Kübersõda –mis see on?

Foorum “Rahvuslikust Julgeolekust”

04.12.2009 Tallinn

Johannes Kert

Teema käsitlus

- Küberründed internetis.
- Kas me tunneme ära tänapäeva sõja?
- Internet kui lahinguväli.
- Sõjalis strateegiline komplekssus ja küberelv.
- Kuidas kaitsta?

Küberründed internetis

- Kriminaalsel motiivil toimuvad küberründed
- Huligaansel motiivil toimuvad küberründed
- Poliitilisel motiivil toimuvad küberründed

Kas me tunneme ära tänapäeva sõja?

- Sõda kui poliitika jätkamine teiste vahenditega.
- Sõja eesmärgid.
- Millal sõda algab?
- Kombinatsioonid.

Internet kui lahinguväli.

- * Kübersõda võib olla konventsionaalse sõja osa (nt. vastase radarisüsteemide pimedaks löömine enne lennuväerünnakut, operatiivse tulekasutuse vahend kombinatsioonis konventsionaalsete vahenditega).
- -informatsioonisõja vahend.
- -eraldiseisev fenomen (toimub ainult võrgu kaudu ja IT sihtmärkide vastu).

Internet kui lahinguväli.

- Mitmed riigid on tõsiselt kübersõja võimekuse loomisesse investeerinud.
  Kui need riigid peaksid omavahel sõtta minema, siis näeme ka esimese
  suure kübersõja ära. Varem hoitakse seda võimekust tõenäoliselt reservis, või siis teostatakse n.ö. “luuret lahinguga”.

- Kübersõjas ei loe arvuline ülekaal, geograafiline positsioon ega
  sõjandus-majanduslik võimsus, sest see on iseloomult asümmeetriline.

Internet kui lahinguväli

- Küberrünnete vastu ei ole hetkel töötavat heidutust (deterrence).
- Küberkonflikti osapooled saavad kasutada tsiviilinfrast "inimkilpi"
  ning viia ründeid läbi neutraalsete riikide territooriumilt.
- Kübersõja ohtlikkus seisneb selles, et tänapäeval on võrku ühendatud energia-, kommunikatsiooni-, transpordi- (nt. lennujuhid) ja muude kriitilise infrastruktuuri elementide süsteemid. Kõik need on potentsiaalsed sihtmärgid totaalses sõjas.

Sõjalis strateegiline komplekssus ja küberrelv

- Kahekümnenda sajandi uus väeliik õhuvägi.
- Kas 21.sajandi uus väeliik või vähemalt relvaliik küber?
- Oleksime naiivsed arvates et vastane häbeneks oma poliitiliste eesmärkide saavutamiseks rünnata tsiviil IT infrastruktuuri kübersõja vahenditega. Seda kasutataks seda enam põhjusel et rahvusvahelised lepped sõjaõiguses antud valdkonda seni veel ei käsitle. Kübersõja võimaluste spekter leiaks laialdast kasutust just üleüldise segaduse ja paanika tekitamiseks, tsiviilühiskonna kaitsetahte murdmiseks, teenuste ning tööstuse saboteerimiseks. 2007 aasta aprillisündmused Eestis ja hiljem mujal Ida Euroopas on selgelt näidanud poliitiliselt motiveeritud info, aga ka sõjalisi elemente sisaldavate operatsioonide(poliitika jätkamine teiste vahenditega) kiiret evolutsiooni komplekssuse ja järjest parema orkestreerituse suunas.

Kuidas kaitsta?

- Korralikult ettevalmistatud ja tegutsemisvalmis küberkaitseüksus omab moodsates sõjalistes operatsioonides kriitilist tähtsust.
- Küberkaitse üksus on küll ainult üks element kübervõrkude operatsioonides (kübersõjas või kübersõja elementidega kombineeritud kas siis moodsas konventsionaalses, -irregulaarses sõjalises või informatsiooni operatsioonis).
- Sõjaliste või/ja eriorganisatsioonide poolt läbi viidavate võrgupõhiste või kübersõja elementidega kombineeritud operatsioonide korral kerkib küberkaitse tähtsaimaks prioriteediks.
- Nakatatud kübervõrk aeglustab dramaatiliselt operatiivtempot, võimaldades vastasel dikteerida oma rütm lahinguväljal ja haarata initsiatiiv.
- Nakatatud võrk muutub vastase efektiivseks relvaks mille kaudu nad saavad otseselt mõjutada meie ja meie liitlaste operatsioone. Parem on sel juhul mitte omada võrku ja võrgupõhist (ennast viimsete aastakümnete kõige efektiivsema sõjalise saavutusena näidanud) juhtimissüsteemi kui sõltuda nakatatud võrgust. **Kirjeldatud sõjaliste operatsioonide kohta kehtiv loogika on lihtsalt laiendatav ka tänapäeva tsiviilühiskonnale kus võrguteenuste kasutamisest on saanud elulaad.**

Kuidas kaitsta?

- Küberjulgeoleku strateegia ja selle rakendamine.
- Kriitilise tähtsusega koostöö organiseerimine.
- Küberkaitselise hariduse arendamine eestis.
- Treeningu ja harjutuste keskkonna arendamine

Kuidas kaitsta?

- Eesti CERT
- NATO küberkaitse oivakeskus.
- Küberkaitse üksused kaitseliidus KKL.

Kuidas kaitsta?.... KKL!?

- Võrgu julgeoleku tagamine
- Võrgu monitooring
- Ebatavaliste nähtuste/käitumise ja rünnete tuvastamine
- Rünnete analüüs ja vastumeetmete väljatöötamine/pakkumine.
- Parimate valitud vastumeetmete rakendamine.
- Küberkaitsealane teavitamine ja küberkaitse protseduuride ja meetodite täiustamine.
- Treeningute ja õppuste organiseerimine oma liikmetele ja osalemine rahvusvahelistel õppustel (NATO, EL riigid)
- Hoolitsemine järelkasvu eest. Noori motiveeriva vastava mängu ja võistluskeskkonna loomine ning arendamine.
- Oma liikmetele ja nende kaudu riigikaitse terviku tutvustamine ning kaitsetahte kujundamine.

Tänan tähelepanu eest!

Valmis küsimusteks.