PIARC TF C.1 Security

Aktivni član: **Bine Pengal, ZAG** Trenutni cikel: **2016-2019**

Kratek opis delovne skupine in vloge člana

Posebna delovna skupina *Task Force C.1 Security* je bila ustanovljena kot neposredno nadaljevanje dela, ki je bilo opravljeno v okviru prve takšne delovne skupine, to je TF2 (delovala 2012-2014). Nadaljevali smo z osvetljevanjem tematike zaščite cestne infrastrukture pred namernim poškodovanjem, morebitnih ogrožanj in metodologij za preventivo in ukrepanje.

Narava posebnih delovnih skupin je, da imajo rok delovanja 2 leti (v našem primeru nam je bilo zaradi določenih okoliščin odobreno podaljšanje delovanja do jeseni 2018, da smo lahko zaključili končno poročilo).

V skupini sem nastopal tudi v vlogi administratorja spletne strani.

Sestanki in stroški v letu ali obdobju

V času delovanja skupine smo imeli naslednje sestanke, ki sem se jih udeležil:

- 28. junij 2016 Kick-off sestanek, Pariz, Francija (strošek udeležbe 788 €)
- 14.-15. september 2017 delovni sestanek, Dunaj, Avstrija (strošek udeležbe 286 €)
- 21.-22. marec 2018 delovni sestanek, Rim, Italija (strošek udeležbe 376 €)
- 19.-20. september 2018 delovni sestanek Ljubljana, Slovenija (pogostitev sofinancirana s strani NK PIARC Slovenija v višini 281 €)

Glavni vsebinski poudarki

Na začetnem sestanku v Parizu smo začrtali glavne smernice, teme, ki jih želimo osvetliti v tem mandatu: (1)natančen opis in predstavitev realnih virov ogrožanja cestne infrastrukture; (2) kibernetski napadi na programsko opremo za upravljanje prometa in na centre za vodenje prometa; (3) razlaga glavnih teoretskih pojmov, odpornost, ranljivost; (4) prikaz in analiza nekaj praktičnih študij primerov z razlago ukrepov za zmanjšanje posledic napada.

Glavna usmeritev v metodološkem pristopu k zavarovanju in zaščiti infrastrukture se v zadnjem času uveljavlja koncept »odpornosti«. Obrambe pred vsemi možnimi napadi ni mogoče načrtovati niti si jih ni mogoče zamisliti. Cestno infrastrukturo je potrebno utrditi in zavarovati tako, da lahko napad prenese s čim manjšimi posledicami in se čim prej povrne v delovanje. Seveda se ob tem velik poudarek daje tudi na preventivnih ukrepih, ki otežujejo načrtovanje in samo izvedbo napada. Pomembna sta tu koncepta »security in design« in »security in maintenance«, zavedanje, da mora biti varovanje in zaščita infrastrukture zelo visoko na seznamu prioritet cestnih uprav že pri gradnji, rekonstrukcijah in vzdrževanju objektov.

V porastu je trenutno uporaba vozil za napad na ostale udeležence v prometu, za napade na samo infrastrukturo pa kibernetski napadi (t.i. cyber-attack) oziroma napadi na programski del centrov za vodenje prometa in upravljanje predorov, mostov, semaforjev, itd. V prihodnosti se pričakuje porast zlasti vdorov v informacijske sisteme od zunaj in poskusi prevzema nadzora nad upravljanjem prometa.