Če odpove informacijsko-komunikacijska podpora

Vloga informacijsko-komunikacijske tehnologije je razpeta med državnim interesom in interesom komercialnih operaterjev

DELO - ZNANOST; dr. Tomi Mlinar, Slovensko društvo za elektronske komunikacije

Po osnovni definiciji (UL RS št. 35/2011) je evropska kritična infrastruktura (EKI) tista infrastruktura, ki je postavljena v državah članicah EU in katere okvara ali uničenje bi imela resne posledice v vsaj dveh državah članicah, kritična infrastruktura (KI) državnega pomena pa so tiste zmogljivosti, ki so ključnega pomena za državo in bi prekinitev njihovega delovanja ali pomembno uničenje imelo resne posledice za nacionalno varnost, gospodarstvo ...

Po pomembnosti (sklep vlade RS št. 80200-2/2013/3 z dne 9. januarja 2014) je v Sloveniji kritična infrastruktura razdeljena v naslednjem vrstnem redu: zagotavljanje električne energije, informacijsko-komunikacijska podpora, preskrba s pitno vodo in hrano, zdravstvena oskrba, preskrba z naftnimi derivati, zagotavljanje železniškega in letalskega prometa, delovanje pristaniške dejavnosti itd. Kot vidimo, je informacijsko-komunikacijska podpora na drugem mestu po pomembnosti, saj je njeno pravilno in neprekinjeno delovanje odločilnega pomena tako v vsakdanjem delu kot v primeru kritičnih stanj.

Direktiva o evropski kritični infrastrukturi (114/2008/ES) se osredotoča predvsem na energetski in prometni sektor, pomembno vlogo v prihodnosti pa daje tudi sektorju informacijskih in komunikacijskih tehnologij (IKT), vendar ga ne vključuje.

V slovenski uredbi je med drugim določen postopek za določanje EKI v Sloveniji (kontaktna točka za področje varovanja EKI je v direktoratu za obrambne zadeve na ministrstvu za obrambo). Ta uredba ugotavlja, da spadajo v EKI v energetskem sektorju naslednji podsektorji: (1) obrati za pridobivanje in prenos električne energije, (2) proizvodnja, predelava, skladiščenje in prenos nafte prek naftovodov, (3) proizvodnja, predelava, skladiščenje in prenos plina po plinovodih, v prometnem sektorju pa: (1) cestni, (2) železniški in (3) letalski promet, (4) prevoz po celinskih plovnih poteh ter (5) čezoceanski prevoz in pomorski prevoz na kratke razdalje in pristanišča.

Po dosegljivih podatkih (*http://www.mo.gov.si/si/delovna_podrocja/zascita_kriticne_infrastrukture/*) in po njeni osnovni definiciji evropska kritična infrastruktura na ozemlju Slovenije ni bila ugotovljena. Aprila 2014 je vlada sprejela sklep, s katerim je določila kritično infrastrukturo državnega pomena.

Povezanost kritičnih infrastruktur

Nedvomno so različne infrastrukture med seboj povezane in zaradi tega odvisne ali soodvisne. Najpomembnejši sektor, od katerega so vsaj na srednji in dolgi rok odvisni drugi sektorji, je energetski. Takoj za njim oziroma preskrbo z električno energijo pa je po pomembnosti informacijsko-komunikacijski sektor. Za njim sta celo preskrba z vodo in hrano.

Vlada RS je v sklepu z dne 9. januarja 2014 potrdila pobudo, ki jo je pripravilo ministrstvo za obrambo in s katero je predlagalo sektorske kriterije kritičnosti za določanje kritične infrastrukture državnega pomena v Sloveniji. Ti so določeni za sektorje prometa, financ, varstva okolja in informacijsko-komunikacijske podpore. Slednji zajema nedelovanje elektronsko-komunikacijske opreme, omrežja in storitev, ki podpirajo ključne funkcije v državi, ki se nanašajo na zagotavljanje delovanja enega od sektorjev kritične infrastrukture nacionalnega varnostnega sistema, energetskega sistema in financ, ki povzroči izpad podpore za več kot 6 oziroma 24 ur.

Sektor, ki je globoko vpet v druge in že nekaj desetletij velja za najhitreje rastočega, je sektor informacijsko-komunikacijskih tehnologij. Informatika je danes del tako rekoč vsakega sodobnega sistema. Lahko govorimo o odvisnosti od informacij in od komunikacij. Dober primer je lanska naravna nesreča – žled, ki je po nekaj urah, ko so se izpraznili rezervni napajalni sistemi (baterije), povsem ohromil na stotine baznih postaj mobilnih operaterjev in s tem nujno potrebno komunikacijo. Če bi se podobna naravna nesreča zgodila pred desetletji, ko je imela skoraj vsaka hiša fiksni telefonski priključek z napajanjem iz telefonske centrale Telekoma, bi vsaj te komunikacije delovale.

Iz tega primera lahko sklepamo, da je od operaterjev infrastrukture, ki so lahko v državni ali zasebni lasti, odvisno, kako poskrbijo za podvajanje kapacitet oziroma redundantne zveze. V večini gre za mešanico državnega strateško-varnostnega vprašanja in komercialnega interesa operaterjev, zato si morata še v času brez kritičnih situacij obe strani stopiti nasproti. Zakon o elektronskih komunikacijah operaterjem omrežij sicer predpisuje, da morajo pri izrednih razmerah prednostno zagotavljati delovanje tistih delov omrežja, ki so ključni za delovanje omrežij varnostnega in obrambnega sistema države ter zaščite in reševanja. Predvsem morajo zagotavljati nemoten dostop in uporabo številk za klic v sili, kar pa je v primeru izrednih razmer praktično nemogoče. Ali so operaterji za to usposobljeni, preverja Agencija za komunikacijska omrežja in storitve (AKOS), poudariti pa velja še enkrat, da je bolj kot zakonska prisila in nadzor pomemben enoten pristop k izzivom, saj kratko navadno potegnejo

uporabniki, ko izredne razmere nastopijo. Zato sta se Uprava RS za zaščito in reševanje (URSZR) in AKOS že začela dogovarjati z operaterji mobilne telefonije o določitvi prioritetnih telekomunikacijskih objektov, določitvi energetskih potreb za ustrezno oskrbo z agregati in razdelitvi območij med operaterje.

Izredne razmere pa lahko nastopijo tudi, ko so komunikacijska omrežja ali informacijski sistemi napadeni – govorimo o kibernetskih napadih ali grožnjah. Lahko jih napadejo hekerji za lastno zabavo ali zaslužek ali teroristi z namenom onemogočiti druge pomembne infrastrukture in povzročiti večjo škodo. Kaj bi pomenil kibernetični napad – vdor v informacijski sistem npr. jedrske elektrarne, si lahko mislimo. V britanski *Strategiji nacionalne varnosti* so kibernetski napadi označeni kot grožnja številka ena za nacionalno varnost in so postavljeni ob bok mednarodnemu terorizmu.

Skoraj enakovredno ali še bolj pomembno je delovanje informacijskih sistemov, ki danes krmilijo vse življenjsko pomembne, tudi kritične infrastrukture (dobavo vode, čistilne naprave, elektrarne, prometne tokove pristanišč, letališč itd.). Ker je ta infrastruktura večinoma vodena na daljavo in je povezana z bolj ali manj varno povezavo v neko omrežje, so kibernetični napadi raznih »haktivistov« (= heker + aktivist, politično motiviran heker) vedno bolj enostavni.

Komunikacijska omrežja za kritične razmere

V Sloveniji imamo že dolgo postavljen analogni sistem radijskih zvez ZARE, ki deluje na frekvenčnih območjih VHF in UHF. Poleg tega imamo še mrežo repetitorjev osebnega klica in digitalni sistem ZARE DMR. Po sklepu vlade se predvideva postavitev enotnega digitalnega radijskega omrežja državnih organov s kombinacijo digitalnega radijskega omrežja policije TETRA in digitalnega radijskega omrežja uprave za zaščito in reševanje DMR.

Komunikacijsko omrežje Tetra je neodvisno omrežje, namenjeno komunikaciji državnih organov. S svojimi lastnostmi je prilagojeno komunikacijam v kritičnih razmerah, predvsem v prometu (ceste, letališča …), zato je njegov velik uporabnik policija; pomembna lastnost Tetre je šifriranje komunikacijske povezave.

Naslednje pomembno radijsko omrežje, razvejeno po celotni državi vzdolž železniških povezav, ki je v fazi gradnje, je omrežje GSM-R. Njegova posebnost je prilagojenost za kritične situacije, v katerih bi lahko pripomoglo k uspešnim komunikacijam, vendar za potrebe železniških prometnih povezav.

Že nekaj časa je odprto vprašanje uporabnosti omrežij LTE v izrednih razmerah (t. i. LTE-C). Trenutni standardi ga še ne umeščajo kot takšnega, zato sta trenutno le omrežji GSM-R in Tetra standardizirani za komunikacije v kritičnih razmerah.

Pomemben upravljavec kritične infrastrukture v Sloveniji je sistemski operater energetskega omrežja ELES. Osredotočeni so na upravljanje in vzdrževanje energetskih prenosnih omrežij za prenos energije od proizvajalcev do velikih odjemalcev, vzporedno pa gradijo tudi telekomunikacijsko infrastrukturo – optični kabel je umeščen na strelovodni vrvi daljnovoda, predvsem za potrebe nadzora energetskega omrežja, pa tudi za večje zunanje uporabnike. So edini upravljavec kritične infrastrukture, ki ima tudi čezmejne povezave in posega sočasno v dva sektorja.

Če pogledamo v prihodnost, se z razvejenostjo pametnih mrež (angl. *smart grids*), v katere bodo povezane različne naprave energetskega sistema in druge, pojavlja smiselnost ponovne koristne uporabe frekvenčnega spektra od 450 do 470 MHz tudi za komunikacijo v kritičnih razmerah. V posebno skupino omrežij spadajo tako imenovana ad-hoc mobilna omrežja (evropski projekt ABSOLUTE), ki se postavijo le v izrednih razmerah. Postavljajo se bazne postaje na posebnih zračnih plovilih (angl. *low altitude platform*, LAP) nekaj sto metrov nad tlemi, prav tako mobilne zemeljske postaje. Te so navadno združljive s katerim od obstoječih mobilnih omrežij (npr. LTE). Prednosti takih omrežij so hitra postavitev, hitro pokrivanje velikega območja s širokopasovnim signalom in prilagodljivost. Z njihovim razvojem se ukvarja raziskovalna skupina na Institutu Jožef Stefan.

Za zanesljivo delovanje osnovne infrastrukture (npr. energetske ali telekomunikacijske) je pomemben tudi informacijsko-komunikacijski nadzor nad njo. Večinoma gre za nadzor na daljavo. Strokovnjaki opozarjajo, da je zelo pomembno, da izberemo odprte standardne sisteme, ki omogočajo upravljavcem infrastrukture ali močno lastno vpletenost ali podporo kateregakoli zunanjega partnerja.

Nujno sodelovanje države in zasebnikov

V izrednih razmerah, kot so naravne nesreče ali vojne, se meja med javnim in zasebnim povsem izbriše. V takšnih razmerah je sodelovanje državnih služb in lastnikov zasebne kritične infrastrukture zelo pomembno. Da pa bodo vsi akterji res usklajeno delovali, morajo biti ustrezni načrti narejeni že veliko pred pojavom izrednih razmer. Ker so posamezne infrastrukture znotraj države močno soodvisne, včasih pa soodvisnost preseže državne meje, je potrebno usklajeno delovanje vseh upravljavcev infrastruktur.

V Sloveniji imamo nekatere akcijske dokumente že sprejete, nekateri pa so še v sprejemanju. Dober test organiziranosti so bile nedavna ledena ujma in kasnejše poplave na istih območjih. Kljub nevsakdanjim razmeram so javni in zasebni sistemi delovali dokaj usklajeno.