδριάσεις,

ομάδες εργασίας και φόρα όπου οι ενδιαφερόμενοι φορείς μπορούν να ανταλλάσσουν πληροφορίες και να συνεργάζονται για την ανάπτυξη και την εφαρμογή των προτύπων. Αυτή η συνεργασία είναι ζωτικής σημασίας για την επίτευξη παγκόσμιας ασφάλειας και προστασίας των διαστημικών συστημάτων. Επιπλέον προάγει την εκπαίδευση και την ευαισθητοποίηση για θέματα κυβερνοασφάλειας μέσω διαφόρων εκπαιδευτικών προγραμμάτων, σεμιναρίων και συνεδρίων. Διοργανώνει εργαστήρια και προγράμματα εκπαίδευσης που στοχεύουν στην ενημέρωση των ενδιαφερομένων φορέων για τις καλύτερες πρακτικές και τις τελευταίες εξελίξεις στον τομέα της κυβερνοασφάλειας. Αυτές οι εκπαιδευτικές πρωτοβουλίες συμβάλλουν στην ενίσχυση της ικανότητας των κρατών και των οργανισμών να προστατεύουν τις διαστημικές υποδομές τους από απειλές κυβερνοασφάλειας [87].

Παραδείγματα προτύπων της ITU περιλαμβάνουν το πιο γνωστό ITU-T Recommendation X.800, το οποίο αναφέρεται στο γενικό πλαίσιο ασφαλείας για τα συστήματα τηλεπικοινωνιών και παρέχει μια ενημέρωση γύρω από τις απαιτήσεις ασφαλείας και τους μηχανισμούς προστασίας που μπορούν να χρησιμοποιηθούν για την εξασφάλιση τηλεπικοινωνιακών συστημάτων. Επίσης, το ITU-T Recommendation X.805 παρουσιάζει την αρχιτεκτονική ασφαλείας για τα δίκτυα, εστιάζοντας στη διασφάλιση της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας των δικτύων τηλεπικοινωνιών. Σε ότι αφορά την ασφάλεια των δορυφορικών επικοινωνιών υπάρχει το ITU-R Recommendation S.1003, το οποίο περιέχει οδηγίες για την ασφάλεια και την προστασία των δορυφορικών σημάτων από παρεμβολές καθώς και άλλες απειλές. Το παρακάτω σχήμα παρουσιάζει την αρχιτεκτονική ασφάλειας σύμφωνα με τη σύσταση ITU-T X.805. Το σχήμα οργανώνεται σε τρεις κύριες κατηγορίες: Απαιτήσεις Ασφάλειας, Τύποι Επιτιθέμενων και Μέτρα Ασφάλειας [88].



Σχήμα 12: Η αρχιτεκτονική του προτύπου ITU-T X.805.

Το παραπάνω σχήμα παρουσιάζει τη σύσταση X.805 του ITU-T για την αρχιτεκτονική ασφάλειας. Η σύσταση X.805 του ITU-T για την αρχιτεκτονική ασφάλειας ξεκινά με τις βασικές απαιτήσεις ασφάλειας, όπως η ταυτοποίηση, η εξουσιοδότηση, η εμπιστευτικότητα, η ακεραιότητα, η επαληθευσιμότητα, η ιδιωτικότητα και η διαθεσιμότητα. Αυτές οι απαιτήσεις διασφαλίζουν ότι οι χρήστες και οι συσκευές ταυτοποιούνται σωστά, ότι η πρόσβαση είναι ελεγχόμενη, ότι τα δεδομένα παραμένουν εμπιστευτικά και ακεραία, και ότι οι πόροι είναι διαθέσιμοι όταν χρειάζεται.

Οι επιτιθέμενοι κατηγοριοποιούνται σε εσωτερικούς και εξωτερικούς, παθητικούς και ενεργητικούς, καθώς και σκόπιμους και τυχαίους. Εσωτερικοί επιτιθέμενοι είναι εντός του οργανισμού, ενώ εξωτερικοί προέρχονται από έξω. Παθητικές επιθέσεις παρακολουθούν τα δεδομένα, ενώ ενεργητικές τα αλλοιώνουν. Οι επιθέσεις μπορεί να είναι προσχεδιασμένες ή τυχαίες.

Οι μηχανισμοί επιβολής ασφάλειας περιλαμβάνουν ψηφιακά πιστοποιητικά και υπογραφές, τείχη προστασίας, κρυπτογράφηση, συναρτήσεις κατακερματισμού, μηχανισμούς ελέγχου πρόσβασης (MAC), και συστήματα ανίχνευσης και πρόληψης εισβολών (IDS/IDP). Αυτά τα εργαλεία προστατεύουν την ταυτότητα, την εμπιστευτικότητα, την ακεραιότητα των δεδομένων, και την ασφάλεια του δικτύου από κακόβουλες δραστηριότητες.

Τέλος άλλο ένα γνωστό και σημαντικό πρότυπο είναι το ITU-T Recommendation X.1121 το οποίο αφορά την ασφάλεια για τα κινητά δίκτυα και τις υπηρεσίες τρίτης γενιάς (3G), καθορίζοντας τις απαιτήσεις και τις λύσεις ασφαλείας για την προστασία των κινητών επικοινωνιών [89].

6.2.2 Επιτροπή των Ηνωμένων Εθνών για την Ειρηνική Χρήση του Διαστήματος (COPUOS)

Η Επιτροπή των Ηνωμένων Εθνών για την Ειρηνική Χρήση του Διαστήματος (COPUOS) είναι ένας διεθνής οργανισμός που ιδρύθηκε το 1959 με σκοπό την προώθηση της ειρηνικής χρήσης του διαστήματος και την επίβλεψη της ανάπτυξης διεθνών κανόνων και κανονισμών. Ο ρόλος της είναι κρίσιμος για την εξασφάλιση του δεδομένου ότι οι διαστημικές δραστηριότητες πραγματοποιούνται με ασφάλεια, βιωσιμότητα και σε συμφωνία με το διεθνές δίκαιο. Επίσης αναπτύσσει οδηγίες και συστάσεις για την ασφάλεια και τη βιωσιμότητα των διαστημικών δραστηριοτήτων. Αυτές οι κατευθυντήριες γραμμές καλύπτουν θέματα όπως η αποφυγή διαστημικών συγκρούσεων, η διαχείριση των διαστημικών απορριμμάτων και η προστασία των δορυφόρων από κυβερνοεπιθέσεις. Στο πλαίσιο της κυβερνοασφάλειας, προτείνει μέτρα για την προστασία των διαστημικών συστημάτων από κακόβουλες ενέργειες, καθώς και τη διασφάλιση της ακεραιότητας και της διαθεσιμότητας των διαστημικών δεδομένων και υπηρεσιών. Επιπλέον λειτουργεί ως πλατφόρμα για τη διεθνή συνεργασία, συγκεντρώνοντας εκπροσώπους από διάφορα κράτη και διεθνείς οργανισμούς. Μέσω των συνεδριάσεων και των ομάδων εργασίας της, διευκολύνεται η ανταλλαγή γνώσεων, εμπειριών και βέλτιστων πρακτικών στον τομέα της διαστημικής ασφάλειας. Η επιτροπή προωθεί τη συνεργασία μεταξύ των κρατών για την επίλυση ζητημάτων ασφάλειας στο διάστημα, αναγνωρίζοντας ότι οι προκλήσεις στον τομέα αυτό απαιτούν συντονισμένες και συλλογικές προσπάθειες. Τέλος συμβάλλει στην ανάπτυξη και την επικαιροποίηση του νομικού πλαισίου που διέπει τη χρήση του διαστήματος. Το νομικό αυτό πλαίσιο περιλαμβάνει διεθνείς συνθήκες, συμφωνίες και κανονισμούς που διασφαλίζουν ότι οι διαστημικές δραστηριότητες πραγματοποιούνται με υπευθυνότητα και σε συμφωνία με τις αρχές της ειρηνικής χρήσης. Λαμβάνοντας υπόψη τις νέες τεχνολογικές εξελίξεις και τις αυξανόμενες απειλές κυβερνοασφάλειας, η COPUOS εργάζεται για την ενημέρωση των κανονισμών και τη δημιουργία νέων που να ανταποκρίνονται στις σύγχρονες προκλήσεις [90].

6.2.3 Οργανισμός Διεθνούς Πολιτικής Αεροπορίας (ICAO)

Ο ICAO, αν και κυρίως ασχολείται με την πολιτική αεροπορία, έχει επίσης εμπλακεί σε θέματα που αφορούν την ασφάλεια και τη ρύθμιση των διαστημικών πτήσεων, ιδιαίτερα καθώς αυτές γίνονται ολοένα και πιο συνδεδεμένες με τις αεροπορικές δραστηριότητες. Ο ICAO εργάζεται για την ανάπτυξη προτύπων και κανονισμών που διασφαλίζουν την ασφαλή διεξαγωγή των πτήσεων σε κοντινή απόσταση από τη Γη και την αρμονική συνύπαρξη των αεροπορικών και διαστημικών πτήσεων. Με την αυξανόμενη εμπορευματοποίηση του διαστήματος και την ανάπτυξη νέων τεχνολογιών, όπως οι υπερηχητικές πτήσεις και τα επαναχρησιμοποιήσιμα διαστημόπλοια, οι διαστημικές δραστηριότητες αρχίζουν να αλληλοεπιδρούν όλο και περισσότερο με τις παραδοσιακές αεροπορικές δραστηριότητες. Ο ICAO εργάζεται για την ανάπτυξη ενός ενιαίου πλαισίου κανονισμών που θα διευκολύνει τη διαχείριση αυτής της συνύπαρξης, διασφαλίζοντας ότι οι πτήσεις που εισέρχονται και εξέρχονται από την ατμόσφαιρα πραγματοποιούνται με ασφάλεια και αποτελεσματικότητα. Ένα σημαντικό πεδίο δράσης του ICAO είναι η ανάπτυξη κανονισμών για τις πτήσεις κοντά στη Γη, που περιλαμβάνουν τις χαμηλής τροχιάς διαστημικές πτήσεις και τις υποτροχιακές πτήσεις, οι οποίες συχνά χρησιμοποιούν τον ίδιο εναέριο χώρο με τις εμπορικές αερογραμμές. Οι κανονισμοί αυτοί στοχεύουν στην ελαχιστοποίηση του κινδύνου συγκρούσεων και στη διασφάλιση ότι όλες οι πτήσεις τηρούν τις ίδιες αυστηρές απαιτήσεις ασφάλειας. Επιπλέον, προωθεί τη συνεργασία και τον συντονισμό μεταξύ των διαστημικών και των αεροπορικών φορέων σε διεθνές επίπεδο. Αυτό περιλαμβάνει τη διευκόλυνση της ανταλλαγής δεδομένων και πληροφοριών, καθώς και την ανάπτυξη κοινών πρωτοκόλλων για την ανταπόκριση σε έκτακτες ανάγκες. Με την ενίσχυση της συνεργασίας και του συντονισμού, ο ICAO συμβάλλει στη δημιουργία ενός ασφαλούς και βιώσιμου περιβάλλοντος τόσο για τις αεροπορικές όσο και για τις διαστημικές δραστηριότητες [91].

6.2.4 Ευρωπαϊκός Οργανισμός Διαστήματος(ESA)

Ο ESA είναι υπεύθυνος για τη συντονισμένη διαστημική πολιτική και για τις δραστηριότητες των ευρωπαϊκών χωρών. Η ESA αναπτύσσει και εφαρμόζει κανονισμούς που αφορούν την εκτόξευση δορυφόρων, την παρακολούθηση της Γης, και την προστασία των διαστημικών υποδομών από κυβερνοεπιθέσεις. Ο οργανισμός συνεργάζεται με εθνικές διαστημικές υπηρεσίες, διεθνείς οργανισμούς και τον ιδιωτικό τομέα για την ανάπτυξη προηγμένων τεχνολογιών και την προώθηση της διεθνούς συνεργασίας, προάγει επίσης την εκπαίδευση και την καινοτομία στον τομέα του διαστήματος, συμβάλλοντας στη βιωσιμότητα και την ασφάλεια των ευρωπαϊκών διαστημικών δραστηριοτήτων [92].

6.2.5 Ιαπωνική Υπηρεσία Εξερεύνησης του Διαστήματος (JAXA)

Η Ιαπωνική Υπηρεσία Εξερεύνησης του Διαστήματος (JAXA) κατέχει σημαντικό ρόλο στην προώθηση των διαστημικών δυνατοτήτων της Ιαπωνίας και της διεθνούς συνεργασίας στο διάστημα. Ιδρύθηκε το 2003 μέσω της συγχώνευσης τριών αεροδιαστημικών οργανισμών και επικεντρώνεται σε ένα ευρύ φάσμα διαστημικών δραστηριοτήτων, όπως η ανάπτυξη δορυφόρων, η εξερεύνηση του διαστήματος και η διαστημική επιστήμη. Η JAXA συμβάλλει ενεργά στην ανάπτυξη διεθνών προτύπων και κανονισμών για την κυβερνοασφάλεια στο διάστημα, εξασφαλίζοντας την προστασία των κρίσιμων διαστημικών υποδομών από κυβερνοαπειλές. Ο οργανισμός συνεργάζεται με διεθνή σώματα όπως η ITU και η COPUOS για την προώθηση της ασφαλούς και βιώσιμης χρήσης του εξωτερικού διαστήματος. Η JAXA δίνει επίσης έμφαση στην προστασία του περιβάλλοντος στις αποστολές της, τηρώντας αυστηρές κατευθυντήριες γραμμές για την ελαχιστοποίηση των διαστημικών απορριμμάτων και των περιβαλλοντικών επιπτώσεων. Μέσω των εκπαιδευτικών πρωτοβουλιών και της δημόσιας ενημέρωσης, η JAXA ενισχύει την

ευαισθητοποίηση και τη γνώση σχετικά με την ασφάλεια και την κυβερνοασφάλεια στο διάστημα, συμβάλλοντας στην παγκόσμια προσπάθεια για τη διατήρηση ενός ασφαλούς και βιώσιμου διαστημικού περιβάλλοντος [93].

6.2.6 Καναδική Υπηρεσία Διαστήματος (CSA)

Η Καναδική Υπηρεσία Διαστήματος (CSA) είναι αφιερωμένη στην ειρηνική χρήση και εξερεύνηση του διαστήματος, υποστηρίζοντας τόσο επιστημονικές όσο και εμπορικές διαστημικές δραστηριότητες. Ιδρύθηκε το 1989 και επιβλέπει τα διαστημικά προγράμματα του Καναδά, επικεντρώνοντας στην επικοινωνία μέσω δορυφόρων, την παρακολούθηση της Γης και την έρευνα στη διαστημική επιστήμη. Η CSA δεσμεύεται να διατηρεί υψηλά πρότυπα ασφάλειας και πολιτικές περιβαλλοντικής προστασίας για τις αποστολές της, εξασφαλίζοντας τη συμμόρφωση με διεθνείς κανονισμούς και βέλτιστες πρακτικές. Συνεργάζεται με άλλες διαστημικές υπηρεσίες και διεθνείς οργανισμούς για την ανάπτυξη και εφαρμογή μέτρων κυβερνοασφάλειας που προστατεύουν τα διαστημικά συστήματα από κυβερνοαπειλές. Συμμετέχοντας σε παγκόσμια forum και ομάδες εργασίες, η CSA συμβάλλει στην ανάπτυξη διεθνών προτύπων για τις διαστημικές δραστηριότητες, τονίζοντας τη σημασία της συνεργασίας και της ανταλλαγής γνώσεων. Η CSA προάγει επίσης την ευαισθητοποίηση και την εκπαίδευση του κοινού σε θέματα διαστήματος, ενθαρρύνοντας την επόμενη γενιά επιστημόνων και μηχανικών να ασχοληθούν με την εξερεύνηση και την καινοτομία στο διάστημα [94].

6.3 Εθνικές Πολιτικές και Κανονισμοί Διαστήματος Εθνικών Χώρων

Οι εθνικές πολιτικές και κανονισμοί διαστήματος παίζουν καθοριστικό ρόλο στη διαχείριση και ρύθμιση των διαστημικών δραστηριοτήτων κάθε χώρας. Αυτές οι πολιτικές καθορίζουν το πλαίσιο για την ανάπτυξη, την εκμετάλλευση και την ασφάλεια των διαστημικών υποδομών και υπηρεσιών. Οι πολιτικές αυτές διαμορφώνονται με γνώμονα τις εθνικές προτεραιότητες, τις στρατηγικές ανάγκες και τις διεθνείς υποχρεώσεις κάθε χώρας .Κάθε χώρα αναπτύσσει τις δικές της πολιτικές και κανονισμούς διαστήματος, προσαρμοσμένους στις εθνικές της προτεραιότητες και τις ειδικές συνθήκες της.

Οι Ηνωμένες Πολιτείες, μέσω της NASA και άλλων αρμόδιων φορέων, έχουν δημιουργήσει ένα ευρύ και ολοκληρωμένο πλαίσιο πολιτικής που καλύπτει την επιστημονική έρευνα, την εξερεύνηση του διαστήματος και την εμπορική εκμετάλλευση των διαστημικών πόρων. Η πολιτική αυτή περιλαμβάνει την υποστήριξη της ιδιωτικής πρωτοβουλίας, την ενίσχυση της διεθνούς συνεργασίας, και την προώθηση της ασφάλειας και της βιωσιμότητας των διαστημικών δραστηριοτήτων [95].

Η Ρωσία, μέσω της Roscosmos, εστιάζει στη διατήρηση και την ανάπτυξη των διαστημικών της δυνατοτήτων με έμφαση στη διεθνή συνεργασία και την ασφάλεια. Οι πολιτικές της Ρωσίας περιλαμβάνουν την αξιοποίηση του Διεθνούς Διαστημικού Σταθμού (ISS), την ανάπτυξη νέων διαστημικών τεχνολογιών και την ενίσχυση της εθνικής ασφάλειας μέσω των διαστημικών υποδομών [96].

Η Κίνα, μέσω της CNSA, έχει επιταχύνει την ανάπτυξη των διαστημικών της υποδομών και επεκτείνει την επιρροή της στο διάστημα. Οι πολιτικές της Κίνας περιλαμβάνουν την εξερεύνηση του φεγγαριού και του Άρη, την ανάπτυξη δορυφορικών συστημάτων για τηλεπικοινωνίες και

παρακολούθηση της Γης, καθώς και την ενίσχυση της στρατιωτικής της παρουσίας στο διάστημα [97].

Το Ηνωμένο Βασίλειο, μέσω της UK Space Agency, επικεντρώνεται στην υποστήριξη της εμπορικής εκμετάλλευσης του διαστήματος και στην ενίσχυση της διεθνούς συνεργασίας. Η πολιτική του Ηνωμένου Βασιλείου περιλαμβάνει την υποστήριξη των νέων επιχειρήσεων και της καινοτομίας, την προώθηση της εκπαίδευσης και της κατάρτισης στον τομέα του διαστήματος, και τη συμμετοχή σε διεθνή προγράμματα και αποστολές [98].

Ο παρακάτω πίνακας συγκρίνει τις πολιτικές και κανονισμούς διαστήματος τεσσάρων μεγάλων χωρών: Ηνωμένες Πολιτείες, Ρωσία, Κίνα και Ηνωμένο Βασίλειο. Οι κατηγορίες πολιτικής που εξετάζονται περιλαμβάνουν την επιστημονική έρευνα, την εξερεύνηση του διαστήματος, την εμπορική εκμετάλλευση, τη διεθνή συνεργασία, την ασφάλεια και βιωσιμότητα, και τη στρατιωτική παρουσία.

Κατηγορία Πολιτικής	**ΗΠΑ**	**Ρωσία**	**Κίνα**	**Ηνωμένο Βασίλειο**
Επιστημονική Έρευνα	Υψηλή	Μέτρια	Υψηλή	Μέτρια
Εξερεύνηση Διαστήματος	Υψηλή	Μέτρια	Υψηλή	Μέτρια
Εμπορική Εκμετάλλευση	Υψηλή	Χαμηλή	Μέτρια	Υψηλή
Διεθνής Συνεργασία	Υψηλή	Υψηλή	Μέτρια	Υψηλή
Ασφάλεια και Βιωσιμότητα	Υψηλή	Υψηλή	Υψηλή	Μέτρια
Στρατιωτική Παρουσία	Μέτρια	Υψηλή	Υψηλή	Χαμηλή

Πίνακας 3: Σύγκριση πολιτικών και κανονισμών διαστήματος.

6.4 Πολιτικές και Κατευθύνσεις Διαστημικών Υπηρεσιών

Οι πολιτικές και οι κατευθύνσεις διαστημικών υπηρεσιών καθορίζουν τις αρχές και τις διαδικασίες που πρέπει να ακολουθούνται κατά την εκτέλεση διαστημικών δραστηριοτήτων. Αυτές οι πολιτικές εξασφαλίζουν ότι οι διαστημικές επιχειρήσεις διεξάγονται με τρόπο που προωθεί την ασφάλεια, την βιωσιμότητα και την ειρηνική χρήση του διαστήματος. Οι οδηγίες αυτές αναπτύσσονται τόσο σε εθνικό όσο και σε διεθνές επίπεδο και καλύπτουν μια σειρά από θέματα, όπως η εκτόξευση δορυφόρων, η διαχείριση διαστημικών απορριμμάτων και η προστασία των διαστημικών υποδομών.

Στο πλαίσιο των εθνικών διαστημικών υπηρεσιών, όπως η NASA στις Ηνωμένες Πολιτείες, η Roscosmos στη Ρωσία, η UK Space Agency στο Ηνωμένο Βασίλειο και η CNSA στην Κίνα, οι πολιτικές αυτές περιλαμβάνουν κανονισμούς για την αδειοδότηση, τη συμμόρφωση με τα πρότυπα ασφαλείας και την προστασία του περιβάλλοντος. Επιπλέον, οι διαστημικές υπηρεσίες συχνά

αναπτύσσουν πρωτόκολλα για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης και την προστασία των διαστημικών υποδομών από απειλές όπως οι κυβερνοεπιθέσεις.

Όπως μπορούμε να συμπεράνουμε και από τα προηγούμενα κεφάλαια οι διεθνείς κατευθυντήριες οδηγίες, όπως αυτές που αναπτύσσονται από την Επιτροπή των Ηνωμένων Εθνών για την Ειρηνική Χρήση του Διαστήματος (COPUOS), επιδιώκουν να προάγουν την παγκόσμια συνεργασία και να διασφαλίσουν ότι όλες οι χώρες ακολουθούν κοινά πρότυπα και πρακτικές. Αυτές οι οδηγίες συμβάλλουν στη δημιουργία ενός πλαισίου που επιτρέπει την ειρηνική συνύπαρξη και συνεργασία στο διάστημα. Ο παρακάτω πίνακας συγκρίνει διάφορους τομείς κανονισμών και πρακτικών μεταξύ τεσσάρων διαστημικών οργανισμών: της NASA, της Roscosmos, της UK Space Agency και της CNSA. Η NASA διέπεται από τον Εθνικό Νόμο Αεροναυτικής και Διαστήματος, η Roscosmos από τους ρωσικούς νόμους, η UK Space Agency από το Space Industry Act του 2018 και η CNSA από εθνικούς κινεζικούς νόμους. Στα πρότυπα ασφάλειας, η NASA εστιάζει στην υγεία των αστροναυτών, η Roscosmos στον αυστηρό έλεγχο, η UK Space Agency στη συμμόρφωση με διεθνή πρότυπα, και η CNSA στην τεχνολογική καινοτομία. Στην προστασία του περιβάλλοντος, η NASA ακολουθεί το NEPA, η Roscosmos τις ρωσικές και διεθνείς κατευθυντήριες γραμμές, η UK Space Agency απαιτεί αυστηρές αξιολογήσεις και η CNSA εστιάζει στον μετριασμό διαστημικών απορριμμάτων. Τα πρωτόκολλα έκτακτης ανάγκης είναι λεπτομερή σε όλους τους οργανισμούς, με έμφαση στην ετοιμότητα. Στην κυβερνοασφάλεια, η NASA έχει προηγμένα πρωτόκολλα, η Roscosmos συστήματα κυβερνοάμυνας, η UK Space Agency τηρεί το UK-GDPR και η CNSA εφαρμόζει εθνικούς νόμους κυβερνοασφάλειας.

Space Agency	Licensing Regulations	Safety Standards	Environmental Protection	Emergency Protocols	Cybersecurity Measures
NASA	Governed by the National Aeronautics and Space Act	Focus on astronaut health, mission safety, and rigorous equipment testing	Policies under NEPA for minimizing environmental impacts	Detailed emergency procedures for launch, in-flight, and landing emergencies	Advanced cybersecurity protocols with continuous monitoring and updates
Roscosmos	Governed by the Federal Space Program and Russian Federation laws	Emphasis on robust testing and validation of spaceflight systems	Policies aligning with Russian environmental regulations and international guidelines	Comprehensive emergency response plans for all mission phases	Cyber defense systems to safeguard critical space infrastructure
UK Space Agency	Governed by the Space Industry Act 2018 and the Outer Space Act 1986	Compliance with international safety standards, including those of the ESA	Strict environmental impact assessments required for all missions	Integrated with national emergency preparedness frameworks	Adherence to UK-GDPR, Data Protection Act 2018, and NIS Regulations 2018

CNSA	Governed by national laws and regulations specific to China	Emphasis on technological innovation and safety in spacecraft design	Focus on space debris mitigation and sustainable practices	Detailed protocols for handling in-orbit emergencies and re-entry procedures	Implementation of measures as per national cybersecurity laws

Πίνακας 4 : Βασικές πολιτικές και κατευθυντήριες γραμμές των διαστημικών υπηρεσιών.

6.5 Διμερείς και Πολυμερείς Συμφωνίες

Οι διμερείς και πολυμερείς συμφωνίες είναι κρίσιμες για την προώθηση της διεθνούς συνεργασίας και της ασφάλειας στο διάστημα. Αυτές οι συμφωνίες μπορούν να καλύπτουν ένα εύρος θεμάτων, από την κοινή έρευνα και ανάπτυξη διαστημικών τεχνολογιών έως τη συνεργασία για την παρακολούθηση και τη διαχείριση διαστημικών απορριμμάτων.

Ο Διεθνής Διαστημικός Σταθμός (ISS) είναι ένα από τα πιο εντυπωσιακά επιτεύγματα της διεθνούς συνεργασίας στο διάστημα. Το πρόγραμμα ISS ξεκίνησε τη δεκαετία του 1990 και αποτελεί αποτέλεσμα της συνεργασίας μεταξύ της NASA (ΗΠΑ), της Roscosmos (Ρωσία), της ESA (Ευρωπαϊκή Υπηρεσία Διαστήματος), της JAXA (Ιαπωνική Υπηρεσία Διαστήματος) και της CSA (Καναδική Υπηρεσία Διαστήματος). Η συμφωνία μεταξύ των Ηνωμένων Πολιτειών και της Ρωσίας περιλαμβάνει διάφορες πτυχές. Οι Ηνωμένες Πολιτείες και η Ρωσία συνεργάστηκαν στην ανάπτυξη και την κατασκευή των βασικών μονάδων του ISS. Η Ρωσία ανέλαβε την κατασκευή και την εκτόξευση των πρώτων μονάδων, όπως το Zarya και το Zvezda, ενώ οι ΗΠΑ ανέλαβαν την κατασκευή και την εκτόξευση μονάδων όπως το Unity και το Destiny. Η συνεργασία περιλαμβάνει την ανταλλαγή αστροναυτών και κοσμοναυτών. Τα πληρώματα του ISS αποτελούνται από αστροναύτες από διάφορες χώρες, συμπεριλαμβανομένων των ΗΠΑ και της Ρωσίας, οι οποίοι συνεργάζονται σε επιστημονικά πειράματα και καθημερινές δραστηριότητες. Οι επιστήμονες από τις ΗΠΑ και τη Ρωσία συνεργάζονται σε διάφορα πειράματα και έρευνες που διεξάγονται στο ISS. Τα πειράματα αυτά καλύπτουν ένα ευρύ φάσμα τομέων, από τη βιολογία και τη φυσική έως τις διαστημικές επιστήμες και την τεχνολογία υλικών. Η συνεργασία στο ISS προάγει την ανταλλαγή γνώσεων και τεχνολογίας μεταξύ των δύο χωρών. Οι μηχανικοί και οι επιστήμονες ανταλλάσσουν τεχνογνωσία και εμπειρίες, ενισχύοντας έτσι τις δυνατότητες και των δύο πλευρών. Οι Ηνωμένες Πολιτείες και η Ρωσία έχουν αναπτύξει κοινά πρωτόκολλα και πρακτικές για την ασφάλεια και την αποτελεσματική διαχείριση του ISS. Αυτά περιλαμβάνουν διαδικασίες για την αντιμετώπιση καταστάσεων έκτακτης ανάγκης, τη διαχείριση των αποθεμάτων και τη συντήρηση των συστημάτων του σταθμού . Το όλο σχέδιο για τον ISS έχει περάσει από διάφορες φάσεις και προκλήσεις, αλλά η συνεργασία έχει παραμείνει ισχυρή λόγω της αμοιβαίας εξάρτησης και των κοινών στόχων. Η λειτουργία των Αμερικανικών διαστημικών λεωφορείων ξεκίνησε το 1981.Το πρώτο διαστημικό λεωφορείο, το Columbia, πραγματοποίησε την αποστολή STS-1 στις 12 Απριλίου 1981, σηματοδοτώντας την αρχή μιας νέας εποχής για την επανδρωμένη διαστημική εξερεύνηση. Τα διαστημικά λεωφορεία ήταν υπεύθυνα για πολλές σημαντικές αποστολές, όπως η κατασκευή και η συντήρηση του Διεθνούς Διαστημικού Σταθμού (ISS) και η αποστολή του διαστημικού τηλεσκοπίου Hubble. Μετά από 30 χρόνια λειτουργίας, η NASA ανακοίνωσε την αποστρατεία των διαστημικών λεωφορείων της το 2011. Η τελευταία αποστολή πραγματοποιήθηκε από το διαστημικό λεωφορείο Atlantis τον Ιούλιο του 2011, σηματοδοτώντας το τέλος μιας εποχής για το διαστημικό πρόγραμμα των Ηνωμένων Πολιτειών. Η απόφαση για την αποστρατεία των Αμερικανικών διαστημικών λεωφορείων ελήφθη για λόγους που είχαν να κάνουν κυρίως με την ασφάλεια, το κόστος, την τεχνολογική αναβάθμιση αλλά και την γενική στροφή της NASA σε νέες

προτεραιότητες. Αρχικά η λειτουργία και η συντήρηση των διαστημικών λεωφορείων ήταν εξαιρετικά ακριβή, καθιστώντας πιο βιώσιμη την ανάπτυξη νέων και πιο οικονομικών μεθόδων για την αποστολή ανθρώπων και φορτίων στο διάστημα. Επιπλέον, η ιστορία των διαστημικών λεωφορείων περιλαμβάνει δύο τραγικά δυστυχήματα, το Challenger το 1986 και το Columbia το 2003, τα οποία κόστισαν τη ζωή σε 14 αστροναύτες και υπογράμμισαν τους κινδύνους που συνδέονται με το πρόγραμμα. Επίσης, τα διαστημικά λεωφορεία σχεδιάστηκαν τη δεκαετία του 1970 και η τεχνολογία τους ήταν πλέον ξεπερασμένη. Η NASA ήθελε να επικεντρωθεί στην ανάπτυξη νέων, πιο προηγμένων διαστημικών σκαφών που θα μπορούσαν να υποστηρίξουν μελλοντικές αποστολές σε μεγαλύτερες αποστάσεις, όπως στον Άρη. Η στροφή της NASA κατά κύριο λόγο έχει να κάνει με την γενικότερη επιθυμία της για την παροχή πόρων σε νέα προγράμματα όπως την ανάπτυξη του διαστημικού σκάφους Orion και του πυραύλου Space Launch System (SLS), που θα μπορούσαν να υποστηρίξουν επανδρωμένες αποστολές πέρα από τη χαμηλή γήινη τροχιά. Η παύση των διαστημικών λεωφορείων επέτρεψε στη NASA να επικεντρωθεί στην ανάπτυξη νέων τεχνολογιών και προσεγγίσεων για την εξερεύνηση του διαστήματος, ανοίγοντας τον δρόμο για να πετύχει νέους στόχους και να κάνει νέες καινοτόμες ανακαλύψεις. Μετά την αποστρατεία των αμερικανικών διαστημικών λεωφορείων το 2011, η NASA βασίστηκε στους ρωσικούς πυραύλους Soyuz για τη μεταφορά αστροναυτών στον ISS. Αυτή η εξάρτηση υπογράμμισε τη σημασία της συνεργασίας και της αμοιβαίας υποστήριξης [99].

Η λειτουργία και η συντήρηση του ISS απαιτεί σημαντικούς πόρους και χρηματοδότηση. Οι Ηνωμένες Πολιτείες και η Ρωσία μοιράζονται το κόστος και τη διαχείριση αυτών των πόρων, εξασφαλίζοντας έτσι τη βιωσιμότητα του προγράμματος. Ο συντονισμός των αποστολών, από την εκτόξευση νέων μονάδων και εφοδίων έως την αντικατάσταση των πληρωμάτων, απαιτεί στενή συνεργασία και συντονισμό μεταξύ των δύο χωρών. Οι αποστολές προγραμματίζονται με ακρίβεια για να εξασφαλιστεί η συνεχής παρουσία ανθρώπων στο σταθμό και η ομαλή λειτουργία του. Οι προκλήσεις και οι τεχνικές δυσκολίες αντιμετωπίζονται μέσω της συνεργασίας και της κοινής προσπάθειας. Τα προβλήματα που προκύπτουν, όπως μηχανικές βλάβες ή έκτακτες ανάγκες, επιλύονται με τη συντονισμένη δράση και την ανταλλαγή τεχνογνωσίας. Η διμερής συνεργασία μεταξύ των Ηνωμένων Πολιτειών και της Ρωσίας για τον ISS αποτελεί ένα λαμπρό παράδειγμα του πώς η διεθνής συνεργασία μπορεί να οδηγήσει σε σημαντικά επιτεύγματα στο διάστημα. Η επιτυχία αυτής της συνεργασίας ενισχύει την ειρηνική και επιστημονική χρήση του διαστήματος και προάγει την αμοιβαία κατανόηση και συνεργασία μεταξύ των χωρών [100].

Ο παρακάτω πίνακας παρουσιάζει μια σύγκριση μεταξύ των αμερικανικών διαστημικών λεωφορείων (Space Shuttle, STS) και των ρωσικών διαστημικών σκαφών Soyuz, με βάση διάφορα χαρακτηριστικά.

Characteristic	**Space Shuttle (STS)**	**Soyuz**
Country	United States	Russia
First Launch	1981	1967
Last Launch	2011	Active
Reusable	Yes	Partially (Only the capsule portion)

Crew	7 astronauts	3 cosmonauts
Cost per Launch	Approximately $450 millions	Approximately $80 millions
Total Number of Launces	135	>140 (As of now)
Primary Mission	Transporting humans and cargo to the International Space Station (ISS), satellite repairs, scientific missions	Transporting crews to the ISS and returning to Earth
Return to Earth	Runaway Landing	Parachute landing on land
Payload Capacity	Up to 24,400 kg	Limited Cargo Space
Mission Duration	Up to 17 days	Up to 6 months (when docked at ISS)
Launch Vehicle	Solid Rocket Boosters and External Tank	Soyuz Rocket
Launch Site	Kennedy Space Center, Florida	Baikonur Cosmodrome, Kazakhstan
Development Cost	Approximately $49 Billions	Approximately $4 Billions
Key Achievements	Hubble Space Telescope deployment, construction of the ISS	Longest-serving manned spacecraft program
Orbital Altitude Range	185-643 km	200-400 km
Speed	28,000 km/h (17,500 mph)	27,580 km/h(17,150 mph)
Deorbit Burn Duration	~30 minutes	~4.5 Minutes

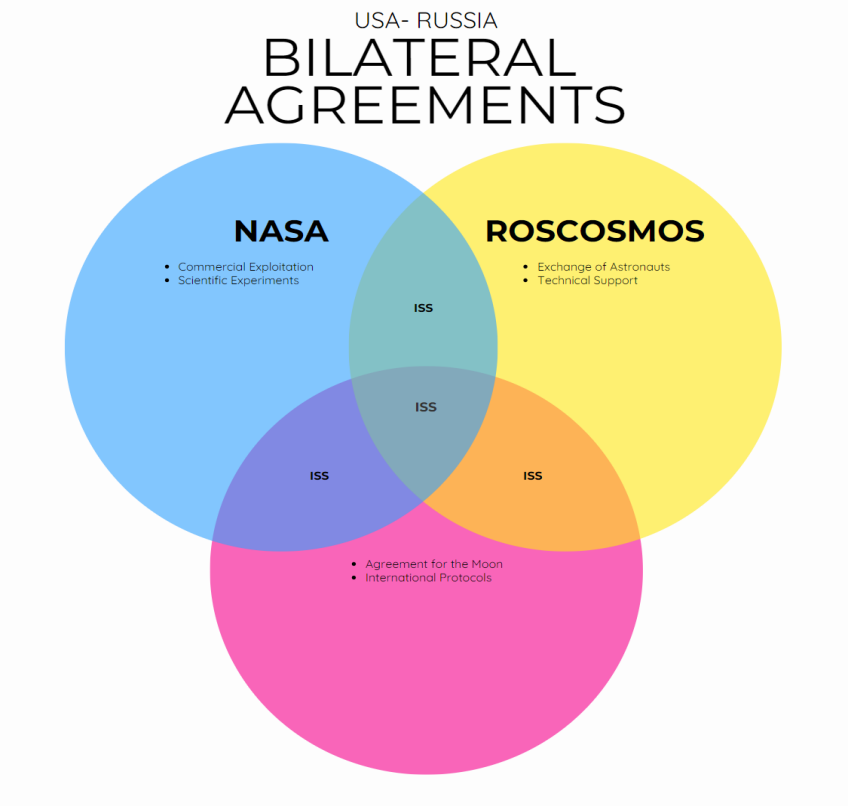
Πίνακας 5 : Συγκριτικός πίνακας Space Shuttle - Soyuz.

Τα Space Shuttle και τα Soyuz έχουν διαφορετικές καταβολές και στόχους .Αρχικά τα Space Shuttle αναπτύχθηκαν από τις Ηνωμένες Πολιτείες και λειτούργησαν από το 1981 έως το 2011, ενώ τα Soyuz είναι ρωσικά σκάφη που πρωτοεκτοξεύτηκαν το 1967 και εξακολουθούν να είναι ενεργά.

Αν και τα Space Shuttle ήταν πλήρως επαναχρησιμοποιήσιμα και μπορούσαν να μεταφέρουν έως 7 αστροναύτες, σε αντίθεση με τα Soyuz που είναι μόνο μερικώς επαναχρησιμοποιήσιμα (μόνο το μέρος της κάψουλας) και μεταφέρουν έως 3 κοσμοναύτες, το κόστος ανά εκτόξευση των Space Shuttle ήταν πολύ υψηλότερο (περίπου 450 εκατομμύρια δολάρια) σε σύγκριση με τα Soyuz (περίπου 80 εκατομμύρια δολάρια). Επίσης τα Space Shuttle πραγματοποίησαν συνολικά 135 εκτοξεύσεις, ενώ τα Soyuz έχουν πάνω από 140 εκτοξεύσεις μέχρι το 2024. Οι κύριες αποστολές των Space Shuttle περιλάμβαναν τη μεταφορά ανθρώπων και φορτίων στον Διεθνή Διαστημικό Σταθμό (ISS), επισκευές δορυφόρων και επιστημονικές αποστολές, ενώ τα Soyuz επικεντρώνονται στη μεταφορά πληρωμάτων στον ISS και την επιστροφή στη Γη. Τα Space Shuttle προσγειώνονταν σε διάδρομο, ενώ τα Soyuz χρησιμοποιούν αλεξίπτωτο για να προσγειωθούν στην ξηρά. Επιπλέον, τα Space Shuttle είχαν μεγαλύτερη χωρητικότητα φορτίου (έως 24.400 κιλά) και μέγιστη διάρκεια αποστολής 17 ημερών, σε σύγκριση με τα Soyuz που έχουν περιορισμένο χώρο για φορτίο και μπορούν να παραμείνουν συνδεδεμένα στον ISS για έως και 6 μήνες. Τα Space Shuttle χρησιμοποιούσαν Solid Rocket Boosters και External Tank για την εκτόξευση τους, ενώ τα Soyuz χρησιμοποιούν τον Soyuz Rocket και εκτοξεύονται από το Baikonur Cosmodrome στο Καζακστάν. Επιπροσθέτως το κόστος ανάπτυξης των Space Shuttle ήταν περίπου 49 δισεκατομμύρια δολάρια, ενώ το κόστος ανάπτυξης των Soyuz είναι σημαντικά χαμηλότερο, εκτιμώμενο στα περίπου 3.55 δισεκατομμύρια δολάρια (προσαρμοσμένο με βάση τον πληθωρισμό). Τα Space Shuttle είναι γνωστά για την ανάπτυξη του διαστημικού τηλεσκοπίου Hubble και την κατασκευή του ISS, ενώ τα Soyuz είναι το πρόγραμμα επανδρωμένων διαστημικών σκαφών με τη μεγαλύτερη διάρκεια υπηρεσίας. Τα Space Shuttle λειτουργούσαν σε εύρος υψομέτρου από 185 έως 643 χιλιόμετρα με ταχύτητα 28,000 km/h (17,500 mph), ενώ τα Soyuz λειτουργούν σε εύρος υψομέτρου από 200 έως 400 χιλιόμετρα με ταχύτητα 27,580 km/h (17,150 mph). Η διάρκεια καύσης για επιβράδυνση των Space Shuttle ήταν περίπου 30 λεπτά, ενώ των Soyuz περίπου 4.5 λεπτά. Αυτές οι διαφορές αντανακλούν τις διαφορετικές προσεγγίσεις και προτεραιότητες των δύο χωρών στην εξερεύνηση του διαστήματος. Οι Ηνωμένες Πολιτείες επένδυσαν σε ένα προηγμένο και επαναχρησιμοποιήσιμο διαστημικό σύστημα, ενώ η Ρωσία επικεντρώθηκε σε ένα πιο οικονομικό και δοκιμασμένο σύστημα για επανδρωμένες αποστολές.

Η Συμφωνία για τη Σελήνη του 1979, γνωστή και ως "Συμφωνία για τις Δραστηριότητες των Κρατών στη Σελήνη και Άλλα Ουράνια Σώματα", είναι μια πολυμερής συμφωνία που στοχεύει στο να ρυθμίσει τις δραστηριότητες των χωρών στη Σελήνη και σε άλλα ουράνια σώματα. Υιοθετήθηκε από τη Γενική Συνέλευση των Ηνωμένων Εθνών στις 5 Δεκεμβρίου 1979 και τέθηκε σε ισχύ στις 11 Ιουλίου 1984. Η συμφωνία αυτή αποτελεί το 5ο διεθνές κείμενο του διαστημικού δικαίου μετά τη Συνθήκη του Διαστήματος του 1967, τη Συμφωνία Διάσωσης του 1968, τη Σύμβαση για την Ευθύνη του 1972 και τη Σύμβαση Καταχώρησης του 1976. Η συμφωνία αυτή αποφασίζει ότι η Σελήνη και οι πόροι της αποτελούν κοινή κληρονομιά της ανθρωπότητας. Αυτό σημαίνει ότι η Σελήνη δεν μπορεί να ανήκει αποκλειστικά σε κανένα κράτος ή ιδιωτική οντότητα και ότι οι δραστηριότητες στη Σελήνη πρέπει να πραγματοποιούνται προς όφελος όλων των χωρών, ανεξαρτήτως του επιπέδου οικονομικής ή επιστημονικής ανάπτυξής τους. Η συμφωνία επισημαίνει ότι η εξερεύνηση και η χρήση της Σελήνης πρέπει να γίνονται για ειρηνικούς σκοπούς και ότι πρέπει να αποφεύγεται κάθε μορφή στρατιωτικής δραστηριότητας, όπως η εγκατάσταση στρατιωτικών βάσεων ή η δοκιμή όπλων μαζικής καταστροφής. Επιπλέον, η συμφωνία απαγορεύει την καταστροφή ή την αλλοίωση του περιβάλλοντος της Σελήνης και απαιτεί από τα κράτη να λαμβάνουν τα απαραίτητα μέτρα για την αποτροπή της επιβάρυνσης του σεληνιακού περιβάλλοντος από τις δραστηριότητές τους. Επίσης, η συμφωνία προβλέπει ότι οι επιστημονικές έρευνες και τα αποτελέσματά τους πρέπει να είναι διαθέσιμα σε όλα τα κράτη και ότι η εξερεύνηση της Σελήνης πρέπει να πραγματοποιείται με διαφάνεια και σεβασμό προς τα άλλα κράτη. Ένα από τα πιο σημαντικά θέματα που ρυθμίζει η Συμφωνία για τη Σελήνη είναι η διαχείριση των φυσικών πόρων της. Η συμφωνία προβλέπει ότι η εκμετάλλευση των φυσικών πόρων της Σελήνης πρέπει να

γίνει αντικείμενο ενός διεθνούς καθεστώτος που θα θεσπιστεί από μια μελλοντική διεθνή συμφωνία. Το καθεστώς αυτό θα πρέπει να εξασφαλίζει ότι τα οφέλη από την εκμετάλλευση των πόρων θα διανέμονται δίκαια μεταξύ όλων των κρατών και ότι οι δραστηριότητες εκμετάλλευσης θα πραγματοποιούνται με σεβασμό στο περιβάλλον της Σελήνης. Η Συμφωνία για τη Σελήνη έχει υιοθετηθεί από ένα περιορισμένο αριθμό χωρών και δεν έχει λάβει την υποστήριξη των κύριων διαστημικών δυνάμεων, όπως οι Ηνωμένες Πολιτείες, η Ρωσία και η Κίνα. Η κριτική που δέχεται η συμφωνία επικεντρώνεται κυρίως στην αρχή της "κοινής κληρονομιάς της ανθρωπότητας" και στην απαίτηση για διεθνή διαχείριση των πόρων, καθώς αυτά θεωρούνται ότι περιορίζουν την εθνική κυριαρχία και την ελευθερία δράσης των κρατών στο διάστημα. Παρά τις προκλήσεις και την περιορισμένη υποστήριξή της, η Συμφωνία για τη Σελήνη παραμένει ένα σημαντικό κείμενο που θέτει τις αρχές και τις αξίες που πρέπει να διέπουν την ανθρώπινη δραστηριότητα στη Σελήνη και σε άλλα ουράνια σώματα. Η συζήτηση για τη διαχείριση των πόρων της Σελήνης και η ανάγκη για διεθνή συνεργασία και κανονισμούς συνεχίζεται, ιδιαίτερα καθώς οι διαστημικές αποστολές και η τεχνολογία εξελίσσονται [101].



Σχήμα 13: Διάγραμμα Venn διμερών συμφωνιών ΗΠΑ - Ρωσίας.

Το παραπάνω διάγραμμα Venn απεικονίζει τις διμερείς συμφωνίες στο διάστημα μεταξύ των ΗΠΑ και της Ρωσίας. Κάθε κύκλος αντιπροσωπεύει μία ομάδα και οι κοινές περιοχές δείχνουν τις κοινές δραστηριότητες ή πρωτοβουλίες μεταξύ των ομάδων αυτών. Το διάγραμμα δείχνει ότι η NASA και η ROSCOSMOS έχουν ξεχωριστές περιοχές εξειδίκευσης και συνεργασίας, αλλά οι βασικοί τομείς όπου υπάρχει αλληλεπίδραση και συνεργασία είναι γύρω από τον Διεθνή Διαστημικό Σταθμό (ISS). Επιπλέον, πέρα από την κοινή αυτή βάση, υπάρχουν και πρόσθετες συμφωνίες που σχετίζονται με τη Σελήνη και τα διεθνή πρωτόκολλα, τα οποία ενισχύουν τη συνεργασία τους και επεκτείνουν τις κοινές τους προσπάθειες πέρα από τον ISS.

6.6 Κανονισμοί Εμπορικού Διαστήματος

Με την αυξανόμενη δραστηριότητα στο διάστημα και την είσοδο πολλών ιδιωτικών εταιρειών στον τομέα αυτό, οι κανονισμοί εμπορικού διαστήματος καθίστανται όλο και πιο σημαντικοί. Οι κανονισμοί αυτοί είναι απαραίτητοι για τη διασφάλιση της ασφάλειας, της βιωσιμότητας και της νομιμότητας των εμπορικών διαστημικών δραστηριοτήτων, καθώς και για την προστασία των συμφερόντων των κρατών και των ιδιωτικών φορέων που εμπλέκονται.

Σε εθνικό επίπεδο, οι κανονισμοί εμπορικού διαστήματος ορίζονται και επιβλέπονται από διάφορους κυβερνητικούς οργανισμούς. Στις Ηνωμένες Πολιτείες, η FAA είναι υπεύθυνη για την παροχή αδειών των εκτοξεύσεων και των επιστροφών διαστημικών οχημάτων. Η FAA διασφαλίζει ότι οι εμπορικές δραστηριότητες στο διάστημα συμμορφώνονται με τα πρότυπα ασφαλείας και τις περιβαλλοντικές απαιτήσεις. Επιπλέον, η NOAA επιβλέπει τη χρήση των συστημάτων παρακολούθησης της Γης, ενώ η FCC ρυθμίζει τις τηλεπικοινωνιακές συχνότητες που χρησιμοποιούνται από δορυφόρους. Η Ρωσία, μέσω της Roscosmos και άλλων κυβερνητικών φορέων, έχει δημιουργήσει κανονισμούς που διέπουν τις εμπορικές δραστηριότητες στο διάστημα, συμπεριλαμβανομένης της παροχής αδειών εκτοξεύσεων και της διαχείρισης διαστημικών πόρων. Η Roscosmos συνεργάζεται επίσης με διεθνείς εταίρους για τη διασφάλιση της συμμόρφωσης με τα διεθνή πρότυπα. Η Ευρωπαϊκή Ένωση, μέσω του ESA και της Ευρωπαϊκής Επιτροπής, έχει αναπτύξει ένα ρυθμιστικό πλαίσιο για τις εμπορικές διαστημικές δραστηριότητες. Το πλαίσιο αυτό περιλαμβάνει κανονισμούς για την εκτόξευση δορυφόρων, την παρακολούθηση της Γης και την προστασία των διαστημικών υποδομών από κυβερνοεπιθέσεις [102].

Σε διεθνές επίπεδο, διάφοροι οργανισμοί και συνθήκες συμβάλλουν στη ρύθμιση των εμπορικών διαστημικών δραστηριοτήτων όπως είδαμε και στα προηγούμενα κεφάλαια. Η ITU είναι υπεύθυνη για την κατανομή των τηλεπικοινωνιακών συχνοτήτων και τη διασφάλιση ότι οι δορυφόροι δεν παρεμβαίνουν ο ένας στον άλλο καθώς επίσης και για πρότυπα για την ασφάλεια των δορυφορικών επικοινωνιών και την πρόληψη των συγκρούσεων στο διάστημα .Η COPUOS αναπτύσσει οδηγίες και συστάσεις για την ασφάλεια και τη βιωσιμότητα των διαστημικών δραστηριοτήτων. Η Συνθήκη του Εξώτερου Διαστήματος του 1967, η οποία αποτελεί τη βάση του διεθνούς διαστημικού δικαίου, καθορίζει ότι το διάστημα είναι ελεύθερο για εξερεύνηση και χρήση από όλα τα κράτη, αλλά απαιτεί ότι οι δραστηριότητες πρέπει να πραγματοποιούνται προς όφελος όλης της ανθρωπότητας. Η συνθήκη αυτή απαγορεύει την τοποθέτηση πυρηνικών όπλων στο διάστημα και απαιτεί την αποτροπή της επιβάρυνσης του διαστημικού περιβάλλοντος [103].

Η ρύθμιση των εμπορικών διαστημικών δραστηριοτήτων παρουσιάζει διάφορες προκλήσεις και ευκαιρίες. Μία από τις κύριες προκλήσεις είναι η διαχείριση των διαστημικών απορριμμάτων, τα οποία αποτελούν απειλή για τα λειτουργικά δορυφορικά συστήματα και τις μελλοντικές αποστολές. Η ανάπτυξη τεχνολογιών και κανονισμών για την απομάκρυνση των απορριμμάτων είναι κρίσιμη για τη βιωσιμότητα του διαστημικού περιβάλλοντος. Η κυβερνοασφάλεια αποτελεί επίσης σημαντική πρόκληση, καθώς οι δορυφόροι και τα διαστημικά συστήματα είναι ευάλωτα σε κυβερνοεπιθέσεις. Οι κανονισμοί πρέπει να διασφαλίζουν ότι οι εμπορικές διαστημικές εταιρείες λαμβάνουν τα απαραίτητα μέτρα για την προστασία των συστημάτων τους από τέτοιες απειλές. Παρά τις προκλήσεις, οι εμπορικές διαστημικές δραστηριότητες προσφέρουν σημαντικές ευκαιρίες για οικονομική ανάπτυξη και τεχνολογική πρόοδο. Η ανάπτυξη της διαστημικής τουριστικής βιομηχανίας, η εξόρυξη αστεροειδών και άλλων ουράνιων σωμάτων, και η παροχή δορυφορικών υπηρεσιών υψηλής ακρίβειας είναι μερικές από τις πολλές ευκαιρίες που αναδύονται. Ο ορισμός σαφών και αυστηρών κανονισμών είναι απαραίτητη για την προώθηση της ασφάλειας, της

βιωσιμότητας και της ανάπτυξης του εμπορικού τομέα του διαστήματος. Με την αύξηση της εμπορικής δραστηριότητας στο διάστημα, η ανάγκη για ρύθμιση γίνεται όλο και πιο αναγκαστική, διασφαλίζοντας ότι οι διαστημικές δραστηριότητες πραγματοποιούνται με υπευθυνότητα και σε συμφωνία με τα διεθνή πρότυπα. Οι εθνικές αρχές και οι διεθνείς οργανισμοί πρέπει να συνεργαστούν για να διαμορφώσουν ένα συνολικό και αποτελεσματικό ρυθμιστικό πλαίσιο που θα ενισχύσει την ασφάλεια και την ανάπτυξη του διαστημικού τομέα [104].

7

Συμπεράσματα

Η παρούσα διπλωματική εργασία εξέτασε αναλυτικά την αλληλεπίδραση μεταξύ κυβερνοασφάλειας και διαστημικών συστημάτων, με ιδιαίτερη έμφαση στη χρήση τεχνητής νοημοσύνης. Μέσα σε αυτή την έρευνα φαίνεται η σημασία της κυβερνοασφάλειας με τη χρήση τεχνητής νοημοσύνης. Η ανάλυση των κινδύνων και ευπαθειών που σχετίζονται με τα διαστημικά συστήματα ανέδειξε κρίσιμα σημεία που πρέπει να ληφθούν υπόψη για την ανάπτυξη ασφαλών και αξιόπιστων τεχνολογιών. Η έρευνα έδειξε ότι τα διαστημικά συστήματα είναι στόχοι υψηλής προτεραιότητας για κυβερνοεπιθέσεις, οι οποίες μπορούν να προέλθουν από κρατικές οντότητες, ιδιωτικές εταιρείες ή ακόμα και μεμονωμένους χάκερ. Η τεχνητή νοημοσύνη προσθέτει επιπλέον επίπεδα πολυπλοκότητας και ευπάθειας, καθώς μπορεί να γίνουν αντικείμενα εκμετάλλευσης μέσω κακόβουλων αλγορίθμων ή επεξεργασμένων δεδομένων. Η ανάλυση των πολιτικών των ΗΠΑ, της Ρωσίας, της Κίνας και του Ηνωμένου Βασιλείου αποκάλυψε σημαντικές διαφορές στις προσεγγίσεις και τις προτεραιότητες σχετικά με την κυβερνοασφάλεια στο διάστημα. Η έλλειψη ενοποιημένων και αυστηρών διεθνών προτύπων παραμένει μια σημαντική πρόκληση .Οι συμφωνίες, όπως αυτή του Διεθνούς Διαστημικού Σταθμού (ISS), αποτελούν υποδειγματικά παραδείγματα διεθνούς συνεργασίας. Η ενίσχυση της διεθνούς συνεργασίας και η δημιουργία κοινών πρωτοκόλλων ασφάλειας είναι κρίσιμες για την προστασία των διαστημικών υποδομών. Οι τεχνικές λύσεις που εξετάστηκαν, όπως η κρυπτογράφηση, τα συστήματα ανίχνευσης και πρόληψης εισβολών, και η ασφαλής διαχείριση πρωτοκόλλων επικοινωνίας, είναι ζωτικής σημασίας για την ενίσχυση της ασφάλειας των διαστημικών συστημάτων. Η ανάπτυξη και εφαρμογή αυτών των τεχνολογιών απαιτεί συνεχή έρευνα και επένδυση. Η εκπαίδευση και η ευαισθητοποίηση στην κυβερνοασφάλεια για το προσωπικό που ασχολείται με διαστημικές τεχνολογίες είναι κρίσιμης σημασίας. Η δημιουργία εκπαιδευτικών προγραμμάτων και η προώθηση μιας κουλτούρας ασφάλειας μπορεί να συμβάλλει σημαντικά στην ελαχιστοποίηση των κινδύνων. Το προσωπικό πρέπει να είναι ενήμερο για τις τελευταίες εξελίξεις στις κυβερνοαπειλές και να έχει την ικανότητα να αναγνωρίζει και να αντιμετωπίζει τις απειλές αυτές αποτελεσματικά. Συνολικά, η έρευνα υποδεικνύει ότι η ασφάλεια των διαστημικών συστημάτων που χρησιμοποιούν τεχνητή νοημοσύνη δεν μπορεί να επιτευχθεί χωρίς συνδυασμό τεχνικών, οργανωτικών και εκπαιδευτικών μέτρων. Η ενίσχυση της διεθνούς συνεργασίας, η ανάπτυξη και εφαρμογή προηγμένων τεχνολογιών και η προώθηση της εκπαίδευσης στην κυβερνοασφάλεια είναι οι βασικοί πυλώνες για την αντιμετώπιση των σύγχρονων προκλήσεων στον τομέα αυτό .Τα αποτελέσματα δείχνουν ότι οι τεχνολογίες AI μπορούν να προσφέρουν σημαντική υποστήριξη στην ανίχνευση και την πρόληψη κυβερνοεπιθέσεων. Ωστόσο, απαιτείται συνεχής έρευνα και ανάπτυξη καθώς οι τεχνολογίες και οι απειλές εξελίσσονται συνεχώς. Η διεθνής συνεργασία είναι κρίσιμη για την αντιμετώπιση των αυξανόμενων απειλών στον κυβερνοχώρο, ενώ η ανάπτυξη και η υιοθέτηση διεθνών προτύπων και

κανονισμών είναι απαραίτητη. Η εκπαίδευση των επαγγελματιών του κλάδου πρέπει να ενισχυθεί για την καλύτερη κατανόηση και αντιμετώπιση των κυβερνοαπειλών. Τέλος μέσω πιθανής μελλοντικής έρευνας θα μπορούν να αναδειχθούν νέες λύσεις και τεχνολογίες που να βοηθούν στα παραπάνω ζητήματα. Αυτές οι κατευθύνσεις παρέχουν ένα πλαίσιο για τη βελτίωση της ασφάλειας και της αξιοπιστίας των διαστημικών συστημάτων στο μέλλον.

7.1 Προτάσεις για Μελλοντική Έρευνα

Η μελλοντική έρευνα θα πρέπει να επικεντρωθεί σε διάφορους τομείς για να αντιμετωπιστούν οι εξελισσόμενες προκλήσεις στην κυβερνοασφάλεια των διαστημικών συστημάτων:

- Ανάπτυξη Κοινών Διεθνών Προτύπων και Κανονισμών και Ενίσχυση της Διεθνούς Συνεργασίας:

  Η ανάπτυξη κοινών διεθνών προτύπων και κανονισμών είναι ζωτικής σημασίας για την ενίσχυση της παγκόσμιας ασφάλειας στον τομέα των διαστημικών συστημάτων. Καθώς τα διαστημικά συστήματα γίνονται ολοένα και πιο περίπλοκα και διεθνοποιημένα, η έλλειψη κοινών προτύπων μπορεί να δημιουργήσει ευπάθειες που εκμεταλλεύονται οι κυβερνοεπιθέσεις. Οι διεθνείς οργανισμοί, οι εθνικές αρχές και οι ιδιωτικές εταιρείες πρέπει να συνεργαστούν για τη διαμόρφωση και την υιοθέτηση αυτών των προτύπων. Η υιοθέτηση κοινών προτύπων ενισχύει τη συνεργασία μεταξύ των κρατών και των οργανισμών, διευκολύνοντας την ανταλλαγή πληροφοριών και την κοινή αντιμετώπιση των απειλών. Τα ενοποιημένα πρότυπα βοηθούν στη διασφάλιση της συνέπειας στην εφαρμογή των μέτρων ασφάλειας, μειώνοντας τα κενά και τις ευπάθειες στα συστήματα. Η χρήση τους απλοποιεί την ανάπτυξη και τη διαχείριση των συστημάτων, μειώνοντας τα κόστη και την πολυπλοκότητα που σχετίζονται με την προσαρμογή σε πολλαπλά πρότυπα .Η ύπαρξη κοινών και καλά καθορισμένων διαδικασιών απόκρισης επιτρέπει την ταχύτερη και πιο αποτελεσματική αντίδραση σε συμβάντα κυβερνοασφάλειας, περιορίζοντας τις συνέπειες των επιθέσεων.

- Έρευνα και Ανάπτυξη Νέων Τεχνολογιών Ασφάλειας:

Η συνεχής επένδυση σε νέες τεχνολογίες ασφάλειας είναι απαραίτητη για την αντιμετώπιση των συνεχώς εξελισσόμενων κυβερνοαπειλών. Η ταχύτητα με την οποία αναπτύσσονται και εξελίσσονται οι τεχνολογίες καθιστά αναγκαία τη συνεχή καινοτομία στον τομέα της κυβερνοασφάλειας. Προτεινόμενες περιοχές έρευνας περιλαμβάνουν την ανάπτυξη προηγμένων αλγορίθμων ανίχνευσης εισβολών, συστημάτων πρόβλεψης απειλών και τεχνολογιών για την προστασία των δορυφόρων. Μέθοδοι οι οποίες μπορούν να αναλυθούν περαιτέρω είναι η μηχανική μάθηση, τα δίκτυα νευρωνικών συστημάτων και τα συστήματα βασισμένα σε υπογραφές κακόβουλου λογισμικού.

- Εκπαίδευση και Ευαισθητοποίηση

Η ανάπτυξη εκπαιδευτικών προγραμμάτων και η ευαισθητοποίηση στην ασφάλεια για το προσωπικό που ασχολείται με διαστημικές τεχνολογίες είναι απαραίτητα για την ενίσχυση της ανθεκτικότητας των συστημάτων. Οι κυβερνοαπειλές είναι διαρκώς εξελισσόμενες, και οι επαγγελματίες που εργάζονται στον τομέα των διαστημικών συστημάτων πρέπει να είναι ενημερωμένοι και εκπαιδευμένοι για να μπορούν να ανταποκριθούν αποτελεσματικά στις

προκλήσεις αυτές. Προτείνεται η δημιουργία προγραμμάτων πιστοποίησης και συνεχιζόμενης εκπαίδευσης για το προσωπικό, τα οποία θα διασφαλίζουν την επάρκεια γνώσεων και δεξιοτήτων. Αυτά τα προγράμματα θα πρέπει να καλύπτουν θέματα όπως η ανίχνευση και η απόκριση σε κυβερνοεπιθέσεις, η διαχείριση κρίσεων και η εφαρμογή βέλτιστων πρακτικών ασφαλείας. Επιπλέον, η ευαισθητοποίηση σχετικά με τις απειλές και τις αδυναμίες που μπορεί να εκμεταλλευτούν οι επιτιθέμενοι είναι σημαντική για την πρόληψη παραβιάσεων και την προστασία των διαστημικών υποδομών.

- Ανάλυση και Διαχείριση Κινδύνων

Η μελλοντική έρευνα πρέπει να περιλαμβάνει την ανάπτυξη μεθόδων για την ανάλυση και τη διαχείριση των κινδύνων σε διαστημικά συστήματα. Η ανάλυση κινδύνων είναι η διαδικασία αξιολόγησης των πιθανών απειλών και των ευπαθειών, καθώς και των επιπτώσεών τους, ενώ η διαχείριση κινδύνων περιλαμβάνει την ανάπτυξη και την εφαρμογή στρατηγικών για την ελαχιστοποίηση αυτών των κινδύνων. Προτείνεται η ανάπτυξη εργαλείων και τεχνικών για την αξιολόγηση των κινδύνων που σχετίζονται με τις κυβερνοαπειλές στα διαστημικά συστήματα. Αυτά τα εργαλεία θα πρέπει να επιτρέπουν την ανάλυση δεδομένων σε πραγματικό χρόνο και την πρόβλεψη πιθανών επιθέσεων, ώστε να λαμβάνονται προληπτικά μέτρα. Επίσης, η έρευνα πρέπει να επικεντρωθεί στην ανάπτυξη διαδικασιών και πρωτοκόλλων για την αποτελεσματική απόκριση σε περιστατικά ασφαλείας, διασφαλίζοντας ότι οι οργανισμοί μπορούν να ανακάμψουν γρήγορα και να συνεχίσουν τη λειτουργία τους με ελάχιστες διαταραχές.

Άρα καταλήγουμε ότι η μελλοντική έρευνα πρέπει να περιλαμβάνει την ανάπτυξη μεθόδων για την ανάλυση και τη διαχείριση των κινδύνων σε διαστημικά συστήματα. Η ανάλυση κινδύνων είναι η διαδικασία αξιολόγησης των πιθανών απειλών και των ευπαθειών καθώς και των επιπτώσεών τους, ενώ η διαχείριση κινδύνων περιλαμβάνει την ανάπτυξη και την εφαρμογή στρατηγικών για την ελαχιστοποίηση αυτών των κινδύνων. Προτείνεται η ανάπτυξη εργαλείων και τεχνικών για την αξιολόγηση των κινδύνων που σχετίζονται με τις κυβερνοαπειλές στα διαστημικά συστήματα. Αυτά τα εργαλεία θα πρέπει να επιτρέπουν την ανάλυση δεδομένων σε πραγματικό χρόνο και την πρόβλεψη πιθανών επιθέσεων, ώστε να λαμβάνονται προληπτικά μέτρα. Επίσης, η έρευνα πρέπει να επικεντρωθεί στην ανάπτυξη διαδικασιών και πρωτοκόλλων για την αποτελεσματική απόκριση σε περιστατικά ασφαλείας, διασφαλίζοντας ότι οι οργανισμοί μπορούν να ανακάμψουν γρήγορα και να συνεχίσουν τη λειτουργία τους με ελάχιστες διαταραχές.

8

Βιβλιογραφία

[1] Harvard Medical School. (2017). History of artificial intelligence. Science in the News. https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/

[2] T. Harrison. "Space Threat Assessment." https://www.csis.org/analysis/space-threat-assessment-2022 (accessed.

[3] S. Hilton, R. Sabatini, A. Gardi, H. Ogawa, and P. Teofilatto, "Space Traffic Management: Towards Safe and Unsegregated Space Transport Operations," Progress in Aerospace Sciences, vol. 105, 02/01 2019, doi: 10.1016/j.paerosci.2018.10.006.

[4] J. P. a. J. Slay, "Space Systems Security Definition and Domain Mapping," Journal of Information Warfare, vol. 21, 2022.

[5] A. Console, "Space Resilience – Why and How?," JAPCC Journal, no. 27, 2018. [Online]. Available: https://www.japcc.org/space-resilience-why-and-how/.

[6] Lu, Chien-Ping. (2017). AI, Native Supercomputing and The Revival of Moore's Law. APSIPA Transactions on Signal and Information Processing. 6. 10.1017/ATSIP.2017.9.

[7] Alam, Azmir. (2023). What is Machine Learning?. 10.5281/zenodo.8231580.

[8] Carlo, A. (2021). Cyber Threats to Space Communications: Space and Cyberspace Policies. In A. Froehlich (Ed.), **Outer Space and Cyber Space** (Vol. 33, pp. 269–278). Springer, Cham. http://dx.doi.org/10.1007/978-3-030-70740-8_17

[9] Khan, Ilyas. (2018). Natural Language Generation in Artificial Intelligence.

[10] Torres, P. J., Martínez, L., Comesaña, P. S., & Iglesia, D. M. (2019). Review: Machine learning techniques applied to cybersecurity. **International Journal of Machine Learning and Cybernetics**, 10, 2823–2836. https://doi.org/10.1007/s13042-018-00906-1

[11] Giuffrida, Gianluca & Fanucci, Luca & Meoni, Gabriele & Batic, Matej & Buckley, Léonie & Dunne, Aubrey & Dijk, Chris & Esposito, Marco & Hefele, John & Vercruyssen, Nathan & Furano, Gianluca & Pastena, Massimiliano & Aschbacher, Josef. (2021). The Φ-Sat-1 Mission: The First On-Board Deep Neural Network Demonstrator for Satellite Earth Observation. IEEE Transactions on Geoscience and Remote Sensing. 60. 1-1. 10.1109/TGRS.2021.3125567.

[12] Innefu Labs. (2022). How AI Can Ensure Better Cyber Security? Retrieved from https://www.innefu.com/blog/how-ai-can-ensure-better-cyber-security

[13]Mazareanu, E. Number of Public and Private Airports in the United States from 1990 to 2019*. 2020. Available online: https://www.statista.com/statistics/183496/number-of-airports-in-the-united-states-since-1990/ (accessed on 28 November 2020).

[14] Brundage, M.; Avin, S.; Clark, J.; Toner, H.; Eckersley, P.; Garfinkel, B.; Dafoe, A.; Scharre, P.; Zeitzoff, T.; Filar, B.; et al. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv 2018, arXiv:1802.07228.

[15] Tanase, Stefan. Satellite Turla: APT command and control in the sky. Kaspersky. 2015. https://media.kaspersky.com/pdf/SatTurla_Solution_Paper.pdf

[16] Andrew Dalton. Russia Hopes to Block Cruise Missile Attacks with Cell Towers. Engadget. 2016. https://www.engadget.com/2016/10/17/russia-jamming-cruise-missile-attacks-with-cell-towers/

[17] Li, Xiangjun & Chen, Lei & Lu, Zukun & Wang, Feixue & Liu, Wenxiang & Xiao, Wei & Liu, Peiguo. (2023). Overview of Jamming Technology for Satellite Navigation. Machines. 11. 768. 10.3390/machines11070768.

[18] M. Scholl, "Introduction to Cybersecurity for Commercial Satellite Operations," Draft NISTIR 8270, National Institute of Standards and Technology 2021, doi: https://doi.org/10.6028/NIST.IR.8270-draft.

[19] Jammer Master, “The Complete Guide to Signal Jammers” , Accessed from: “https://jammermaster.com/blog/the-complete-guide-to-signal-jammers/”

[20] Čerka, P., Grigienė, J., & Sirbikytė, G. (2015). Liability for Damages Caused by Artificial Intelligence. **Computer Law & Security Review**, 31(3), 376-389.

[21] GPS.gov,”Information About GPS Jamming”, Accessed from:”https://www.gps.gov/spectrum/jamming/”

[22] Hansen, Petersen & Henry, Wayne & Reith, Mark & Thummala, Rajiv & Falco, Gregory. (2024). Hijacking Satellites and Defensive Techniques.

[23] Falco, G., & Rossenbach, E. (2022). **Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity**. Oxford University Press.

[24] Tripathi, Nikhil & Mehtre, Babu. (2013). DoS and DDoS Attacks: Impact, Analysis and Countermeasures. 1-6.

[25] Yadav, Deepali & Kumar, Gautam & Kameshwari, D. & Gunjan, Vinit & Kumar, Sheo. (2022). Malware Techniques and Its Effect: A Survey. 10.1007/978-981-16-7985-8_127.

[26] U.S.-China Economic and Security Review Commission. 2011 Report to Congress. U.S. Government Printing Office. 2011. https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf

[27] Martin, Paul. NASA Cybersecurity: An Examination of the Agency’s Information Security. Testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology. 2012. https://oig.nasa.gov/docs/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf

[28] Muntode, Antonette. (2019). An Overview on Phishing- its types and Countermeasures. International Journal of Engineering Research and. V8. 10.17577/IJERTV8IS120260.

[29] Hutchins, Ryan. Cyber Defense of Space Assets. 2016. http://www.cs.tufts.edu/comp/116/archive/fall2016/rhutchins.pdf

[30] Schmitt, M. N. (Ed.). (2017). **Tallinn Manual 2.0 On The International Law Applicable to Cyber Operations** (2nd ed.). Retrieved from http://csef.ru/media/articles/3990/3990.pdf

[31]Santamarta, Ruben. A wake-up call for SATCOM security. IOActive. 2014. https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

[32] Ibeobi, Samuel & Pan, Xuchao. (2021). Study of electromagnetic pulse (EMP) effect on surveillance unmanned aerial vehicles (UAVs). Journal of Mechanical Engineering, Automation and Control Systems. 2. 10.21595/jmeacs.2021.21926.

[33] 2 Leonard David. "Sweating the Small Stuff: CubeSats Swarm Earth Orbit." Scientific American. 2017. https://www.scientificamerican.com/article/sweating-the-small-stuff-cubesats-swarm-earth-orbit/. 3

[34] Ryan Schradin. "Government Space Leaders Look To Commercial Satellites for More Resilient Communications." The Government Satellite Report. 2016. https://ses-gs.com/govsat/defense-intelligence/government-space-leaders-look-to-commercial-satellites-for-more-resilient-communications/.

[35] Tereza Pultarova. "Could Cubesats Trigger a Space Junk Apocalypse?" Space.com. 2017. https:// www.space.com/36506-cubesats-space-junk-apocalypse.html.

[36] Kaspersky's Global Research and Analysis Team (GReAT). "The Epic Turla Operation." SecureList. 2014. https://securelist.com/the-epic-turla-operation/65545/.

[37] J.M. Porup. "It's Surprisingly Simple to Hack a Satellite." Motherboard. 2015. https://motherboard. vice.com/en_us/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite.

[38] Chris Lo, "GPS spoofing: what's the risk for ship navigation?," Ship Technology, (15 April 2019), https://www.ship-technology.com/features/ship-navigation-risks/?cfview. Accessed on 18 March 2024

[39] IG Inside Gnss :"Reports of Mass GPS Spoofing Attack in the Black Sea Strengthen Calls for PNT Backup" Accessed from: "https://insidegnss.com/reports-of-mass-gps-spoofing-attack-in-the-black-sea-strengthen-calls-for-pnt-backup/"

[40] Lisa Vaas. "Drone Hijacked By Hackers From Texas College With $1,000 Spoofer." Naked Security. 2012. https://nakedsecurity.sophos.com/2012/07/02/drone-hackedwith-1000-spoofer/.

[41] "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-inDepth Strategies." Industrial Control System Cyber Emergency Response Team. 2016. http:// www.verizonenterprise.com/verizon-insights-lab/VES/obscurity-no-more-4-steps-to-securing-the-ot-environment-for-manufacturing.

[42] Jinwoo Hwang. "The Secure Sockets Layer and Transport Layer Security." IBM Developer Works. 2012. https://www.sslshopper.com/what-is-ssl.html.

[43] Carlo, A. (2021). **Artificial Intelligence in the Defence Sector**, MESAS20, Prague, Czech Republic, 269–278. http://dx.doi.org/10.1007/978-3-030-70740-8_17

[44] Paul Martin. “NASA Cybersecurity: An Examination of the Agency’s Information Security.” Testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology. 2012. https://oig.nasa.gov/congressional/FINAL_written_statement_ for_%20IT_%20hearing_February_26_edit_v2.pdf.

[45] Michael Sampson. “NASA Parts Selection List.” NASA Electronic Parts and Packaging Program. 2016. https://nepp.nasa.gov/npsl/npsl_UsePolicy.htm.

[46] John Sprague. “Collaboration that Pays NASA Back.” NASA IT Talk. 2012. https://www.hq.nasa.gov/ office/itcd/notices/010410-1.htm

[47] “AT&T Powers NASA’s Deep Space Network.” AT&T. 2016. http://about.att.com/story/att_powers_ nasa_deep_space_network.html

[48] J.M. Porup. “It’s Surprisingly Simple To Hack A Satellite.” Motherboard. 2015. https://motherboard. vice.com/en_us/article/bmjq5a/its-surprisingly-simple-to-hack-a-satellite

[49] Zulfikar Abbany. “SpaceX’s Starlink satellite internet: It’s time for tough talk on cyber security in space.” Deutsche Welle. 2018. http://www.dw.com/en/spacexs-starlink-satellite-internet-its-timefor-tough-talk-on-cyber-security-in-space/a-42678704.

[50] Nir Kshetri,Chapter 3 - Amplifying the value of blockchain in supply chains: combining with other technologies, Editor(s): Nir Kshetri, Blockchain and Supply Chain Management, Elsevier, 2021, Pages 67-88, ISBN 9780323899345, https://doi.org/10.1016/B978-0-323-89934-5.00003-9.

[51] Zhang, Yan. (2024). Digital Twin: Architectures, Networks, and Applications. 10.1007/978-3-031-51819-5.

[52] Mohammed, Ishaq Azhar. (2017). Identity-based Encryption: From Identity and Access Management to Enterprise Privacy Management. SSRN Electronic Journal. 4. 719-722.

[53] Abdullah, Ako. (2017). Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data.

[54] Bhattarai, Pradip. (2020). Summary on Public Key Infrastructure (PKI). 10.13140/RG.2.2.34199.70562.

[55] Feng, Mengqing. (2019). Network Security Management and Implementation Based on ACL: Applications and Techniques in Cyber Security and Intelligence. 10.1007/978-3-319-98776-7_80.

[56] Alsafi, Hassen & Abduallah, Wafaa & Pathan, Al-Sakib. (2012). IDPS: An Integrated Intrusion Handling Model for Cloud.

[57] Spiceworks:What Is Intrusion Detection and Prevention System? Definition, Examples, Techniques, and Best Practices Accessed from:” https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-idps/”

[58] Aldwairi, Monther & Aldhanhani, Saoud. (2017). Multi-Factor Authentication System.

[59] Satapathy, Ashutosh & Livingston, Jenila. (2016). A Comprehensive Survey on SSL/ TLS and their Vulnerabilities. International Journal of Computer Applications. 153. 31-38. 10.5120/ijca2016912063.

[60] Molina, Elías & Jacob, Eduardo & Matías, Jon & Moreira, Naiara & Astarloa, Armando. (2015). Availability Improvement of Layer 2 Seamless Networks Using OpenFlow. The Scientific World Journal. 2015. 10.1155/2015/283165.

[61] Granadillo, Gustavo & González-Zarzosa, Susana & Diaz, Rodrigo. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors. 21. 4759. 10.3390/s21144759.

[62] Sedek, Khairul Anwar & Norlis, Osman & Osman, Mohd & Jusoff, Kamaruzaman. (2009). Developing a Secure Web Application Using OWASP Guidelines. Computer and Information Science. 2. 10.5539/cis.v2n4p137.

[63] Venter, Isabella & Blignaut, Renette & Renaud, Karen & Venter, M.. (2019). Cyber security education is as essential as “the three R's”. Heliyon. 5. e02855. 10.1016/j.heliyon.2019.e02855.

[64] Kadioglu, Serdar & Malitsky, Yuri & Sellmann, Meinolf & Tierney, Kevin. (2010). ISAC - Instance-Specific Algorithm Configuration. Frontiers in Artificial Intelligence and Applications. 215. 751-756. 10.3233/978-1-60750-606-5-751.

[65] Rodriguez, Roberto. (2011). The Space Program of the People's Republic of China.

[66] Adaev, Vadim. (2021). Concept Of Information Security Of The Russian Federation: Ways Of Implementation. 38-44. 10.15405/epsbs.2021.02.02.5.

[67]Kshetri, Nir. (2016). Cybersecurity in Russia:. 10.1007/978-3-319-40554-4_13.

[68] El Hassane, Laaji & Azizi, Abdelmalek & Ezzouak, Siham. (2020). Two Quantum Attack Algorithms Against NTRU When the Private Key and Plaintext Are Codified in Ternary Polynomials. 10.1007/978-3-030-36778-7_61.

[69] Zavorina, Lyubov & Selifanov, Valentin. (2019). Development of the system of protection of information of a significant object of critical infrastructure of the Russian Federation. Transaction of Scientific Papers of the Novosibirsk State Technical University. 123-131. 10.17212/2307-6879-2019-1-123-131.

[70] Pynnöniemi, Katri. (2018). Russia’s National Security Strategy: Analysis of Conceptual Evolution. The Journal of Slavic Military Studies. 31. 240-256. 10.1080/13518046.2018.1451091.

[71] Karasev, Oleg & Velikanova, Natalia & Edelkina, Anastasia. (2015). Russia: Space Exploration and Development Prospects. 10.1007/978-3-7091-1827-6_8.

[72] Joseph, Shawn. (2023). Leaflet- Know to guide of Data Protection Act 2018. 10.13140/RG.2.2.10319.66721/1.

[73] Piggin, Richard. (2018). Securing Critical Services - The Network and Information Systems (NIS) Directive. ITNOW. 60. 58-61. 10.1093/itnow/bwy057.

[74] Stevens, Tim. (2020). United Kingdom. 10.4324/9780429399718-17.

[75] HM Government. (2016). *National Cyber Security Strategy 2016-2021*. Retrieved from https://assets.publishing.service.gov.uk/media/5fbceaf08fa8f559e32b4cc1/6.6788_CO_National-Cyber-Security-Strategy-2016-2021_WEB3.pdf

[76]Vidmar, Matjaz & Rosiello, Alessandro & Golra, Owais. (2020). Resilience of New Space Firms in the United Kingdom during the Early Stages of COVID-19 Crisis: The Case for Strategic Agility. New Space. 8. 172-178. 10.1089/space.2020.0057.

[77] HM Government. (2021). *National Space Strategy*. Retrieved from https://www.gov.uk/government/publications/national-space-strategy

[78] Harrop, Wayne & Matteson, Ashley. (2015). Cyber Resilience: A Review of Critical National Infrastructure and Cyber-Security Protection Measures Applied in the UK and USA. 10.1057/9781137455550_10.

[79] Trump, D. J. (2017). *Space Policy Directive 1: Reinvigorating America's Human Space Exploration Program*. Retrieved from https://www.nasa.gov/press-release/trump-signs-space-policy-directive-1

[80] United States. Congress. (2018). *Cybersecurity and Infrastructure Security Agency Act of 2018*. Public Law 115-278, 132 Stat. 4168. Available at GovInfo: https://www.govinfo.gov/app/details/COMPS-15296

[81] **National Intelligence Authority. (1946). Presidential Directive on Coordination of Foreign Intelligence Activities. Established by President Harry S. Truman.** Retrieved from the American Presidency Project: American Presidency Project

[82] National Security Agency. (1952). *NSA/CSS: Defending Our Nation. Securing The Future*. Retrieved from NSA

[83] The White House. (2018). *National Cyber Strategy of the United States of America*. Retrieved from White House

[84] **Executive Office of the President. (2020). National Space Policy of the United States of America.** Retrieved from the Office of Space Commerce: National Space Policy.

[85] **Cybersecurity and Infrastructure Security Agency. (2020). Space Infrastructure Cyber Resilience Program.** Retrieved from CISA.

[86] United States Space Command. (2019). *United States Space Command Fact Sheet*. Retrieved from U.S. Space Command

[87] Shahin, Jamal. (2010). The International Telecommunication Union. *Wereldbeeld*. 34, 11-16.

[88] Almomani, Iman, Al-Banna, Eman, & AL-Akhras, Mousa. (2013). Logic-Based Security Architecture for Systems Providing Multihop Communication. *International Journal of Distributed Sensor Networks*. 2013. https://doi.org/10.1155/2013/768489.

[89] International Telecommunication Union. (n.d.). *Recommendation X.1121: Guidelines on the implementation of the secure application layer protocol*. https://www.itu.int/rec/T-REC-X.1121.

[90] Martinez, Peter. (2021). The UN COPUOS Guidelines for the Long-term Sustainability of Outer Space Activities. *Journal of Space Safety Engineering*. 8, 10. https://doi.org/10.1016/j.jsse.2021.02.003.

[91] Oellers-Frahm, Karin, & Zimmermann, Andreas. (2001). International Civil Aviation Organization (ICAO). *Encyclopedia of Public International Law*. https://doi.org/10.1007/978-3-642-56626-4_36.

[92] Turner, Barry. (2008). European Space Agency (ESA). *Encyclopedia of International Organizations*. https://doi.org/10.1007/978-1-349-74027-7_17.

[93]Japan Aerospace Exploration Agency (JAXA). (2024). In *Encyclopaedia Britannica*. Retrieved from https://www.britannica.com/topic/Japan-Aerospace-Exploration-Agency.

[94] Canadian Space Agency (CSA). (2024). In *Encyclopaedia Britannica*. Retrieved from https://www.britannica.com/topic/Canadian-Space-Agency.

[95] National Aeronautics and Space Administration (NASA). (2023). *NASA Science Policies and Reports*. Retrieved from https://www.nasa.gov/space-policy-history-documents/.

[96]Roscosmos. (2021). *Russia: From Space Programs to Space Strategy?*. SpaceNews. Retrieved from https://spacenews.com.

[97] China National Space Administration (CNSA). (2022). *China's Space Program: A 2021 Perspective*. Retrieved from https://www.cnsa.gov.cn/english/n6465652/n6465653/c6813100/content.html.

[98] UK Space Agency. (2021). *National Space Strategy*. Retrieved from https://www.gov.uk/government/publications/national-space-strategy.

[99] Ruttley, Tara & Robinson, Julie & Gerstenmaier, William. (2017). The International Space Station: Collaboration, Utilization, and Commercialization*: The International Space Station. Social Science Quarterly. 98. 1160-1174. 10.1111/ssqu.12469.

[100] Mauduit, J.. (2017). Collaboration around the International Space Station: science for diplomacy and its implication for US-Russia and China relations.

[101] yall, Francis. (2008). Exploring celestial bodies: Useful aspects of the Moon Agreement, 1979. 14. 9109-9114.

[102] Niles, Mark. (2002). On the Hijacking of Agencies (and Airplanes): The Federal Aviation Administration, "Agency Capture," and Airline Security.

[103] Lyall, Francis & Larsen, Paul. (2017). The Outer Space Treaty, 1967. 10.4324/9781315610139-3.

[104] Pace, Scott. (1996). Promoting Commercial Space Activity. 9.