

Eesti ja NATO artikkel 5

Estonia and NATO Article Five

Kui Baltimaad poleks NATO ja Euroopa Liiduga ühineda saanud, võidutseks regioonis praegu kahtlemata ebastabiilsus, madal turvalisus ja vähene majandusedu. Üheks tähtsaks sammuks Baltikumi arenguprotsessis on olnud USA-Balti harta, mis allkirjastati kümme aastat tagasi. Harta süvendas Baltimaade kindlustunnet ja kohustas USA-d aitama Eestit, Lätit ja Leedut nende integreerumisel läände. Vastutasuks andsid Balti riigid oma panuse: nad pühendusid läänelikele väärtustele, poliitilistele ja majandusreformidele, vähemusrahvaste õiguste kaitsmisele ja regionaalsele koostööle. Harta aitab kaotada Baltimaade ajaloolist umbusku globaalsete julgeolekuorganisatsioonide, nagu ÜRO ja OSCE suhtes. (WSJ, 16.01)

Neli aastat pärast NATO ja Euroopa Liiduga liitumist ihkavad Baltimaad suuremat integreeritust ühisesse julgeolekupoliitikasse. Eesti ei soovi leida end olukorrast, kus tuleb valida NATO ja ELi vahel. Edendamaks Euroopa kaitsepoliitikat, tuleks esmalt edendada ELi-NATO suhteid. Nii ajaloolistel kui ka geograafilistel põhjustel on Venemaa-küsimus Balti riikide jaoks keskne. Suhted võimuka idanaabriga on jäänud probleemseks, seda näitasid ka mullused küberrünnakud Eestile. Seega on Baltimaade huvi suurema integreerituse

If the Baltic states wouldn't have joined NATO and the EU, the region would without a doubt not enjoy its current stability, high security and economic growth. One of the most important milestones in the development of the Baltic states was the US-Baltic Charter concluded ten years ago. The Charter added to the feeling of the nations' security and the United States undertook to support Estonia's, Latvia's and Lithuania's integration with the West. In return, the Baltic countries also contributed: they committed to Western values, political and economic reforms, protecting the rights of ethnic minorities, and regional co-operation. The Charter helped to decrease the Baltic nations' historical lack of trust in global security organisations like the UN and the OSCE. (WSJ, 16.01)

Four years after joining NATO and the EU, the Baltic states crave a more deeply integrated common security policy. Estonia wishes to avoid a situation where a choice between NATO and the EU would have to be made. EU-NATO relations should be advanced first and foremost to advance Europe's security policy. For both historical and geographical reasons, the issue of Russia is central for the Baltics. Relations with their powerful eastern neighbour remain challenging, as last year's cyber attacks against Estonia demonstrated. So their desire to achieve

saavutamiseks ELi julgeoleku-, energia- ja naabruspoliitika küsimustes igati loogiline. (*La Croix*, 22.04)

Balti riikide sõjajõud on tibatillukesed ja valmis toetama kaugeid NATO missioone, selle asemel et reaalselt oma piirkonda Venemaa rünnaku eest kaitsta. NATO sõjaline kohalolek aga kujutab endast vaid käputäit hävitajaid, mille baas paikneb Leedus, ning küberkaitsekeskust Eestis. Kõigil kolmel on NATO standarditele vastavad radarid, mis võimaldavad vaadata sügavale Venemaale. Samas oodatakse Balti riikidelt suuremaid kaitsekulutusi, mis pole majanduslanguse tingimustes sugugi kerge. (*The Economist*, 4.09)

Eesti üksus Afganistanis on küll väikese arvuline, ent olnud siiani pidevalt tegevuses ning kandnud ka kaotusi. Ehkki Eestil on Afganistanis ISAFi 40 riigi seas välja panna üks väiksemaid väekontingente, on eestlased osalenud tulistes lahingutes. Eesti sõdurite osalemine Iraagi ja Afganistani missioonidel ei leia alati kõigi eestlaste ühtset toetust, kuid vaatamata väikeriigi kasinale inimressursile on ka Eestil kanda vastutus NATO tegevuse õnnestumise eest. Kui eestlased tahavad, et neile vajadusel appi tuldaks, peavad nad ka ise olema võimelised aitama. (*Deutsche Welle World*, 1.06)

Venemaa tegevus Gruusias on olnud Eesti NATO-liikmesuse pooldajatele tõestuseks, et Eesti liitumine NATOga oli õige. Seoses viimaste päevade sündmustega suureneb tõenäoliselt ka Eesti Kaitseministeeriumi järgmise aasta eelarverida. (*TS*, 30.08)

Üha sagedamini küsitakse, milline on Eesti ELi ja NATOsse integreerumise väärtus. Rahva arvamus pole Eestis ühtne. Vene vähemus, kes

better integration in terms of the EU's security, energy and neighbourhood policy makes sense. (*La Croix*, 22.04)

The Baltic armed forces are tiny and configured to support NATO efforts in faraway countries, not to defend the region against a real attack from Russia. NATO's military presence consists only of a handful of fighter aircraft based at an air base in Lithuania and a cyber defence centre in Estonia. All three countries have NATO-standard radars that can look deep into Russia. At the same time, the Baltic states will be expected to spend more on defence – no easy task as a sharp economic slowdown bites. (*The Economist*, 4.09)

Estonia's unit in Afghanistan may be small, but it's already seen plenty of action and suffered several casualties. Although Estonia fields one of the smaller contingents among the 40 countries of the ISAF in Afghanistan, its soldiers have seen some of the heaviest fighting. The Estonian public has mixed feelings about the foreign involvement in Iraq and Afghanistan, but regardless of limited human resources, Estonia also has a responsibility before NATO to succeed. If Estonians want to receive help when in need, they have to be able to deliver in return. (*Deutsche Welle World*, 1.06)

Russian activities in Georgia have underpinned for the Estonians supporting NATO that NATO membership is well justified. In the light of recent events, the Estonian Ministry of Defence will probably be allocated more funds in the state budget than it would have otherwise received. (*TS*, 30.08)

It is more and more often asked: what value does Estonia's integration with NATO and the EU create? The Estonian public has mixed feelings.



Saksamaa liidukantsler Angela Merkel rõhutas dialoogi olulisust suhetes Venemaaga.
German Chancellor Angela Merkel emphasised the significance of dialogue in relations with Russia.

saab informatsiooni eelkõige Moskva telekanalitest, mõtleb teisiti kui suurem osa ülejäänud rahvast. Venekeelsed elanikud mõistavad üldiselt Moskva teguviisi. (FAZ, 27.08)

Palsamina Baltimaade elanike kõrvadele kõlasid Saksamaa liidukantsleri Angela Merkeli sõnad, et NATO partnerid on Eestile, Lätile ja Leedule solidaarsed. Kriis Kaukaasias on Balti riikides suurendanud hirmu, et Venemaa võib kallale tungida ka nendele riikidele ning NATO ei astu ka siis Venemaaga vastasseisu. Merkeli Eesti-visitide tähtsaim teema oligi Gruusia-konflikt. Kui Eesti peaminister Andrus Ansip jätkaks dialoogi Venemaaga alles pärast rahuplaani elluviimist, siis Merkel sõnas, et probleeme ei saa lahendada seeläbi, et teineteisega enam ei räägita. (FR, 27.08)

USA kutsus NATOt Balti riike sõjalise rünnaku korral paremini kaitsma. USA uus suursaadik NATO juures, Kurt Volker ütles, et NATO on kohustatud Baltimaaid kaitsma, kuna erinevalt Gruusiast kehtib nende suhtes NATO artikkel 5,

The Russian minority, which mostly gets information from Moscow TV channels, sees things differently than most of the Estonian population. As a rule, the Russian-speaking community sides with Moscow. (FAZ, 27.08)

The confirmation by German Chancellor Angela Merkel that NATO partners are loyal to Estonia, Latvia and Lithuania was music to the ears of the people of the Baltic countries. The crisis in the Caucasus has increased the Baltic nations' fear of Russia potentially attacking their countries and of NATO not confronting Russia in that situation. The main topic during Merkel's visit to Estonia was the Georgia conflict. While the Estonian prime minister would continue the dialogue with Russia only after the peace plan has been implemented, Merkel said that problems cannot be solved by not talking to each other. (FR, 27.08)

The US called on NATO to be better prepared to defend the three Baltic states from military attack. Kurt Volker, the new US ambassador to NATO, said NATO was firmly committed to defending

mis tagab rünnaku puhul ühe liikmesriigi vastu teiste liikmesriikide abi. Pärast Venemaa jõukasutust suveräänse riigi vastu on Balti riigid hirmul, mistõttu peab NATO saatma selgeid signaale Balti riikide kaitsmisest sõjalise planeerimise ja vastavate õppuste näol. Volkeri sõnul peab NATO tagama, et ohu korral on artikkel 5 rakendatav mitte ainult poliitilises, vaid ka sõjalises mõttes. (*FT*, 2.09)

Alliansis on tekkinud diskussioon, kas Venemaal tuleks jälle näha võimalikku sõjalist ohtu. Balti riigid seadsid end suvel demonstratiivselt Gruusia kõrvale ning Eesti president nõudis NATOlt avalikult, et allianss koostaks Balti riikide kaitseplaani. Baltimaid on toetanud NATO Ida-Euroopa liikmesriigid ning USA. Balti riikide nõudmise lükkavad NATO tagasi eelkõige Lääne-Euroopa liitlased. NATO Ida-Euroopa liikmesriikide reaktsioon Gruusia sõjale tekitab kahtluse, et nad võivad tõsise ohu puhul loota ainult Ühendriikidele. Selliste kahtluste hajutamiseks meenutavad sakslased ikka jälle, et osalevad reeglipäraselt Baltimaade õhuruumi valvamisest. Seda tuleks võtta ka poliitilise signaalina, et Saksamaa seisab oma idapoolsete liitlaste kõrval, tekkigu Moskva kui tahes tõsine olukord. (*FAZ*, 3.11)

Kas kübersõda on ikka sõda?

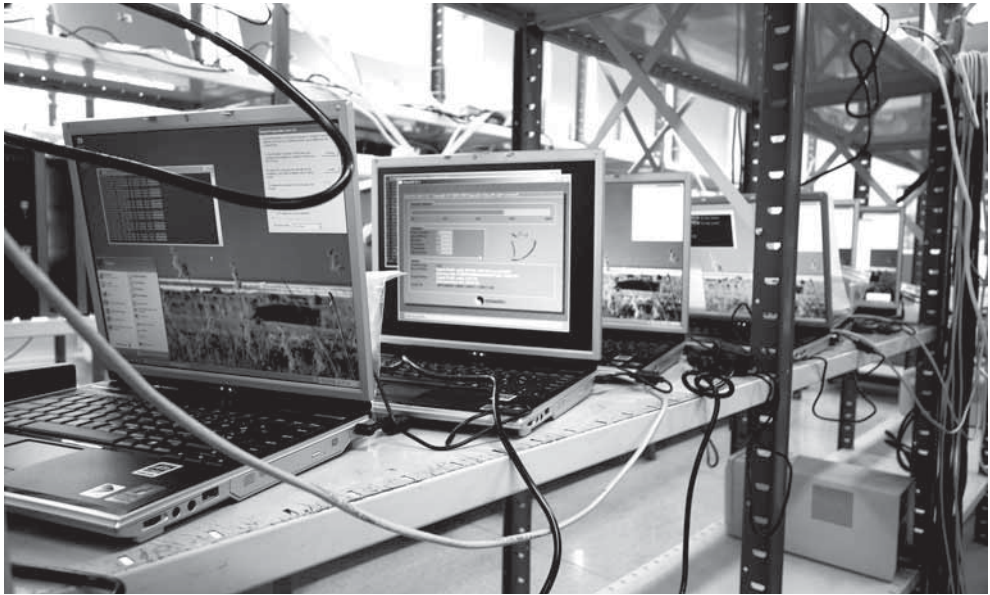
Viimase 15 aastaga on küberruum muutunud aktiivsemaks ning ohtlikumaks, kuna terved riigid sõltuvad kommunikatsiooni, majandustehingute ja info säilitamise vallas arvutivõrgust.

the Baltic states from attack because, unlike Georgia, they were signatories to the alliance's Article 5, which guarantees defence of one ally by all the rest. The Baltic states are feeling a little rattled by seeing Russia use military force to invade a small, sovereign country, and NATO must therefore send signals in the area of military "planning and exercising" that it intends to help shore up the Baltic states. According to Volker, NATO has to make sure that the Article 5 commitment is realisable not just as a political matter, but as a military matter too. (*FT*, 2.09)

The discussion on whether Russia should be seen as a potential military threat has been raised in the alliance. The Baltic nations demonstratively sided with Georgia this summer, and the Estonian president demanded openly that NATO would draw up a defence plan for the Baltic states. The United States and the Eastern European members of NATO have backed the Baltic states. The request made by the Baltic nations is primarily rejected in NATO by the Western European allies. The reaction of Eastern European NATO members to the war in Georgia reveals the concern that they only have the United States to rely on in case of a serious threat. To erase all doubt, Germans remind us every now and again of their regular participation in safeguarding the Baltic airspace. The fact that Germany is supporting its Eastern neighbours, no matter how serious the situation with Moscow could become, should also be taken as a political signal. (*FAZ*, 3.11)

Cyberwar = war?

Cyberspace has become a much busier and more dangerous place in the last 15 years, as entire nations rely on computer networks for communications, economic transfers and information storage. Computers and computer



Eesti soovib jagada oma teadmisi ja kogemusi küberkaitsest.
Estonia is willing to share its expertise in cyber defence.

Seetõttu on arvutid ja arvutivõrgud tõhusad sihtmärgid kurjategijatele. Teisisõnu, 21. sajandil tähendab rünnak riigi elektroonilise infrastruktuuri vastu tõelist sõda. Maailma esimest massilist ja organiseeritud küberrünnakut kogeti 2007. aasta aprilli lõpul Eestis. (*Strategy Page, 1.01*)

Kübersõja ajalugu ei alga Eesti arvutisüsteemidele korraldatud rünnakuga, nagu avalikkusele mulje on jäänud. Olgugi et rünnak Eesti paberivaba valitsuse arvutivõrgu pihta oli üks viimaste aegade enim kajastatud häkkerlusi, ei olnud see esmakordne juhtum. Küberkaitseagentuuri teatel oli Eestit tabanud rünne vaid jäämäe tipp. Sarnaseid küberrünnakuid on korraldatud ka Iisraelist, Indiast, Pakistanist ja USAst. Kõige aktiivsemaks peetakse aga Hiinat, kust lähtunud rünnakud on tabanud nii Pentagoni kui ka Euroopa suurriikide valitsuste arvutivõrke. (*Council of Foreign Relations, 27.02*)

Kui maailma üldsuseni jõudsid teated, et Eesti mõistis mullu kevadistes küberrünnakutes süüdi ühe 20-aastase noormehe, on paljud

networks are lucrative targets for criminals. In other words, in the 21st century targeting a nation's electronic infrastructure is an act of war. The world got a look at the first massed and co-ordinated "hack" at the end of April 2007 in Estonia. (*Strategy Page, 1.01*)

Contrary to popular belief, the evolution of cyberwar does not begin with the attacks organised against Estonian ICT systems. Although the attack on Estonia's paperless government was one of the most publicised hacks in recent history, it wasn't the first case. According to the Cyber Defence Agency, it's the tip of the iceberg. Israel, India, Pakistan and the United States have all been accused of launching similar attacks. China, however, may be the most active. Attacks emanating from China have been targeting the computer systems of the Pentagon as well as major European government agencies. (*Council of Foreign Relations, 27.02*)

After the news of Estonia convicting a 20-year-old man for the cyber attacks last spring, many media outlets raised the question of the cyber

meediaväljaanded kogu kübersõja kui nähtuse kahtluse alla seadnud. Meediat vapustas mulje, et Eestit tabanud DDoS-rünnakud (*Distributed Denial of Service*) ei lähtunud sugugi vihaste Vene sõdalaste käe alt, vaid sõjamonumendi teisaldamise vastu protestinud nooruki häkkeritegevusest. Küberrünnakud Eesti vastu olid tähenduslikud, kuna väikese riigi infrastruktuur sõltub suuresti internetist ning võrguhäired mõjutavad otseselt elanikkonna igapäevaelu. Vaatamata kõigele polnud möödunudkevadiste juhtumite puhul tegemist mitte sõja, vaid protestiga. Maailma esimese tõelise „kübersõja” korral lõigatakse riigi kommunikatsioonikanalid läbi satelliitide hävitamise või telefoniliinide segamisega, katsetatakse finantsvõrkude külmutamist ja võib-olla ka lööki elektrisüsteemi põhivõrkude pihta. (*Information Week, 24.01*)

Nii Gruusia kui ka Eesti vastu suunatud küberrünnakud näitavad, kui raske on defineerida „kübersõda” ja kui raske on selle vastu kaitset leida. Mõnede definitsioonide kohaselt võib kübersõjaks pidada seda rünnakut, mis on suunatud elektrijaamadele või mis pärsib hädaabiteenuseid. Mõni väidab, et küberrünnak kuulub sõja kategooriasse vaid siis, kui see toimub paralleelselt tavasõjaga. Seega oli Gruusias kübersõda, Eestis aga mitte. Euroopa Nõukogu küberkuritegude konventsiooni kohaselt tuleks eraldiseisvat indiviidi, kes kahjustab Eesti veebilehekülgi, kohelda samaväärselt huligaaniga, kes lõhub poevitriini ja põgeneb seejärel Venemaale. Küberkurjategija tuvastamine on aga palju kordi raskem, kui paku läinud huligaani tabamine. Siiski oleks tarvis küberrünnakud ja kübersõda defineerida. Kui see on tõesti sõja liik, siis on rünnaku ohvril õigus enesekaitseks tavasõjas tuntud vahenditega. Sellel on eriti suur tähendus NATO liikmetele, kuna sel juhul peaksid kõik olema valmis

war phenomenon as such. The media was shocked by the implication that the DDoS (Distributed Denial of Service) crippling Estonia were not the result of Russian warriors clicking their mice but the hactivism of a young man protesting the removal of a Soviet war memorial. These attacks against the Baltic nation of Estonia were significant, as a majority of the small nation’s infrastructure is heavily dependent on the internet and crippling the networks directly affects the everyday life of the population. Nonetheless, it wasn’t a war, but a protest. In the world’s first cyberwar, we would witness a nation’s communications blacked out through the destruction of satellites or the tactical crippling of telecommunication lines, attempts at freezing financial networks, and probably a swipe at the power grid. (*Information Week, 24.01*)

The cyber attacks against Georgia and Estonia once again illustrate how complicated it is to define “cyberwar” and how difficult to defend against it. Some define an attack on a power station or an emergency-services call centre an act of cyberwar. Some observers argue it can be classified as war only if taking place alongside actual military operations. The attacks on Georgia might qualify as cyber warfare by this definition, but those on Estonia would not. According to the Council of Europe Convention on Cybercrime, a private individual who defaces an Estonian website ought to be treated in a similar fashion to a hooligan who breaks a shop window and goes into hiding in Russia. But identifying a cyber attacker is far from easy compared with catching a run-off hooligan. However, agreement on the definitions of “cyber attack” and “cyberwar” is needed. If it is truly defined as war, the victim has the right to self-defence with conventional military means. It carries a special meaning for members of NATO, being

sõjaliseks vastuseks, kui mõni riik langeb küberrünnakute ohvriks. Nende küsimustega tegelemiseks ja küberkaitseexpertide ühe katuse alla koondamiseks on NATO avanud Tallinnas uurimiskeskuse. (*The Economist*, 4.12)

Eesti – NATO küberkaitseexpert

Eesti valmistub uute võimalike küberrünnakute tõrjumiseks. Viimase kaheteistkümne kuu jooksul on täheldatud valitsuse infosüsteemide häkkimise mitmeid väiksemaid katseid, kuid need pole olnud aprillikuiste küberrünnakutega võrreldes nii organiseeritud ega mõjusad. Eesti vastu sihitud küberründega seoses hakati spekuloida, et häkkerlust võib kasutada nii luurevahendi kui ka relvana. NATO võttis küberkuritegevuse vastase võitluse päevakorda ning hiljuti Bukarestis toimunud tippkohtumisel arutati Tallinnasse rajatava küberkaitsekeskuse tulevikuplaane. (*The Guardian*, 7.04)

NATO kavandab veel käesoleval aastal küberkaitsekeskuse rajamist Tallinnasse. Eesti püüab poliitilisest hädavajadusest voores teha ning täita kindlat turunišši. NATO kindral John Craddock nimetas Eesti ekspertide saavutusi „äratuskella helinaks” alliansile. (*FTD*, 22.04)

Eesti ning veel seitse NATO liikmesriiki – USA, Saksamaa, Itaalia, Hispaania, Slovakkia, Läti ja Leedu – allkirjastavad mais lepingu, et luua Tallinnasse NATO küberkaitsekeskus. Kuigi ametlikult avatakse keskus alles 2009. aasta alguses, on töö Tallinnas juba käimas. Eesti pakkus NATOle IT-alast abi juba 2004. aastal, kui riik NATOga liitus. (*TS*, 3.04)

Turvaspetsialist Tõnu Samuel on „heahtlik arvutihäkker”: tema tööks on avastada valitsuse

duty-bound to respond to an attack on any of their members. To grapple with questions like these, NATO has set up a cyber centre in Tallinn. (*The Economist*, 4.12)

Estonia as a NATO cyber defence expert

Estonia is bracing itself for a repeat of the internet attacks. There had been many smaller attempts to hack into government systems during the last 12 months but they were not as organised or successful as last year's attacks. The attacks against Estonia prompted speculation that computer hacking was being widely used as a weapon, not just espionage. NATO put combating cybercrimes on the agenda, and the future of a centre for cyber defence in Tallinn was also discussed at a recent NATO summit in Bucharest. (*The Guardian*, 7.04)

NATO plans to open its cyber defence centre in Tallinn before the end of this year. Estonia tried to turn the political necessity into a virtue and fill a specific market niche. NATO general John Craddock dubbed the achievements of Estonian experts a “wake-up call” for the alliance. (*FTD*, 22.04)

In May, Estonia and seven other NATO members – the USA, Germany, Italy, Spain, the Slovak Republic, Latvia and Lithuania – signed a contract to establish the NATO Cyber Defence Centre in Tallinn. The centre is already open, but will be formally inaugurated at the beginning of 2009. Estonia was already offering NATO IT support in 2004 when the country joined the alliance. (*TS*, 3.04)

Security expert Tõnu Samuel is a “benign” hacker: he is employed to find security loopholes in the

ja ettevõtete arvutisüsteemides turvaauke ja testida süsteemide turvalisust. Tänu Samueli-sugustele Eestist pärit arvutiekspertidele suudeti Eestis 2007. aasta kevadel toimunud küberründe käigus halvim ära hoida. Nüüd soovib Eesti jagada oma teadmisi ja kogemusi rahvusvahelisel tasandil, mistõttu rajatakse Tallinnasse esimene rahvusvaheline NATO küberkaitsekeskus. (*The Daily Telegraph*, 26.02)

Küberkaitsekeskus asub vaid kiviviske kaugusel pronksõduri praegusest asupaigast. Uhkest nimest hoolimata meenutab keskus pigem väikest arvutiinstituuti kui maailma võimsaima sõjalise alliansi küberkaitsekeskust. Turvakontroll ja osaline pildistamiskeeld annavad aimu, et tegemist on sõjalise objektiga. See on uurimis-, arendus- ning praktika-keskus, mille ülesanne on luua uusi vahendeid võitluses uute ohtudega. (*HS*, 15.05)

Eestist on saanud NATO kõige parem kübersõjaekspert ja nüüd võivad ka teiste liikmesriikide esindajad tulla siia oma teadmisi täiendama. Aasta eest toimunud küberrünnakud ei suutnud riiki eluliselt haavata, vaid kiirendasid hoopis küberkaitsekeskuse rajamist Tallinnasse. (*Top News*, 12.05)

Kui NATO uue riigi oma liikmeks võtab, peab sel olema alliansile pakkuda muudki lisaks alarahastatud sõjaväele. Eesti on oma tugeva külje leidnud, luues oma jõududega Tallinnasse küberkaitsekeskuse, millest arendatakse seitsme NATO riigi allkirjastatud lepingu kohaselt kompetentsikeskus. Ideed hakati Eestis arendama juba 1990. aastatel, mil Eestist taheti luua IT tipptegijat. (*Kaleva*, 19.05)

Ei ole tavaline, et riik koondab julgeoleku küsimustes kogu tähelepanu avalikesse kanalitesse.

computer systems of government and businesses to identify their weaknesses. Thanks to home-grown computer whizzes like Mr Samuel, the country managed to fend off the worst of April's cyber attack. Now the Estonian government is extending its expertise internationally by opening the first-ever international cyber defence school for NATO. (*The Daily Telegraph*, 26.02)

The building of the Cyber Defence Centre is only a stone's throw from the current site of the Bronze Soldier. The centre is, despite its name, more like a small computer institute than the cyber defence centre of the world's mightiest military alliance. A security check and the fact that you cannot photograph everything reveal that it is a military object. It is a centre of research, development and practice, aimed at creating new means to combat new threats. (*HS*, 15.05)

Estonia has become the top cyberwar expert in NATO, and now professionals from other NATO countries are expected in Tallinn to receive additional training. The cyber attacks of a year ago were not enough to paralyse the nation and stimulated the establishment of a cyber defence centre in Tallinn. (*Top News*, 12.05)

If a country is accepted as a NATO member, it has to have more to offer to the alliance than just under-funded armed forces. Estonia has found its strength through self-reliantly opening the cyber defence centre in Tallinn, which is going to be developed into a Centre of Excellence according to an agreement entered into by seven NATO members. The idea emerged in Estonia in the 1990s already, along with plans to transform Estonia into a leading IT country. (*Kaleva*, 19.05)

Eesti, tõenäoliselt esimene küberrünnaku ohvriks langenud riik, teeb aga just seda. Riigi 36-leheküljeline küberkaitse strateegia annab ülevaate tähtsamatest vastuvõtmist vajavatest otsustest ja täideviimist nõudvatest plaanidest, et kujundada ja turvata julgeoleku seisukohalt vajalikke suhtluskanaleid. Seetõttu on Eesti küberkaitse strateegia möödapääsmatult vajalik lugemismaterjal ka kõigile poliitilise romaani autoreile. (*LeMagIT*, 30.09)

It's unusual for a nation to focus its defence and security issues entirely on public channels. But this is exactly what Estonia, probably the first victim of cyber attack, is doing. The 36-page cyber defence strategy recaps the most important decisions to be made and the plans that are to be implemented to design and defend critical communication channels in terms of security. It also makes the Estonian cyber defence strategy a must-read for all political novelists. (*LeMagIT*, 30.09)