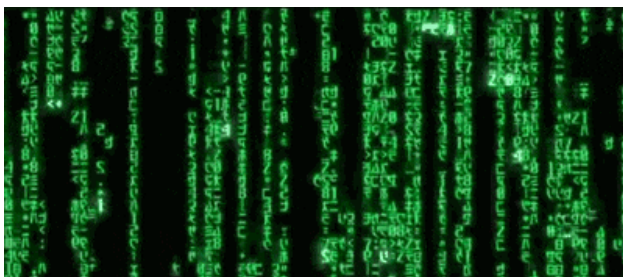


Διπλωματική Εργασία

ΟΙ ΘΕΩΡΗΣΕΙΣ ΤΩΝ ΔΙΕΘΝΩΝ ΣΧΕΣΕΩΝ & ΤΟ ΠΛΗΡΟΦΟΡΙΑΚΟ ΠΕΡΙΒΑΛΛΟΝ Ο Κυβερνοχώρος ως Πεδίο Διεθνούς Ανταγωνισμού Ισχύος



Επιβλ. Καθηγητής: Δρ. Κουσκουβέλης Ηλίας
Εισηγητής: Κων/νος Καλκετινίδης

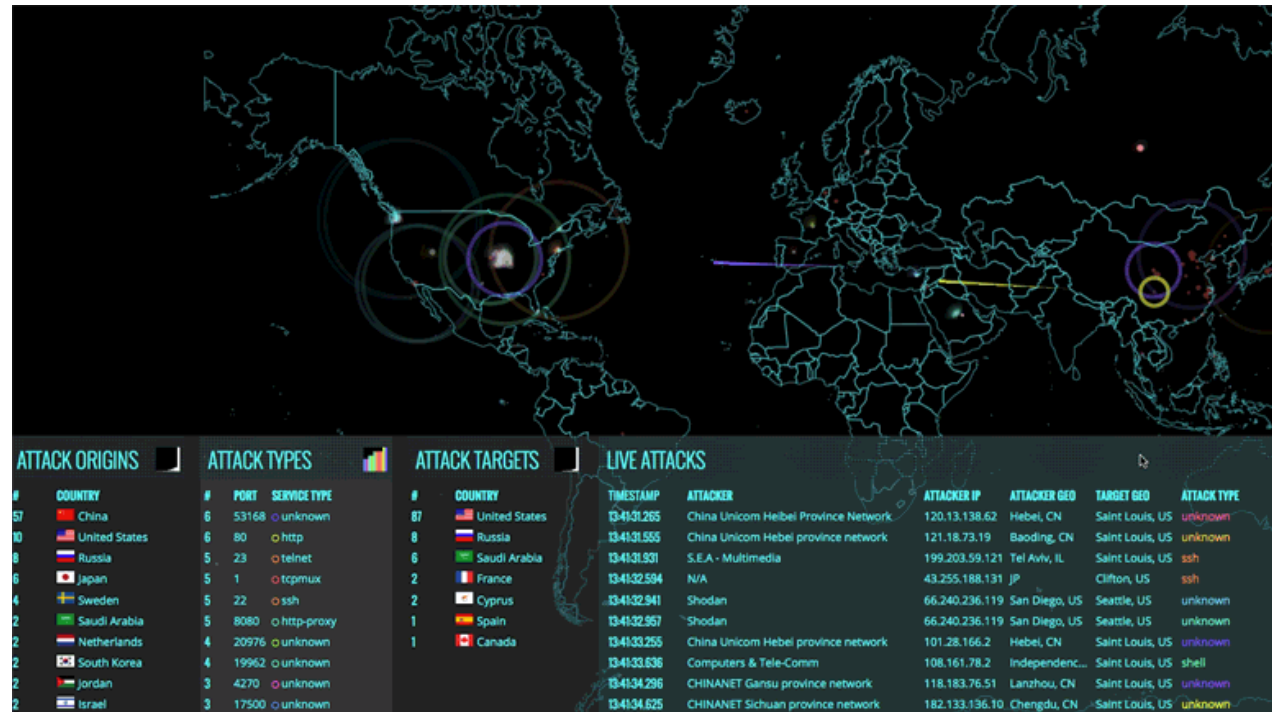
Εισαγωγή ...στις Διεθνείς
«Κυβερνοσχέσεις»

Ο Άνθρωπος, το Κράτος και το
Διεθνές Σύστημα στην Ψηφιακή
Εποχή

Οι Θεωρήσεις των Διεθνών Σχέσεων
Συναντούν τον Κυβερνοχώρο

Ψηφιακές Προκλήσεις Ασφαλείας

Συμπεράσματα

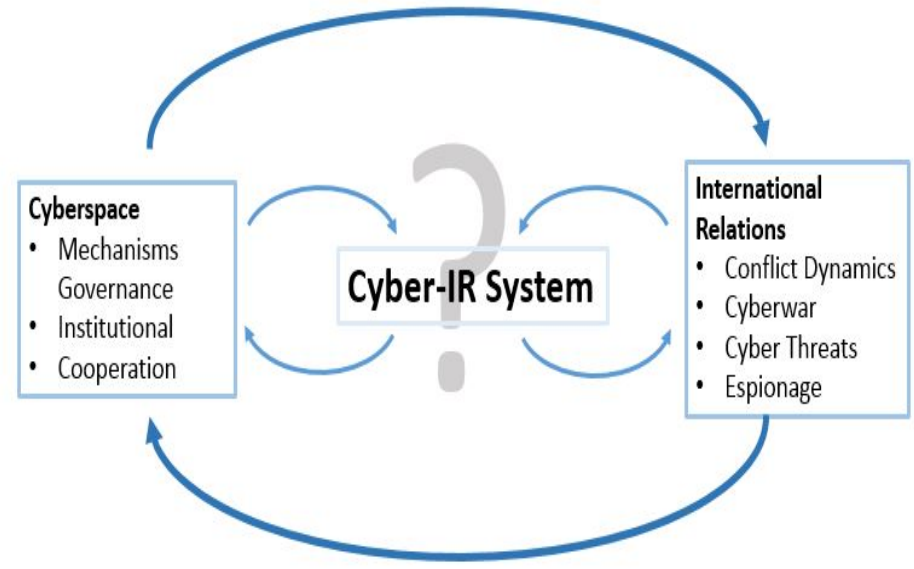


Η Ψηφιακή Εποχή (μια κοινοτυπία)

Ο επαναστατικός χαρακτήρας της τεχνολογικής εξέλιξης

✓ Η ψηφιακή τεχνολογία διαρρηγνύει το κέλυφος που διαχωρίζει το εσωτερικό των Κρατών από τον άναρχο χώρο στον οποίο αυτά ανταγωνίζονται.

- Τι τελικά σημαίνει αυτή η “ψηφιακή εισβολή” στη διεθνή πολιτική αρένα για τον χαρακτήρα, τη δομή και την ισορροπία του διεθνούς συστήματος
- ποιες οι απορρέουσες προκλήσεις ασφαλείας που καλείται να αντιμετωπίσει το Κράτος και ο Άνθρωπος.



DIGITAL ERA



Η Ψηφιακή Εποχή

✓ Digital Information Environment

- Digitization – digitalization
- Net of Networks
- “Απειρότητα” και φύσει παγκοσμιοποιημένη λειτουργικότητά του.
- Κάθε προσπάθεια περιορισμού και οριοθέτησης μοιάζει/είναι απελπιστικά μάταιη.

✓ «Πληροφοριακό» = Υβριδικό περιβάλλον

- Το πεδίο φυσικής δραστηριοποίησης των ανθρώπων και μηχανών σε συνδυασμό με
- το ψηφιακό πεδίο του κυβερνοχώρου με τα παράγωγα εικονικά καθεστώτα και με τα αποτελέσματα που επηρεάζουν τον φυσικό κόσμο.

✓ «Κυβερνοχώρος» = ψηφιακό περιβάλλον

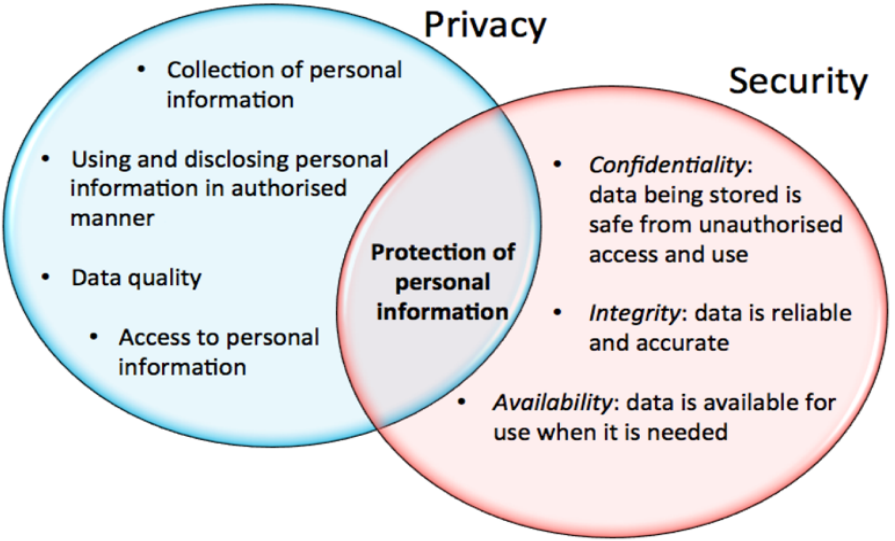
- Το σύνολο των ψηφιακών διασυνδέσεων μεταξύ ηλεκτρονικών υπολογιστών και συσκευών επικοινωνίας με τις λεωφόρους ροών ανταλλαγής ψηφιακών μηνυμάτων και
- τις ροές αυτές.

Ο Κυβερνοχώρος λοιπόν, αποτελεί τον πυρήνα του Πληροφοριακού Περιβάλλοντος, καθώς ενυπάρχει σε αυτό και ορίζει την ύπαρξή του.

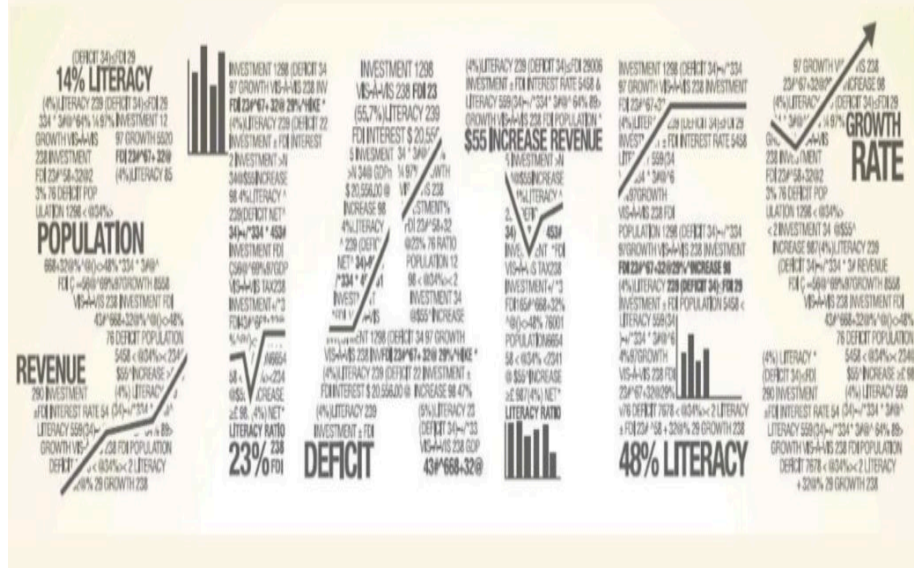


Η Ψηφιακή Εποχή Οι βασικές συνέπειες

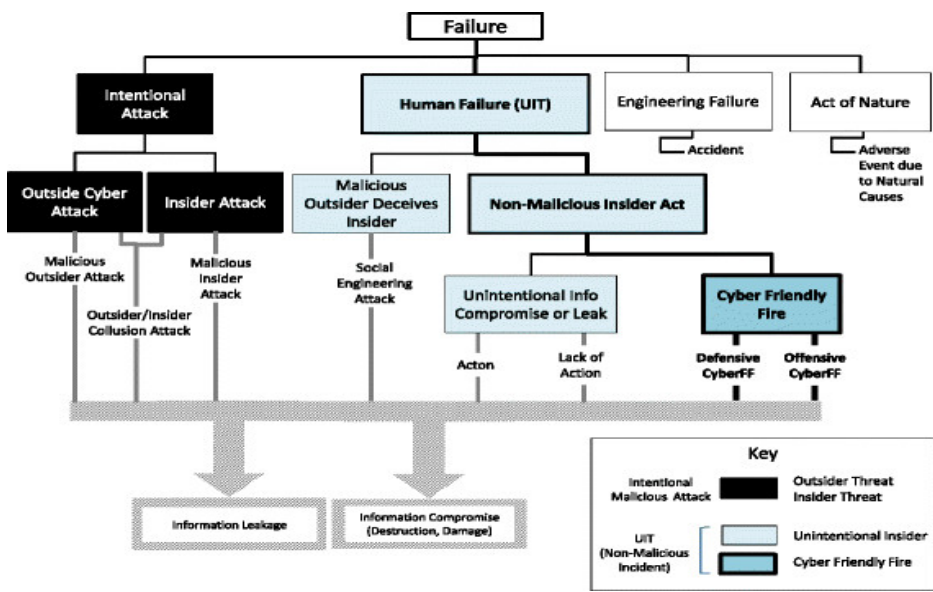
Comprehensive review of perspectives and policies



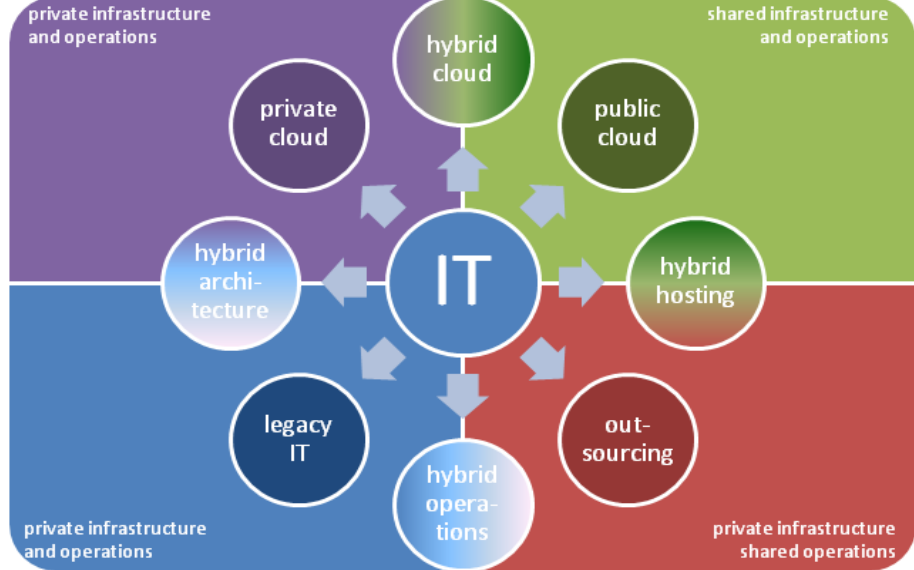
Corrosion of State status and competitiveness



Systemic loss of economic values at state level



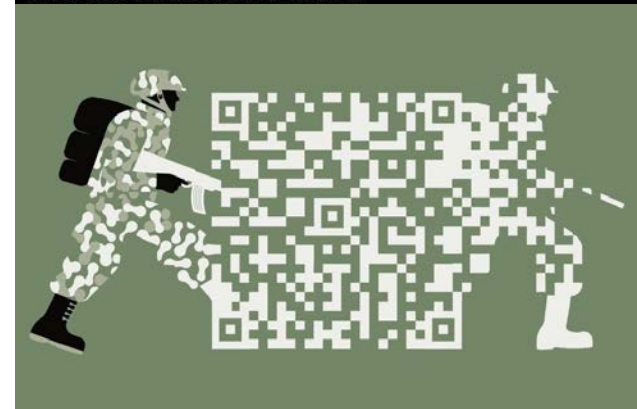
Infrastructure adaptation to a new security architecture



Ο Κυβερνοχώρος και οι Θεωρήσεις των Διεθνών Σχέσεων

Ρεαλισμός & Κυβερνοχώρος

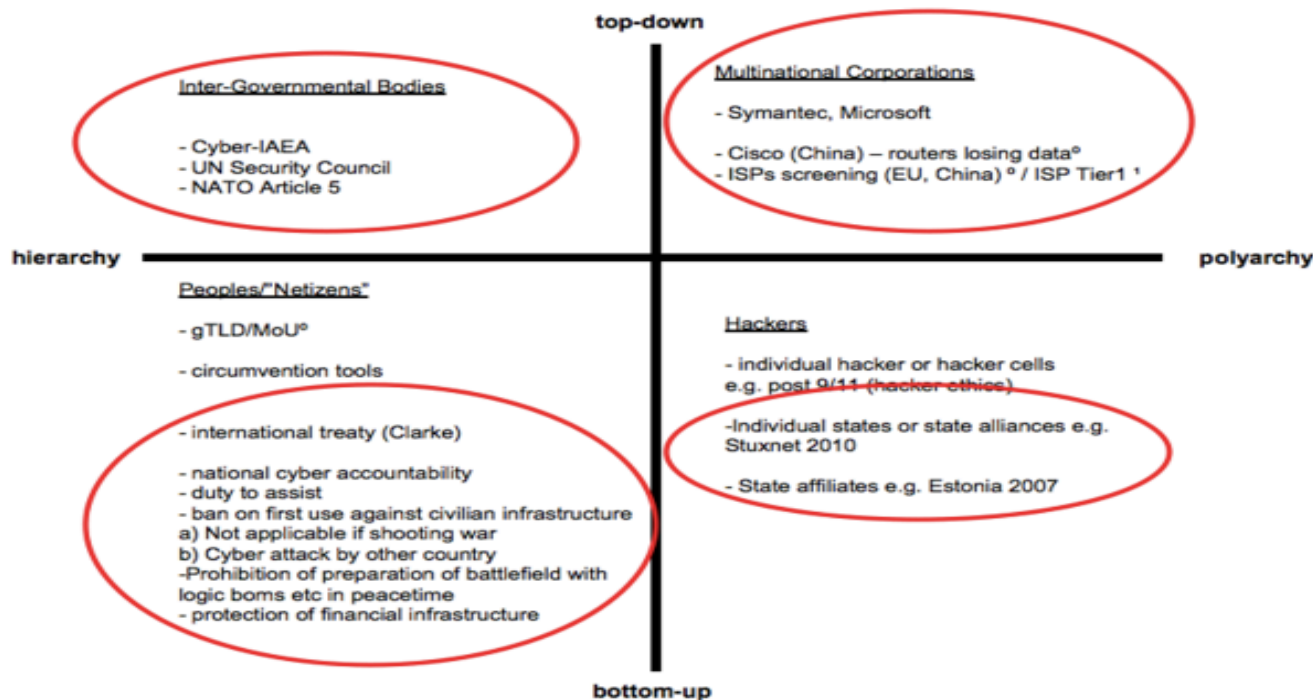
- ✓ **Κυβερνοχώρος: Το νέο διεθνές πεδίο μάχης (James Adams)**
 - Χώρος δραστηριοποίησης κρατικών και μη κρατικών δρώντων.
 - Κανείς δεν μπορεί να εμπιστεύεται πλήρως κανένα.
- ✓ **Σκοπός του Ανταγωνισμού**
 - Η σώρευση ψηφιακής ισχύος και επιρροής
 - Η προστασία των διαθέσιμων ψηφιακών και ψηφιοποιημένων συντελεστών ισχύος,
- ✓ **“Ψηφιακογενής” Φόβος - Αίσθηση Ανασφάλειας - Απόδοση Ευθύνης**
(Digital Fear – Insecurity Perception - Attribution of Responsibility)
- ✓ **Η “Τραγικότητα” του Κυβερνοχώρου**
 - Πεδίο κλασσικού ανταγωνισμού ισχύος
 - Φύσει ενισχυτής διεθνιστικών ιδεών, του κοσμοπολιτισμού και της παγκοσμιοποίησης,
- ✓ **Το “δίλημμα ασφαλείας” σε δύο επίπεδα**
 - Το κλασσικό πρότυπο: το ένστικτο της αυτοσυντήρησης – επιβίωσης του Κράτους.
 - Το συστημικό επίπεδο: το ένστικτο της αυτοσυντήρησης – επιβίωσης του Συστήματος



Ο Κυβερνοχώρος και οι Θεωρήσεις των Διεθνών Σχέσεων

Φιλελευθερισμός, Κονστρουκτιβισμός και Κυβερνοχώρος

- ✓ Οι “Θεωρητικές” αδυναμίες του Νεορεαλισμού στον κυβερνοχώρο (Διεθνικό έγκλημα, τρομοκρατία)
- ✓ Οι Μη Κρατικοί Δρώντες:
 - αναγκαστικά συμπεριλαμβάνονται.
 - απόδοση ευθύνης σε κρατικούς και μη δρώντες.
 - προς το παρόν, δεν μπορούν να διεξάγουν κλασικούς πολέμους, ωστόσο στον κυβερνοχώρο...
- ✓ Η στρατηγική πρώτου – προληπτικού χτυπήματος: πρακτικά αδύνατο να απαγορευθεί στον ή στους αντιπάλους να μην ανταποδώσουν με μια ανάλογη, ή εξίσου μαζική ή μη ανάλογη αντεπίθεση.
- ✓ Η αξία των καθεστώτων συνεργασίας **VS** έμμεση παραχώρηση Κρατικής Κυριαρχίας
- ✓ Κονστρουκτιβισμός: Το διαδίκτυο ως κοινωνικοπολιτικός εξισωτής (equalizer)
- ✓ Οι “Θεωρητικές” αδυναμίες του Κονστρουκτιβισμού: κακόβουλες επιθέσεις μη κρατικών δρώντων εναντίων άλλων κρατικών ή μη κρατικών δρώντων αλλά και εναντίων ιδιωτών.



Κυβερνοχώρος και Προκλήσεις Ασφαλείας

Η Απειλή: η πηγή του Φόβου

Το διαδίκτυο θολώνει τα όρια και τις διαχωριστικές γραμμές των υφιστάμενων κοινωνικών, ηθικών, πολιτικών και οικονομικών θεσπισμάτων.

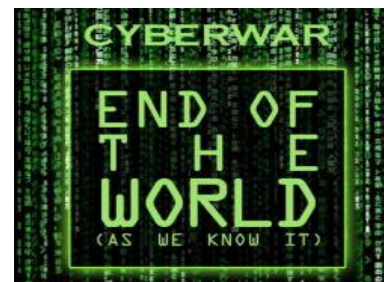
- Τι είναι νόμιμο και τι παράνομο στον κυβερνοχώρο;
- Τι είναι ανεκτό και τι όχι στον κυβερνοχώρο;
- Τι είναι τρομοκρατική και τι εγκληματική διαδικτυακή δράση;
- Τι είναι κυβερνο-έγκλημα και τι κυβερνο-διαμαρτυρία;
- Τι είναι Κυβερνοπόλεμος και τι Κυβερνοειρήνη;
- Πως επαναπροσδιορίζεται η ηθική, η ευημερία, η δημόσια ασφάλεια, η δημοκρατία;
- Πως επαναπροσδιορίζεται η ελευθερία του λόγου, της διακίνησης προσώπων, ιδεών και αγαθών;
- Πως ορίζεται η αλληλεξάρτηση και η ανεξαρτησία;
- Πως προσδιορίζεται η ιδιωτική και η δημόσια σφαίρα;



Cyber Law



Stop Cyber Censorship.
Protect Online Free Speech.



Cyber Peace
Foundation

Η Ισχύς, η Δημοκρατία και η Κυβερνοασφάλεια

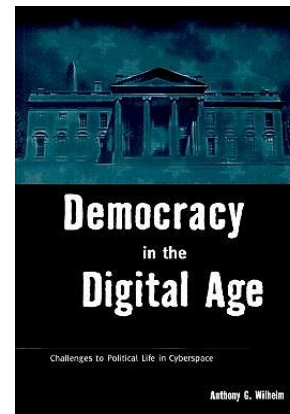
Κυβερνοάμυνα VS Κυβερνοεπίθεση

- ✓ Οι λιγότερο ισχυροί & οι λιγότερο δημοκρατικοί
 - πιο πρόθυμοι να χρησιμοποιήσουν ή να αναπτύξουν κυβερνο-όπλα,
 - πιο πρόθυμοι να εκμεταλλευτούν τα αποτελέσματα κυβερνοεπιθέσεων
- ✓ Οι σχετικά ισχυρότεροι & οι περισσότερο δημοκρατικοί
 - δείχνουν δυσκολία να αποδεχτούν την πρόκληση και να ανταπαντήσουν με όμοιο ή ανάλογο τρόπο.
- ✓ «Μετάβαση από το ξίφος στο πυροβόλο όπλο»
- ✓ Ανοίγει η ατζέντα και θέτει σε νέες βάσεις στα ζητήματα διεθνούς και συλλογικής ασφάλειας (πχ. άρθρο 5 NATO)



“The future is here, it's just not widely distributed yet.”

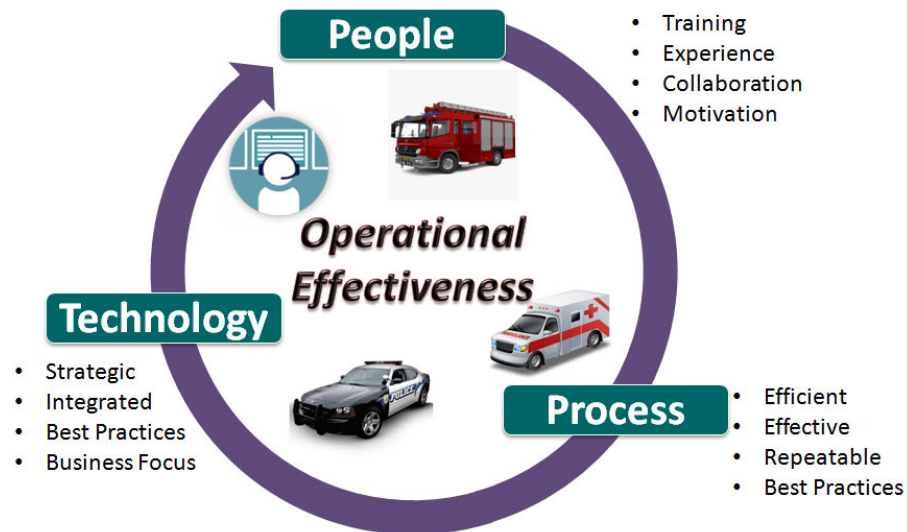
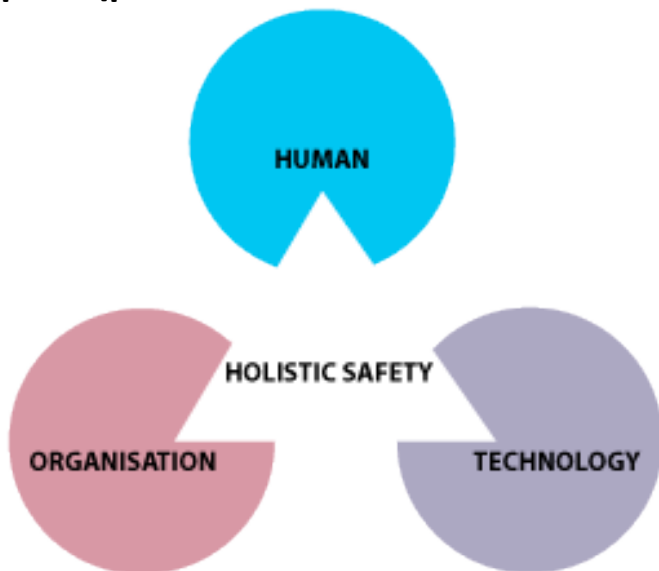
William Gibson (°1948)
Canadian science fiction author,
introduced the term "cyberspace"



Το Ζητούμενο της Κυβερνοασφάλειας και οι Γραμμές Επιχειρησιακής Δράσης

Το Ζητούμενο

- ✓ Η αντιμετώπιση των κυβερνοαπειλών και ο μετριασμός των συνεπειών τους θα πρέπει να έχει χαρακτήρα ολιστικό.



HOLISTIC APPROACH TO SAFETY



PREVENTION:

Inspection
Maintenance
Call Before You Dig
Standards/RPs



MITIGATION:

Leak Detection
Shut-off Valves
Operator Qualifications
Standards/RPs



RESPONSE:

ER Training
Education
Drills & Exercises
Standards/RPs

Το Ζητούμενο της Κυβερνοασφάλειας και οι Γραμμές Επιχειρησιακής Δράσης

Οι Γραμμές Επιχειρησιακής Δράσης

✓ Πολιτική Κατεύθυνση

- θεσμική αναθεώρηση και πολιτική κατοχύρωση,
- ανώτατη διοικητική - ηγετική εκπροσώπηση στην κυβέρνηση,
- ενίσχυση της συμβουλευτικής διαδικασίας και της λογοδοσίας με την συνέργεια όλων των διοικητικών βαθμίδων (ομάδες δράσης, τοπικές κοινότητες, δήμοι, περιφέρειες κλπ).



✓ Οικοδόμηση της Ψηφιακής Ικανότητας (Digital Capacity Building)

- Προώθηση την ευαισθητοποίησης για τους κινδύνους.
- Δημιουργία κατάλληλου εκπαιδευτικού συστήματος.
- Επανακατάρτιση του εργατικού δυναμικού και προσέλκυση επιπλέον εξειδικευμένου.
- Αποκατάσταση περιβάλλοντος ασφαλείας και ενίσχυση της επιχειρηματικότητας ώστε να συμπεριλάβει την έξυπνη διαχείριση των κυβερνοπειλών στα επιχειρηματικά πλάνα της.



Το Ζητούμενο της Κυβερνοασφάλειας και οι Γραμμές Επιχειρησιακής Δράσης

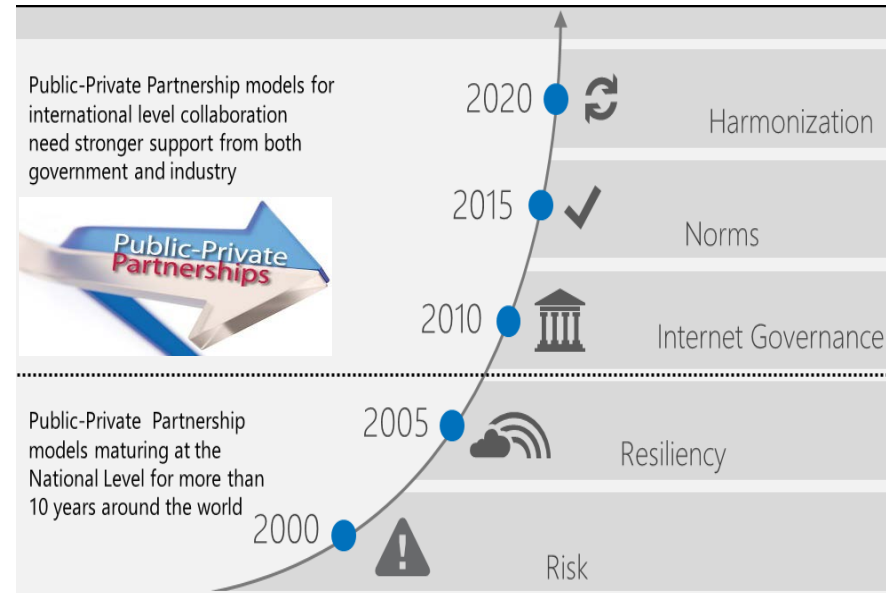
Οι Γραμμές Επιχειρησιακής Δράσης

✓ Σύμπραξη Δημόσιου και Ιδιωτικού Τομέα

- βελτίωσης της εταιρικής σχέσης μεταξύ του ιδιωτικού τομέα και της κυβέρνησης / κράτους (όχι πάντα αθώες πχ SAUDU ARAMCO),
- αξιολόγηση και άρση των δυνητικών φραγμών
- αποκατάσταση αποτελεσματικής συνεργασίας του Κράτους με τη Διεθνή Κοινωνία (Κράτη, ΔΟ, ΜΚΟ, εταιρείες, συλλογικότητες και ιδιώτες)

✓ Αποκατάσταση πλαισίου ανταλλαγής πληροφοριών και απόκρισης σε περιστατικά κυβερνοεπιθέσεων

- δημιουργία πλαισίου δράσης με διαδικασίες ανταλλαγής πληροφοριών, αρμοδιότητες και εξουσιοδοτήσεις
- ενίσχυση της κοινής χρήσης και διαχείρισης πληροφοριών για τη βελτίωση των δυνατοτήτων απόκρισης στις κυβερνοεπιθέσεις
- Στη βελτίωση της παθητικής και ενεργητικής κυβερνοπροστασίας όλων των υποδομών



Το Ζητούμενο της Κυβερνοασφάλειας και οι Γραμμές Επιχειρησιακής Δράσης

Οι Γραμμές Επιχειρησιακής Δράσης

- ✓ **Ενθάρρυνση της καινοτομίας**
 - η διατήρηση της επιχειρηματικής αυτοπεποίθησης αλλά και της εμπιστοσύνης σε αυτή
 - Το Κράτος έχει κάθε συμφέρον να ενισχύσει την τεχνολογική καινοτομία στον ενιαίο τομέα της πληροφορίας και επικοινωνίας
- ✓ **Διαμόρφωση Διεθνούς Νομικού και Ρυθμιστικού Πλαισίου Δικαιωμάτων και Υποχρεώσεων**
 - Εποχή εικονικής Άγριας Δύσης (εθιμικό χτίσιμο δικαίου)
 - Η Σύμβαση της Βουδαπέστης (2001): η πρώτη σοβαρή απόπειρα για το κυβερνο-έγκλημα
 - Απόφ.57/239 του 2003 απαιτεί μεγαλύτερη ευαισθητοποίηση και ευθύνη από ικανά κράτη για την πρόληψη, τον εντοπισμό και την αντιμετώπιση των κυβερνο-απειλών!
 - Ψήφ. 58/199 του 2004 καλεί τα μέλη με εθνικές στρατηγικές για την κυβερνοασφάλεια να βοηθήσουν τα άλλα έθνη να καταρτίσουν παρόμοιες στρατηγικές!



The cyber world is sort of the Wild, Wild West, and to some degree, we're asked to be the sheriff.

— Barack Obama —

A Digital Geneva Convention

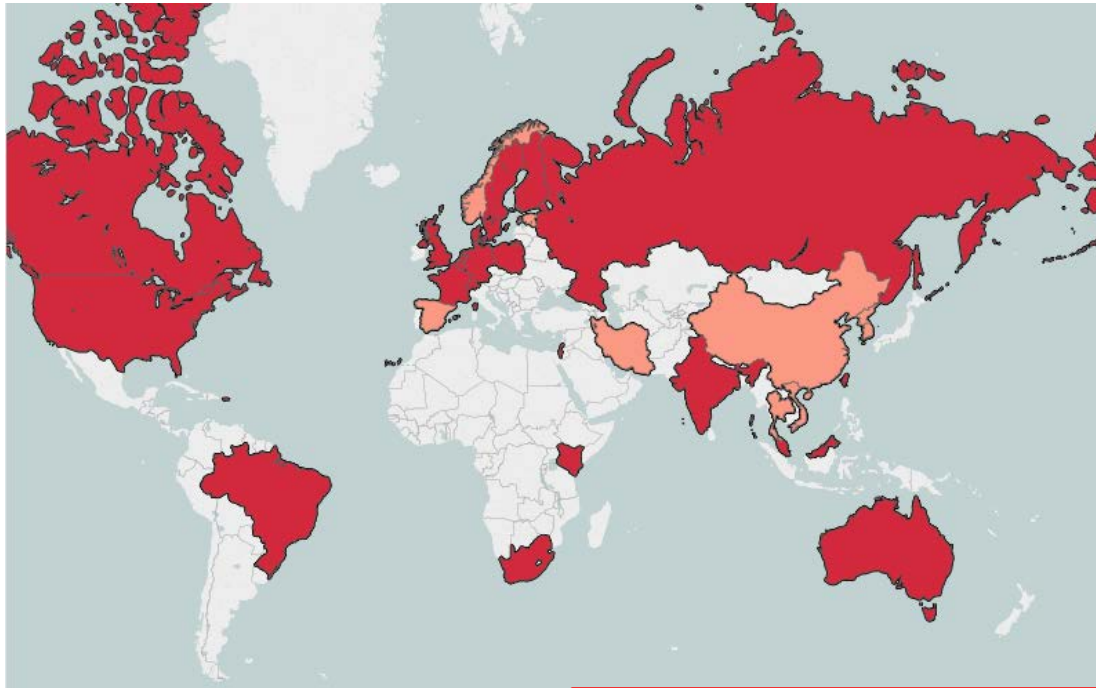
- | | | |
|---|---|--|
| 1. | 2. | 3. |
| No targeting of tech companies, private sector, or critical infrastructure | Assist private sector efforts to detect, contain, respond to, and recover from events | Report vulnerabilities to vendors rather than to stockpile, sell or exploit them |
| 4. | 5. | 6. |
| Exercise restraint in developing cyber weapons and ensure that any developed are limited, precise, and not reusable | Commit to nonproliferation activities to cyberweapons | Limit offensive operation to avoid a mass event |



The United Nations Group of Governmental Experts on Developments (UN GGE) in the Field of Information and Telecommunications

Αρχές υπεύθυνης συμπεριφοράς των κρατών

- Συνεργασία
- Διερεύνηση περιστατικών
- Απαγόρευση χρήσης της επικράτειάς τους
- Ανταλλαγή πληροφοριών
- Σεβασμό αποφάσεων για την προώθηση, προστασία και απόλαυση των ανθρωπίνων δικαιωμάτων στο Διαδίκτυο
- Αποχή από δραστηριότητες που βλάπτουν σκόπιμα ζωτικές υποδομές ή αλλοιώνουν τη χρήση ή λειτουργία τους
- Λήψη μέτρων προστασίας ζωτικών υποδομών
- Ανταπόκριση σε αιτήσεις συνδρομής από άλλα Κράτη
- Διασφάλιση της αλυσίδας εφοδιασμού
- Αναφορά τρωτών σημείων των ΤΠΕ
- Προστασία και χρηστή χρησιμοποίηση των εξουσιοδοτημένων ομάδων αντιμετώπισης καταστάσεων έκτακτης ανάγκης



Recorded Capabilities
■ Offensive capabilities(evidences) - 22 countries
■ Offensive capabilities(indications) - 8 countries

Global Cybersecurity Index ranking 2017

Country	GCI score*	2017 ranking	2015 ranking
Singapore	0.92	1	6
United States	0.91	2	1
Malaysia	0.89	3	3
Oman	0.87	4	3
Estonia	0.84	5	5
Mauritius	0.82	6	9
Australia	0.82	7	3
Georgia	0.81	8	12
France	0.81	9	9
Canada	0.81	10	2

*Normalised





ΠΟΛΙΤΙΚΗ ΔΕΣΜΕΥΣΗ – ΣΥΛΛΟΓΙΚΗ ΑΣΦΑΛΕΙΑ

- 1999: Κοσσυφοπέδιο (Denial of Services, Defacements)
- 2002: Σύνοδος κορυφής στην Πράγα (Cyber Defence Program)
- 2005: Σύνοδος κορυφής στην Ρίγα (Comprehensive Political Guidance)
- 2007: Μαζικές κυβερνοεπιθέσεις στην Εσθονία
- 2008: Σύνοδος κορυφής στο Βουκουρέστι (Policy on Cyber Defence)
- 2010: Σύνοδος κορυφής στη Λισσαβόνα (Strategic Concept)
- 2012: Σύνοδος κορυφής στο Σικάγο (Cyber Defence and Action Plan)

- ✓ Cyber Defence Management Board – CDMB
- ✓ NATO Computer Incident Response Capability - NCIRC
- ✓ Cooperative Cyber Defence Centre of Excellence – CCDCOE
- ✓ Cyber Defense Conferences (MoD)
- ✓ Cyber Defence EX



«Το Βορειοατλαντικό Συμβούλιο διατηρεί την εξουσία να δηλώνει εάν μια επιθέσεις στον κυβερνοχώρο συνιστά «ένοπλη επίθεση» στο πλαίσιο της Βορειοατλαντικής Συνθήκης»

(Ενεργοποίηση Άρθρου 5 περί Συλλογικής Άμυνας)

Ειδικά Θέματα Διεθνών Σχέσεων

ΟΙ ΘΕΩΡΗΣΕΙΣ ΤΩΝ ΔΙΕΘΝΩΝ ΣΧΕΣΕΩΝ & ΤΟ ΠΛΗΡΟΦΟΡΙΑΚΟ ΠΕΡΙΒΑΛΛΟΝ:

Ο Κυβερνοχώρος ως Πεδίο Διεθνούς Ανταγωνισμού Ισχύος

ΠΗΓΕΣ*

Βιβλιογραφία – Αρθρογραφία

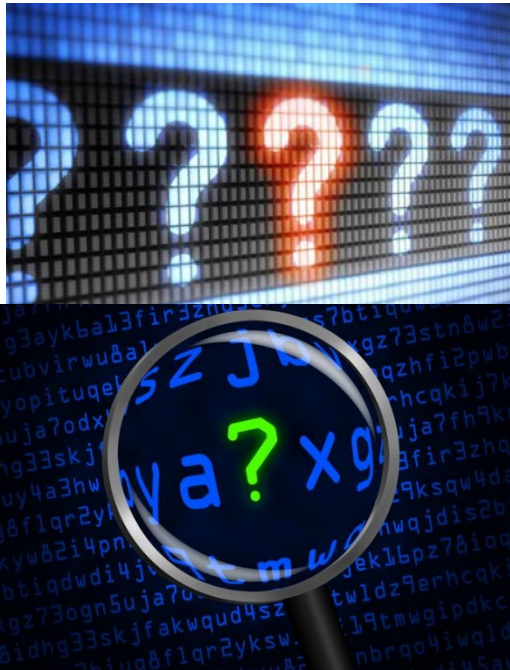
1. George Doukidis, Nikos Mylonopoulos, and Nancy Pouloudi, "Social and Economic Transformation in the Digital Era", Athens, June 2003
2. Bruce R. Guile (Editor), "Information Technologies and Social Transformation", National Academy of Engineering;
3. Melvin Kranzberg, "The Information Age: Evolution or Revolution?", NATIONAL ACADEMY PRESS, Washington D.C. 1985
4. Robert Reardon and Nazli Choucri, "The Role of Cyberspace in International Relations: A View of the Literature", Department of Political Science, MIT, Paper Prepared for the 2012 ISA Annual Convention, San Diego, CA, April 1, 2012
5. Nazli Choucri, "Cyberpolitics in International Relations", The MIT Press, Cambridge, Massachusetts, London, England, 2012
6. Ηλίας Κουσκουβέλης, "Εισαγωγή στις Διεθνείς Σχέσεις, Εκδόσεις Ποιότητα, Ε' Έκδοση, 2007
7. Adams, James, "Virtual Defense" Foreign Affairs Vol. 80, No. 3 (May - Jun., 2001)
8. Johan Sigholm, "NON-STATE ACTORS IN CYBERSPACE OPERATIONS" Captain, Ph.D. Swedish National Defence College
9. Κ. Αντωνόπουλος, Κ. Μαγκλιβέρας, "Το Δίκαιο της Διεθνούς Κοινωνίας", Εμμανουέλα Δούση, "Η Διεθνής Ευθύνη των Κρατών" ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ, Αθήνα, 2017
10. Andrew Radin, Hybrid Warfare in the Baltics, Threats and Potential Responses, RAND Corporation, Santa Monica, Calif. 19 Oct 2015
11. William Gibson, "Neuromancer", edited by Terry Carr, 1984
12. Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations", International Political Science Review / Revue internationale de science politique, Vol. 27, No. 3, Jul 2006
13. Landers, Chris, "Serious Business: Anonymous Takes on Scientology (and Doesn't Afraid of Anything)". Baltimore City Paper, 04 Apr 2008
14. The Department of Defense Cyber Strategy, 17 Apr 2015
15. Karen Rose, Scott Eldridge, Lyman Chapin "The Internet of Things, An Overview Understanding the Issues and Challenges of a More Connected World", The Internet Society (ISOC), 2015

Διαδίκτυο

1. <https://workingmouse.com.au/innovation/digitisation-digitalisation-digital-transformation>
2. <https://sloanreview.mit.edu/article/the-nine-obstacles-to-digital-transformation/>
3. <https://www.sdmmag.com/articles/94274-cyber-reality-how-the-security-industry-is-adjusting-to-the-new-normal>
4. <http://www.inquiriesjournal.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat>
5. https://medium.com/@chris_doman/the-first-sophisticated-cyber-attacks-how-operation-moonlight-maze-made-history-2adb12cc43f7
6. <https://inmoscowshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/>
7. <https://io9.gizmodo.com/could-an-evil-mega-corporation-ever-exist-in-real-life-1630401831>
8. www.mpepil.com
9. <http://opil.ouplaw.com/abstract/10.1093/law/epil/9780199231690/law-9780199231690-e722?rkey=ePM79E&result=1&prd=OPII>
10. <https://www.dhs.gov/publication/2009-cyberspace-policy-review>
11. <https://www.theguardian.com/technology/audio/2016/jul/29/internet-access-human-right-tech-podcast>
12. <https://www.theverge.com/2016/7/4/12092740/un-resolution-condemns-disrupting-internet-access>
13. <http://www.un.org/en/universal-declaration-human-rights/>
14. <https://www.hellenicparliament.gr/UserFiles/f3c70a23-7696-49db-9148-f24dce6a27c8/001-156%20aggljiko.pdf>
15. <https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/>
16. <https://www.computerworld.com/article/2529316/malware-vulnerabilities/mccolo-takedown--internet-vigilantism-or-online-neighborhood-watch-.html>

Φιλμογραφία

1. "Zero Days" A 2016 American documentary film focused on Stuxnet and directed by Alex Gibney. It was selected to compete for the Golden Bear at the 66th Berlin International Film Festival.



Questions

