



Gas & Oil Infrastructure Protection: Towards a Cyberthreat Landscape Report

George Stergiopoulos

University of the Aegean, Greece

February 2022



Gas & Oil Infrastructure Protection: Towards a Cyberthreat Landscape Report

Γιώργος Στεργιόπουλος, Επίκουρος Καθηγητής

Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων,
Πανεπιστήμιο Αιγαίου

Η εκπόνηση της παρουσίασης αυτής υποστηρίχθηκε από Προγραμματική Σύμβαση, μεταξύ Υπουργείου **Ψηφιακής Διακυβέρνησης** του **Οικονομικού Πανεπιστημίου Αθηνών**, για παροχή ερευνητικών υπηρεσιών στον τομέα της **Κυβερνοασφάλειας** (2021-22).



ΠΕΡΙΕΧΟΜΕΝΑ

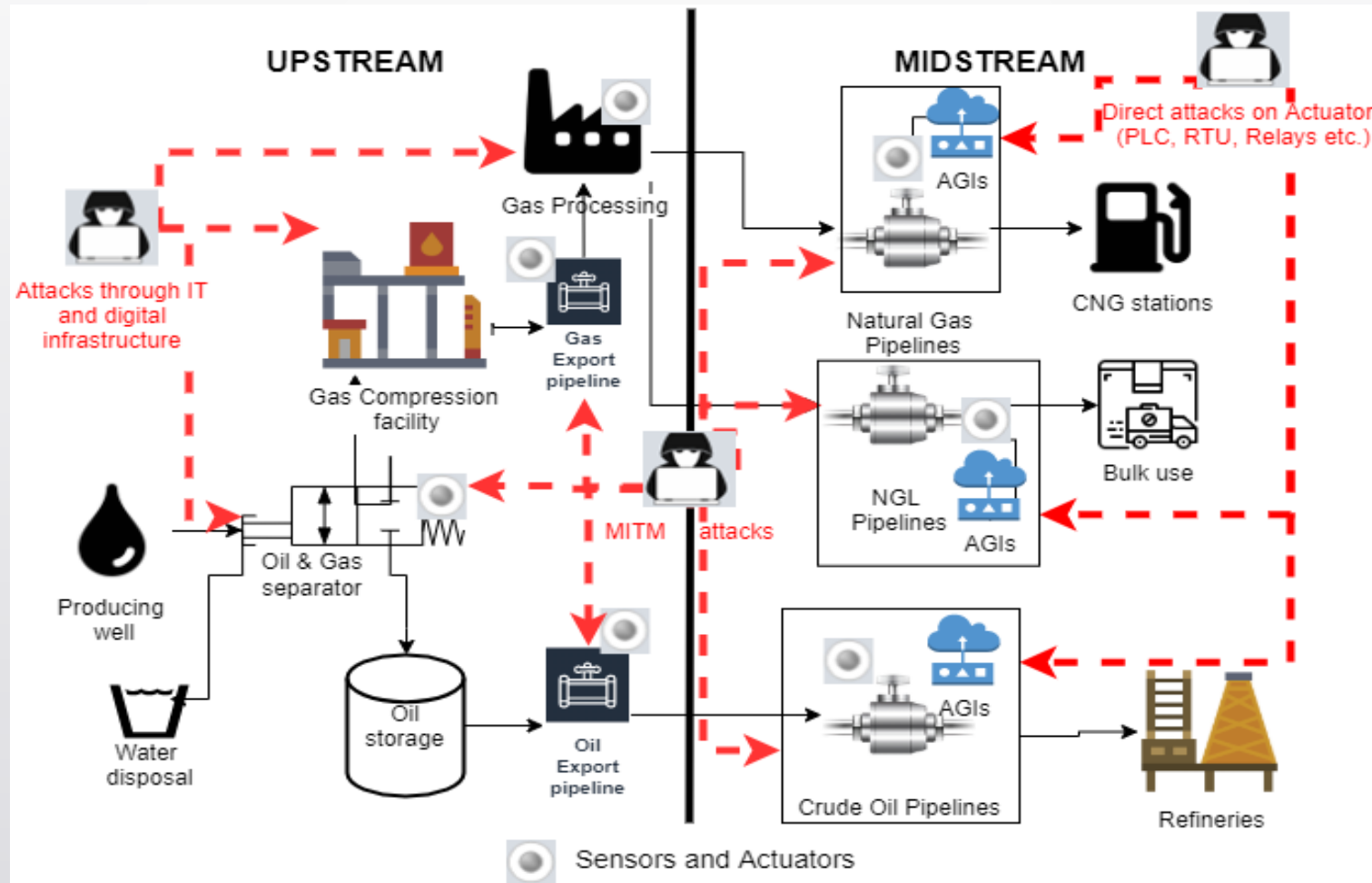
- Τυπικές αρχιτεκτονικές O&G
- Μέθοδος έρευνας
 - MITER ATT&CK και ταξονομίες απειλών
- Ανάλυση & αξιολόγηση κυβερνοεπιθέσεων
- Διδάγματα & Μετριάσμος κινδύνου
- Συμπεράσματα



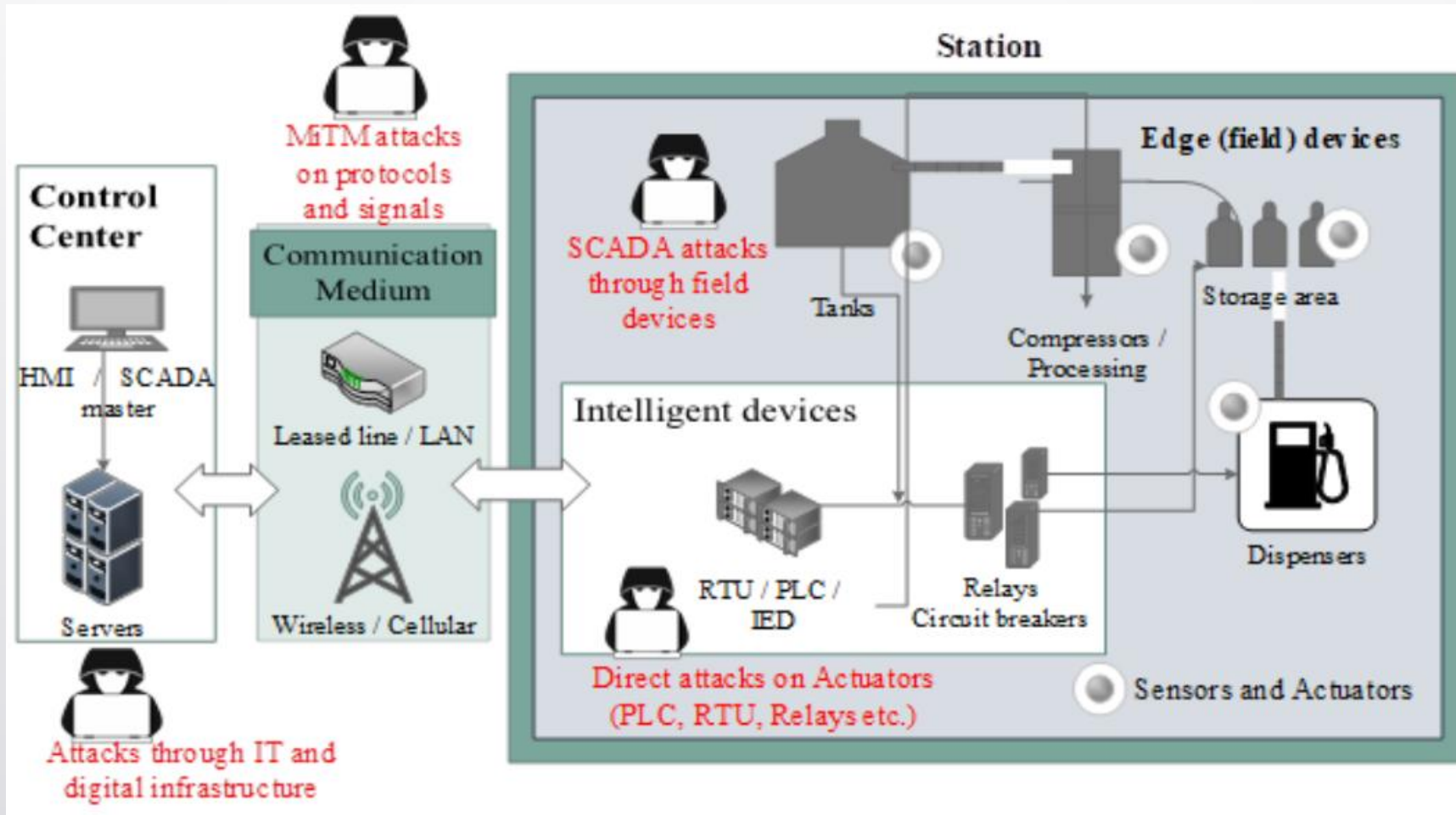
Τυπικές αρχιτεκτονικές O&G

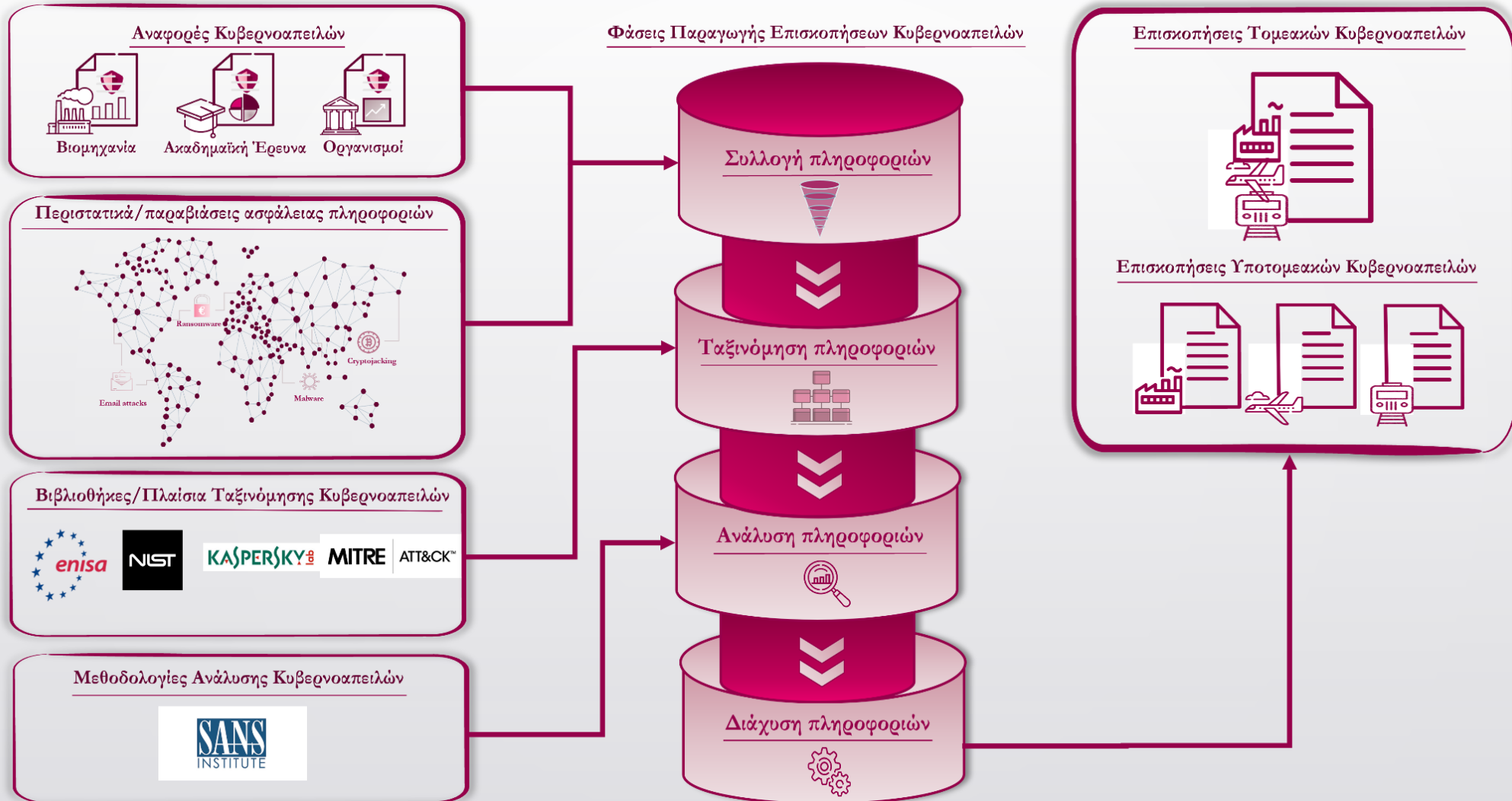
- Τομέας χωρίζεται σε Downstream, Midstream και Upstream
 - Όλα ακολουθούν την ίδια γενική αρχιτεκτονική ICS, παρόλο που η πολυπλοκότητα και τα στοιχεία διαφοροποιούνται.
- Οι υποδομές αναπτύσσουν συστήματα SCADA για παρόμοιους σκοπούς παρακολούθησης.
 - Οι διαδικασίες διαφέρουν και οι έλεγχοι ασφαλείας ποικίλλουν, αλλά
 - Αρχιτεκτονική (π.χ. PLC, RTU, ρελέ, κ.λπ.), συνδεσιμότητα (πρωτόκολλα, συσκευές δρομολόγησης, μέσα επικοινωνίας) και περιπτώσεις χρήσης (HMI, τύποι διακομιστών, κ.λπ.) σε μεγάλο βαθμό ίδιες.

Τυπικές αρχιτεκτονικές Ο&G



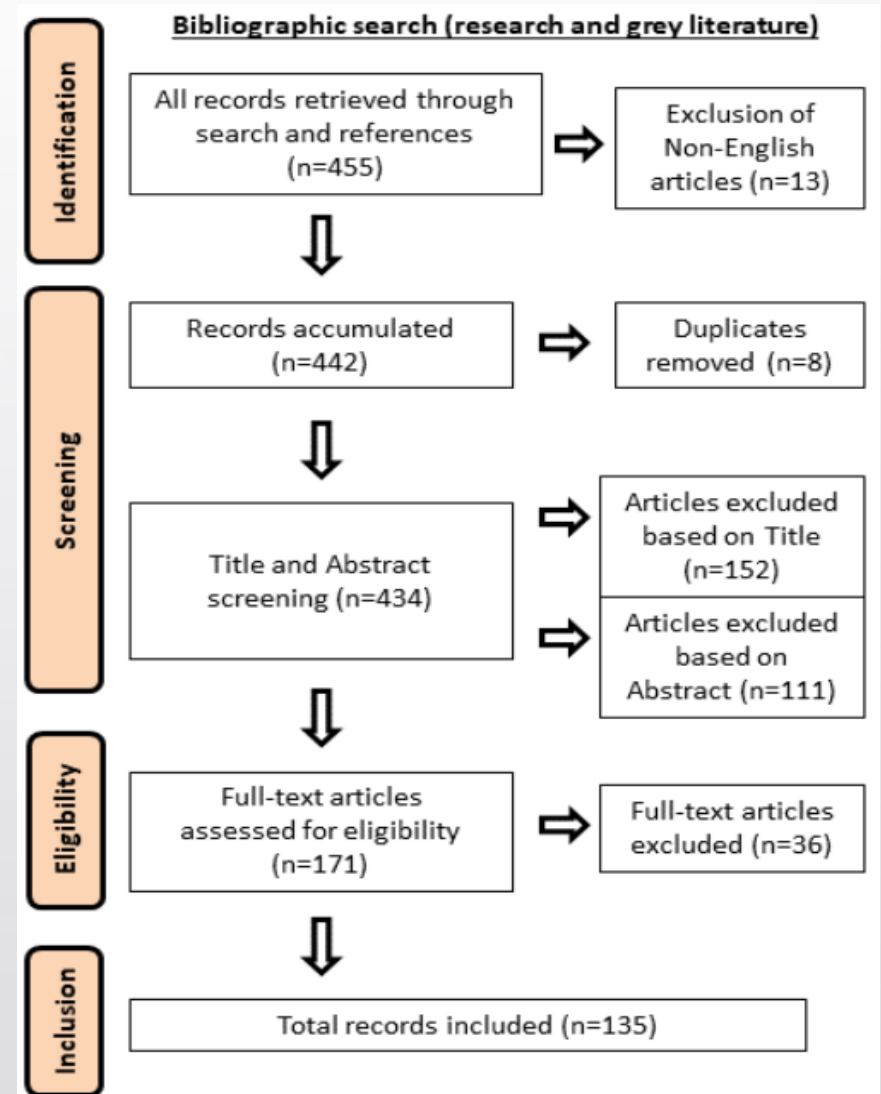
Τυπικές αρχιτεκτονικές Ο&Γ





ΣΥΛΛΟΓΗ ΔΕΔΟΜΕΝΩΝ

- Τέσσερα βήματα:
 - Έρευνα και ανάπτυξη πεδίου εφαρμογής
 - Προσδιορισμός αναφορών με βάση το εύρος
 - Ποιοτικός έλεγχος άρθρων, βάσεις δεδομένων απειλών, ειδήσεις.
 - Αναφορά (εξαγωγή πληροφοριών, ανάλυση και απεικόνιση τάσεων).
- Εγγραφα και δημοσιεύματα (455 στοιχεία) τόσο από την ακαδημαϊκή κοινότητα όσο και από τη γκρίζα λογοτεχνία
- Πληροφορίες μοντελοποιημένες με χρήση **MITRE ATT&CK**





MITRE ATT&CK FRAMEWORK

- Γνωσιακή βάση τακτικών & τεχνικών αντιπάλου βασισμένη σε πραγματικές παρατηρήσεις.
 - Ενότητα τριών επιπέδων για ενέργειες αντιπάλου κατά τη λειτουργία εντός δικτύου ICS.
- Χρησιμοποιείται για την ανάπτυξη μοντέλων και μεθοδολογιών απειλών.
- Κωδικοποιεί 81 τύπους τεχνικών για 11 τακτικές επίθεσης, από την αρχική εκμετάλλευση και εκτέλεση έως τις πλευρικές κινήσεις και την πιθανή πρόσκρουση.

Loss of Availability	Impact	Adversaries may attempt to disrupt essential components or systems to prevent owner and operator from delivering products or services. ^{[6][7][8]} Adversaries may leverage malware to delete or encrypt critical data on HMIs, workstations, or databases.
Loss of Control	Impact	Adversaries may seek to achieve a sustained loss of control or a runaway condition in which operators cannot issue any commands even if the malicious interference has subsided. ^{[6][7][8]}

ΤΑΞΟΝΟΜΙΑ ΠΙΘΑΝΩΝ ΕΠΙΘΕΣΕΩΝ

- Το MITER ATT&CK χρησιμοποιείται για την ταξινόμηση περιστατικών
- Περιστατικά που επισημαίνονται με χρήση τεχνικών που περιγράφονται στο ATT&CK.
- Χαρτογράφηση τύπων επίθεσης, τακτικές και τεχνικές από ATT&CK
- Βοηθά στον εντοπισμό κρίσιμων στοιχείων και τάσεων ανά τύπο επίθεσης.

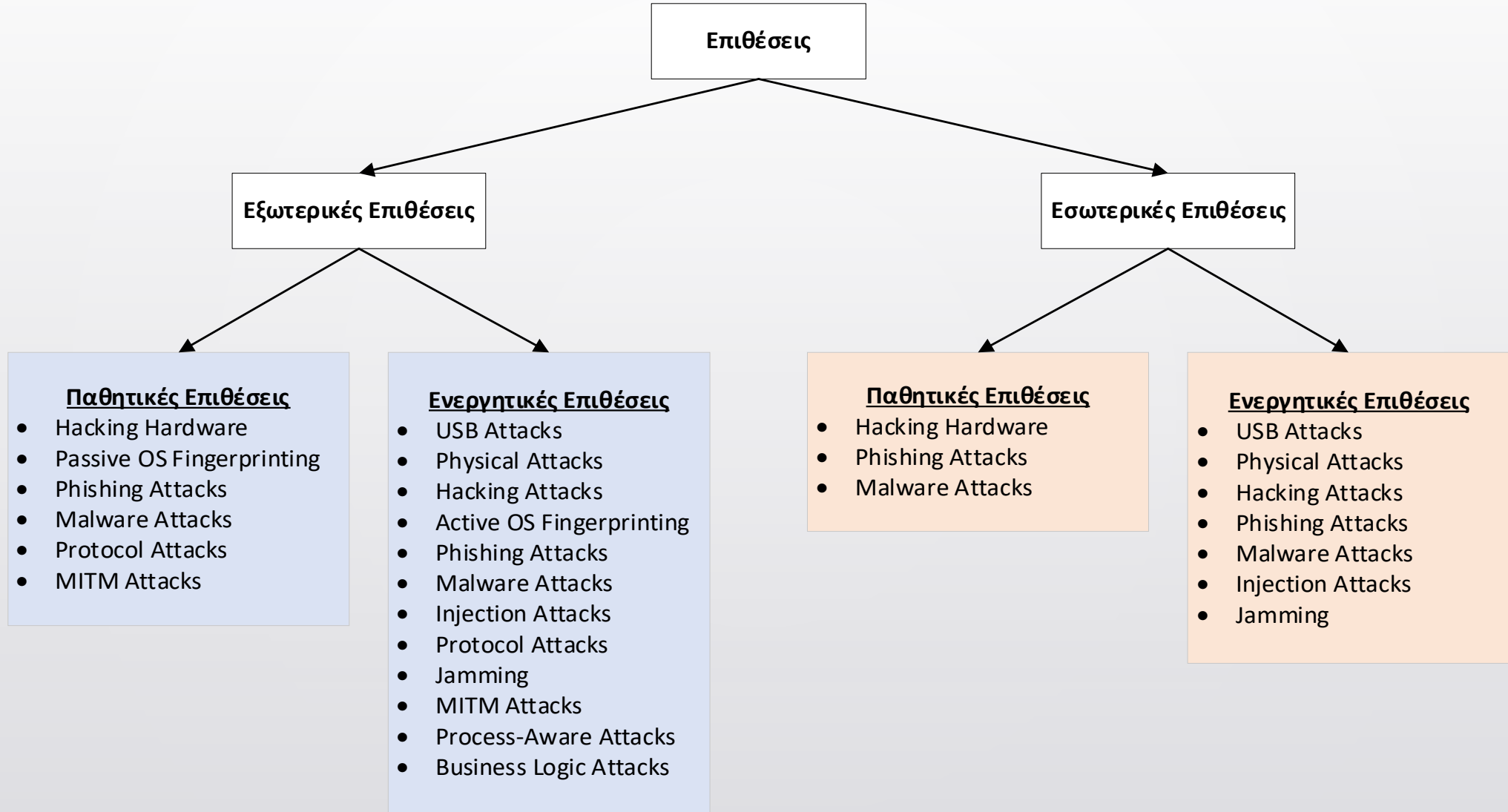
TABLE 6. Taxonomy of potential O&G attacks with ATT&CK Reference ID.

Vulnerability type	ATT&CK Tactic ID	Description
Hardware Layer		
Lack of tamper resistance	T858 - Utilize/Change Operating Mode T848 - Rogue Master Device	Field devices often do not implement hardware security controls that can detect or prevent physical tampering attacks (e.g. key extraction attacks) [81], both in midstream and downstream O&G infrastructures.
Lack of physical security	T825 - Location Identification T801 - Monitor Process State	Physically altering/attacking industrial systems without fail -safe or monitoring mechanisms can lead to leakage affecting nearby communities [41]-[43].
Use of legacy devices & equipment	T858 - Utilize/Change Operating Mode T801 - Monitor Process State T833 - Modify Control Logic	Legacy field devices, PLC and sensors remain active for extended periods, even though they have known vulnerabilities.
Unknown / untrusted Off-The-Shelf devices	T862 - Supply Chain Compromise T811 - Data from Information Repositories	Removable devices are potential attack vectors that can be overlooked by users. COTS components (not custom-made) provide stability, availability and reduce cost but, at the same time, may introduce unknown vulnerabilities, both in mid and downstream ICS.
Firmware Layer		
Outdated OS	T851 – Rootkit T800 - Activate Firmware Update Mode	Unpatched operating systems are a common vulnerability both for ICS and IT systems [12]. Reports consider the lack of OS patching along with software patching as one of the top ICS vulnerabilities since 2016 [18]. This applies to the O&G sector too.
Lack of firmware protection	T839 - Module Firmware T857 - System Firmware T800 - Activate Firmware Update Mode T851 - Rootkit	Facility and ICS are known to lack security measures against firmware modification [45], mostly due to cost cutting this is not happening [7]-[9],[23].



Παραδείγματα

- Επτά (7) τεκμηριωμένα συμβάντα ασφάλειας ICS σε δίκτυα αγωγών (midstream).
 - AGI προταρχικός στόχος.
 - Παράδειγμα 1: Η επίθεση στην Μπακού-Τιφλίδα προκάλεσε προσωρινή διακοπή στη μεταφορά αγωγών με χρήση υπερπίεσης, εικάζεται πως η απειλή εισήλθε μέσω του δικτύου κάμερας.
 - Παράδειγμα 2: Μη επεξεργασμένες εντολές προκάλεσαν έναν ατελείωτο βρόχο να ενεργοποιήσει και να διακόψει τους ελέγχους σε όλους τους τελεστές ροής
- Downstream εγκαταστάσεις ο πιο συνηθισμένος στόχος.
- Το SHAMOON στόχευσε εθνικές εταιρείες πετρελαίου, συμπεριλαμβανομένης της Saudi Aramco της Σαουδικής Αραβίας και της RasGas του Κατάρ, μέσω spear phishing.
- Η επίθεση του Night Dragon προκάλεσε κλοπή δεδομένων και επηρέασε τις downstream υποδομές εταιρειών πετρελαίου, ενέργειας και πετροχημικών σε όλο τον κόσμο.



Χαρακτηριστικό Ανάλυσης	Στατιστικά Αποτελέσματα
Συχνότερα είδη επιθέσεων	<input type="checkbox"/> Εξωτερικές επιθέσεις με χρήση malware (9 συμβάντα) <input type="checkbox"/> Εξωτερικές επιθέσεις τύπου phishing (8 συμβάντα) <input type="checkbox"/> Εσωτερικές επιθέσεις τύπου Injection (6 συμβάντα)
Τομέας υποδομών πετρελαίου ή φυσικού αερίου που επηρεάστηκε	<input type="checkbox"/> Upstream (15 συμβάντα) <input type="checkbox"/> Midstream (13 συμβάντα) <input type="checkbox"/> Downstream (14 συμβάντα)
Πιο συχνά σενάρια επιθέσεων	<input type="checkbox"/> C-C (16 συμβάντα) <input type="checkbox"/> C-P (20 συμβάντα)
Πιο συχνές τεχνικές MITRE ATT&CK	<input type="checkbox"/> Internet Accessible Device (T883)(12 συμβάντα) <input type="checkbox"/> User Execution (T863) (10 συμβάντα) <input type="checkbox"/> Spear phishing (T865) (9 συμβάντα) <input type="checkbox"/> Removable Media (T847) (5 συμβάντα)
Πιο συχνοί τύποι επιπτώσεων MITRE ATT&CK	<input type="checkbox"/> Modify Control Logic (T833) / state(T875) (10 συμβάντα) <input type="checkbox"/> DoS (T814) / Availability Loss (T826) (14 συμβάντα) <input type="checkbox"/> Damage to Property (T879) (9 συμβάντα) <input type="checkbox"/> Information theft (T882) (13 συμβάντα)



Συμπεράσματα

- Σαφής ένδειξη ότι οι τρέχουσες επιθέσεις σε συστήματα πετρελαίου και φυσικού αερίου ακολουθούν παρόμοιες τάσεις επίθεσης με τα κοινά ΠΣ στις ΤΠΕ.
- Τα threat landscapes αναδεικνύονται ως μια χρονικά επαναλαμβανόμενη ανάγκη για την χαρτογράφηση των trends και των ζημιών στο O&G.
- Οι πιο συνηθισμένοι φορείς επίθεσης περιλαμβάνουν:
 - spear phishing μέσω email
 - εξωτερική επίθεση (κακόβουλο λογισμικό ή έγχυση) σε εκτεθειμένες συσκευές
 - λάθη χρήστη, είτε σκόπιμα (κακόβουλοι μυστικοί) είτε εσφαλμένα



References

1. Dedousis P., Stergiopoulos G., Arampatzis P., Gritzalis D., "A security-aware framework for designing industrial engineering processes", *IEEE Access*, Vol. 9, pp. 163065-85, December 2021.
2. Dimitriadis A., Prassas C., Flores J.-L., Kulvatunyou B., Ivezic N., Gritzalis D., Mavridis I., "Contextualized filtering for shared cyber threat information", *Sensors*, Vol. 14 (4890), July 2021.
3. Gritzalis D., Iseppi G., Mylonas A., Stavrou V., "Exiting the risk assessment maze: A meta-survey", *ACM Computing Surveys*, Vol. 51, No. 1, pp. 1-30, January 2018.
4. Kotzanikolaou P., Theoharidou M., Gritzalis D., "Cascading effects of common-cause failures on Critical Infrastructures, in *Proc. of the 7th IFIP International Conference on Critical Infrastructure Protection*, pp. 171-182, Springer (AICT 417), USA, 2013.
5. Lykou G., Moustakas D., Gritzalis D., "Defending airports from UAS: A survey on cyber-attacks and counter-drone sensors technologies", *Sensors*, Vol. 20 (3537), June 2020.
6. Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Lykou G., Gritzalis D., "Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures", *International Journal of Critical Infrastructure Protection*, Vol. 12, pp. 46-60, 2016.
7. Stergiopoulos G., Dedousis P., Gritzalis D., "Automatic analysis of attack graphs for risk mitigation and prioritization on large-scale and complex networks in Industry 4.0", *International Journal of Information Security*, February 2021.
8. Stergiopoulos G., Gritzalis D., Limnaios E., "Cyber-attacks on the Oil & Gas sector: A survey on incident assessment and attack patterns", *IEEE Access*, Vol. 8, pp. 128440-75, July 2020.