Neapolis University

HEPHAESTUS Repository **http://hephaestus.nup.ac.cy**

Department of History, Politics and International Studies MSc in International Relations,Strategy and Security

2022

þÿ Ÿ š Å ² µ Á ½ ¿ À Ì » µ ¼ ¿ Â É Â
þÿ À ¿ » » ± À » ± Ã ¹ ± Ã Ä ® Â ¹ Ã Ç Í ¿ Â

þÿ š ± » ¿ ´ ¬ ½ · Â , š É ½ Ã Ä ± ½ Ä ¯ ½ ¿ Â

þÿ Á Ì ³ Á ± ¼ ¼ ± " ¹ µ ¸ ½ Î ½ £ Ç - Ã µ É ½ , £ Ä Á ± Ä · ³ ¹ º ® Â º ± ¹ ' Ã Æ ¬ » µ ¹ ± Â , £ Ç ¿ » ® • À ¹ Ã Ä
þÿ ± ½ µ À ¹ Ã Ä ® ¼ ¹ ¿ • µ ¬ À ¿ » ¹ Â ¬ Æ ¿ Å

http://hdl.handle.net/11728/12207

Downloaded from HEPHAESTUS Repository, Neapolis University institutional repository

ΙΑΝΟΥΑΡΙΟΣ 2022

ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ, ΤΕΧΝΩΝ ΚΑΙ ΑΝΘΡΩΠΙΣΤΙΚΩΝ ΣΠΟΥΔΩΝ

Ο Κυβερνοπόλεμος ως πολλαπλασιαστής ισχύος

ΚΑΛΟΔΑΝΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΙΑΝΟΥΑΡΙΟΣ 2022

Confidential

Πανεπιστήμιο Νεάπολις Πάφου

ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ, ΤΕΧΝΩΝ ΚΑΙ ΑΝΘΡΩΠΙΣΤΙΚΩΝ ΣΠΟΥΔΩΝ

Ο Κυβερνοπόλεμος ως πολλαπλασιαστής ισχύος

Διατριβή η οποία υποβλήθηκε προς απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου σπουδών στις Διεθνείς Σχέσεις, Στρατηγική και Ασφάλεια στο Πανεπιστήμιο Νεάπολις

ΚΑΛΟΔΑΝΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΙΑΝΟΥΑΡΙΟΣ 2022

Confidential

Πνευματικά δικαιώματα

Copyright © **Κωνσταντίνος Καλοδάνης, 2022**

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Η έγκριση της διατριβής από το Πανεπιστημίου Νεάπολις δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Πανεπιστημίου.

Περιεχόμενα

ΑΚΡΩΝΥΜΙΑ 8

Κεφάλαιο 1 – Εισαγωγή 12

1.1 Εισαγωγή 12

1.2 Σκοπός 14

Κεφάλαιο 2 - Θεωρητική Θεμελίωση / Βιβλιογραφική Ανασκόπηση 15

2.1 Βιβλιογραφική Ανασκόπηση 16

Κεφάλαιο 3 - Μεθοδολογία Έρευνας 17

Κεφάλαιο 4 - Παρουσίαση δεδομένων 20

4.1 Κυβερνοχώρος 20

4.2 Κυβερνοπόλεμος 21

4.3 Κυβερνοασφάλεια 24

4.4 Κυβερνοεπιθέσεις 25

4.4.1. Παραδείγματα Κυβερνοεπιθέσεων 25

4.4.2 Τύποι κυβερνοεπιθέσεων 34

4.5 Υβριδικός Πόλεμος 38

4.6 Κυβερνοαποτροπή & Κυβερνοαντοχή 42

4.7 Ο κυβερνοπόλεμος ως σύγχρονη μορφή πολέμου 45

4.8 Κρατικοί δρώντες 46

4.8.1 ΗΠΑ 48

4.8.2 Ρωσία 50

4.8.3 Κίνα 52

4.8.4 Ιράν 53

4.8.5 Τουρκία 54

4.9 Μη κρατικοί δρώντες 55

4.9.1 Απλοί άνθρωποι/Θύματα 56

4.9.2 Χάκερς – Script Kiddies 57

4.9.3 Χάκερς/Ακτιβίστες 58

4.9.4 Χάκερς – Πατριώτες 59

4.9.5 Κυβερνοτρομοκράτες 59

4.9.6 Οργανωμένο κυβερνοέγκλημα 60

4.9.7 Κυβερνοπολιτοφύλακες 60

Κεφάλαιο 5 - Συζήτηση και Σχολιασμός Αποτελεσμάτων 61

5.1 Κατάσταση στην ΕΕ 61

5.2 Ελλάδα 63
5.3 Στρατηγικοί στόχοι αντιμετώπισης κυβερνοπολέμου – Περίπτωση Ελλάδας 66
5.3.1 Προστασία και αντοχή των κρίσιμων υποδομών 67
5.3.2 Ανάπτυξη εθνικής κυβερνοβάσης 69
5.3.3 Δίκτυο κυβερνοασφάλειας & κουλτούρα επιχειρησιακής κυβερνοασφάλειας 72
5.3.4 Ασφάλεια τεχνολογιών νέας γενιάς 73
5.3.5 Αντιμετώπιση των εγκλημάτων στον κυβερνοχώρο 74
5.3.6 Ανάπτυξη διεθνούς συνεργασίας 74
Συμπεράσματα 75
Βιβλιογραφία 79
ΗΛΕΚΤΡΟΝΙΚΕΣ ΠΗΓΕΣ 81

Κατάλογος Γραφικών Παραστάσεων/Εικόνων/Διαγραμμάτων

Εικόνα 1 25
Εικόνα 2 33
Εικόνα 3 39
Εικόνα 4 57

Ονοματεπώνυμο Φοιτητή: Καλοδάνης Κωνσταντίνος

Τίτλος Μεταπτυχιακής Διατριβής: Ο Κυβερνοπόλεμος ως πολλαπλασιαστής ισχύος

Η παρούσα Μεταπτυχιακή Διατριβή εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολις και εγκρίθηκε στις …… από τα μέλη της Εξεταστικής Επιτροπής.

Εξεταστική Επιτροπή:

Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολις Πάφος) Σπυρίδων Πλακούδας

Μέλος Εξεταστικής Επιτροπής: Σάββας Χατζηχριστοφής

Μέλος Εξεταστικής Επιτροπής: Μερσίλεια Αναστασιάδου

Θα ήθελα να εκφράσω τις θερμές ευχαριστίες στον επιβλέποντα καθηγητή μου κ. Πλακούδα Σπυρίδων, για την καθοδήγηση και τη συνδρομή του.

Η παρούσα διπλωματική εργασία αφιερώνεται στα παιδιά και τη σύζυγό μου για την υποστήριξή τους και την υπομονή που έκαναν όλο το προηγούμενο διάστημα.

ΑΚΡΩΝΥΜΙΑ

AI	Artificial Intelligence
APT	Advanced Persistent Threat
ATM	Automated Teller Machine
BBC	British Broadcasting Corporation
CSIRT	Computer Security Incident Response Team
DESC	Dubai Electronic Security Center
DDOS	Distributed Denial of Service
DoD	Department of Defense
DOS	Denial of Service
ECCC	European Cybersecurity Competence Centre
FBI	Federal Bureau of Investigation
FSB	Federal'naya Sluzhba Bezopastnosti
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GRU	Glavnoye Razvedyvatelnoye Upravlenie
ICTA	Information and Communication Technologies Authority
INFOSEC	Information Security
IoT	Internet of Things
LAN	Local Area Network
MIT	Millî İstihbarat Teşkilatı
MVD	Министерство внутренних дел
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PACAC	Public Administration and Constitutional Affairs Committee
PLC	Programmable Logic Controller
RMA	Revolution in Military Affairs
SCADA	Supervisory control and data acquisition
SOC	Security Operations Center
SORM	Система оперативно-разыскных мероприятий
SSRN	Social Science Research Network
TAO	Tailored Access Operations

TGS	Turkish Ground Services
UAV	Unmanned Aerial Vehicle
USAF	United States Air Force
USCYBERCOM	United States Cyber Command
WAN	Wide Area Network
Γ.Ε.ΕΘ.Α.	Γενικό Επιτελείο Εθνικής Άμυνας
Ε.Δ.	Ένοπλες Δυνάμεις
Ε.Ε	Ευρωπαϊκή Ένωση
ΕΕΤΤ	Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
Ε.Υ.Π.	Εθνική Υπηρεσία Πληροφοριών
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
Η/Υ	Ηλεκτρονικός Υπολογιστής
ΜΜΕ	Μέσα Μαζικής Ενημέρωσης
ΤΠΕ	Τεχνολογίες Πληροφοριών και Επικοινωνιών
ΦΕΒΥ	Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών

Περίληψη

Το διαδίκτυο παρουσιάζει τα τελευταία χρόνια εξαιρετική ανάπτυξη και πολλές ευαίσθητες πληροφορίες διακινούνται μέσα από αυτό. Η ανοιχτή φύση του διαδικτύου είναι ο λόγος της ευελιξίας του, αλλά ίσως και η αιτία των σπουδαιότερων αδυναμιών του που επιτρέπει την κακόβουλη εκμετάλλευσή του από ικανούς χρήστες.

Στη σημερινή εποχή της ψηφιακής τεχνολογίας, η κυβερνοασφάλεια έχει ανέβει στην κορυφή της λίστας προτεραιοτήτων για σχεδόν κάθε οργανισμό. Πώς να διαφυλάξουν την ακεραιότητα των δεδομένων τους, πώς να προστατεύσουν τους χρήστες και τους πελάτες, αλλά και πώς να προστατεύσουν τη φήμη τους. Ο ψηφιακός πόλεμος, είτε μεταξύ εταιρειών, ατόμων ή κυβερνήσεων, είναι ο νέος τρόπος μάχης στη σύγχρονη εποχή. Είναι κρίσιμο για όλους τους οργανισμούς, μεγάλους και μικρούς, να μπορούν να προστατεύουν τα δεδομένα τους διασφαλίζοντας παράλληλα την ομαλή και συνεχή λειτουργία των συστημάτων πληροφορικής τους.

Δεδομένου ότι οι τεχνολογικές εξελίξεις καθορίζουν, σε μεγάλο βαθμό, το χαρακτήρα του πολέμου κάθε εποχής, σήμερα η «επανάσταση στην πληροφορία» οδηγεί πλέον σε μία εποχή «πολέμου πληροφοριών» ο οποίος εκδηλώνεται σε πολλά επίπεδα και ένα από αυτά είναι ο κυβερνοπόλεμος. Στην περίπτωση του κυβερνοπολέμου το πλεονέκτημα δε βρίσκεται πλέον στη μάζα ούτε στην κινητικότητα, αλλά στην κατοχή και κατάλληλη αξιοποίηση των πληροφοριών, σε σχέση πάντα με τον αντίπαλο, καθώς και στη γενικότερη εκμετάλλευση του διαδικτύου και της δυνατότητας πρόσβασης σε αυτό από οποιονδήποτε.

Ο κυβερνοπόλεμος είναι ένας πολλαπλασιαστής ισχύος, ένα όπλο χαμηλού κόστους με υψηλά αποτελέσματα, στον οποίο η εφευρετικότητα και η πρωτοτυπία διαδραματίζουν βασικό ρόλο και αποτελούν σημαντική ασύμμετρη απειλή για την εθνική ασφάλεια και ευημερία των κρατών.

Abstract

The internet has grown tremendously in recent years and a lot of sensitive information is circulating through it. The open nature of the internet is the reason for its flexibility, but also perhaps the cause of its major weaknesses that allow it to be maliciously exploited by capable users.

In today's age of digital technology, cybersecurity has risen to the top of the list of priorities for almost every organization. How to preserve the integrity of their data, how to protect users and customers, but also how to protect their reputation. Digital warfare, whether between companies, individuals or governments, is the new way of fighting in modern times. It is crucial for all organizations, large and small, to be able to protect their data while ensuring the smooth and continuous operation of their computer systems.

As technological developments largely determine the nature of war in every age, today the "information revolution" is now leading to an era of "information warfare" which manifests itself on many levels and one of them is cyber warfare. In the case of cyber warfare, the advantage is no longer in mass or mobility, but in the possession and proper use of information, always in relation to the adversary, as well as in the general exploitation of the internet and the possibility of access to it by anyone.

Cyberwarfare is a power multiplier, a low-cost weapon with high-results, in which ingenuity and originality play a key role and pose a significant asymmetric threat to states' national security and prosperity.