ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΔΙΕΘΝΗΣ ΑΣΦΑΛΕΙΑ

Έκτακτο Διδακτικό Προσωπικό (Δεν προσφέρεται το 2024-25)

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	Κοινωνικών και Πολιτικών Επιστημών		
ΤΜΗΜΑ	Πολιτικής Επιστήμης και Διεθνών Σχέσεων (ΠΕΔιΣ)		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	Προπτυχιακό		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	X2500E	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	E, Z
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Διαδίκτυο και Διεθνής Ασφάλεια		

ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ *σε περίπτωση που οι πιστωτικές μονάδες απονέμονται σε διακριτά μέρη του μαθήματος π.χ. Διαλέξεις, Εργαστηριακές Ασκήσεις κ.λπ. Αν οι πιστωτικές μονάδες απονέμονται ενιαία για το σύνολο του μαθήματος αναγράψτε τις εβδομαδιαίες ώρες διδασκαλίας και το σύνολο των πιστωτικών μονάδων*	**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**	**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
Διαλέξεις	3	1,6
Ατομική Εργασία		1,2
3 Πρόοδοι (αντί εξετάσεων)		2,1
Τελικές Εξετάσεις		2,3
Σύνολο		**5**
Προσθέστε σειρές αν χρειαστεί. Η οργάνωση διδασκαλίας και οι διδακτικές μέθοδοι που χρησιμοποιούνται περιγράφονται αναλυτικά στο (δ).		

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ *γενικού υποβάθρου, ειδικού υποβάθρου, ειδίκευσης γενικών γνώσεων, ανάπτυξης δεξιοτήτων*	Ειδίκευσης γενικών γνώσεων
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:	Κανένα
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνική
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	ΝΑΙ
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://eclass.uop.gr/courses/247/

(2) ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μαθησιακά Αποτελέσματα

Περιγράφονται τα μαθησιακά αποτελέσματα του μαθήματος οι συγκεκριμένες γνώσεις, δεξιότητες και ικανότητες καταλλήλου επιπέδου που θα αποκτήσουν οι φοιτητές μετά την επιτυχή ολοκλήρωση του μαθήματος.

Συμβουλευτείτε το Παράρτημα Α

- *Περιγραφή του Επιπέδου των Μαθησιακών Αποτελεσμάτων για κάθε ένα κύκλο σπουδών σύμφωνα με το Πλαίσιο Προσόντων του Ευρωπαϊκού Χώρου Ανώτατης Εκπαίδευσης*
- *Περιγραφικοί Δείκτες Επιπέδων 6, 7 & 8 του Ευρωπαϊκού Πλαισίου Προσόντων Διά Βίου Μάθησης και το Παράρτημα Β*
- *Περιληπτικός Οδηγός συγγραφής Μαθησιακών Αποτελεσμάτων*

Σκοπός του μαθήματος είναι η εξοικείωση των φοιτητών/-τριών με την πολυπλοκότητα των ζητημάτων διεθνούς ασφάλειας στον κυβερνοχώρο. Μέσω του μαθήματος, οι φοιτητές αναμένεται να είναι σε θέση να κατανοούν τις δυναμικές που αναπτύσσονται στον κυβερνοχώρο και να αναλύουν τα είδη διαδικτυακής δράσης.

Στο τέλος του μαθήματος, οι φοιτητές αναμένεται να διαθέτουν τις παρακάτω δεξιότητες:

- **Γνώση και Κατανόηση**
  - Εξοικείωση με τη συζήτηση γύρω από την υπέρβαση που προσφέρει το διαδίκτυο και τον κίνδυνο του τεχνολογικού ντετερμινισμού
  - Κατανόηση φαινομένων και δυναμικών που αναπτύσσονται στο διαδίκτυο
  - Εξοικείωση με τις τυπολογίες και τις μεθόδους ανάλυσης της παράτυπης χρήσης του διαδικτύου
  - Κατανόηση των λόγων για τους οποίους δυσχεραίνεται, τόσο η προσπάθεια των κρατών να «τιθασεύσουν» το διαδίκτυο, όσο και η διεθνής συνεργασία για την αντιμετώπιση φαινομένων κατάχρησης του διαδικτύου.

- **Δεξιότητες και Ικανότητες**
  - Εξοικείωση με τη διαδικτυακή έρευνα
  - Δυνατότητα αναγνώρισης και κατηγοριοποίησης φαινομένων «κατάχρησης» του διαδικτύου.
  - Ικανότητα διασύνδεσης θεωρίας-παραδείγματος
  - Ικανότητα περιληπτικής σύνοψης και επισκόπησης της σχετικής βιβλιογραφίας

Γενικές Ικανότητες

Λαμβάνοντας υπόψη τις γενικές ικανότητες που πρέπει να έχει αποκτήσει ο πτυχιούχος (όπως αυτές αναγράφονται στο Παράρτημα Διπλώματος και παρατίθενται ακολούθως) σε ποια / ποιες από αυτές αποσκοπεί το μάθημα;.

Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών	*Σχεδιασμός και διαχείριση έργων*
Προσαρμογή σε νέες καταστάσεις	*Σεβασμός στη διαφορετικότητα και στην πολυπολιτισμικότητα*
Λήψη αποφάσεων	*Σεβασμός στο φυσικό περιβάλλον*
Αυτόνομη εργασία	*Επίδειξη κοινωνικής, επαγγελματικής και ηθικής υπευθυνότητας και ευαισθησίας σε θέματα φύλου*
Ομαδική εργασία	*Άσκηση κριτικής και αυτοκριτικής*
Εργασία σε διεθνές περιβάλλον	*Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης*
Εργασία σε διεπιστημονικό περιβάλλον	*……*
Παράγωγή νέων ερευνητικών ιδεών	*Άλλες…*
	…….

Το μάθημα θα βοηθήσει τους φοιτητές να διευρύνουν τις εξής δεξιότητες:

- **Εργασία**: Αυτόνομη εργασία, Άσκηση κριτικής και αυτοκριτικής, Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης, Εργασία σε διεπιστημονικό περιβάλλον, Ικανότητα χρήσης γραπτού λόγου, Ανάπτυξη Επιχειρήματος
- **Πρόοδοι***:* Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών
- **Γραπτές εξετάσεις:** Άσκηση κριτικής και αυτοκριτικής, Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης, Ικανότητα χρήσης γραπτού λόγου

(3) ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Η επερχόμενη τέταρτη βιομηχανική επανάσταση, με βασικό άξονα την αυξημένη συνδεσιμότητα σε επίπεδο ατόμων και πραγμάτων, υπόσχεται την οριστική υπέρβαση της γεωγραφίας και της γεωγραφικά-προσδιορισμένης διεθνούς πολιτικής. Ο στόχος του μαθήματος είναι να σκιαγραφήσει τις εκφάνσεις και τα όρια αυτής της υπέρβασης στο πλαίσιο του διαδικτύου και να αναδείξει τα ζητήματα διεθνούς ασφάλειας που ανακύπτουν.

Το μάθημα θα μελετήσει την μορφολογία και την ανθρωπογεωγραφία του διαδικτύου και θα εξετάσει ζητήματα, όπως η δυσκολία εντοπισμού και απόδοσης ευθυνών στο διαδίκτυο, οι προσπάθειες κρατικού έλεγχο και οι δυσκολίες στην επίτευξη διεθνούς συνεργασίας. Παράλληλα, το μάθημα, θα εξετάσει περιπτώσεις «εκμετάλλευσης» του διαδικτύου από ετερόκλητους δρώντες, όπως κράτη, οργανώσεις πολιτικής βίας, ομάδες πίεσης και κοινούς εγκληματίες. Αντίστοιχα, θα μελετήσει ένα ευρύ φάσμα φαινομένων, όπως ο κυβερνο-πόλεμος, η κυβερνο-τρομοκρατία, τα fake-news, το hacktivism, τα κρυπτο-νομίσματα και το κυβερνο-έγκλημα. Στο πλαίσιο αυτό, το μάθημα θα μελετήσει περιπτώσεις αντιπαράθεσης και ενίοτε ιδιότυπης συνέργειας, που αναπτύσσονται στις περισσότερο ή λιγότερο αφανείς γωνιές του διαδικτύου και επηρεάζουν άμεσα τη διεθνή ασφάλεια.

Θεματικές ενότητες:

Μάθημα	**Θεματική**	**Προτεινόμενη βιβλιογραφία**
1ο	**«Τα ανδροειδή ονειρεύονται ηλεκτρικά πρόβατα»;** *η πληροφοριακή*	**<u>Βιβλιογραφία στην ελληνική γλώσσα</u>**: Tegmark, M. (2018). Καλωσορίσατε στην πιο σημαντική συζήτηση της εποχής μας. Στο *Life 3.0: Τι θα σημαίνει να είσαι άνθρωπος στην εποχή της τεχνητής νοημοσύνης;*. Αθήνα: Τραυλός. 43-82 Ferguson, N. (2018). Η ψεύτικη προφητεία της υπερδιασύνδεσης. *Foreign Affairs*

	επανάσταση μεταξύ υπέρβασης και τεχνολογικού ντετερμινισμού	*(Hellenic Edition)*. https://bit.ly/3c3xvAi Βλάχος, Γ. Κ. (2011). Η τεχνολογική επανάσταση και η πολιτική. *Επιστήμη και Κοινωνία*, 27, 125-139. Φρυδάς, Ν. (2018) Ο κυβερνοχώρος και η ασφάλειά του. Στο Σπυριδάκης, Μ., Κουτσούκου, Η., & Μαρινοπούλου, Α. (Eds.). *Κοινωνία του Κυβερνοχώρου*. Αθήνα: Σιδέρης. 25-72 **Βιβλιογραφία στην αγγλική γλώσσα:** Schwab, K. (2015). The Fourth Industrial Revolution: What It Means and How to Respond. *Foreign Affairs*. https://fam.ag/3eF7wKR Bremmer, I. (2021). The Technopolar Moment: How Digital Powers Will Reshape the Global Order. *Foreign Affairs*, https://fam.ag/3ywMmuq. Walt, S. (2021). Big Tech Won't Remake the Global Order. *Foreign Policy*. https://bit.ly/3yRl83d Morozov, E. (2011). Texting Like It's 1989. In *The net delusion: The dark side of Internet freedom*. New York: PublicAffairs. 33-56 Al-Rawashdeh, Mohammad Salim, (2014). The Impact of the Information Revolution on International Relations. *Global Journal of Political Science and Administration*, 2(5). 1-22
2ο	**Διαδίκτυο και το πρόβλημα της «διπλής χρήσεως»:** *καλόβουλη και κακόβουλη χρήση του διαδικτύου*	**Βιβλιογραφία στην ελληνική γλώσσα:** Webster, G. & Sherman, J. (2021). Η πτώση και η άνοδος της τεχνο-παγκοσμιοποίησης. Graham. *Foreign Affairs (Hellenic Edition)*. https://bit.ly/3IHqfXb Zegart, A. & Morell, M. (2020). Κατάσκοποι, ψέματα και αλγόριθμοι. *Foreign Affairs (Hellenic Edition)*. https://bit.ly/3nSyOVu Kornbluh, K. (2019). Η χαμένη υπόσχεση του Διαδικτύου. *Foreign Affairs (Hellenic Edition)*. https://bit.ly/2CDxy4a Ηλιοπούλου, Φ. (2018). Η σκοτεινή πλευρά του διαδικτύου: στα άδυτα των deep web και darknet. Στο Σπυριδάκης, Μ., Κουτσούκου, Η., & Μαρινοπούλου, Α. (Eds.). *Κοινωνία του Κυβερνοχώρου*. Αθήνα: Σιδέρης. 425-42 Δρόσος, Δ., Βουγιούκας, Δ., Καλλίγερος, Ε., Κοκολάκης, Σ., & Σκιάνης, Χ. (2015). Κοινωνικές επιπτώσεις των τεχνολογιών πληροφορικής και επικοινωνιών. Στο *Εισαγωγή στην επιστήμη των υπολογιστών & επικοινωνιών*. Κάλλιπος, Ανοικτές Ακαδημαϊκές Εκδόσεις. κεφ 7. http://hdl.handle.net/11419/4589 **Βιβλιογραφία στην αγγλική γλώσσα**: Turner, F. (2019). Machine Politics: The rise of the internet and a new age of authoritarianism. *Harper's Magazine*, 29, 25-33. Smith, B., & Browne, C. A. (2019). Tools and weapons: The promise and the peril of the digital age. New York: Penguin. pp. 61-76 Kenney, M. (2015). Cyber-terrorism in a post-stuxnet world. *Orbis*, 59(1), 111-128. Assange, J., Appelbaum, J., Müller-Maguhn, A., & Zimmermann, J. (2012). *Cypherpunks: Freedom and the Future of the Internet*. New York: OR books. pp. 21-32
3ο	**Whodunnit και το ζήτημα της απόδοσης ευθυνών στο διαδίκτυο:** *κράτη, hackers, hacktivists και κοινοί εγκληματίες σε ένα ρευστό περιβάλλον*	**Βιβλιογραφία στην ελληνική γλώσσα:** Σπυρόπουλος, Φ. (2014). *Αθέμιτη πρόσβαση σε ηλεκτρονικά δεδομένα*. Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών (ΕΚΠΑ), Αθήνα. 51-90 Βεράτης, Χ. (2015). Κυβερνοχώρος-Κυβερνοεπιθέσεις- Κυβερνοάμυνα. *ΚΕΔΙΣΑ*. https://bit.ly/3jdMYN5 **Βιβλιογραφία στην αγγλική γλώσσα:** Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, 38(1-2), 4-37. Goel, S. (2020). How improved attribution in cyber warfare can help de-escalate

		cyber arms race. *Connections*, 19(1), 87-95. Brenner, S. W. (2006) At light speed: Attribution and response to cybercrime/terrorism/warfare, *Journal of Criminal Law and Criminology*, 97(2), pp. 379-475. (σσ. 405-440) Skopik, F., & Pahi, T. (2020). Under false flag: Using technical artifacts for cyber attack attribution. *Cybersecurity*, 3(1), 1-20. Sigholm, J. (2013). Non-state actors in cyberspace operations. *Journal of Military Studies*, 4(1), 1-37.
	ΕΙΔΙΚΑ ΘΕΜΑΤΑ ΔΙΑΔΙΚΤΥΟΥ ΚΑΙ ΔΙΕΘΝΟΥΣ ΑΣΦΑΛΕΙΑΣ	
4ο	**Κυβερνο-πόλεμος Ι:** **διακρατικές συγκρούσεις στον κυβερνο-χώρο** *η πληροφοριακή διάσταση του πολέμου Ρωσίας-Γεωργίας (2008) και Ρωσίας-Ουκρανίας (2022)*	**<u>Βιβλιογραφία στην ελληνική γλώσσα</u>:** Θεοφίλης, Α. (2018). Οι Κυβερνοεπιθέσεις ως Μέσο Στρατηγικής. *Στρατηγικόν*, 2, 119-132. Βεράτης, Χ. (2016). Κυβερνοχώρος – Κυβερνοασφάλεια: Ιράν – Ρωσία. *ΚΕΔΙΣΑ* https://bit.ly/315uB3g **<u>Βιβλιογραφία στην αγγλική γλώσσα</u>:** Wired. (2019). The WIRED Guide to Cyberwar. (August 23, 2019). https://www.wired.com/story/cyberwar-guide/ Lewis, J. (2022). *Cyber War and Ukraine*. Center for Strategic & International Studies. https://www.csis.org/analysis/cyber-war-and-ukraine Maschmeyer, L., & Cavelty, M. D. (2022). Goodbye Cyberwar: Ukraine as Reality Check. *Policy Perspectives*, 10(3). Deibert, R. J., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue*, 43(1), 3-24. Hollis, D. (2011). Cyberwar Case Study: Georgia 2008. *Small Wars Journal* (January 6, 2011). https://bit.ly/3jdrAre
5ο	**Κυβερνο-πόλεμος ΙΙ:** **κατάσκοποι, ιοί και σκουλήκια** *χακάροντας το ιρανικό πυρηνικό πρόγραμμα (Stuxnet)*	**<u>Βιβλιογραφία στην ελληνική γλώσσα</u>:** Valeriano, B., & Maness, R. (2012). Η ομίχλη του κυβερνο-πολέμου. *Foreign Affairs* (Hellenic Edition). (10 Δεκεμβρίου 2012). https://bit.ly/2MqC1dm Βεράτης, Χ. (2016). Κυβερνοχώρος – Κυβερνοασφάλεια: Ιράν – Ρωσία. *ΚΕΔΙΣΑ* https://bit.ly/315uB3g Fortune Greece. (2015). Ο «πατέρας» της ψηφιακής κατασκοπείας. (8 Φεβρουαρίου 2015) https://bit.ly/2yok9rm **<u>Βιβλιογραφία στην αγγλική γλώσσα:</u>** Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22(3), 365-404. Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3), 49-51. Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, 53(1), 23-40.
6ο	**Κυβερνο-τρομοκρατία Ι:** **προπαγάνδα και ριζοσπαστικοποίηση στο διαδίκτυο** *Memes και gifs στην υπηρεσία της ισλαμιστικής και ακροδεξιάς*	**<u>Βιβλιογραφία στην ελληνική γλώσσα</u>:** Ελευθεριάδου, Μ. (2022). *Ριζοσπαστικοποίηση*. Αθήνα: Ευρασία, 54-62 Γιαννάκη, Ν., & Πάνος, Δ. (2017). Από την ριζοσπαστικοποίηση στον βίαιο εξτρεμισμό και την τρομοκρατία: επίπεδα ανάλυσης, θεωρητικές προσεγγίσεις και ο ρόλος του Διαδικτύου. *Επιστήμη και Κοινωνία*, 35, 103-134. Neumann, P. R. (2016). *Οι Νέοι Τζιχαντιστές: Ισλαμικό Κράτος, Ευρώπη και το επόμενο κύμα τρομοκρατίας*. Αθήνα: Διάμετρος. 79-184 Gartenstein-Ross, D., & Barr, N. (2016). Ο μύθος της τρομοκρατίας του «μοναχικού λύκου». *Foreign Affairs* (Hellenic Edition). (28 Ιουλίου 2016) https://bit.ly/2ymqdk7

	πολιτικής βίας	Byman, D. & Meserole, C. (2019). Πώς οι Big Tech εταιρείες θα καταπολεμήσουν την λευκή ρατσιστική τρομοκρατία. *Foreign Affairs (Hellenic Edition)*. https://bit.ly/31p6bVE **Βιβλιογραφία στην αγγλική γλώσσα**: Winter, C., Neumann, P., Meleagrou-Hitchens, A., Ranstorp, M., Vidino, L., & Fürst, J. (2020). Online extremism: research trends in internet activism, radicalization, and counter-strategies. *International Journal of Conflict and Violence (IJCV)*, 14(2), 1-20. Cinelli, M., Morales, G. D. F., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*, 118(9). Burke, J. (2016) The age of selfie jihad: How evolving media technology is changing terrorism, *CTC Sentinel*, 9(11), pp. 1-8. Berger, J. (2015) Tailored online interventions: The Islamic State's recruitment strategy, *CTC Sentinel*, 8(10), pp. 19-23. Macklin, G. (2019) The Christchurch Attacks: Livestream Terror in the Viral Video Age, *CTC Sentinel*, 12(6).
7ο	**Κυβερνο-τρομοκρατία ΙΙ:** **πέρα από την ριζοσπαστικοποίηση** *εκπαίδευση, 3-D printing και κυβερνο-επιθέσεις*	**Βιβλιογραφία στην ελληνική γλώσσα**: Γεωργιτσόπουλος, Ν. (2018). Τρισδιάστατη Εκτύπωση (3D Printing) Πιθανές Συνέπειες σε Θέματα Ασφαλείας. *Ερευνητική Εργασία No. 11*, ΚΕΔΙΣΑ. https://kedisa.gr/wp-content/uploads/2018/03/Ergasia_no_11_georgitsopoulos.pdf Gershenfeld, N. (2012). Πώς να φτιάξετε σχεδόν τα πάντα! Η επανάσταση των ψηφιακών κατασκευών. *Foreign Affairs* (Hellenic Edition). https://bit.ly/2WlTebZ Ελευθεριάδου, Μ. (2014) Η «εικονική βάση» του σαλαφικού-τζιχαντικού κινήματος στο διαδίκτυο. Στο *Ανταρτοπόλεμος και διασυνοριακές βάσεις (Safe Haven): οι διεθνείς σχέσεις των ασύμμετρων συγκρούσεων*. Πανεπιστήμιο Πελοποννήσου. 293-330 **Βιβλιογραφία στην αγγλική γλώσσα:** Koehler, D. (2019). The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat. *CTC Sentinel*, 12(11), 14-20. https://bit.ly/3qW0Roo Walther, G. (2015). Printing insecurity? The security implications of 3d-printing of weapons. *Science and engineering ethics*, 21(6), 1435-1445. Ranstorp, M. (2007). The Virtual Sanctuary of Al-Qaeda and Terrorism in an Age of Globalisation. In J. Eriksson & G. Giacomello (eds.), *International Relations and Security in the Digital Age*. London: Routledge. Coll, S., & Glasser, S. B. (2005). Terrorists turn to the Web as base of operations. *The Washington Post*. https://wapo.st/2LOghII Stenersen, A. (2008). The Internet: A Virtual Training Camp? *Terrorism and Political Violence*, 20(2), 215-233.
8ο	**Κυβερνο-επιρροή Ι:** **hacktivism** *η απόπειρα των Anonymous και του Wikileaks να επιφέρουν την πολιτική αλλαγή μέσω του διαδικτύου*	**Βιβλιογραφία στην ελληνική γλώσσα**: Μποζανίνου, Τ. (2012). Ο πολιτικός ακτιβισμός είναι σήμερα «Anonymous». *Το Βήμα*. (12 Φεβρουαρίου 2012). https://bit.ly/2OsrLB4 Σπυρόπουλος, Φ., & Τεχνίτης, Μ. (2015). Τζούλιαν Ασάνζ: Ήρωας ή Εγκληματίας;. *The Art of Crime*, 28. https://bit.ly/2WrXDdh Σπυρόπουλος, Φ. (2013). Anonymous - χακτιβισμός με "ονοματεπώνυμο";. *The Art of Crime*, 25. https://bit.ly/3jaZInJ **Βιβλιογραφία στην αγγλική γλώσσα**: Romagna, M. (2020). Hacktivism: Conceptualization, techniques, and historical view. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 743-769). Cham: Palgrave Macmillan. George, J. J., & Leidner, D. E. (2019). From clicktivism to hacktivism: Understanding digital activism. *Information and Organization*. Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The internet as a

		tool for influencing foreign policy. In Arquilla, J., & Ronfeldt, D. *Networks and netwars: The future of terror, crime, and militancy*: Rand Corporation. 239-88 Kushner, D. (2014). The masked avengers: How Anonymous incited online vigilantism from Tunisia to Ferguson. *New Yorker*. (September 8, 2014) https://www.newyorker.com/magazine/2014/09/08
9ο	**Κυβερνο-επιρροή ΙΙ:** **fake-news** *παραπληροφόρηση και συνωμοσιολογία στην εποχή των QAnon και του COVID-19*	**Βιβλιογραφία στην ελληνική γλώσσα**: Χαλαβαζής Ι. (2022). Προσεγγίζοντας το φαινόμενο των παραποιημένων ειδήσεων (fake news). *Επιστήμη και Κοινωνία: Επιθεώρηση Πολιτικής και Ηθικής Θεωρίας*, 41, 189–202. https://doi.org/10.12681/sas.29159 Παπαντζίκου, Ζ., & Αναστασίου, Β. (2021). Παραπληροφόρηση στο διαδίκτυο – Fake news -Διάδοση και Αντιμετώπιση. *Επιθεώρηση Δικαίου Πληροφορικής*, 2(2). https://ejournals.lib.auth.gr/infolawj/article/view/8456/8127 RISE TV. (2019). Fake News: Μια σύγχρονη μάστιγα από τα παλιά. (15 Μαρτίου 2019). https://www.youtube.com/watch?v=5OPgKRen_lA **Βιβλιογραφία στην αγγλική γλώσσα:** Associated Press. Not Real News. https://apnews.com/NotRealNews Tandoc Jr, E. C., Lim, Z. W., & Ling, R. (2018). Defining "fake news": A typology of scholarly definitions. *Digital journalism*, 6(2), 137-153. Bleakley, P. (2021). Panic, pizza and mainstreaming the alt-right: A social media analysis of Pizzagate and the rise of the QAnon conspiracy. *Current Sociology*, https://doi.org/10.1177/00113921211034896 Hannah, M. (2021). QAnon and the information dark age. *First Monday*, 26(2). https://bit.ly/3Lw8Guo Simon, F. M., & Camargo, C. Q. (2021). Autopsy of a metaphor: The origins, use and blind spots of the 'infodemic'. *New media & Society*, 1-22. Banerjee, D., & Meena, K. S. (2021). COVID-19 as an "Infodemic" in Public Health: Critical Role of the Social Media. *Frontiers in Public Health*, 9.
10ο	**Διαδίκτυο και οικονομία Ι:** **κυβερνο-έγκλημα** *συναλλαγές στα βάθη του darknet*	**Βιβλιογραφία στην ελληνική γλώσσα**: Συκάς, Σ. (2019). Ψηφιακή παραβατικότητα και παραβατικότητασε ψηφιακό περιβάλλον: Η περίπτωση της παιδικής πορνογραφίας. *Homo Virtualis*, 2(1), 57–62. https://doi.org/10.12681/homvir.20195 Glenny, M. (2012). *DarkMarket: η αόρατη απειλή πίσω από την οθόνη του υπολογιστή σου*. Αθήνα: Πάπυρος. 1-16 Παπαθανασίου, Α., & Γερμανός, Γ. (2016). Εξέλιξη και ανάπτυξη νέων μορφών ψηφιακής εγκληματικότητας στον Κυβερνοχώρο σε εποχές κρίσης. *Crime in Crisis*. https://bit.ly/2IIkLzk Παπάζογλου, Ν. (2016). Το Darknet γίνεται mainstream. *Insider.gr*. https://bit.ly/3j40Rxk **Βιβλιογραφία στην αγγλική γλώσσα**: Payne, B. K. (2020). Defining Cybercrime. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 3-25. Wall, D. (2005/15) The Internet as a Conduit for Criminal Activity in Pattavina, A. (ed.) *Information Technology and the Criminal Justice System*. Thousand Oaks, CA: Sage, pp. 77-98. Anderson, R. et.al. (2019). Measuring the changing cost of cybercrime. Presented at: *The 2019 Workshop on the Economics of Information Security*, Boston, US, 3-4 Jun 2019 Liggett, R., Lee, J. R., Roddy, A. L., & Wallin, M. A. (2020). The dark web as a platform for crime: An exploration of illicit drug, firearm, CSAM, and cybercrime markets. In *The Palgrave Handbook of international cybercrime and cyberdeviance*, 91-116.
11ο	**Διαδίκτυο και οικονομία ΙΙ:**	**Βιβλιογραφία στην ελληνική γλώσσα**:

	κρυπτο-νομίσματα και παράλληλες οικονομίες *από την hawala στο bitcoin*	Χουζούρης, Κ. (2021) Bitcoin και εθνική κυριαρχία. *Foreign Affairs* (Hellenic Edition). https://bit.ly/3PukCy4 Ανδρουλάκη, Ε. (2014). Πληρώνοντας με bitcoins... *The Art of Crime*, 26. https://bit.ly/30gNOAa TechieChan. (2013). Η φαντασιακή θέσμιση του bitcoin και ο σκρούτζ μακ ντακ στο κλονταϊκ. http://www.techiechan.com/?p=1954 **Βιβλιογραφία στην αγγλική γλώσσα**: Berentsen, A. & Schär, F. (2018). A Short Introduction to the World of Cryptocurrencies. *FRB of St. Louis Working Review* http://dx.doi.org/10.20955/r.2018.1-16 Kfir, I. (2020). Cryptocurrencies, national security, crime and terrorism. *Comparative strategy*, 39(2), 113-127. Whyte, C. (2019). Cryptoterrorism: Assessing the utility of blockchain technologies for terrorist enterprise. *Studies in Conflict & Terrorism*, 1-24. https://doi.org/10.1080/1057610X.2018.1531565 Katz, R. (2019). Tales of Crypto-Currency: Bitcoin Jihad in Syria and Beyond. *Daily Beast*. https://bit.ly/393JZSM
12ο	**Το κράτος απέναντι στο διαδίκτυο:** *ελεγχος και λογοκρισία στον κυβερνοχώρο*	**Βιβλιογραφία στην ελληνική γλώσσα**: Ανθόπουλος, Χ. (2021). Η Ελευθερία της Πληροφόρησης στην Εποχή των Ψηφιακών Πλατφορμών. *Επιθεώρηση Δημόσιας Διοίκησης* 1(1), 1-11. https://www.lawjournals.unic.ac.cy/index.php/pareview Τσιριγωτάκη, Ε. (2022). Η πανδημία «ευνοεί» τη λογοκρισία στο διαδίκτυο. *EPTnews*. https://www.ertnews.gr/eidiseis/mono-sto-ertgr/i-pandimia-eynoei-ti-logokrisia-sto-diadiktyo/ Maus, G. (2015). Παρακολουθώντας το Skynet. *Foreign Affairs* (Hellenic Edition). https://bit.ly/2K1Hs0C Σμυρναίος, Ν. (2013). Το σκάνδαλο Prism και η κοινωνία της επιτήρησης που ανατέλλει. *Ephemeron*. http://ephemeron.eu/998 MacKinnon, R. (2012). Το ίντερνετ βρίσκεται υπό εντεινόμενη παρακολούθηση. *Foreign Affairs* (Hellenic Edition). (23 Ιουνίου 2012). https://bit.ly/2YvmQ4L **Βιβλιογραφία στην αγγλική γλώσσα**: Meserve, S. A., & Pemstein, D. (2020). Terrorism and internet censorship. *Journal of Peace Research*, 57(6), 752-763. Zittrain, J. L., Faris, R., Noman, H., Clark, J., Tilton, C., & Morrison-Westphal, R. (2017). The shifting landscape of global internet censorship. *Berkman Klein Center Research Publication*. https://bit.ly/3h3yLAw Stoycheff, E., Burgess, G. S., & Martucci, M. C. (2020). Online censorship and digital surveillance: The relationship between suppression technologies and democratization across countries. *Information, Communication & Society*, 23(4), 474-490.
13ο	**Ζητήματα ασφάλειας στο διαδίκτυο και διεθνής συνεργασία:** *μια σχεδόν ανώφελη προσπάθεια για διεθνή συνεννόηση*	**Βιβλιογραφία στην ελληνική γλώσσα:** Cohen, J. & Fontaine, R. (2022). Ενώνοντας τις Τεχνο-Δημοκρατίες. *Foreign Affairs* (Hellenic Edition). https://bit.ly/3zu47fR Παρασκευάς, Μ., Ασημακόπουλος, Γ., & Τριανταφύλλου, Β. (επ.). (2015). *Κοινωνία της πληροφορίας*: Κάλλιπος. 192-8 Τσιούρτος, Κ. (2019). Παγκόσμιοι κανόνες στον κυβερνοχώρο και το κόστος μη συνεργασίας. *Brief*. https://bit.ly/2DK6VLb **Βιβλιογραφία στην αγγλική γλώσσα:** Liaropoulos, A. (2017). Cyberspace Governance and State Sovereignty. In: Bitros, G., Kyriazis, N. (eds) Democracy and an Open-Economy World Order. Cham: Springer Mueller, M. L. (2020). Against sovereignty in cyberspace. *International Studies Review*, 22(4), 779-801.

		Cornish, P. (2015). Governing Cyberspace through Constructive Ambiguity. *Survival*, 57(3), 153-176. Slack, C. (2016). Wired yet Disconnected: The Governance of International Cyber Relations. *Global Policy*, 7(1), 69-78.

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ *Πρόσωπο με πρόσωπο, Εξ αποστάσεως εκπαίδευση κ.λπ.*	Η διδασκαλία του μαθήματος γίνεται μέσω διαλέξεων. Κάθε διάλεξη εξετάζει ένα ζήτημα ή μία περίπτωση με τρόπο αυτοτελή, ακολουθώντας, ωστόσο, μια λογική εξέλιξη που θα επιτρέπει την προοδευτική κατανόηση των υπό εξέταση ζητημάτων.
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ *Χρήση Τ.Π.Ε. στη Διδασκαλία, στην Εργαστηριακή Εκπαίδευση, στην Επικοινωνία με τους φοιτητές*	Στο πλαίσιο του μαθήματος, όπου είναι εφικτό, θα γίνεται χρήση οπτικοακουστικού υλικού (σύντομα βίντεο και ηχητικά ντοκουμέντα) για να καθίσταται περισσότερο άμεσο και ενδιαφέρον το μάθημα. Η διάλεξη (powerpoint), επιπλέον οπτικοακουστικό υλικό και κείμενα εμβάθυνσης θα αναρτώνται στην ηλεκτρονική πλατφόρμα (eclass) και στα οποία θα έχουν πρόσβαση όλοι οι φοιτητές. Θα γίνει χρήση, επίσης, άλλων δυνατοτήτων που προσφέρει το eclass, όπως η ηλεκτρονική κατάθεση εργασιών, ασκήσεις πολλαπλής επιλογής και σύντομης ανάλυσης και ανάρτηση βαθμολογίας.
ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ *Περιγράφονται αναλυτικά ο τρόπος και μέθοδοι διδασκαλίας.* *Διαλέξεις, Σεμινάρια, Εργαστηριακή Άσκηση, Άσκηση Πεδίου, Μελέτη & ανάλυση βιβλιογραφίας, Φροντιστήριο, Πρακτική (Τοποθέτηση), Κλινική Άσκηση, Καλλιτεχνικό Εργαστήριο, Διαδραστική διδασκαλία, Εκπαιδευτικές επισκέψεις, Εκπόνηση μελέτης (project), Συγγραφή εργασίας / εργασιών, Καλλιτεχνική δημιουργία, κ.λπ.* *Αναγράφονται οι ώρες μελέτης του φοιτητή για κάθε μαθησιακή δραστηριότητα καθώς και οι ώρες μη καθοδηγούμενης μελέτης σύμφωνα με τις αρχές του ECTS*	<table><tr><th>Δραστηριότητα</th><th>Φόρτος Εργασίας Εξαμήνου</th></tr><tr><td>Διαλέξεις</td><td>13 εβδ. x 3 ώρες = 39 ώρες</td></tr><tr><td>Ατομική Εργασία</td><td>7 Εβδ. x 3 ώρες x 1,5 = 31,5 ώρες</td></tr><tr><td>3 Πρόοδοι (αντί εξετάσεων)</td><td>(4 Εβδ. x 3 ώρες x 1,5) χ 3 = 54 ώρες</td></tr><tr><td>Τελικές Εξετάσεις</td><td>13 Εβδ x 3 ώρες x 1,5 = 58,5 ώρες</td></tr><tr><td>Σύνολο</td><td>124,5 ή 129 ώρες</td></tr></table>
ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ *Περιγραφή της διαδικασίας αξιολόγησης* *Γλώσσα Αξιολόγησης, Μέθοδοι αξιολόγησης, Διαμορφωτική ή Συμπερασματική, Δοκιμασία Πολλαπλής Επιλογής, Ερωτήσεις Σύντομης Απάντησης, Ερωτήσεις Ανάπτυξης Δοκιμίων, Επίλυση Προβλημάτων, Γραπτή Εργασία, Έκθεση / Αναφορά, Προφορική Εξέταση, Δημόσια Παρουσίαση, Εργαστηριακή Εργασία, Κλινική Εξέταση Ασθενούς, Καλλιτεχνική Ερμηνεία, Άλλη / Άλλες* *Αναφέρονται ρητά προσδιορισμένα κριτήρια αξιολόγησης και εάν και που είναι προσβάσιμα από τους φοιτητές.*	Η αξιολόγηση των φοιτητών γίνεται με τρεις τρόπους: 1. Τελικές γραπτές εξετάσεις (60%) 2. Ατομική εργασία (40%) 3. Τρεις (3) πρόοδοι (προαιρετικά) **Γραπτές εξετάσεις** Ο βαθμός των γραπτών εξετάσεων στο τέλος του εξαμήνου αντιστοιχεί στο 60% του τελικού βαθμού. **Εργασία** Οι φοιτητές, επίσης, θα πρέπει να παραδώσουν στο τέλος του εξαμήνου μια σύντομη εργασία (2000-2500 λέξεις). Ο βαθμός της εργασίας θα συνυπολογιστεί (με βαρύτητα 40%) στον καθορισμό του τελικού βαθμού. Το θέμα της εργασίας θα πρέπει να αφορά ένα επίκαιρο παράδειγμα «κατάχρησης» του διαδικτύου που σχετίζεται με κάποιο από τα ζητήματα διεθνούς ασφάλειας που εξετάζονται στο μάθημα.

	Πρόοδοι Αντί των γραπτών εξετάσεων, οι φοιτητές μπορούν να εξεταστούν με τη μέθοδο των προόδων. Οι πρόοδοι θα πραγματοποιούνται σε προκαθορισμένες ημερομηνίες και θα περιλαμβάνουν ερωτήσεις πολλαπλής επιλογής και ερωτήσεις σύντομης απάντησης (2-3 παράγραφοι). Για να ληφθεί υπόψη ο βαθμός των προόδων, ο φοιτητής/-τρια θα πρέπει να βαθμολογηθεί με **βαθμό πάνω από τη βάση σε δύο (2) από τις τρεις (3) συνολικά προόδους**. Για τον υπολογισμό του συνολικού βαθμού των προόδων, θα ληφθεί υπόψη **ο μέσος όρος των δύο προόδων με τον υψηλότερο βαθμό**. Ο προκύπτων βαθμός θα αντικαθιστά τον βαθμό των εξετάσεων και θα αντιστοιχεί στο 60% του τελικού βαθμού. Σε περίπτωση που ο φοιτητής/-τρια δεν έχει βαθμό πάνω από τη βάση στις δύο από τις τρεις προόδους ή θέλει να βελτιώσει τον βαθμό του/της, έχει το δικαίωμα να ζητήσει να μην ληφθεί υπόψη ο βαθμός των προόδων και να συμμετάσχει στις τελικές εξετάσεις. Σε αυτή τη περίπτωση, υπολογίζεται ο βαθμός των εξετάσεων, ανεξάρτητα αν είναι χαμηλότερος από αυτόν των προόδων.

(5) ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:

Βασικά εγχειρίδια:

Eric Schmidt, Jared Cohen, *Η Νέα Ψηφιακή Εποχή*, Αθήνα: Δίαυλος, 2014
Kello Lucas, *Το Κυβερνο-Όπλο και η Διεθνής Τάξη*, Αθήνα: Παπαζήση, 2020

Για συμπληρωματική βιβλιογραφία ανά θεματική ενότητα βλ. παραπάνω «Περιεχόμενο Μαθήματος / Θεματικές Ενότητες». Οι πηγές για τις οποίες δεν παρέχεται σύνδεσμος (link) είναι διαθέσιμες στη βιβλιοθήκη ή είναι αναρτημένες στο eclass, στα Έγγραφα, στον αντίστοιχο φάκελο.

- Συναφή επιστημονικά περιοδικά:

International Journal of Cyber Criminology	Computer Law and Security Review
Journal of Cybersecurity	Journal of Cyber Policy
IEEE Security & Privacy	International Journal of Cyber Warfare and Terrorism

-Άλλες πηγές

Wired (Security, Threat Level)	https://www.wired.com/category/security https://www.wired.com/category/threatlevel/
Global Guerrillas	https://globalguerrillas.typepad.com/globalguerrillas/
Center for Cybersecurity	http://cyber.nyu.edu/
Public Intelligence	https://publicintelligence.net/
Cyber Conflict Studies Association (CCSA)	http://www.cyberconflict.org/
Snopes	https://www.snopes.com/
Associated Press. Not Real News	https://apnews.com/NotRealNews
Ellinika Hoaxes	https://www.ellinikahoaxes.gr/