

2024-05

þÿ ‘ Ã Æ ± » μ<sup>1</sup> ¿ À ¿<sup>-</sup> · Ã · Ä ¿ Å<sup>0</sup> Å<sup>2</sup> μ Á ½ ¿  
þÿ Ã Ä ¿ À » ±<sup>-</sup> Ã<sup>1</sup> ¿ Ä · Â ••: μ Í Á ¿ Â  
þÿ À ¿ »<sup>1</sup> Ä<sup>1</sup> 0<sup>1</sup> ½, ± À ¿ Ä μ » μ Ã ¼ ± Ä<sup>1</sup> 0<sup>1</sup> Ì Ä  
þÿ ‘ Å ½ ± Ä Ì Ä · Ä μ Â<sup>2</sup> μ » Ä<sup>-</sup> É Ã · Â

þÿ £ Ä ± Å Á ±<sup>0</sup> ¿ À ¿ Í » ¿ Å, ¡É Ä μ<sup>1</sup> ½ ®

þÿ œ μ Ä ± Ä Ä Å Ç<sup>1</sup> ±<sup>0</sup> Ì Á<sup>3</sup> Á ± ¼ ¼ ± ”<sup>1</sup> μ, ½<sup>1</sup> ½<sup>1</sup> £ Ç - Ä μ É ½, £ Ä Á ± Ä ·<sup>3</sup> 1<sup>0</sup> ® Ä<sup>0</sup> ±<sup>1</sup> ‘ Ã Æ ¬ » μ<sup>1</sup> ±<sup>1</sup> /  
þÿ š ¿<sup>1</sup> ½<sup>1</sup> É ½<sup>1</sup> 0<sup>1</sup> ½ · Ä<sup>1</sup> Ä Ä · ¼<sup>1</sup> ½, ¢ μ Ç ½<sup>1</sup> ½<sup>1</sup> 0 ±<sup>1</sup> ‘ ½, Á É À<sup>1</sup> Ä Ä<sup>1</sup> 0<sup>1</sup> ½<sup>1</sup> £ À ¿ Á<sup>1</sup> ½, ± ½ μ Ä<sup>1</sup> Ä Ä ®

---

<http://hdl.handle.net/11728/12606>

Downloaded from HEPHAESTUS Repository, Neapolis University institutional repository



**ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ, ΤΕΧΝΩΝ  
ΚΑΙ  
ΑΝΘΡΩΠΙΣΤΙΚΩΝ ΣΠΟΥΔΩΝ**

**Ασφαλειοποίηση του κυβερνοχώρου στο πλαίσιο της  
ΕΕ: εύρος πολιτικών, αποτελεσματικότητα,  
δυνατότητες βελτίωσης**

**ΦΩΤΕΙΝΗ ΣΤΑΥΡΑΚΟΠΟΥΛΟΥ**

**ΜΑΙΟΣ 2024**



**ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ, ΤΕΧΝΩΝ  
ΚΑΙ  
ΑΝΘΡΩΠΙΣΤΙΚΩΝ ΣΠΟΥΔΩΝ**

**Ασφαλειοποίηση του κυβερνοχώρου στο πλαίσιο της  
ΕΕ: εύρος πολιτικών, αποτελεσματικότητα,  
δυνατότητες βελτίωσης**

**Διπλωματική Εργασία η οποία υποβλήθηκε προς απόκτηση  
Μεταπτυχιακού τίτλου σπουδών στις Διεθνείς Σχέσεις,  
Στρατηγική και Ασφάλεια στο Πανεπιστήμιο Νεάπολις Πάφος.**

**ΦΩΤΕΙΝΗ ΣΤΑΥΡΑΚΟΠΟΥΛΟΥ**

**ΜΑΙΟΣ 2024**

## **Πνευματικά δικαιώματα**

Copyright © **Φωτεινή Σταυρακοπούλου, 2024**

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Η έγκριση της Διπλωματικής Εργασίας από το Πανεπιστημίου Νεάπολις δεν υποδηλώνει απαραίτητως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Πανεπιστημίου.

**Όνοματεπώνυμο Φοιτητή/Φοιτήτριας:** Φωτεινή Σταυρακοπούλου

**Τίτλος Διπλωματικής Εργασίας:** «Ασφαλειοποίηση του κυβερνοχώρου στο πλαίσιο της ΕΕ: εύρος πολιτικών, αποτελεσματικότητα, δυνατότητες βελτίωσης».

Η παρούσα Διπλωματική Εργασία εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολης και εγκρίθηκε στις 10 Ιουνίου 2024 από τα μέλη της Εξεταστικής Επιτροπής.

**Εξεταστική Επιτροπή:**

Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολης Πάφος): Ιωάννης Γαλαριώτης

Μέλος Εξεταστικής Επιτροπής: Μάριος Ευθυμίουπουλος

Μέλος Εξεταστικής Επιτροπής: Μάριος Ευρυβιάδης

**ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ**

Η Φωτεινή Σταυρακοπούλου, γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα ότι η παρούσα εργασία με τίτλο «Ασφαλειοποίηση του κυβερνοχώρου στο πλαίσιο της ΕΕ: εύρος πολιτικών, αποτελεσματικότητα, δυνατότητες βελτίωσης», αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές που έχω χρησιμοποιήσει, έχουν δηλωθεί κατάλληλα στις βιβλιογραφικές παραπομπές και αναφορές. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Η Δηλούσα

# Περιεχόμενα

<b>ΠΕΡΙΛΗΨΗ.....</b>	<b>6</b>
<b>ABSTRACT .....</b>	<b>7</b>
<b>ΕΙΣΑΓΩΓΗ .....</b>	<b>8</b>
Γενικό πλαίσιο.....	3
Σκοπός εργασίας και μεθοδολογία.....	3
<b>1. ΘΕΩΡΗΤΙΚΟ ΠΛΑΙΣΙΟ.....</b>	<b>11</b>
<b>1.1 Βασικές έννοιες .....</b>	<b>11</b>
1.1.1 Ο κυβερνοχώρος.....	11
1.1.2 Η κυβερνοασφάλεια .....	12
1.1.3 Η ασφαλειοποίηση .....	15
<b>2 ΕΥΡΩΠΑΙΚΟ ΠΛΑΙΣΙΟ ΚΑΙ ΠΟΛΙΤΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ.....</b>	<b>16</b>
<b>2.1 Σχέση κυβερνοασφάλειας και ασφαλειοποίησης σε ευρωπαϊκό επίπεδο.....</b>	<b>16</b>
<b>2.2 Ιστορική εξέλιξη κυβερνοασφάλειας στην Ευρωπαϊκή Ένωση .....</b>	<b>19</b>
<b>2.3 Ευρωπαϊκή Στρατηγική για την Κυβερνοασφάλεια .....</b>	<b>21</b>
<b>2.4 Νομοθεσίες και Όργανα εντός Ευρωπαϊκής Ένωσης.....</b>	<b>21</b>
2.4.1 Γενικός Κανονισμός για την Προστασία Δεδομένων .....	22
2.4.2 Οδηγία για την Ασφάλεια Δικτύων και Πληροφοριών (NIS Directive) .....	22
<b>2.5 Οργανισμοί αντιμετώπισης κινδύνων κυβερνοασφάλειας.....</b>	<b>23</b>
2.5.1 Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) .....	23
2.5.2 Ευρωπαϊκή Αρχή Προστασίας Δεδομένων (EDPS) .....	24
2.5.3 EUROPOL .....	25
<b>2.6 Συνεργασία Κρατών Μελών σε Θέματα Κυβερνοασφάλειας.....</b>	<b>26</b>
<b>2.7 Σύγκριση πολιτικών άλλων οργανισμών-χωρών με την ΕΕ .....</b>	<b>26</b>
<b>3 ΠΡΟΚΛΗΣΕΙΣ - ΑΠΕΙΛΕΣ .....</b>	<b>30</b>
<b>3.1 Κυβερνοεγκλήματα.....</b>	<b>30</b>
<b>3.2 Επιθέσεις ενάντια σε Κρίσιμες Υποδομές.....</b>	<b>31</b>
<b>3.3 Παραβίαση εταιρικής ασφάλειας.....</b>	<b>31</b>
<b>3.4 Διαδικτυακή απάτη .....</b>	<b>32</b>
<b>3.5 Spearphishing .....</b>	<b>33</b>
<b>3.6 Παραβίαση προσωπικών δεδομένων .....</b>	<b>34</b>
<b>4 ΑΝΑΛΥΣΗ ΠΟΛΙΤΙΚΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ – ΠΕΡΙΠΤΩΣΙΟΛΟΓΙΚΕΣ ΜΕΛΕΤΕΣ ( CASE STUDIES).....</b>	<b>36</b>
<b>4.1 Κυβερνοεπίθεση κατά των Γερμανικών Υπουργείων.....</b>	<b>36</b>
<b>4.2 Παραβίαση δεδομένων ΕΚΤ.....</b>	<b>38</b>

<b>4.3</b>	<b>Παραβίαση δεδομένων COSMOTE.....</b>	<b>40</b>
<b>4.4</b>	<b>Παραβίαση δεδομένων Yahoo.....</b>	<b>41</b>
<b>4.5</b>	<b>Αξιολόγηση αποτελεσματικότητας των πολιτικών κυβερνοασφάλειας.....</b>	<b>43</b>
4.5.1	Γενικό πλαίσιο.....	43
4.5.2	Αξιολόγηση αποτελεσματικότητας-Εμπειρικά δεδομένα περιπτώσιολογικών μελετών.....	49
<b>5</b>	<b><i>ΠΡΟΟΠΤΙΚΕΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ</i>.....</b>	<b>54</b>
<b>5.1</b>	<b>Τεχνολογικό υπόβαθρο .....</b>	<b>54</b>
<b>5.2</b>	<b>Νομοθετικές εξελίξεις.....</b>	<b>55</b>
<b>6</b>	<b><i>ΣΥΜΠΕΡΑΣΜΑΤΑ</i> .....</b>	<b>57</b>
<b>6.1</b>	<b>Κριτική αποτίμηση.....</b>	<b>57</b>
<b>6.2</b>	<b>Προτάσεις για Μελλοντική Ενίσχυση.....</b>	<b>59</b>
<b>6.3</b>	<b>Προκλήσεις-Δυσκολίες.....</b>	<b>60</b>
<b>7</b>	<b><i>ΒΙΒΛΙΟΓΡΑΦΙΑ</i>.....</b>	<b>61</b>
<b>8</b>	<b><i>ΠΑΡΑΡΤΗΜΑ</i>.....</b>	<b>66</b>

## Πίνακας Συντομογραφιών

<b>CCPA</b>	California Consumer Privacy Act
<b>CER Directive</b>	Critical Entities Resilience Directive
<b>CERT</b>	Computer Emergency Response Team
<b>CIO</b>	Chief information officer
<b>CIRClA</b>	Cyber Incident Reporting for Critical Infrastructure Act
<b>CSIRT</b>	Computer Security Incident Response Team
<b>DDoS</b>	Distributed Denial-of-Service
<b>DHS</b>	Department of Homeland Security
<b>DoD</b>	Department of Defense
<b>DORA</b>	Digital Operational Resilience Act
<b>EDPS</b>	European Data Protection Supervisor
<b>EE</b>	Ευρωπαϊκή Ένωση
<b>EKT</b>	Ευρωπαϊκή Κεντρική Τράπεζα
<b>ENISA</b>	European Union Agency for Cybersecurity
<b>GDPR</b>	General Data Protection Regulation
<b>IAEA</b>	International Atomic Energy Agency
<b>IAM</b>	Identity and Access Management
<b>IDS</b>	Intrusion Detection System
<b>NATO</b>	North Atlantic Treaty Organization
<b>NCCIC</b>	National Cybersecurity and. Communications Integration Center
<b>NICP</b>	National Institute of Crime Prevention
<b>NIS Directive</b>	Directive on security of network and information systems
<b>OECD</b>	Organisation for Economic Co-operation and Development
<b>PSD2</b>	Payment Services Directive 2
<b>SOAR</b>	Security Orchestration, Automation, and Response
<b>UN</b>	United Nations
<b>ΗΠΑ</b>	Ηνωμένες Πολιτείες Αμερικής
<b>IoT</b>	Internet of Things
<b>ΚΕΠΠΑ</b>	Κοινή Εξωτερικής Πολιτική και Πολιτική Ασφάλειας
<b>ΤΠΕ</b>	Τεχνολογίες Πληροφορικής και Επικοινωνιών



## ΠΕΡΙΛΗΨΗ

Η κυβερνοασφάλεια αποτελεί κρίσιμο παράγοντα στο σύγχρονο ψηφιακό περιβάλλον του κυβερνοχώρου, αφού αναφέρεται στην προστασία των δικτύων, των συστημάτων και των δεδομένων από κυβερνοαπειλές. Οι κυβερνοεπιθέσεις εξελίσσονται συνεχώς, και έτσι η κυβερνοασφάλεια απαιτεί σταθερή προσαρμογή και εξέλιξη. Στόχος της είναι η διασφάλιση της ακεραιότητας, της διαθεσιμότητας και της εχεμύθειας των πληροφοριών, καθώς και η προστασία από επιπτώσεις όπως η διαρροή δεδομένων και οι διακοπές υπηρεσιών. Η κυβερνοασφάλεια αποτελεί προτεραιότητα, ειδικά σε τομείς όπως η υγεία και οι κρίσιμες υποδομές, όπου οι επιπτώσεις μπορούν να είναι σοβαρές. Η σχέση μεταξύ κυβερνοασφάλειας και ασφαλειοποίησης είναι στενή και συμπληρωματική, ενώ αφορά διαφορετικές πτυχές του κυβερνοχώρου. Η κυβερνοασφάλεια επικεντρώνεται στην προστασία των ψηφιακών συστημάτων, των δικτύων και των δεδομένων από κινδύνους όπως κυβερνοεπιθέσεις και κακόβουλο λογισμικό. Από την άλλη πλευρά, η ασφαλειοποίηση αφορά στην προστασία σε περίπτωση που συμβούν προβλήματα ασφάλειας ή κυβερνοεπιθέσεις και προσφέρει αντιμετώπιση των επιπτώσεων σε περίπτωση ανεπάρκειας των μέτρων ασφαλείας. Η Ευρωπαϊκή Ένωση έχει εφαρμόσει πολλές πρωτοβουλίες για την κυβερνοασφάλεια στο διαδίκτυο, λαμβάνοντας υπόψη την ανάγκη να προστατευθούν οι πολίτες, οι χώρες και οι επιχειρήσεις από κυβερνοεπιθέσεις και κυβερνοαπειλές. Ειδικότερα, η ΕΕ έχει εγκρίνει νομοθεσίες όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR), που θέτει πρότυπα για την προστασία των προσωπικών δεδομένων των πολιτών της ΕΕ. Επίσης έχει θέσει σε λειτουργία οργανισμούς όπως ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), που παρέχει εμπειρογνωμοσύνη και στήριξη στα κράτη μέλη για θέματα κυβερνοασφάλειας. Παράλληλα, η ΕΕ συνεργάζεται με διεθνείς εταίρους και οργανισμούς για την αντιμετώπιση κοινών κυβερνοασφαλειακών προκλήσεων. Αυτή η συνεργασία περιλαμβάνει την ανταλλαγή πληροφοριών και την κοινή ανάπτυξη καλύτερων πρακτικών. Η αντιμετώπιση των κυβερνοεπιθέσεων στα πλαίσια της ΕΕ διαμορφώνεται δυναμικά, καθώς η τεχνολογική εξέλιξη και οι απειλές στον κυβερνοχώρο συνεχώς εξελίσσονται. Η ΕΕ επιδιώκει να δημιουργήσει ένα ισχυρό κοινό πλαίσιο κυβερνοασφάλειας, να αναπτύξει νέες τεχνολογίες και μεθόδους, καθώς και να ενισχύσει τη συνεργασία μεταξύ των κρατών μελών, των δημόσιων αρχών και των ιδιωτικών εταιρειών για την αντιμετώπιση των διαφόρων προκλήσεων-απειλών και την επίτευξη της ασφαλειοποίησης του κυβερνοχώρου.

**Λέξεις κλειδιά:** κυβερνοχώρος, ασφαλειοποίηση, κυβερνοασφάλεια, ΕΕ

## **ABSTRACT**

Cybersecurity is essential in today's digital landscape of cyberspace as it involves safeguarding networks, systems, and data from cyber threats. With the continuous evolution of cyberattacks, cybersecurity must also constantly adapt and evolve. Its primary goal is to ensure the integrity, availability, and confidentiality of information while preventing issues such as data breaches and service disruptions. Cybersecurity is particularly crucial in sectors like healthcare and critical infrastructure, where the consequences can be severe. The relationship between cybersecurity and securitization is close and complementary, while addressing different aspects of cyberspace. Cybersecurity focuses on protecting digital systems, networks and data from risks such as cyber-attacks and malware. On the other hand, securitization is about protection in case of security problems or cyber-attacks and offers to deal with the consequences in case of inadequacy of security measures. The European Union has launched numerous initiatives to enhance cybersecurity on the internet, recognizing the need to shield citizens, countries and businesses from cyber-attacks and threats. Notably, the EU has enacted legislation such as the General Data Protection Regulation (GDPR), which establishes standards for protecting the personal data of EU citizens. Additionally, the EU has created entities like the European Union Agency for Cybersecurity (ENISA), which offers expertise and support to member states on cybersecurity matters. At the same time, the EU works with international partners and organizations to address common cybersecurity challenges. This cooperation includes the sharing of information and the joint development of best practices. The EU's approach to responding to cyberattacks is continually evolving in response to ongoing technological advancements and emerging threats in cyberspace. The EU aims to create a strong common cybersecurity framework, develop new technologies and methods, as well as strengthen cooperation between member states, public authorities and private companies to address the various challenges-threats and achieve the securitization of cyberspace.

**Keywords:** cyberspace, securitization, cybersecurity, EU