# Summaria Europensia 2/2013

Käesoleva Summaria Europensia teemaks on küberjulgeolek.

Koostanud Giina Kaskla, ettepanekud ja tagasiside Giina.Kaskla@nlib.ee

**Märksõnad:** küberjulgeolek, küberkaitse, küberturve, Euroopa Liit, rahvusvaheline õigus

Nimestik sisaldab Rahvusraamatukogus ja teistes Eesti raamatukogudes leiduvaid väljaandeid ja võrguteavikuid ning teadusajakirjade artikleid, millele on juurdepääs Rahvusraamatukogu võrgus.

Referaatväljaanne kajastab teemakohast infot seisuga juuni 2013.

## SISUKORD

# 1. Sissejuhatus

Veebruaris 2013 avaldas Euroopa Komisjon koos liidu välisasjade ja julgeolekupoliitika kõrge esindajaga Euroopa Liidu küberturbe strateegia „Avatud ohutu ja turvaline küberruum" ning direktiiviettepaneku võrgu- ja infoturbe kohta.

Strateegia kajastab ELi küberturbe prioriteete: kübervastupanuvõime saavutamist; küberkuritegevuse vähendamist; küberkaitsepoliitika väljatöötamist ja selle seostamist ühise julgeoleku- ja kaitsepoliitikaga; küberturbeks vajaliku tehnoloogia ja tööstuse arendamist; rahvusvahelises küberruumipoliitikas osalemist ja Euroopa Liidu põhiväärtuste edendamist.

Strateegia näeb ette konkreetsed tegevused, et parandada liikmesriikide ja Komisjoni vahelist küberturbe alast koordineeritud koostööd, tulemuslikult võidelda küberkuritegevusega ja tõhustada elutähtsate infrastruktuuride kaitset.

Küberturbe strateegia esitab tervikliku visiooni sellest, kuidas kaitsta ja tagada turvalisus küberruumis ning rõhutab Euroopa vabaduse ja demokraatia väärtuste edendamise olulisust küberpoliitika kontekstis.

Allikas: EL kaitseb avatud internetti ning internetivabadust ja -võimalusi, Euroopa Komisjoni pressiteade, 2. veebruar 2013
http://europa.eu/rapid/press-release_IP-13-94_et.htm

# 2. Euroopa Liidu poliitika

## 2.1. Euroopa Liidu dokumendid

Euroopa Parlamendi raport 19. juunist 2013 „Ettepanek võtta vastu Euroopa Parlamendi ja nõukogu direktiiv, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega tunnistatakse kehtetuks nõukogu raamotsus 2005/222/JSK"
(KOM(2010)0517 – C7-0293/2010 – 2010/0273(COD))
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2013-0224+0+DOC+XML+V0//ET

Komisjoni 7. veebruri 2013. aasta ettepanek: Euroopa Parlamendi ja nõukogu direktiiv meetmete kohta, millega tagada võrgu- ja infoturbe ühtlaselt kõrge tase kogu Euroopa Liidus, COM(2013) 48 final
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52013PC0048:ET:NOT

7. veebruri 2013. aasta ühisteatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- Ja Sotsiaalkomiteele ning Regioonide Komiteele „Euroopa Liidu küberjulgeoleku strateegia: avatud, ohutu ja turvaline küberruum", JOIN(2013) 1 final
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:ET:PDF

Euroopa Parlamendi 22. novembri 2012. aasta resolutsioon küberjulgeoleku ja -kaitse kohta, P7_TA(2012)0457
http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0457&language=ET&ring=A7-2012-0335

Euroopa Parlamendi raport 17. oktoobrist 2012 „Küberjulgeolek ja -kaitse" A7-0335/2012. Raportöör: Tunne Kelam
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2012-0335+0+DOC+XML+V0//ET

Euroopa Parlamendi menetlustoimik „Cyber security and defence" INI 2012/2096
http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2012/2096(INI)&l=en

Komisjoni 31. märtsi 2011. aasta teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele elutähtsate infoinfrastruktuuride kaitse kohta „Saavutused ja edasised sammud: üleilmse küberjulgeoleku suunas", KOM(2011) 163 lõplik
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011DC0163:ET:NOT

Komisjoni 22. novembri 2010. aasta teatis Euroopa Parlamendile ja nõukogule "ELi sisejulgeoleku strateegia toimimine: viis sammu turvalisema Euroopa suunas", KOM(2010) 673 lõplik
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0673:ET:NOT

Komisjoni 30. septembri 2010. aasta ettepanek: Euroopa Parlamendi ja Nõukogu direktiiv, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega tunnistatakse kehtetuks nõukogu raamotsus 2005/222/JSK, KOM(2010) 517 lõplik
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010PC0517:ET:NOT

Komisjoni 19. mai 2010. aasta teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Euroopa digitaalne tegevuskava.", KOM(2010)245 lõplik
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245:ET:NOT

Komisjoni 20. aprilli 2010. aasta teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ja Regioonide Komiteele – Vabadusel, turvalisusel ja õigusel rajanev ala Euroopa kodanikele Stockholmi programmi rakendamise tegevuskava, KOM(2010) 171 lõplik
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0171:ET:NOT

Komisjoni 22. mai 2007. aasta teatis Euroopa Parlamendile, nõukogule ja Regioonide Komiteele - Küberkuritegevuse vastase võitluse üldise poliitika kujundamine {SEK(2007) 641} {SEK(2007) 642}, KOM/2007/0267 lõplik
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0267:ET:NOT

Komisjoni 31. mai 2006. aasta teatis nõukogule, Euroopa Parlamendile, Euroopa Majandus- ja Sotsiaalkomiteele ja Regioonide Komiteele - Turvalise infoühiskonna strateegia – dialoog, partnerlus ja aktiivne osalemine {SEK(2006) 656}, KOM(2006) 251 lõplik
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0251:ET:NOT

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach. Brussels, 6.6.2001 COM(2001)298 final
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52001DC0298:EN:NOT

## 2.2. Euroopa Liidu ametid

**Euroopa Võrgu- ja Infoturbeamet (ENISA)**
http://www.enisa.europa.eu/

National Cyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace. May 2012
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport

Cyber Europe 2012: Peamised järeldused ja soovitused. Detsember 2012
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/ENISA_2012_00490000_ET_TRA.pdf

**Küberkuritegevuse vastase võitluse Euroopa keskus (European Cybercrime Center EC³)** Euroopa Politseiameti juures
https://www.europol.europa.eu/ec3

Frequently asked questions: The European Cybercrime Center EC³. Rapid MEMO/13/6, 09/01/2013
http://europa.eu/rapid/press-release_MEMO-13-6_en.htm

Feasibility Study for a European Cybercrime Centre. RAND Corporation, 2012
http://www.rand.org/pubs/technical_reports/TR1218.html

# 3. Eesti seisukohad

Valitsuse raamdokumendis „Eesti Euroopa Liidu poliitika 2011–2015" osutatakse interneti juurdepääsule kui põhiõigusele ja -vabadusele ning rõhutatakse küberturvalisuse tähtsust nii digitaalse ühtse turu toimimise tagamisel kui ka inimeste igapäevaelus. Selles kontekstis on eriti oluline elutähtsate infoinfrastruktuuride kaitse tagamine ja toimepidevuse kindlustamine. Eesti pooldab miinimumstandardide kehtestamist Euroopa Liidus küberkuritegude koosseisudele ja karistustele. Eesti peab samuti oluliseks küberjulgeoleku kinnistumist ühises välis- ja julgeolekupoliitika alases tegevuses ning ELi kaalukuse ja esindatuse osakaalu suurendamist selleteemalises rahvusvahelises suhtluses.

Vt lähemalt 7. pt „Küberpoliitika" (lk 45-49):
https://valitsus.ee/UserFiles/valitsus/et/riigikantselei/euroopa/Eesti%20EL%20poliitika_EST.pdf

Eesti Euroopa Liidu poliitika tegevuseesmärgid küberpoliitika vallas aastaiks 2011–2015 on järgmised:
1) Digitaalse ühtse turu toimimiseks vajaliku turvalise ruumi väljaarendamine Eesti aktiivsel osalusel Euroopa Liidu küberturvalisuse poliitika kujundamises.
2) Küberkuritegude ennetamine, tõkestamine ja uurimine: Eesti toetab küberkuritegevust käsitlevate direktiivide väljatöötamist ja vastuvõtmist.
3) Küberjulgeoleku tugevdamine Euroopa Liidus ja maailmas. Eesti pooldab ühises julgeoleku- ja kaitsepoliitikas küberjulgeoleku globaalse mõõtme tugevdamist ja ELi sisese küberkaitse alase võimekuse kasvu. Eesti toetab igati ELi ja NATO Küberkaitse Kompetentsikeskuse vahelise koostöö arendamist.

Küberpoliitika vt lk 31-32:
https://valitsus.ee/UserFiles/valitsus/et/riigikantselei/euroopa/eesti-eesmargid-euroopa-liidus/ELPOL_2011-2015_tegevuseesm%C3%A4rgid.pdf

# 4. Refereeringud

## 4.1. Küberrünnakute tõlgendamisest rahvusvahelises õiguses

**Russell Buchan. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?**
**Journal of Conflict & Security Law (2012), vol. 17 no. 2, p. 211–227.**

Artikkel vaatleb küberrünnakuid rahvusvahelise õiguse kontekstis. Üldiselt toetutakse küberrünnakute õiguslikul hindamisel ÜRO põhikirja artiklile 2(4), mis keelab jõu tarvitamise riikidevahelistes suhetes.

Infoühiskonna areng on riigid muutnud aina sõltuvamaks infotehnoloogiast, selle on teadvustanud ka vaenulikud osapooled ning tulemuseks ongi küberrünnakutena tuntud sündmuste kiire kasv.

Traditsiooniliselt tõlgendatakse artiklit 2(4) selliselt, et ainult füüsilist kahju tekitavad sekkumised kvalifitseeruvad õigusvastase jõu kasutamisena. Järelikult – küberrünnakud, mis füüsilist kahju ei põhjusta, ei ole vastuolus rahvusvahelise kirjutatud õigusega ega riku ÜRO põhikirja artikli 2(4) keeldu. ÜRO põhikiri pärineb interneti-eelsest ajast ja on täiesti selge, et selles pole küberrünnakutega arvestatud. Tegelikkuses võivad küberrünnakud olla samavõrra hävitava toimega kui füüsilist kahju tekitavad rünnakud.

Kübersõja spetsialistid pooldavad rahvusvahelise õiguse reformi, et paremini kaitsta riikide julgeolekut küberruumis. Välja on pakutud erinevaid lahendusi, kuid võimalust (ükskõik millise lahenduse osas) rahvusvahelisel tasandil kokkuleppele jõuda hindab artikli autor äärmiselt ebatõenäoseks. Samas väidab Russell Buchan, et küberrünnakuid saab siiski käsitleda rahvusvahelise tavaõiguse raamides ja osutab võimalusele nende puhul toetuda riikide siseasjadesse mittesekkumise põhimõttele.

Lähemalt analüüsib autor artiklis kahte juhtumit: 2007. aastal Eesti vastu toime pandud küberründeid ja Stuxneti viiruse kasutamist Iraani vastu 2010. aastal. Mõlemal juhul uurib autor ÜRO põhikirja artikli 2(4) ulatust ja rakendamise võimalusi. Eesti puhul oli tegemist hajutatud teenusetõkestamise rünnetega ja nii meedia kui ka akadeemilise maailma poolt on esitatud küsimus, kas tegu oli õigusvastase jõu tarvitamisega. Autori arvates Eesti-vastaste rünnete puhul artiklit 2(4) ei saa rakendada. Iraani puhul on hinnangu andmine keerulisem, kuna pole täpselt teada, millised olid tuumajaama vastase viirusrünnaku tagajärjed. Üldiselt arvatakse siiski, et arvutiviirus põhjustas tsentrifuugide füüsilist kahjustumist ja seega on olemas ka õiguslik alus artikli 2(4) rakendamiseks.

Buchan näitab, et riikide siseasjadesse mittesekkumise põhimõte on kasulik õiguslik instrument, mis võimaldab riikidel end kaitsta küberrünnakute vastu ka siis kui otsest füüsilist kahju ei teki, aga tagajärjed on siiski ühiskonda kahjustavad. Tema argumendid tuginevad väidetele, et sellise sekkumise eesmärgiks on soov sundida teist riiki oma käitumist muutma ja et tegemist on taolise sunni tahtliku tarvitamisega juhtudel, kui

sihtriigil on täielik õigus vabalt otsustada. Autor leiab, et Eesti-vastased küberrünnakud vastavad täpselt nendele kriteeriumidele ning seega on tegemist Eesti suveräänsuse rikkumisega ja õigusvastase sekkumisega.

Autori eesmärk ei ole eitada küberruumi puudutava rahvusvahelise õiguse reformi vajadust, kuid tal on vähe usku selle kiiresse teostumisse. Tema soov on osutada olemasolevatele õiguslikele võimalustele, millele seni on vähe tähelepanu pööratud.

*Refereerinud Giina Kaskla*

## 4.2. Euroopa Liidu küberjulgeoleku poliitikast

**Annegret Bendiek; Andrew L. Porter. European Cyber Security Policy within a Global Multistakeholder Structure**
**European Foreign Affairs Review (2013) vol. 18, no. 2, p. 155-180.**

Artikkel käsitleb küberturvalisuse võtmeküsimusi, vaatleb Euroopa küberjulgeoleku poliitika põhimõtteid ja institutsionaalset korraldust ning kõrvutab seda USA küberjulgeoleku strateegia, poliitika ja korraldusega.

Autorid osutavad kõige olulisematele probleemidele küberjulgeoleku poliitika kujundamisel. Poliitika formuleerimisel ja rakendamisel tuleb arvestada mitmetasandiliste struktuuridega ja paljude erinevate sidusrühmadega. Tegemist on valdkonnaga, kus tuleb leida tasakaal julgeolekuhuvide ning demokraatlike väärtuste ja individuaalsete vabaduste vahel. Edukas küberjulgeoleku ja -kaitse poliitika ei saa järgida tavapärast ning selget sise- ja välispoliitika, seadusandliku ja täitevvõimu vastutuse ning avalike ja erahuvide eristamist.

Riskide hindamisel ja haldamisel on võtmeküsimuseks informatsioon. Praegu puudub ELis süstemaatiline küberohtude kohta käiva info kogumise ja jagamise skeem. Nii riiklikul kui ka rahvusvahelisel tasandil jääb puudu tehnilisest suutlikkusest ja õiguslikust pädevusest, et küberrünnakuid empiiriliselt analüüsida.

Küberjulgeolek jagatakse sageli kolmeks valdkonnaks:

- küberkuritegevus – pettus ja võltsimine küberruumis, ebaseadusliku sisu levitamine (nt lapsporno), infosüsteemide rünne;
- küberspionaaž – nuhkvara kasutamine, häkkimine ja ebaseaduslik info kogumine;
- kübersõda – riik riigi vastu kübervahenditega.

Veel kasutatakse tihti mõisteid küberterrorism ja kübervandalism. Autorid osutavad, et rahvusvahelisel tasandil pole jõutud kokkuleppele ühistes ja ühestes definitsioonides ning erinevate lähenemiste tõttu on piirid mõistete vahel hägustunud.

Reaalsus on selline, et küberkuritegevus kasvab mahult ja muutub aina keerukamaks. Küberspionaaž muutub aina laiaulatuslikumaks ja ohtlikumaks, eriti kuna hädaohtu ei osata õigesti hinnata. Kui üleüldise tavarelvakonflikti tõenäosus on vähenenud, siis kübersõja oht on püsiv, ehkki need ohud ja võimalikud tagajärjed on halvasti teadvustatud.

Kuigi Internet ei tunne riigipiire, lasub julgeolekuvastutus riikidel. Mitmed suurriigid ongi küberjulgeoleku hõlmanud oma julgeolekustrateegiatega, kuna rahvusvahelisel tasandil ei ole küberkuritegusid määratletud ega karistusi ette nähtud. Kaasaegne teenusmajandus on valdavalt seotud elektrooniliste võrgustikega ja selle toimimise eeltingimuseks on turvaline Interneti-ühendus ja tõhus intellektuaalse omandi kaitse. USAs küberjulgeolek on kuulutatud strateegiliseks prioriteediks nii riiklikus julgeolekus kui ka sisejulgeoleku poliitikas.

Autorid annavad ülevaate ka rahvusvaheliste organisatsioonide küberjulgeoleku alasest tegevusest ja leiavad, et seni on tulemusrikkamad olnud regionaalsed või piiratud liikmeskonnaga ühendused (nt Euroopa Nõukogu ja NATO).

Euroopa Liidu poliitilises agendas on küberjulgeoleku tagamine jõudnud prioriteetide sekka viimastel aastatel. Artikli autorid kirjeldavad ELi jõupingutusi rahvusvahelises koostöös, katseid üle saada sise- ja välispoliitikat eraldavast barjäärist (eriti tähtis on see elutähtsate infrastruktuuride kaitse puhul) ning probleeme, mis on seotud eraelu puutumatuse ja andmekaitsega. Oluline, aga samas küllalt keeruline, on koostöö erasektori ja valitsusväliste osalejatega.

Autorite hinnangul on Euroopa Liidul USA kogemusest mõndagi kasulikku õppida. Nad osutavad, kui tähtis on sisse seada tsiviilkontroll julgeolekuprogrammide üle ja leida tõhus mudel koostööks erasektoriga. Samas hoiatavad nad USA valitsuse poliitika järgimise eest isikuandmete kogumise ja kasutamise osas.

*Refereerinud Giina Kaskla*

# 5. Raamatuviiteid

Võõrkeelsete raamatute kirje lõppu on nurksulgudes lisatud nende leidumus Eesti raamatukogudes. Kasutatud on järgmisi lühendeid:
RR – Rahvusraamatukogu
TLÜAR – Tallinna Ülikooli Akadeemiline Raamatukogu
TTÜR – Tallinna Tehnikaülikooli raamatukogu
TlnKR – Tallinna Keskraamatukogu
TÜR – Tartu Ülikooli raamatukogu
KMAR – Eesti Kirjandusmuuseumi Arhiivraamatukogu

## 5.1. Käsiraamatud, monograafiad ja kogumikud

**Laaneoks, Erkki**. Sissejuhatus võrgutehnoloogiasse / Tartu Ülikool, matemaatika-informaatikateaduskond, arvutiteaduse instituut. - Tartu : Tartu Ülikooli Kirjastus, 2010. - 205 lk. - Sisust: Võrguturve lk. 180-193.
Kättesaadav ka võrguväljaandena: http://hdl.handle.net/10062/18478

**Mägi, Harri ; Vitsut, Lauri**. Infosõda: visioonid ja tegelikkus. - Tallinn : [Eesti Ekspressi Kirjastus], 2008. - 192 lk.

**Schifreen, Robert**. Kuidas võita häkkerit : [häkkeritõrje käsiraamat] / tõlge: Mart Kalvet. - Tallinn : Lausuja Kirjastus, 2008. - 416 lk.

**Tikk, Eneken ; Nõmper, Ants**. Informatsioon ja õigus. - Tallinn : Juura, 2007. - 186 lk.

**Clarke, Richard A. ; Knake, Robert K**. Cyber war : the next threat to national security and what to do about it. - New York : Ecco, 2010. - xiv, 290 lk. [RR, TlnKR]

**Cyber-conflict** and global politics / edited by Athina Karatzogianni. - London ; New York : Routledge, 2009. - xvi, 246 lk. [RR, TLÜAR]
TÄISTEKST RR arvutivõrgus (registreeritud kasutajale)

**Cyberterrorism** : the use of the internet for terrorist purposes / Council of Europe. - Strasbourg : Council of Europe Publishing, c2007. - 497 lk. [RR]

**Gallaher, Michael P. ; Link, Albert N. ; Rowe, Brent**. Cyber security : economic strategies and public policy alternatives. - Cheltenham, UK ; Northampton, MA : Edward Elgar, 2008. - xi, 266 lk. [RR]

**Large** scale Internet attacks : [the Internet attacks on Estonia ; Sweden's emergency preparedness for Internet attacks]. - Stockholm : Swedish Emergency Management Agency, 2008. - 54 lk. [RR]

**Modelling** cyber security : approaches, methodology, strategies / edited by Umberto Gori. - Amsterdam [etc.] : IOS Press ; [Brussels] : published in cooperation with NATO Public Diplomacy Division, 2009. - xxiii, 215 lk. [RR]

**Palojärvi, Pia.** A battle in bits and bytes : computer network attacks and law of armed conflict / Helsinki : Erik Castrén Institute of International Law and Human Rights. - University of Helsinki, 2009. - vi, 186 lk. [RR]

**Rid, Thomas**. Cyber war will not take place. - London : Hurst, 2013. - xvi, 218 lk. [RR]

**Strategic** intelligence management : national security imperatives and information and communications technologies / edited by Babak Akhgar, Simeon Yates. - Amsterdam [etc.] : Butterworth-Heidemann, 2013. - xxiv, 316 lk. [RR]

**Tallinn** manual on the international law applicable to cyber warfare : prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence / general editor, Michael N. Schmitt. - Cambridge ; New York : Cambridge University Press, 2013. - xix, 282 lk. [RR, TLÜAR, TÜR, Balti Kaitsekolledži rmtk, TÜ Iuridicumi teabekeskus]

**The fog** of cyber defence / eds. Jari Rantapelkonen & Mirva Salminen. - Helsinki : National Defence University, Department of Leadership and Military Pedagogy, 2013. - 248 lk. - (Publication Series 2, Article Collection n:o 10) [Balti Kaitsekolledži rmtk] Kättesaadav ka võrguväljaandena: http://www.doria.fi/bitstream/handle/10024/88689/The%20Fog%20of%20Cyber%20Defence%20NDU%202013.pdf?sequence=1

**The Routledge** handbook of new security studies / edited by J. Peter Burgess. - London ; New York : Routledge, 2010. - xii, 316 lk. [RR]

**The virtual** battlefield : perspectives on cyber warfare / edited by Christian Czosseck and Kenneth Geers. - Amsterdam [etc.] : IOS Press, 2009. - xx, 305 lk. [RR, TLÜAR, TTÜR]

**Wu, Chwan-Hwa ; Irwin, J. David**. Introduction to computer networks and cybersecurity. - Boca Raton (Fla.) [etc.] : CRC Press, 2013. - xlv, 1336 lk. [TLÜAR]

**Дашян, Микаэл**. Право информационных магистралей : вопросы правового регулирования в сфере Интернет = Law of information highways. - Москва : Волтерс Клувер, 2007. - X, 275 lk. [RR]

**Глушаков, С. В. ; Бабенко, М. И. ; Тесленко, Н. С.** Секреты хакера : защита и атака. - Москва : Хранитель : АСТ, 2008. - 536, [1] lk. [TTÜR]

**Новиков, В. К.** Информационное оружие - оружие современных и будущих войн. - Москва : Горячая линия - Телеком, 2011. - 262 lk. [TLÜAR]

**Паршин, С. А. ; Горбачев, Ю. Е. ; Кожинов, Ю. А.** Кибервойны - реальная угроза национальной безопасности? / Институт проблем международной безопасности РАН, Факультет мировой политики МГУ им. М. В. Ломоносова. - Москва : [Красанд, 2011]. - 93, [1] lk. [RR]

## 5.2. Konverentsimaterjalid

**Conference of the Baltic Assembly** "Threat from the net" : 28-29 February 2008 in Tallinn, Estonia. - [Tallinn : Välisministeerium, 2008]. - 18 lk. [RR]

**Conference on Cyber Warfare** : June 17-19, 2009, Tallinn, Estonia. - [Tallinn] : Rahvusvaheline Kaitseuuringute Keskus, [2009]. - 56 lk. [RR, TLÜAR, TTÜR]

**Proceedings of the 10th European Conference** on Information Warfare and Security, The Institute of Cybernetics at the Tallinn University of Technology, Estonia, 7-8 July 2011 / edited by Rain Ottis. - Reading : Academic Publishing Limited, 2011. - x, 341 lk. [TLÜAR, TTÜ Küb Inst rmtk]

**Proceedings of the 9th European Conference** on Information Warfare and Security, University of Macedonia and Strategy International, Thessaloniki, Greece, 1-2 July 2010 / ed. by Josef Demergis. - Reading : Academic Publishing Limited, 2010. - xii, 430 lk. [TTÜ Küb Inst rmtk]

## 5.3. OECD väljaanded

**Cybersecurity** policy making at a turning point : analysing a new generation of national cybersecurity strategies for the Internet economy / Organisation for Economic Co-operation and Development. - Paris : OECD Publishing, 2012. - 57 lk.
TÄISTEKST RR arvutivõrgus

**Non-governmental** perspectives on a new generation of national cybersecurity strategies / Organisation for Economic Co-operation and Development. - Paris : OECD Publishing, 2012. - 23 lk.
TÄISTEKST RR arvutivõrgus

**The role** of the 2002 security guidelines: towards cybersecurity for an open and interconnected economy / Organisation for Economic Co-operation and Development. - Paris : OECD Publishing, 2012. - 14 lk.
TÄISTEKST RR arvutivõrgus

## 5.4. NATO Küberkaitse Kompetentsikeskuse väljaanded

Conference on Cyber Conflict : proceedings 2010 / edited by Christian Czosseck and Karlis Podins. - Tallinn : Cooperative Cyber Defence Centre of Excellence, 2010. - 245 lk. [RR, TTÜ Küb Inst rmtk, Balti Kaitsekolledži rmtk]

2011 3rd international conference on cyber conflict : proceedings : 7-10 June, 2011, Tallinn, Estonia / Cooperative Cyber Defence Centre of Excellence, Institute of Electrical and Electronics Engineers ; edited by Christian Czosseck, Enn Tyugu, Thomas Wingfie. - Tallinn : Cooperative Cyber Defence Centre of Excellence, 2011. - XVIII, 186 lk.
Kättesaadav ka võrguväljaandena:
http://www.ccdcoe.org/publications/2011proceedings/2011_Proceedings.pdf

2012 4th international conference on cyber conflict : 5-8 June, 2012 Tallinn, Estonia : proceedings / NATO Cooperative Cyber Defence Centre of Excellence, IEEE ; edited by C. Czosseck, R. Ottis, K. Ziolkowski. - Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, 2012. - VIII, 453 lk.
Kättesaadav ka võrguväljaandena:
http://www.ccdcoe.org/publications/2012proceedings/CyCon_2012_Proceedings.pdf

**Geers, Kenneth**. Strategic cyber security. - Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, 2011. - 168 lk.
Kättesaadav ka võrguväljaandena:
http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF

**International** cyber security : legal & policy proceedings : 2010 / edited by Eneken Tikk, Anna-Maria Talihärm. - Tallinn : Cooperative Cyber Defence Centre of Excellence, 2010. - 140 lk. [Balti Kaitsekolledži rmtk, KMAR võõrk. raamat]

**National** cyber security framework manual / edited by Alexander Klimburg. - Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, 2012. - XVII, 235 lk.
Kättesaadav ka võrguväljaandena:
http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

**Tikk, Eneken**. Frameworks for international cyber security. 2, International case law. - Tallinn : Cooperative Cyber Defence Centre of Excellence, 2010. - 1279 lk. [Balti Kaitsekolledži rmtk, KMAR võõrk. raamat]

**Tikk, Eneken ; Kaska, Kadri ; Vihul, Liis**. International cyber incidents : legal considerations. - Tallinn : Cooperative Cyber Defence Centre of Excellence, 2010. - 130 lk. [RR, TLÜAR, TTÜR]

## 5.5. Väitekirjad

**Aavekukk-Tamm, Merit**. Küberkaitse rahvusvahelises õiguses : magistritöö / juhendaja: René Värk ; Tartu Ülikool, õigusteaduskond Tallinnas, avaliku õiguse instituut. - Tallinn : Tartu Ülikool, 2011. - 75 lk. [Õigusteadusk. teabekeskus Tallinnas]

**Czosseck, Christian Günter**. An evaluation of state-level strategies against botnets in the context of cyber conflicts : dissertation for a Doctor of Philosophy degree / Estonian Business School. - Tallinn : EBS Print, 2012. - 166 lk. - Eestikeelne resümee lk 159-164.
Kättesaadav ka võrguväljaandena:
http://www.ebs.ee/public/oppeosakond/doktoriope/Czosseck_web.pdf4.pdf

**Geers, Kenneth**. Strategic cyber security : evaluating nation-state cyber attack mitigation strategies with DEMATEL = Strateegiline küberjulgeolek : küberrünnaku leevendamise strateegiate hindamine riiklikul tasandil : DEMATEL-i meetod. Tallinn : Tallinn University of Technology Press, 2011. - (Tallinna Tehnikaülikooli väitekirjad. C; 64). - Eestikeelne kokkuvõte lk 8-9.
Kättesaadav ka võrguväljaandena: http://digi.lib.ttu.ee/i/?592

**Ottis, Rain**. A systematic approach to offensive volunteer cyber militia = Vabatahtlikud küberründegrupid: süsteemiteoreetiline vaade. - Tallinn : Tallinn University of Technology Press, 2011. - 118 lk. - (Tallinna Tehnikaülikooli väitekirjad. C; 60). - Eestikeelne kokkuvõte lk 39.
Kättesaadav ka võrguväljaandena: http://digi.lib.ttu.ee/i/?585

**Tikk, Eneken**. Comprehensive legal approach to cyber security. - Tartu : Tartu University Press, 2011. - 170 lk. - (Dissertationes iuridicae Universitatis Tartuensis 35). - Eestikeelne kokkuvõte lk 133-139.
Kättesaadav ka võrguväljaandena: http://dspace.utlib.ee/dspace/handle/10062/17914

**Tänav, Kerttu**. Dettering and countering botnets on the CERT level – the competence and authorities of CERTs in botnet mitigation : master's thesis / supervisors: L. Mälksoo, M. Dion ; University of Tartu, Faculty of Law, Institute of Constitutional and International Law. - Tartu : University of Tartu, 2011. - 89 lk. [TÜ Iuridicumi teabekeskus]

**Vihul, Liis**. Internetiliikluse jälgimine internetiteenuse osutajate poolt andmesidevõrkude turvalisuse tagamiseks : magistritöö / juhendajad K. Kaska, C. Ginter ; Tartu Ülikool, õigusteaduskond, riigi- ja rahvusvahelise õiguse instituut. - Tartu : Tartu Ülikool, 2012. - 78 lk. [TÜ Iuridicumi teabekeskus]

# 6. Artikliviiteid

## 6.1. Artiklid teadusajakirjades

**Buchan, Russell**. Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions? // Journal of Conflict and Security Law (2012) vol. 17, no. 2, pp. 212-227.

**Calderoni, Francesco**. The European legal framework on cybercrime: striving for an effective implementation // Crime, Law and Social Change (2010) vol. 54, no. 5, pp. 339-357.

**Cerf, Vinton G**. Safety in cyberspace // Daedalus (2011) vol. 140, no. 4, pp. 59-69.

**Clough, Jonathan**. The Council of Europe Convention on Cybercrime: defining "crime" in a digital world // Criminal Law Forum (2012) vol. 23, no. 4, pp. 363-391.

**Colarik, Andrew M**. ; Janczewski, Lech. Establishing Cyber Warfare Doctrine // Journal of Strategic Security (2012) vol. 5, no. 1, pp. 31-48.

**Dipert, Randall R**. The Ethics of Cyberwarfare // Journal of Military Ethics (2010) vol. 9, no. 4, pp. 384-410.

**Fleck, Dieter**. Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual // Journal of Conflict and Security Law (2013) vol. 18, no. 2, 21 p.

**Gillespie, Alisdair A**. Jurisdictional issues concerning online child pornography // International Journal of Law and Information Technology (2012) vol. 20, no. 3, pp.151-177.

**Goldsmith, Jack**. How cyber changes the laws of war // European Journal of International Law (2013) vol. 24, no. 1, pp. 129-138.

**Guinchard, Audrey**. Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy // Journal of Strategic Security (2011) vol. 4, no. 2, pp. 75-96.

**Handler, Stephenie Gosnell**. The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare // Stanford Journal of International Law (2012) vol. 48, no. 1, pp. 209-237.

**Herzog, Stephen**. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses // Journal of Strategic Security (2011) vol. 4, no. 2, pp. 49-60.

**Kigerl, Alex**. Routine Activity Theory and the Determinants of High Cybercrime Countries // Social Science Computer Review (2012) vol. 30, no. 4, pp. 470-486.

**Kim, Seung Hyun ; Wang, Qiu-Hong ; Ullrich, Johannes B. A**. Comparative Study of Cyberattacks // Communications of the ACM (2012) vol. 55, no. 3, pp. 66-73.

**Kodar, Erki**. Computer network attacks in the grey areas of Jus ad Bellum and Jus in Bello // Baltic yearbook of international law. - Vol. 9 (2009). - Leiden, 2010. - Pp. 133-155. [RR, TÜ Iuridicumi teabekeskus]

**Li, Sheng**. When does Internet denial trigger the right of armed self-defence? // The Yale journal of international law (2013) vol. 38, no. 1, pp. 179-216.
*2007. a. küberrünnakutest Eestile.*

**Mulligan, Deirdre K. ; Fred B. Schneider**. Doctrine for cybersecurity // Daedalus (2011) vol. 140, no. 4, pp. 70-92.

**O'Connell, Mary Ellen**. Cyber Security without Cyber War // Journal of Conflict and Security Law (2012) vol. 17, no. 2, pp.187-209.

**Park, Gabriel K**. Granting an Automatic Authorization for Military Response: Protecting National Critical Infrastructure from Cyberattack // Brooklyn Journal of International Law (2013) vol. 38, no. 2, pp. 797-827.

**Rahman, Rizal**. The legal measure against Denial of Service (DoS) attacks adopted by the United Kingdom legislature: should Malaysia follow suit? // International Journal of Law and Information Technology (2012) vol. 20, no. 2, pp. 85-101.

**Schmitt, Michael**. Classification of Cyber Conflict // Journal of Conflict and Security Law (2012) vol. 17, no. 2, pp. 245-260.

**Tikk, Eneken**. Global cybersecurity – thinking about the niche for NATO // The SAIS Review of International Affairs (2010) vol. 30, no. 2, pp. 105-119.

**Tsagourias, Nicholas**. Cyber attacks, self-defence and the problem of attribution // Journal of Conflict and Security Law (2012) vol. 17, no. 2, pp. 229-244.

**Van Der Meulen, Nicole S**. DigiNotar: Dissecting the First Dutch Digital Disaster // Journal of Strategic Security (2013) vol. 6, no. 2, pp. 46-58.

## 6.2. Artiklid Eesti väljaannetes

**Ashmore, William C**. Impact of alleged Russian cyber attacks // Baltic Security and Defence Review. 11 / Baltic Defence College. - Tartu, 2009. - Pp. 4-40.
*Erinevatele riikidele tehtud küberrünnakute tagamaadest ja õppetundidest, rahvusvaheliste organisatsioonide abinõud efektiivseks võitluseks küberrünnakute vastu.*

https://www.bdcol.ee/files/files/documents/Research/BSDR2009/1_%20Ashmore%20-%20Impact%20of%20Alleged%20Russian%20Cyber%20Attacks%20.pdf

**Ergma, Ene**. Küberjulgeolekule teed rajades // Riigikogu toimetised. 15. - Tallinn, 2007. - Lk. 27-29.
*Riigikogu esimees analüüsib aprillisündmustega kaasnenud küberrünnakute tagamaid ning toob välja vajaduse kujundada küberrünnakute suhtes Euroopa Liidus ja NATOs ühtne poliitika.*
http://www.riigikogu.ee/rito/index.php?id=11594&op=archive2

**Geers, Kenneth**. Valmistumine kübersõjaks / inglise keelest tõlkinud Marek Laane // Diplomaatia (2010) nr. 9, sept., lk. 8-9.
*Küberkaitseõppuste vajalikkus ja Tallinnas 2010 a. korraldatud küberkaitseõppused "Balti küberkilp".*
http://www.diplomaatia.ee/en/article/valmistumine-kubersojaks/

**Ilves, Toomas Hendrik**. Järgmine väljakutse: küberkaitse : infotehnoloogia areng sunnib meid vaatama uue pilguga eesseisvatele ohtudele / tõlkinud Marek Laane // Diplomaatia (2012) nr. 5, mai, lk. 4-7.
http://www.diplomaatia.ee/artikkel/jargmine-valjakutse-kuberkaitse/

**Ilves, Toomas Hendrik**. Küberohud ja küberreageerimine. Avaliku ja erasektori partnerlus // Suurem Eesti : valik presidendikõnesid ja -kirjutisi 2006-2011 / Toomas Hendrik Ilves. - Tallinn, 2011. - . Lk. 295-302.
*Ettekanne NATO küberkaitsekeskuse kolmandal konverentsil 8. juunil 2011 Tallinnas.*

**Kaju, Andreas**. Küberkaitse – Eesti võimalus ja vastutus // Maailma Vaade (2008) nr. 5, lk. 24-26.
*Ülevaade NATO küberkaitse kompetentsikeskuse asutamise arengust Eestis ning riiklikust küberjulgeoleku strateegiast, mis hõlmab endas küberjulgeoleku ohuhinnangut, kriitilise informatsiooni infrastruktuuri kaardistamist ning küberkaitsealast väljaõpet.*
http://www.maailmavaade.ee/?d=kuberkaitse0408

**Kasenõmm, Evelin**. Küberkuritegevusest kui silmale nähtamatust ohust // ViAble security = Haritud turvalisus. - Tallinn, 2012. - Lk. 283-302. - (Sisekaitseakadeemia toimetised ; 11)
*Levinumatest ohtudest ja kaitsemeetmetest, interneti kasutamisest kaabliga ja traadita, kaugtööst ja mobiilseadmete kasutamisest, andmete kaitsmisest ja hävitamisest, füüsilisest turvalisusest.*
http://riksweb.sisekaitse.ee/index.asp?action=102&tid=55188

**Kelam, Tunne**. Lahendus ühele murdosasekundile? // Maailma Vaade (2012) nr. 18, lk. 3-5.
*Rahvusvahelise küberjulgeoleku tagamisest.*
http://www.maailmavaade.ee/?d=kyber_kelam_1112

**Kivimaa, Jüri**. Küberkaitse/küberturbega seostuvatest põhiterminitest // Sõdur (2008) nr. 2, apr., lk. 19-23.
*Artiklis tutvustatakse küberkaitsega seotud mõisteid (küberruum, kriitiline infrastruktuur, küberturve, küberkaitse, küberjulgeolek) ning tuuakse välja andmeturve ja küberturve erinevused.*

**Kivimägi, Agu**. Küberkaitsest ja küberkorrakaitsest // Turvalisuspoliitika 2011: kokkuvõte "Eesti turvalisuspoliitika põhisuunad aastani 2015" täitmisest. - Tallinn, 2011. - Lk. 99-104.
*Ülevaade küberrünnakutest maailmas, küberturve tähtsus riikliku julgeoleku tagamisel.*

**Klein, Merli**. Küberkuriteod 2005-2011 / kommenteerinud Raigo Haabu // Radar (2012) nr. 13, lk. 38-41.
*Kokkuvõte Politsei- ja Piirivalveameti analüüsist: "Küberkuriteod 2005-2011 ja politsei tegevus valdkonnas".*

**Klimburg, Alexander ; Tiirmaa-Klaar, Heli**. Cybersecurity and cyberpower: concepts, conditions, and capabilities for cooperation and action within the EU // The Estonian foreign policy yearbook 2011. - Tallinn, 2012. - Pp. 59-102.
*Küberturve Euroopa Liidu ühise välis- ja julgeolekupoliitika aspektist.*
http://www.evi.ee/lib/valispol2011.pdf

**Küberrünnakud** Eesti vastu = Cyber attacks hit Estonia // Pilk peeglisse 2007 = Glance at the mirror 2007. - Tallinn, 2008. - Lk. 58-71.
*Eestile osaks saanud küberrünnakute põhjused ja õppetunnid, vastukajad maailmas.*
http://web-static.vm.ee/static/failid/115/cyber_attacks.pdf

**Lorents, Peeter**. Kivikirvest kübersõjani // Sõdur (2008) nr. 1, lk. 11-15.
*Artiklis selgitatakse süsteeme ning nende arenguid, vigade ja tõrgete olemust, vaadeldakse süsteemide kahjustamist ning nende kaitset, tutvustatakse küberrelvade ja küberkaitse olemust ja olulisemaid iseärasusi.*

**Oorn, Reet**. Kübersõda ja Eesti // Infotehnoloogia avalikus halduses : aastaraamat 2007. - Tallinn, 2008. - Lk. 80-83.
*Kübersõda ja Eesti - õiguslikest aspektidest.*
http://www.riso.ee/et/pub/2007it/Aastaraamat2007.pdf

**Ottis, Rain**. Küberründevõime loomisest // Sõdur (2008) nr. 6, lk. 22-25.
*Organiseeritud küberründest ja riigi suhete võimalikkusest küberkurjategijatega.*

**Ottis, Rain**. Konfliktid infoajastul – küberründed ja kodanikuühiskond // Akadeemia (2009) ak. 21, nr. 9, lk. 1795-1804.
*Küberkonfliktid ja küberründed kui rahvusvahelise poliitika osa, riigi ja kodanike koostööst küberjulgeoleku tagamisel.*

**Ottis, Rain**. Küberrünnete klassifitseerimine // Sõdur (2008) nr. 3, juuni, lk. 9-14.
*NATO Küberkaitse Kompetentsikeskuse teadur leitnant Rain Ottis analüüsib kübermaailmas aset leidvate rünnete klassifitseerimise viise.*

**Raidma, Mati**. Gruusia konflikti mittesõjalised õppetunnid // Riigikogu toimetised. 18. - Tallinn, 2008. - Lk. 36-38.
*Riigikogu liige Gruusia-Venemaa konflikti õppetundidest, sh infoühiskonnaga seotud väljakutsetest.*
http://www.riigikogu.ee/rito/index.php?id=13557

**Talbot, David**. Moore'i seadusetus – lindpriid kasvatavad internetis edumaad // HEI : Hea Eesti Idee (2010) nr. 26, dets., lk. 32-39.
*Küberkuritegevuse probleemid konkreetsete küberünnakute näitel: sh ka Eesti vastu 27. apr. 2007.*

**Tammet, Tanel**. Küberrünnakute moos aprillirahutuste kibedal pudrul // Vikerkaar (2008) nr. 4/5, lk. 135-138.
*Küberrünnakute põhimeetodist, eesmärkidest ning vastumeetmetest.*

**Tiirmaa-Klaar, Heli**. Küberruumi kaitse eri tasanditel: nõrkused ja reageerimine // Välisministeeriumi aastaraamat 2011. - Tallinn, 2011. - Lk. 22-29.
http://www.vm.ee/?q=node/10897

**Tiirmaa-Klaar, Heli**. Rahvusvaheline koostöö küberjulgeoleku tagamisel // Diplomaatia (2010) nr. 9, sept., lk. 6-7.
*Globaalne küberjulgeolek ja Eesti osa selles.*
http://www.diplomaatia.ee/en/article/rahvusvaheline-koostoo-kuberjulgeoleku-tagamisel/

**Tikk, Eneken**. Informatsioon ja õigus // Õiguskeel (2007) nr. 4, lk. 3-12. Ilmunud ka: Õiguskeel 2005-2007 : artiklikogumik. - Tallinn, 2008. (Juura keeleraamat). - Lk. 62-71.
*Andmekogu ja infosüsteemi käsitlusest Eesti õiguses, karistusseadustiku terminitest infotehnoloogiasõnastike vaatenurgast ning küberjulgeolekust.*
TÄISTEKST RR arhiivis DIGAR

**Tikk, Eneken**. Kübersõda ja tagantjärele tarkus // Ärielu (2007) nr. 3, 16. okt., lk. 41-42.
*Eesti-vastaste küberrünnete kajastamisest avalikkuses ja poliitikute poolt kasutatud terminitest. Lisa: Rünnete kronoloogia.*

**Tikk, Eneken**. Kübersuverään - Eesti kaart maailma jõumängus // Iganenud või igavene? : tekste kaasaegsest suveräänsusest. - Tartu, 2010. - Lk. 303-320.
*Riikide võimalustest valitseda internetti, küberrünnakutest ja -kaitsest.*

**Tikk-Ringas, Eneken**. Küberjulgeoleku õiguslik raamistik // Juridica (2012) nr. 4, lk. 274-283.
*Küberjulgeoleku mõistest ja olemusest, kübertemaatikast riikidevahelistes suhetes, küberjulgeoleku õigusruumist küberintsidentide (Eesti 2007. aasta sündmused, Wikileaks, Stuxnet, Bredolab) näitel.*

# 7. Valik võrguväljaandeid ja internetiallikaid

## 7.1. Võrguväljaanded

**Baud, Michel**. Cyberguerre : En quête d'une stratégie / Institut Français des Relations Internationales (Ifri) // Focus stratégique n° 44, mai 2013, 43 p.
http://www.ifri.org/index.php?page=contribution-detail&id=7700&lang=uk

**Bendiek, Annegret**. European Cyber Security Policy // SWP Research Paper 2012/RP 13, October 2012, 27 p.
http://www.swp-berlin.org/en/publications/swp-research-papers/swp-research-paper-detail/article/european_cyber_security_policy.html

**Klimburg, Alexander ; Tiirmaa-Klaar, Heli**. Cybersecurity and cyberpower: Concepts, conditions and capabilities for cooperation for action within the EU : Study / European Parliament, Directorate-General for External Policies of the Union, Policy Department, April 2011, 75 p.
http://www.europarl.europa.eu/committees/en/sede/studiesdownload.html?languageDocument=EN&file=41648

**Lewis, James Andrew**. Cyberwarfare and its impact on international security // UNODA Occasional Papers No. 19, June 2010, 20 p.
http://www.un.org/disarmament/HomePage/ODAPublications/OccasionalPapers/PDF/OP19.pdf

**Porcedda, Maria Grazia**. Data Protection and the Prevention of Cybercrime: The EU as an area of security? // EUI Working Papers, LAW 2012/25, 81 p.
http://hdl.handle.net/1814/23296

**Tuohy, Emmet.** Toward an EU Cybersecurity Strategy: The Role of Estonia / International Centre for Defence Studies = Rahvusvaheline Kaitseuuringute Keskus // Policy Paper, December 2012, 6 p.
http://icds.ee/fileadmin/failid/Toward%20an%20EU%20Cybersecurity%20Strategy%20-%20The%20Role%20of%20Estonia.pdf

**Umbach, Frank**. Critical energy infrastructure at risk of cyber attack / Konrad Adenauer Foundation // KAS International Reports 9|2012, pp. 35-66.
http://www.kas.de/wf/doc/kas_32075-544-2-30.pdf?120913173625

## 7.2. Internetiallikad

**Security and Defence Agenda (SDA)**
Brüsselis asuv julgeolekule ja kaitsele pühendunud mõttekoda

SDA cyber-security initiative
http://www.securitydefenceagenda.org/Contentnavigation/CyberInitiative/tabid/1331/Default.aspx

Uudiseid ja artikleid küberjulgeoleku teemal
http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/CategoryView/categoryId/62/New-Threats.asp

**RAND Europe**
Sõltumatu uurimisinstituut

Research on Cyber Security and Information Assurance
http://www.rand.org/randeurope/research/defence/cyber.html

**Chatham House (The Royal Institute of International Affairs)**
Briti juhtiv mõttekoda

Cyber Security
http://www.chathamhouse.org/research/security/current-projects/cyber-security

**Center for Strategic and International Studies (CSIS**)
USA mõjukas kaitse- ja julgeolekupoliitika mõttekoda

A list of significant cyber events since 2006 by James Andrew Lewis (täiendatud mais 2013)
http://csis.org/publication/cyber-events-2006

**EurActiv**
Euroopa Liidu uudiste portaal

Cybersecurity: Protecting the digital economy (published 19 November 2012, updated 10 December 2012)
http://www.euractiv.com/infosociety/cybersecurity-protecting-digital-linksdossier-508217

**Euroopa Parlamendi raamatukogu**

Cybercrime: Key sources by the Library of European Parliament. May 3, 2012
http://libraryeuroparl.wordpress.com/2012/05/03/cybercrime/

**Eurobaromeeter**

Cyber security : Special Eurobarometer 390, 2012
http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

**Eurostat**

ICT security in enterprises (2011 veebruari seisuga)
http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/ICT_security_in_enterprises