

An aerial, high-angle view of a city at night, rendered in a dark blue monochrome palette. The buildings are densely packed and their lights are dimly visible, creating a complex geometric pattern of light and shadow. The overall atmosphere is somber and futuristic.

**Cyberwar ante portas :
The role and importance
of national cyber-defense
exercises**

Dimitris Gritzalis

June 2010

Κυβερνοπόλεμος ante portas ...

Ο ρόλος και η σημασία
των εθνικών ασκήσεων Κυβερνοάμυνας

Καθηγητής Δημήτρης Γκριτζαλης (dgrit@aueb.gr, www.cis.aueb.gr)



Διευθυντής Διαπανεπιστημιακής Ερευνητικής Ομάδας
Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών
Τμήμα Πληροφορικής - Οικονομικό Πανεπιστήμιο Αθηνών

Ο απώτατος στόχος...

*“Το να επιτύχεις εκατό νίκες σε εκατό μάχες
δεν είναι το απόγειο της επιτυχίας.
Η καθυπόταξη του στρατού του αντιπάλου
δίχως μάχη,
αυτό είναι το πραγματικό απόγειο της επιτυχίας”*

*Sun Tzu
The Art of War*



Κυβερνοεπίθεση και Κυβερνοπόλεμος

Κυβερνοεπίθεση ονομάζεται κάθε μη σύννομη πράξη, που διαπράττεται μέσω της χρήσης ΤΠΕ, προικλώντας τη διακοπή ή υποβάθμιση της παροχής υπηρεσιών, με σκοπό την πρόκληση ανησυχίας, σύγχυσης και αβεβαιότητας και στόχο να επηρεάσει τις Αρχές ή τον πληθυσμό και να τους αναγκάσει να προσαρμοσθούν σε συγκεκριμένες πολιτικές, κοινωνικές ή ιδεολογικές επιδιώξεις.

Κυβερνοπόλεμος είναι η χρήση ΤΠΕ και ειδικά του διαδικτύου για τη διεξαγωγή πολέμου στον κυβερνοχώρο, που κηρύσσεται με βάση πρωτόκολλο αξιολόγησης συγκεκριμένων κυβερνοεπιθέσεων ως πράξεων πολέμου και διεξάγεται μέσω κυβερνοεπιθέσεων/κυβερνοάμυνας.

Αλληλεξαρτήσεις και δικτυώματα



Ρόλος του Κράτους: Ποιός και γιατί;

Ρόλος;

- Προστασία κρατικών υποδομών
- Στοχευμένη χρηματοδότηση Ε&ΤΑ
- Άμυνα σε ειδικές επιθέσεις κλίμακας (DDOS, malware)
- Δράσεις ευαισθητοποίησης, πρόληψης και προετοιμασίας.

Γιατί;

- Διαθέτει τους αναγκαίους αυξημένους πόρους
- Μπορεί να επιστρατεύσει υψηλή τεχνογνωσία
- Νομιμοποιείται να δράσει συντονιστικά, σε εθνικό επίπεδο
- Νομιμοποιείται να δράσει συνεργατικά, σε διεθνές επίπεδο

Εθνικές ασκήσεις Κυβερνοάμυνας

Οι πιθανές συνέπειες ενός κυβερνοπολέμου καθιστούν αναγκαία την έγκαιρη προετοιμασία, σε εθνική κλίμακα.

Μέρος της προετοιμασίας αποτελούν και οι **εθνικές ασκήσεις Κυβερνοάμυνας**, με στόχο:

- ✓ **Ευαισθητοποίηση** της κοινής γνώμης στις πραγματικές διαστάσεις του φαινομένου, χωρίς υπερβολές, ούτε απλουστεύσεις.
- ✓ **Εκπαίδευση** του προσωπικού των φορέων, ώστε να είναι σε θέση να **εντοπίσουν** έγκαιρα και να **περιορίσουν** μια κυβερνοεπίθεση ενάντια στην υποδομή τους.
- ✓ **Βελτίωση** του **συντονισμού**, της **επικοινωνίας** και της **συνεργασίας** μεταξύ των αρμόδιων φορέων και υπηρεσιών.
- ✓ **Αξιολόγηση** του **στρατηγικού σχεδίου** εντοπισμού και αντιμετώπισης κυβερνοαπειλών.

Διεθνής εμπειρία σε ασκήσεις

ΗΠΑ:

Εμπειρία: Διεξαγωγή δύο ασκήσεων κυβερνοάμυνας (Cyberstorm I και Cyberstorm II).

Cyberstorm III (2010): Διεθνής, με συμμετοχή δημοσίων και ιδιωτικών φορέων από ΗΠΑ, Αυστραλία, Νέα Ζηλανδία, Καναδά και Ενωμένο Βασίλειο.

Cyber Shockwave (2010): Οργάνωση από μη κυβερνητικό φορέα (Bipartisan Policy Center).

Κυβερνοχώρος: Το 5^ο πεδίο επιχειρήσεων (Στρατός, Ναυτικό, Αεροπορία, Διάστημα, Κυβερνοχώρος).

NATO:

NCDEX '08 και NCDEX '09: Διεξαγωγή δύο ασκήσεων κυβερνοάμυνας (συμμετείχε η Ελλάδα).

NCDEX '10: Προετοιμάζεται για τα τέλη του 2010.

Αρχές και όροι συνεργασίας

Μια αποτελεσματική εθνική άσκηση Κυβερνοάμυνας θα πρέπει να βασίζεται στις εξής κομβικές αρχές και όρους:

1. **Αλληλεγγύη** των συμμετεχόντων φορέων
(στόχος η επίτευξη συνεργειών, χωρίς ανταγωνισμούς υπηρεσιών)
2. **Ανοιχτές-συμμετοχικές** διαδικασίες
(αξιοποίηση όλων των ανθρώπινων πόρων, χωρίς αποκλεισμούς, χωρίς εσωστρεφείς-επιλεκτικές πολιτικές)
3. **Πολύδρομη** επικοινωνία και συνδρομή
(όλοι συνεισφέρουν σε όλους, όχι μονόδρομες συνδρομές)



1^η εθνική άσκηση κυβερνοάμυνας

ΠΑΝΟΠΤΗΣ - 2010

18-20 Μάη 2010

Συντονισμός: Διεύθυνση Κυβερνοάμυνας
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)

Πρόσκληση συμμετοχής διαβιβάστηκε σε όλα Υπουργεία και σε άλλους φορείς

Αποδοχή συμμετοχής: Υπουργείο Εσωτερικών, Αποιέντρωσης και Ηλεκ/κής Διακ/σης
(15.03.2010) Υπουργείο Εξωτερικών
Υπουργείο Οικονομικών
Υπουργείο Μεταφορών, Υποδομών και Δικτύων
Υπουργείο Προστασίας του Πολίτη
Πανεπιστήμια (12) και ΤΕΙ (3)
Ερευνητικά Ιδρύματα (ΕΑΙΤΥ, ΙΤΕ)
Ανεξάρτητες Αρχές (ΑΔΑΕ, ΑΠΠΔ)
Τεχνικό Επιμελητήριο Ελλάδας (ΤΕΕ)



ΠΑΝΟΠΤΗΣ 2010

1^η Εθνική Άσκηση Κυβερνοάμυνας

18-20 Μαΐη 2010

Ομάδα Ακαδημαϊκών και Ερευνητικών Ιδρυμάτων
Συντονιστής: Καθ. Δημήτρης Γκριτζαλης (ΟΠΑ)



References

1. Denault, M., Gritzalis, D., Karagiannis, D., Spirakis, P., "Intrusion detection: Evaluation and performance issues of the SECURENET system", *Computers & Security*, Vol. 13, No. 6, pp. 495-508, 1994.
2. Doumas, A., Mavroudakos, K., Gritzalis, D., Katsikas, S., "Design of a neural network for recognition and classification of computer viruses", *Computers & Security*, Vol. 14, No. 5, pp. 435-448, 1995.
3. Dritsas, S., Tsoumas, B., Dritsou, V., Konstantopoulos, P., Gritzalis, D., "OntoSPIT: SPIT Management through Ontologies", *Computer Communications*, Vol. 32, No. 2, pp. 203-212, 2009.
4. Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., Gritzalis, D., "An Insider Threat Prediction Model", *Proc. of the 7th International Conference on Trust, Privacy, and Security in Digital Business*, pp. 26-37, Springer, Spain, 2010.
5. Katsikas, S., Spyrou, T., Gritzalis, D., Darzentas, J., "Model for network behaviour under viral attack", *Computer Communications*, Vol. 19, No. 2, pp. 124-132, 1996.
6. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk-based criticality analysis", in *Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection*, pp. 35-49, Springer, USA, 2009.
7. Theoharidou M., Stougiannou E., Gritzalis D., "A CBK for Information Security and Critical Infrastructure Protection", in *Proc. of the 5th IFIP Conference on Information Security Education*, pp. 49-56, Springer, USA, 2007.
8. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Risk assessment methodology for interdependent critical infrastructures", *International Journal of Risk Assessment and Management*, Vol. 15, Nos. 2/3, pp. 128-148, 2011 (to appear).
9. Tsoumas, B., Gritzalis, D., "Towards an ontology-based security management", *Proc. of the 20th International IEEE Conference on Advanced Information Networking and Applications*, pp. 985-990, IEEE, Austria 2006.
10. Virvilis, N., Dritsas, S., Gritzalis, D., "Secure Cloud Storage: Available Infrastructure and Architecture Review and Evaluation", *Proc. of the 8th International Conference on Trust, Privacy & Security in Digital Business*, pp. 74-85, Springer, France 2011.
11. Virvilis, N., Dritsas, S., Gritzalis, D., "A cloud provider-agnostic secure storage protocol", *Proc. of the 5th International Workshop on Critical Information Infrastructure Security*, pp. 104-115, Springer, Greece 2010.