Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

KYBERNETICKÁ BEZPEČNOST

BSS469

Základní informace

- Přednášející: pracovníci Národního úřadu pro kybernetickou a informační bezpečnost a FSS MU
- CO JE NÚKIB https://www.govcert.cz/
- Místnost a čas: Út 10:00--11:40 U43

Cíle kurzu

- úvodní seznámení s problematikou kybernetické bezpečnosti
- teorie, historie, případové studie a částečně také technické aspekty
- osvojení praktických informací od pracovníků NÚKIB

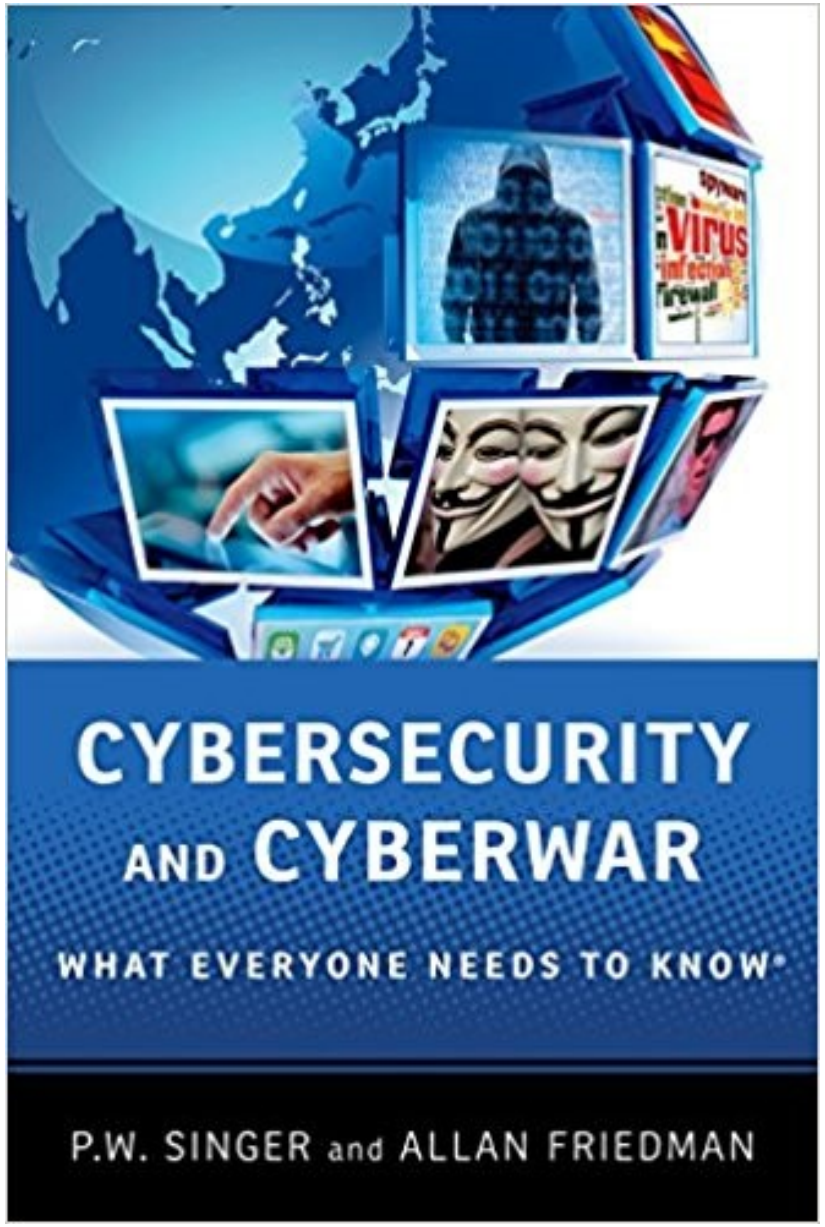
2. KONCEPTUÁLNÍ A TEORETICKÉ ASPEKTY KYBERNETICKÉ BEZPEČNOSTI - 25. 9

PŘEDNÁŠEJÍCÍ: PhDr. Roman Pačka

- Úvod do kyberprostoru a způsob jeho fungování.
- Kybernetické útoky: základní terminologie a aktuální trendy.
- Co je kybernetická bezpečnost? Proč je kybernetická bezpečnost dnes tak významná?
- Konceptuální vymezení kybernetické bezpečnosti a kybernetické obrany
- Tvorba kybernetické bezpečnostní politiky
- Role a funkce státu v zajišťování kybernetické bezpečnosti

Povinná četba:

- SINGER, P.W. a Allan FRIEDMAN. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014. **s. 67 – 166**. Dostupné z: https://goo.gl/S5iF3C
- PAČKA, Roman. Role státu v zajišťování kybernetické bezpečnosti. *Bezpečnostní teorie a praxe*. Praha: Policejní akademie České republiky v Praze, 2015(3), **s. 93 - 110**.



- v knihovně na FSS i MZK

3. BEZPEČNÉ POUŽÍVÁNÍ ICT – 9. 10

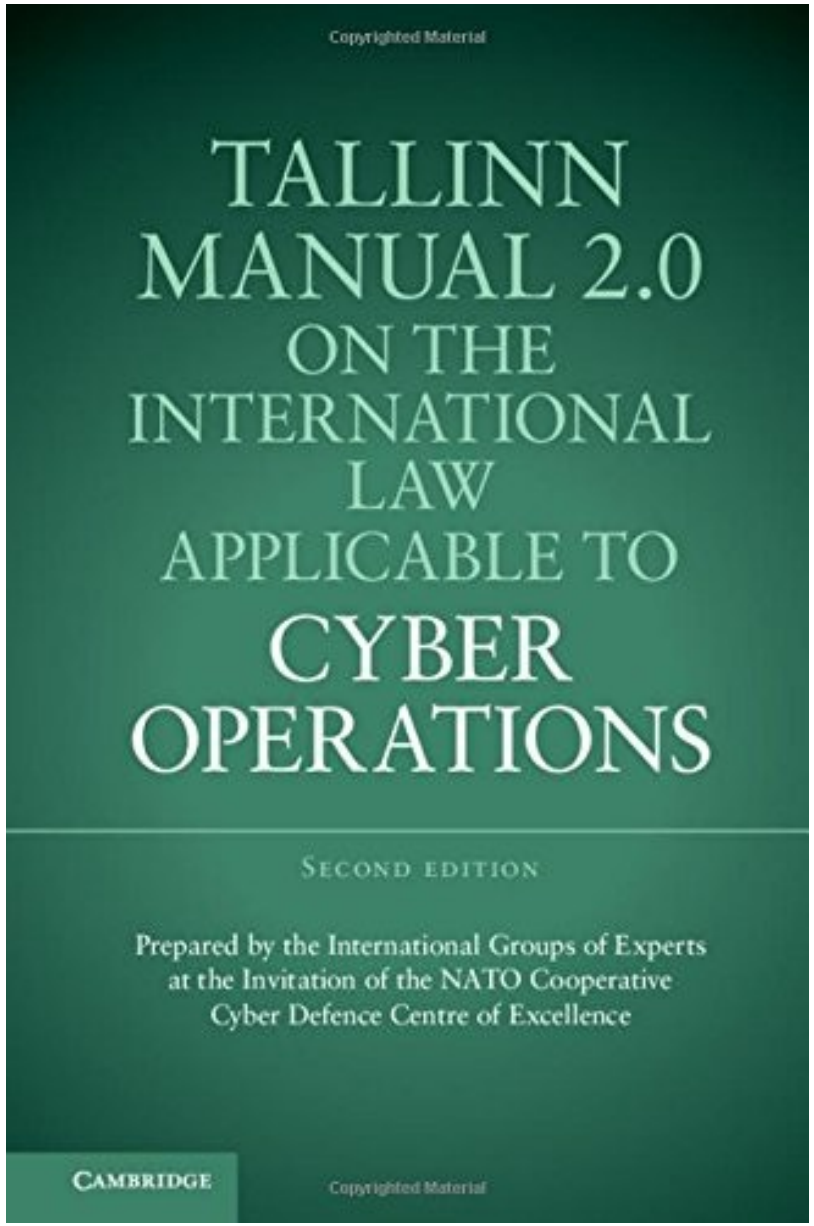
- **PŘEDNÁŠEJÍCÍ: Mgr. Bc. Jakub Melichar**
- Kritéria bezpečnosti dat
- Prvky zabezpečení počítače a mobilních zařízení
- Bezpečnost elektronické komunikace
- Bezpečné používání webu
- Hrozby a rizika používání ICT

4. MEZINÁRODNÍ PRÁVO OPERACÍ V KYBERPROSTORU - 16. 10.

- **PŘEDNÁŠEJÍCÍ: Mgr. David Komárek**
- Úvod do mezinárodního práva veřejného
- Suverenita a Due diligence v kyberprostoru
- Kybernetické operace v době míru
- Protiopatření, plea of necessity, sebeobrana, atribuce
- Použití síly kybernetickými prostředky

Povinná četba:

- SCHMITT, Michael N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press. 2017. ISBN: 978-1316630372. Kapitoly **1,2, 4 a 14 (154 s.)**


Copyrighted Material
TALLINN MANUAL 2.0
ON THE INTERNATIONAL LAW APPLICABLE TO
CYBER OPERATIONS
SECOND EDITION
Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence
CAMBRIDGE
Copyrighted Material

5. ROLE CERT/CSIRT V SYSTÉMU ZAJIŠŤOVÁNÍ NÁRODNÍ BEZPEČNOSTI – 23. 10.

- **PŘEDNÁŠEJÍCÍ: PhDr. Roman Pačka**
- Historie CERT/CSIRT
- Typologie CERT/CSIRT
- Funkce a role CERT/CSIRT v systému zajišťování národní bezpečnosti
- Kultura CERT komunity a aktuální výzvy
- Případová studie České republiky

Povinná četba:

- MORGUS, Robert, Isabel SKIERKA, Mirko HOHMANN a Tim MAURER. *National CSIRTs and Their Role in Computer Security Incident Response*. Tallin: CCDCOE, 2015. **34 s**. Dostupné také z: https://bit.ly/2BDskCP
- http://www.cert.org/

6. KYBERNETICKÁ OBRANA A PREDIKCE VÝVOJE OPERAČNÍHO PROSTŘEDÍ – 30. 10.

PŘEDNÁŠEJÍCÍ: PhDr. Roman Pačka

- Historický vývoj operačního prostředí
- Konceptualizace kybernetické obrany
- Cyber a Information Warfare (CW a IW)
- Charakter současných a budoucích ozbrojených konfliktů
- Predikce požadavků na ozbrojené síly na taktické, operační a strategické úrovni

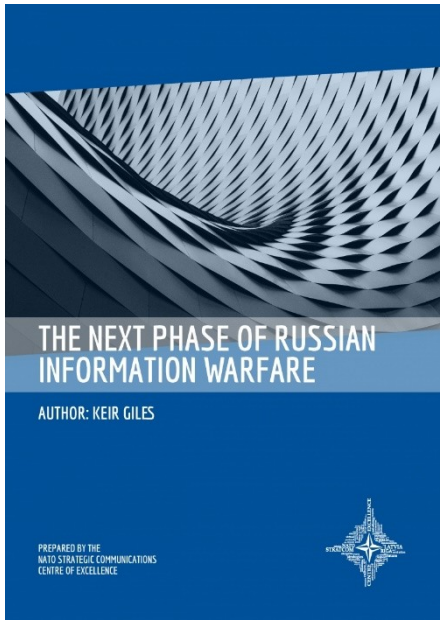
Povinná četba:

DEWAR, Robert S. *Active Cyber Defense*. Zürich: Center for Security Studies (CSS), ETH Zürich, 2017. **23 s**. Dostupné také z: https://bit.ly/2O5LlRy

7. PROPAGANDA A INFORMAČNÍ VÁLKA – 6. 11.

PŘEDNÁŠEJÍCÍ: Mgr. Miroslava Pavlíková

- Současné teoretické přístupy k výzkumu IW
- Způsoby a metody manipulace s informacemi
- Ruská informační válka



Povinná četba:

- GILES, Kier. *The Next Phase of Russian Information Warfare*. NATO STRATCOM, 2016. 16. s. Dostupné z: https://bit.ly/2Nxk5hQ

8. KYBERTERORISMUS - 13. 11.

PŘEDNÁŠEJÍCÍ: Michaela Semecká, M.A.

- Kyberterorismus jako hypotetický fenomén?
- Jak velká je dnešní hrozba kyberterorismu?
- Případová studie *Daeš*
- Reakce a opatření

Povinná četba:

- DRMOLA, Jakub. Konceptualizace kyberterorismu. *Vojenské rozhledy*, roč. 22 (54), č. 2, 2013. s. **94–102**, ISSN 1210-3292.

9. PRAKTICKÁ UKÁZKA: EXKURZE NA NCKB, adresa: Mučednická 31, Brno – 15. 11. (začátek od 9:00 - 10:45)

- **POVEDE: Ing. Miriam Sedláčková, Mgr. Veronika Netolická**
- Národní autorita KB a struktura NCKB
- Strategický a organizační rámec kybernetické bezpečnosti v ČR
- Představení činnosti a kompetencí GovCERT a Odboru kybernetických bezpečnostních politik
- Mezinárodní spolupráce při zajišťování kybernetické bezpečnosti (nejdůležitější organizace a hráči na poli zajišťování kybernetické bezpečnosti)

Povinná četba:

- *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020*. NCKB, 2015. **35 s**. Dostupné z: https://bit.ly/2CyK4RS
- *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020*. 2015, **24 s**. Dostupné také z: https://bit.ly/2wT618j
- Co je NÚKIB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. 2018 [cit. 2018-09-08]. Dostupné z: https://www.govcert.cz/cs/
- *Zpráva o stavu kybernetické bezpečnosti 2017*, **49 s**. Dostupné také z: https://goo.gl/4zzxdj

10. PŘÍSTUPY K ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI: „THE WEST VERSUS THE REST“? – 20. 11.

PŘEDNÁŠEJÍCÍ: Ondřej Rojčík, Ph.D., MSc.

- *Internet Governance* jako kolbiště pro střet různých pojetí kybernetické bezpečnosti
- Komparace a přehled přístupů ke kybernetické bezpečnosti hlavních globálních aktérů: USA, EU, Rusko a Čína.
- V čem se jejich přístupy liší? Jaké jsou mezinárodně-bezpečnostní implikace těchto odlišností?
- Je možné najít shodu a vytvořit mezinárodní systém dohledu nad kyberprostorem?

Povinná četba:

- GILES, Keir, ZIOLKOWSKI, K., C CZOSSECK a R. OTTIS, ed. *Russia's Public Stance on Cyberspace Issues*. NATO CCD COE Publications, Tallinn: 4th International Conference on Cyber Conflict, 2012, **13 s**. Dostupné z: https://bit.ly/2wVvm2e
- CHANG, Amy. *Warring State: China's Cybersecurity Strategy*. Centrum for New American Security, 2014, **43 s**. Dostupné také z: https://bit.ly/2Me1xyC

11. ZAJIŠŤOVÁNÍ KYBERNETICKÉ BEZPEČNOSTI VOLEB A VOLEBNÍHO PROCESU - 27. 11.

PŘEDNÁŠEJÍCÍ: Mgr. Petr Novotný

- Vztah kybernetické bezpečnosti a voleb v moderní společnosti
- Jak je možné narušit nebo ovlivnit volby a jejich výsledek akcemi v kybernetickém prostoru?
- Významné případy narušení kybernetické bezpečnosti voleb a volebního procesu ve světě
- Jakým způsobem je vytvrzován proces voleb z pohledu kybernetické bezpečnosti v České republice?

Povinná četba:

- United States of America. *Criminal no. 18 u.s.c. §§ 2, 371, 1030, 1028a, 1956, and 3551 et seq*. In the United States district court for the district of Columbia, 2018. 29 s. Dostupné z: https://www.justice.gov/file/1080281/download
- BRATTBERG, Erik a Tim MAURER. Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks. In: *Carnegie Endowment for International Peace* [online]. 23. 5. 2018 [cit. 2018-09-08]. Dostupné z: https://bit.ly/2QdjD6Z

12. TABLE-TOP CVIČENÍ – 4. 12.

- **POVEDOU: Mgr. Alena Leciánová, Mgr. Kateřina Hábová, Mgr. Veronika Netolická**
- Vyhodnocení před hodinou 11. 12. 2018

Povinná četba:

- HEALEY, Jason a Klara TOTHOVA JORDAN. *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*. BRENT CENTER ON INTERNATIONAL SECURITY: Atlantic Council, 2014, 9 s. Dostupné z: https://bit.ly/1lLFa5U
- SINGER, P.W. a Allan FRIEDMAN. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2014. **s. 247- 257**. Dostupné z: https://goo.gl/S5iF3C

13. VZNIK MEZINÁRODNÍHO REŽIMU PRO KYBERNETICKOU BEZPEČNOST – 11. 12.

- **PŘEDNÁŠEJÍCÍ: Jakub Otčenášek, MA., MSc.**
- Úvod do problematiky normotvorby v kyberprostoru
- Přednáška formou řízené diskuze (Oxbridge formát)

Povinná četba:

- Bude doplněna, aby diskuze probíhala nad aktuálními texty.

14. PŘEDTERMÍN ZÁVĚREČNÉHO PÍSEMNÉHO PŘEZKOUŠENÍ – 18.12.

HODNOCENÍ

- SEMINÁRNÍ PRÁCE **(25)**
- ZÁVĚREČNÉ PÍSEMNÉ PŘEZKOUŠENÍ **(25)**
- TABLE-TOP CVIČENÍ

Hodnocení

- 50 – 46 b A
- 45 – 41 B
- 40 – 36 C
- 35 – 31 D
- 30 – 26 E
- 25 a méně F

SEMINÁRNÍ PRÁCE

- měla by být textem odborně reflektujícím aktuální témata kybernetické či informační bezpečnosti
- doporučovaný rozsah seminární práce je **10 normostran**
- maximální dosažený počet bodů za seminární práci je **25**
- Hodnocena bude schopnost vědecké argumentace, využití teorií souvisejících s kurzem a bezpečnostními studiemi, stejně jako relevance závěrů.
- Úvod-cíle práce-metodologie-teoretická část-praktická/analytická část-závěr.
- Varianty témat seminární práce budou

a) předem zadané (návrhy v IS ve studijních materiálech) nebo

b) b) dobrovolné na základě předchozího schválení vyučujícím.

Témata seminárních prací musí být nahlášena do **9. 10. 2018** na e-mail pavlikova.myrka@gmail.com. Termín odevzdání seminární práce je **8.1.2019**.