Mnenje Evropskega ekonomsko-socialnega odbora o predlogu direktive Evropskega parlamenta in Sveta o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji

(COM(2013) 48 final – 2013/0027 (COD))

(2013/C 271/25)

Poročevalec: **Thomas McDONOGH**

Svet in Evropski parlament sta 21. februarja oziroma 15. aprila 2013 sklenila, da v skladu s členom 114 Pogodbe o delovanju Evropske unije Evropski ekonomsko-socialni odbor zaprosita za mnenje o naslednjem dokumentu:

Predlog direktive Evropskega parlamenta in Sveta o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji

COM(2013) 48 final – 2013/0027 (COD).

Strokovna skupina za promet, energijo, infrastrukturo in informacijsko družbo, zadolžena za pripravo dela Odbora na tem področju, je mnenje sprejela 30. aprila 2013.

Evropski ekonomsko-socialni odbor je mnenje sprejel na 490. plenarnem zasedanju 22. in 23. maja 2013 (seja z dne 22. maja) s 163 glasovi za, 1 glasom proti in 5 vzdržanimi glasovi.

1. **Sklepi in priporočila**

1.1 Odbor obravnava predlagano direktivo v širšem kontekstu nedavno objavljene strategije za kibernetsko varnost ([1]), katere namen je s celovito vizijo varnosti omrežij in informacij (VOI) zagotoviti varno rast digitalnega gospodarstva ter nadaljnji razvoj evropskih vrednot, kot sta svoboda in demokracija.

1.2 EESO pozdravlja predlog direktive, ki bo zagotovila visoko skupno raven VOI v vsej EU. Harmonizacija in upravljanje VOI na evropski ravni sta bistvenega pomena za dokončno vzpostavitev enotnega digitalnega trga in nemoteno delovanje notranjega trga kot celote. Tako kot Komisija je tudi Odbor zaskrbljen zaradi neizmerne škode, ki bi jo motena VOI lahko pomenila za gospodarstvo in blaginjo državljanov. Vendar pa predlagana direktiva ne izpolnjuje pričakovanj Odbora o odločnih zakonodajnih ukrepih v zvezi s tem občutljivim vprašanjem.

1.3 Odbor je izjemno razočaran, ker v številnih državah članicah ni bilo napredka pri učinkovitem izvajanju VOI na nacionalni ravni. Zato opozarja na povečano tveganje zaradi tega pomanjkanja za državljane ter negativni učinek na dokončanje enotnega digitalnega trga. Vse države članice se morajo nemudoma posvetiti neizpolnjenim obvezam, ki jih imajo na področju VOI.

1.4 Zastoj pri izvajanju ustvarja nov digitalni razkorak med elitno skupino držav članic z izjemno napredno VOI in manj naprednimi državami članicami. Ta razkorak ogroža zaupanje in sodelovanje na področju VOI na ravni EU in če ne bo takoj obravnavan, bo zaradi razlik v zmogljivostih posameznih držav članic verjetno ohromil delovanje notranjega trga.

1.5 Kot je EESO navedel že v prejšnjih mnenjih ([2]), tudi tokrat meni, da neodločni ukrepi, ki temeljijo na prostovoljnem upoštevanju pravil, ne delujejo, zato je treba za države članice pripraviti stroge regulativne obveznosti, da se zagotovijo harmonizacija, upravljanje in uveljavljanje VOI na evropski ravni. Vendar žal meni, da obravnavani predlog direktive ne vsebuje potrebne jasne in odločne zakonodaje. Po mnenju Odbora bi bilo potrebno visoko skupno raven VOI mogoče učinkoviteje zagotoviti z uredbo z jasno opredeljenimi zakonskimi obveznostmi za države članice kot pa z direktivo.

1.6 Kljub nameri Komisije, da sprejme delegirane akte, s katerimi želi zagotoviti nekatere enotne pogoje za izvajanje delov direktive, Odbor ugotavlja, da je v predlogu navedenih premalo standardov, jasnih definicij in kategoričnih obveznosti, kar državam članicam daje preveč svobode pri tolmačenju in prenosu ključnih elementov direktive. Meni, da bi morala direktiva vsebovati veliko natančnejše definicije standardov, zahtev in postopkov, ki veljajo za države članice, javne organe, tržne udeležence in glavne ponudnike spletnih storitev.

([1]) Strategija Evropske unije za kibernetsko varnost: odprt, varen in zanesljiv kibernetski prostor, JOIN(2013) 1.

([2]) Mnenji EESO o *zaščiti kritične informacijske infrastrukture*, UL C 255, 22.9.2010, str. 98 in o *direktivi o napadih na informacijske sisteme*, UL C 218, 23.7.2011, str. 130.

1.7 EESO se zavzema za vzpostavitev organa za VOI na ravni EU, ki bi podobno kot osrednji organ za letalsko industrijo (EASA) ([3]) skrbel za oblikovanje odločnih politik in izvajanje VOI v EU. Poleg tega bi določil standarde in spremljal izvrševanje vseh elementov VOI v Uniji: od certificiranja zaščitenih terminalskih naprav in uporabe do varnosti omrežij in podatkov.

1.8 EESO se zelo dobro zaveda, da so se z uveljavitvijo računalništva v oblaku ([4]) v Evropi povečala tveganja, povezana s kibernetsko varnostjo in zaščito podatkov. Zato se zavzema, da bi bile v predlagano direktivo izrecno vključene posebne dodatne varnostne zahteve in obveznosti v zvezi z zagotavljanjem in uporabo storitev računalništva v oblaku.

1.9 Zaradi zagotavljanja ustrezne odgovornosti za VOI bi moralo biti v predlogu direktive jasno navedeno, da imajo vse pravne in fizične osebe, za katere velja predlagana direktiva, pravico, da dobaviteljem programske in strojne opreme naložijo odgovornost za kakršne koli napake v zvezi z izdelki ali storitvami, ki neposredno prispevajo k incidentom na področju VOI.

1.10 EESO poziva države članice, naj posebno pozornost namenijo izboljšanju znanja o VOI in spretnostih, povezanih s kibernetsko varnostjo, v malih in srednjih podjetjih (MSP). Prav tako opozarja Komisijo, kako uspešno so s „hekerskimi tekmovanji" v ZDA ([5]) in nekaterih državah članicah ([6]) izboljšali ozaveščenost o kibernetski varnosti in vzgojili novo generacijo strokovnjakov za VOI.

1.11 Glede na to, kako pomembno je, da vse države članice upoštevajo VOI v EU, EESO predlaga Komisiji, naj razmisli, kakšno financiranje iz naslova večletnega finančnega okvira bi lahko bilo na voljo v ta namen za države, ki potrebujejo finančno pomoč.

1.12 Namenjanje sredstev za raziskave, razvoj in inovacije na področju tehnologij VOI bi moralo biti ena glavnih prednostnih nalog okvirnega programa EU za raziskave in inovacije Obzorje 2020, če želi Evropa ostati na tekočem z nenehno spreminjajočim se področjem kibernetskih groženj.

1.13 EESO se zavzema, da bi se vsem državam članicam naložila obveznost, da objavijo spletni register vseh fizičnih in pravnih oseb, za katere veljajo zahteve direktive v zvezi z upravljanjem tveganj in poročanjem, zato da se razjasni, katerim pravnim in fizičnim osebam predlagana direktiva nalaga zakonske obveznosti. Taka preglednost in javna odgovornost bi spodbudila zaupanje in spoštovanje ureditve.

1.14 Odbor opozarja Komisijo na svoja številna prejšnja mnenja, v katerih je obravnaval varnost omrežij in informacij ter pozval k varni informacijski družbi in zaščiti kritične infrastrukture ([7]).

2. **Kratka vsebina predloga Komisije**

2.1 Predlagana direktiva o VOI je bila objavljena sočasno s strategijo EU za kibernetsko varnost, katere namen je okrepiti odpornost informacijskih sistemov, zajeziti kibernetsko kriminaliteto, izboljšati mednarodno politiko EU za kibernetsko varnost in obrambo, razviti industrijske in tehnološke vire za kibernetsko varnost ter spodbujati temeljne pravice in vrednote EU.

2.2 VOI se nanaša na zaščito interneta in drugih omrežij, informacijskih sistemov in podpornih storitev, ki omogočajo delovanje naše družbe, in je nepogrešljiva za nemoteno delovanje notranjega trga.

2.3 Pristop, ki temelji izključno na prostovoljnem upoštevanju pravil v zvezi z VOI in ki še vedno velja v EU, ne zagotavlja zadostne zaščite pred tveganji za VOI. Obstoječe zmogljivosti VOI ne zadoščajo za dohajanje hitro spreminjajočih se groženj in ne zagotavljajo skupne visoke ravni zaščite v vseh državah članicah.

([3]) Evropska agencija za varnost v letalstvu: http://easa.europa.eu

([4]) Mnenji EESO o *računalništvu v oblaku (cloud computing) v Evropi*, UL C 24, 28.1.2012, str. 40 in o *sprostitvi potenciala računalništva v oblaku v Evropi*, UL C 76, 14.3.2013, str. 59.

([5]) http://www.nytimes.com/2013/03/25/technology/united-states-wants-to-attract-hackers-to-public-sector.html?pagewanted=all&_r=0

([6]) http://www.bbc.co.uk/news/technology-17333601

([7]) Mnenje EESO o *strategiji za varno informacijsko družbo*, UL C 97, 28.4.2007, str. 21.
Mnenje EESO o *zaščiti kritične informacijske infrastrukture*, UL C 255, 22.9.2010, str. 98.
Mnenje EESO o *„novi" uredbi o Evropski agenciji za varnost omrežij in informacij*, UL C 107, 6.4.2011, str. 58,
Mnenje EESO o *splošni uredbi o varstvu podatkov*, UL C 229, 31.7.2012, str. 90.
Mnenje EESO o *napadih na informacijske sisteme*, UL C 218, 23.7.2011, str. 130.
Mnenje EESO o *elektronskih transakcijah na notranjem trgu*, UL C 351, 15.11.2012, str. 73.
Mnenje EESO o *sprostitvi potenciala računalništva v oblaku v Evropi*, UL C 76, 14.3.2013, str. 59.

2.4 Države članice imajo različne zmogljivosti in so različno pripravljene, zato so tudi pristopi k VOI v EU neenotni. Omrežja in sistemi so med sabo povezani, kar pomeni, da države članice z nezadostno ravnjo zaščite slabijo splošno VOI v Uniji. Tako stanje pa preprečuje tudi vzpostavitev zaupanja med partnerji, kar je pogoj za sodelovanje in izmenjavo informacij. Zato sodelovanje poteka le med nekaj državami članicami z visoko ravnijo zmogljivosti.

2.5 Namen direktive, ki je predlagana v skladu s členom 114 PDEU, je omogočiti dokončno vzpostavitev in nemoteno delovanje enotnega digitalnega trga:

— vzpostaviti minimalno skupno raven VOI v državah članicah ter tako povečati splošno raven pripravljenosti in odzivanja na incidente;

— izboljšati sodelovanje na področju VOI na ravni EU za učinkovito odzivanje na čezmejne incidente in grožnje;

— vzpostaviti kulturo obvladovanja tveganj ter izboljšati izmenjavo informacij med zasebnim in javnim sektorjem.

2.6 Predlagana direktiva med pravnimi zahtevami med drugim določa naslednje:

(a) Vsaka država članica mora sprejeti strategijo VOI in vzpostaviti nacionalni organ za VOI z zadostnimi finančnimi in kadrovskimi sredstvi za preprečevanje in obvladovanje tveganj in incidentov VOI ter odzivanje nanje.

(b) Vzpostaviti je treba mehanizem za sodelovanje med državami članicami in Komisijo za izmenjavo zgodnjih opozoril o tveganjih in incidentih ter organizacijo rednih medsebojnih pregledov.

(c) Določene pravne in fizične osebe v EU bodo morale uvesti prakse za obvladovanje tveganja in nacionalnemu organu za VOI poročati o večjih varnostnih incidentih v zvezi s svojimi osnovnimi storitvami. Mednje sodijo upravljavci kritične informacijske infrastrukture v nekaterih sektorjih (finančne storitve, promet, energija, zdravstvo), ponudniki storitev informacijske družbe (zlasti računalništva v oblaku, platform za e-trgovanje, spletnih plačil, iskalnikov, prodajaln aplikacij in družbenih omrežij) in javne uprave.

2.7 Države članice bodo morale začeti izvajati direktivo v 18 mesecih od njenega sprejetja v Svetu in Evropskem parlamentu (predvidoma leta 2014).

3. **Splošne ugotovitve**

3.1 Razširjenost interneta in razvoj digitalne družbe močno vplivata na vsakdanje življenje. A bolj ko smo odvisni od interneta, bolj so tudi naša svoboda, blaginja in kakovost življenja odvisne od zanesljive varnosti omrežij in informacij. Če se na oddelku za nujno medicinsko pomoč prekine povezava z internetom in so elektronske zdravstvene kartoteke nedostopne, to lahko za paciente pomeni gotovo smrt. Vendar pa je varnost evropske kritične informacijske infrastrukture vse bolj ogrožena in tudi raven VOI je nezadostna.

3.2 Direktor Europola je lani dejal, da ga zelo skrbi vsesplošno slepo zaupanje v neuničljivost interneta ([8]). Poročila o novih kibernetskih napadih kriminalcev, teroristov ali tujih vlad na ključno infrastrukturo so pogosta. Napadene strani večine napadov ne prijavijo, saj se bojijo, da bi to okrnilo njihov ugled; kljub temu pa smo pred kratkim lahko izvedeli za napada na evropsko internetno infrastrukturo ([9]) in bančne sisteme ([10]), ki sta povzročila preveč motenj, da bi ju bilo mogoče prikriti. Po ocenah enega poročila ([11]) je bilo leta 2011 na Nizozemskem 92, v Nemčiji pa 82 milijonov kibernetskih napadov. Vlada Združenega kraljestva ocenjuje, da je bilo leta 2011 na Otoku 44 milijonov kibernetskih napadov, ki so povzročili za 30 milijard EUR gospodarske škode ([12]).

3.3 Svet EU je leta 2007 obravnaval problem VOI v Evropi ([13]). Vendar pa je poznejši politični pristop ([14]) temeljil večinoma na prostovoljnem ukrepanju držav članic, kar je učinkovito storila le peščica. Odbor ugotavlja, da številne države članice niso niti objavile nacionalne strategije za kibernetsko varnost niti pripravile nacionalnega načrta za ravnanje v primeru kibernetskega incidenta, nekatere pa sploh še niso oblikovale skupin za odzivanje na računalniške grožnje (CERT). Poleg tega jih precej še ni ratificiralo Konvencije Sveta Evrope o kibernetski kriminaliteti ([15]).

([8]) http://forumblog.org/2012/05/what-if-the-internet-collapsed/
([9]) http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?pagewanted=all&_r=0
([10]) http://www.dutchnews.nl/news/archives/2013/04/online_retailers_demand_banks.php
([11]) http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011
([12]) UK Cyber Security Strategy – Landscape Review: http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf
([13]) Resolucija Sveta 2007/C 68/01.
([14]) COM(2006) 251 in COM(2009) 149.
([15]) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

3.4 Deset držav članic, ki so izrazito napredne na področju VOI, je za potrebe tesnega sodelovanja in odzivanja na incidente oblikovalo skupino evropskih vladnih CERT (EGC). EGC trenutno ne sprejema novih članic in sedemnajst manj naprednih držav članic ter novoustanovljena skupina CERT-EU ([16]) so iz te elitne skupine izključene. Nastaja nov digitalni razkorak med državami članicami z izjemno napredno VOI in preostalimi. Če ga ne bomo premagali, bo vrzel na področju VOI hud udarec za enotni digitalni trg, saj bo zavrla vzpostavitev zaupanja ter razvoj harmonizacije in interoperabilnosti. Poleg tega se bo brez odločnega ukrepanja vrzel med naprednimi in manj naprednimi državami članicami nemara še poglabljala, z njo pa bodo vse večje tudi pomanjkljivosti notranjega trga, ki so posledica razlik v zmogljivostih posameznih držav.

3.5 Uspeh strategije za kibernetsko varnost in učinkovitost predlagane direktive VOI bosta odvisna od tega, ali bo Evropa imela močno industrijo VOI in dovolj strokovnjakov na tem področju. EESO izraža zadovoljstvo, da je v predlog direktive vključen poziv državam članicam, naj vlagajo v izobraževanje, ozaveščanje in usposabljanje. Rad pa bi videl tudi, da bi si vsaka država članica prav posebej prizadevala za obveščanje, izobraževanje in podporo sektorju MSP na področju kibernetske varnosti. Velika podjetja lahko to znanje dobijo zlahka, MSP pa potrebujejo podporo.

3.6 EESO se veseli sodelovanja z Evropsko agencijo za varnost omrežij in informacij (ENISA) pri promociji VOI v okviru meseca kibernetske varnosti, ki bo v drugi polovici letošnjega leta. Odbor v zvezi s ciljem, navedenim v strategiji za kibernetsko varnost in direktivi VOI, da je treba v Uniji razviti kulturo zavedanja varnosti in dvigniti raven spretnosti na področju VOI, opozarja Komisijo na „hekerska tekmovanja“ za najstnike, s katerimi so v ZDA in nekaterih državah članicah zelo uspešno povečali ozaveščenost.

3.7 Odbor prav tako z veseljem ugotavlja, da je v strategiji za kibernetsko varnost izražena zavezanost k dodeljevanju sredstev za raziskave, razvoj in inovacije na področju VOI.

3.8 S širjenjem računalništva v oblaku se pojavljajo nova tveganja za kibernetsko varnost, ki jih je treba obravnavati. Kibernetski kriminalci imajo danes na primer za razmeroma malo denarja na voljo neznansko zmogljive računalnike, medtem ko so podatki več tisoč podjetij shranjeni v centraliziranih podatkovnih središčih, ki jim grozi nevarnost zaradi usmerjenih napadov. EESO je že pozval k boljši kibernetski odpornosti računalništva v oblaku ([17]).

([16]) CERT-EU je stalna skupina institucij, agencij in organov EU za odzivanje na računalniške grožnje.

([17]) Mnenji EESO o *računalništvu v oblaku (cloud computing) v Evropi*, UL C 24, 28.1.2012, str. 40 in o *sprostitvi potenciala računalništva v oblaku v Evropi*, UL C 76, 14.3.2013, str. 59.

3.9 Odbor se je tudi že zavzel za uvedbo prostovoljne sheme e-identifikacije EU za spletne transakcije, ki bi dopolnila sedanje nacionalne sheme. Omogočila bi višjo stopnjo zaščite pred prevarami, boljše zaupanje med gospodarskimi subjekti, manjše stroške in večjo kakovost zagotavljanja storitev ter boljšo zaščito državljanov.

4. **Posebne ugotovitve**

4.1 Predlog Komisije za direktivo VOI je žal premalo odločen in jasen ter se v preveliki meri zanaša na samourejanje v državah članicah. Zaradi pomanjkanja standardov, jasnih definicij in kategoričnih obveznosti, zlasti v poglavju IV, imajo države članice preveč svobode pri tolmačenju in prenosu ključnih elementov direktive. Uredba z jasno opredeljenimi zakonskimi obveznostmi za države članice bi bila učinkovitejša kot direktiva.

4.2 Odbor ugotavlja, da bi morala vsaka država članica v skladu s členom 6 predlagane direktive določiti „pristojni organ“, ki bi spremljal in zagotovil dosledno uporabo te direktive v vsej Uniji. Ugotavlja tudi, da je v členu 8 predvidena „mreža za sodelovanje“, ki bi bila s Komisijo pristojna za vodenje, upravljanje in po potrebi izvrševanje, tudi na ravni držav članic. Po mnenju EESO bi morala EU glede na ta okvir upravljanja razmisliti o ustanovitvi organa za VOI na ravni EU po vzoru osrednjega organa za letalsko industrijo (EASA), ki določa standarde ter upravlja področji izvrševanja varnostnih zahtev in skladnosti zrakoplovov, letališč in letalskih operaterjev.

4.3 Podlaga za ustanovitev organ za VOI na ravni EU, ki ga predlaga Odbor v točki 4.2, bi lahko bilo delo na področju kibernetske varnosti, ki ga že zdaj opravljajo ENISA, Evropski odbor za standardizacijo (CEN), skupine CERT, skupina EGC in drugi. Tak organ bi oblikoval standarde in spremljal izvrševanje vseh elementov VOI: od certificiranja zaščitenih terminalskih naprav in uporabe do varnosti omrežij in podatkov.

4.4 Glede na visoko stopnjo soodvisnosti med državami članicami pri zagotavljanju VOI v vsej Uniji in potencialne zelo visoke stroške negativnih dogodkov v zvezi z VOI za vse udeležene strani EESO predlaga, naj zakonodaja vsebuje izrecne in sorazmerne kazni za neizpolnjevanje zahtev, ki naj bodo harmonizirane, da bodo odražale vseevropsko razsežnost odgovornosti in obseg škode, ki bi lahko bila povzročena ne samo na domačem trgu, temveč tudi drugod v Uniji. Člen 17, v katerem so določene sankcije, je presplošen, državam članicam pušča preveč manevrskega prostora in ne zagotavlja zadostnih smernic, ki bi se nanašale na čezmejne in vseevropske učinke.

4.5 Vlade in izvajalci ključnih storitev danes ne objavljajo informacij o problemih z varnostjo in odpornostjo, če niso v to prisiljeni. Zaradi nerazkrivanja pa je zmanjšana zmožnost Evrope, da se hitro in učinkovito odzove na kibernetske grožnje ter s skupnim učenjem izboljša splošno VOI. Odbor pozdravlja odločitev Komisije, da je v skladu z direktivo obvezno priglasiti vse pomembnejše incidente v zvezi z VOI. Ne verjame namreč, da bi bilo prostovoljno poročanje o incidentih na lastno pobudo učinkovito, saj strah, povezan z ugledom in odgovornostjo, spodbuja prikrivanje incidentov.

4.6 Vendar v členu 14 direktive, ki obravnava priglasitev, ni izrecno določeno, kaj je incident z „bistvenim vplivom“ na varnost, poleg tega pa je zadevnim fizičnim ali pravnim osebam in državam članicam prepuščeno preveč izbire o priglasitvi ali nepriglasitvi incidenta. Učinkovita zakonodaja terja nedvoumne zahteve. Predlagana direktiva jih opredeljuje preohlapno, zato od udeleženih strani ni mogoče terjati odgovornosti za kršitve, kot je to navedeno v členu 17 direktive.

4.7 Za zagotavljanje VOI skrbi predvsem zasebni sektor, zato je pomembno, da se spodbuja visoka raven zaupanja in sodelovanja z vsemi podjetji, ki so odgovorna za kritično informacijsko infrastrukturo in storitve. Pobudo Evropske komisije iz leta 2009 o evropskem javno-zasebnem partnerstvu za odpornost (EP3R) je treba pozdraviti in ji izraziti vso podporo. Vendar jo je po mnenju Odbora treba okrepiti in podpreti z regulativnimi obveznostmi v direktivi o VOI, da se k sodelovanju zaveže ključne akterje, ki tega še niso storili.

4.8 Vsaka država članica bi morala objaviti spletni register vseh fizičnih in pravnih oseb pod njeno pristojnostjo, za katere veljajo zahteve v zvezi z varnostjo in poročanjem o incidentih v skladu s členom 14 predlagane direktive. To bi omogočilo pregled nad tem, kako posamezne države članice uporabljajo definicije iz člena 3 predlagane direktive, in prispevalo k ustvarjanju zaupanja in kulture obvladovanja tveganj med državljani.

4.9 EESO ugotavlja, da zahteve direktive izrecno ne veljajo za razvijalce programske opreme in proizvajalce strojne opreme, saj ti niso ponudniki storitev informacijske družbe. Vendar Odbor meni, da bi bilo treba v predlogu dati fizičnim in pravnim osebam, na katere se nanašajo zahteve direktive, pravico, da od dobaviteljev programske in strojne opreme zahtevajo odškodnino zaradi pomanjkljivosti pri izdelkih ali storitvah, ki neposredno prispevajo k incidentom na področju VOI.

4.10 Komisija sicer ocenjuje, da bi izvajanje predlagane direktive o VOI stalo približno 2 milijardi EUR na leto, ki bi bili porazdeljeni med evropski javni in zasebni sektor, vendar Odbor ugotavlja, da bodo nekatere države članice, ki so v finančnih težavah, le stežka zagotovile potrebna sredstva za izpolnjevanje zahtev. Treba je razmisliti, kako bi bilo mogoče v sklopu večletnega finančnega okvira zagotoviti podporo za izpolnjevanje zahtev na področju VOI z različnimi instrumenti, med drugim iz Evropskega sklada za regionalni razvoj (ESRR) in morda Sklada za notranjo varnost.

V Bruslju, 22. maja 2013

Predsednik
Evropskega ekonomsko-socialnega odbora
Henri MALOSSE