

UROŠ SVETE

VARNOST
V INFORMACIJSKI
DRUŽBI

Ljubljana, 2005

Uroš Svete
VARNOST V INFORMACIJSKI DRUŽBI

Knjižna zbirka VARNOSTNE ŠTUDIJE
Izdajatelj FAKULTETA ZA DRUŽBENE VEDE
Za založbo Hermina KRAJNC

Copyright © po delih in v celoti FDV 2005, Ljubljana.
Fotokopiranje in razmnoževanje po delih in v celoti je prepovedano.
Vse pravice pridržane.

Recenzenta: dr. Samo KROPIVNIK in dr. Marjan MALEŠIČ
Jezikovni pregled: Andreja Devjak, prof. slovenščine
Naslovnica in prelom: B&V Co.
Tisk tiskarna MARGINALIJA

Knjiga je izšla ob podpori Agencije za raziskovalno dejavnost Republike Slovenije.

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

351.78:316.42:659.2

SVETE, Uroš, 1975-

Varnost v informacijski družbi / Uroš Svete. - Ljubljana :
Fakulteta za družbene vede, 2005. - (Knjižna zbirka Varnostne
študije)

ISBN 961-235-218-6

222824704

PREDGOVOR

Znanje, informacije, podatki in razumevanje tako naravnega kot družbenega okolja, so v človekovi zgodovini odigrali ključno vlogo pri urejanju odnosov med družbami in znotraj njih, izjemno spremembo pa je na tem področju prinesla razširjena uporaba informacijsko-komunikacijske tehnologije, ki je presegla človekove naravne fizične omejenosti, ko gre za zbiranje, obdelavo in prenos podatkov. Široka uporaba informacijsko-komunikacijske tehnologije na vseh področjih človekovega bivanja, ima tudi izrazite varnostne implikacije. Za boljše razumevanje fenomena varnosti v sodobni družbi, avtor Uroš Svete v pričujoči knjigi predstavi raziskovalni model, ki omogoča podrobnejše preučevanje varnostnih implikacij uporabe informacijsko-komunikacijske tehnologije.

Avtor v knjigi odgovarja na vprašanje, ali je lahko tehnologija ključen in najpomembnejši dejavnik, ki na teoretični ravni usmerja varnostno razpravo in odločilno določa razmerja med referenčnimi objekti varnosti v sodobnem svetu. Avtorjeva teza, v nasprotju z nekaterimi izhodišči tehnološkega determinizma, predpostavlja, da sta družbeno-kulturni okvir (v tem okviru še posebej koncepti zagotavljanja varnosti različnih referenčnih objektov od posameznika do globalnega okolja, zgodovinske izkušnje skupnosti na varnostno-obrambnem področju ter trenutni položaj akterjev v mednarodnem okolju) in človek, tista dejavnika, ki določata, kakšne bodo varnostne implikacije uporabe informacijsko-komunikacijske tehnologije v dani skupnosti in kakšni bodo odnosi med temi skupnostmi na globalni ravni. Sama tehnologija, ne glede na to, kako velik je njen pomen v družbi in kakšno družbeno revolucijo je povzročila, v varnostni razpravi ni neodvisna spremenljivka, ki bi imela v različnih družbah enake varnostne implikacije. Varnost je namreč družbeno in zaznavno določena kategorija, z veliko možnostjo proste presoje, tako da tudi tehnologije s tako univerzalnimi lastnostmi kot jih ima informacijsko-komunikacijska, v posameznih različnih okoljih ne moremo obravnavati na enak način.

Pri preučevanju varnostnih implikacij uporabe informacijsko-komunikacijske tehnologije je torej nujno upoštevati družbene, kulturne, politične in socializacijske okvire, v katerih se ta tehnologija uporablja in razvija. Kot najpomembnejši teoretični znanstveni instrumentarij lahko v primeru neposrednih varnostnih implikacij informacijsko-komunikacijske tehnologije izpostavimo konstruktivizem in delno tudi liberalizem, medtem ko je posredne implikacije, ki na varnost vplivajo prek sprememb v posameznih družbenih podsistemih v okviru informacijske družbe, mogoče bolje pojasniti na temelju pozitivistične realistične teore-

tične paradigme, temelječe na racionalizmu in materializmu. V tem duhu avtor v izhodišče teoretične obravnave problema postavi sodobne paradigme obravnavanja varnosti, se pravi strukturalizem, institucionalni liberalizem in konstruktivizem, ustrezno pozornost pa posveti tudi specifični teoriji mednarodnih odnosov in mednarodne varnosti na Kitajskem. Med drugim ga zanima, kako razvoj informacijsko-komunikacijske tehnologije vpliva na spreminjanje teoretičnih paradigem, oziroma do kakšne mere je le-ta v njih prisotna kot fenomen, ki vpliva na koncept družbene moči, strukturo akterjev mednarodne skupnosti in na strategije soočanja s sodobnimi varnostnimi problemi. V nadaljevanju teoretičnega razmišljanja avtor predstavi različne koncepte varnosti, vse od nacionalne, družbene, globalne, človekove, do omrežne in informacijske varnosti.

Avtorjeva empirična analiza ponuja temeljito in poglobljeno primerjalno analizo varnostnih implikacij uporabe informacijsko-komunikacijske tehnologije v Združenih državah Amerike, na Kitajskem, v Nemčiji, na Švedskem in v Švici. Omenjene implikacije ga zanimajo na ravni zagotavljanja nacionalne varnosti, varnosti nedržavnih organizacij in struktur ter posameznika. Prvine za primerjalno analizo pa posegajo na konceptualno področje, v proces sprememb v obrambnem, še posebej vojaškem sistemu ter v proces oblikovanja modelov za zaščito kritične informacijske infrastrukture. Avtorja v analizi zanima predvsem, kako se tradicionalne strukture nacionalnovarnostnih sistemov odzivajo in prilagajajo sodobnim izzivom in nalogam, ki jih prinaša razvoj informacijsko-komunikacijske tehnologije, in ki vplivajo na njihov institucionalni, organizacijski in funkcionalni temelj.

Pomembna prvina empiričnega dela avtorjeve analize je tudi študija primera konflikta med Združenimi državami Amerike in 'protiteroristično koalicijo' na eni strani ter iraškim režimom (v prvi fazi konflikta v letu 2003) oziroma iraškimi islamističnimi uporniki in teroristi iz islamskih držav (v drugi in tretji fazi konflikta v letu 2004 in prvi polovici leta 2005), na drugi strani. Omenjeni primer opozori na vso kompleksnost uporabe informacijsko-komunikacijske tehnologije v sodobnih konfliktih, od razvoja koncepta omreženih oboroženih sil pri nekaterih državah 'protiteroristične koalicije', preko uporabe informacijsko-komunikacijske tehnologije pri širjenju propagande in izvajanju psihološkega bojevanja, do uporabe drugih znanih oblik informacijskega bojevanja.

V sklepnem delu knjige avtor na osnovi teoretičnih izhodišč interpretira empirične ugotovitve in s tem zaokroži svojo analizo, ki je v marsičem izvirna. Tematika po znanih informacijah še ni bila preučena s takim metodološkim pristopom in tako celovito, poleg tega pa sta v celoti izvirna avtorjeva primerjalna analiza vpliva informacijsko-komunikacijske tehnologije na varnostne koncepte sodobnih držav in študija primera uporabe informacijsko-komunikacijske tehnologije v vojni v Iraku v analiziranem obdobju.

Kljub temu, da je avtor v svoji analizi uporabljal zahteven znanstveni instrumentarij, je knjiga stilistično in jezikovno prijazno napisana, besedilo pa kljub svoji znanstveni zahtevnosti berljivo in razumljivo. Avtor je kot svoj prispevek k razvoju obramboslovne vede poslovenil in utemeljil številne strokovne in znanstvene izraze, ki jih je prenašal iz tujih virov. Kljub relativni obsežnosti besedila se avtor pri obravnavi posameznih pojavov ne spušča v ekstenzivne opise, značilne za neznastveni slog pisanja.

Knjiga Uroša Sveteta je izjemen prispevek k razumevanju varnosti v informacijski družbi. Napisal jo je predstavnik mlajše generacije obramboslovcev, ki so se raziskovalno osredotočili na nekonvencionalne obramboslovne teme in s tem vzpostavili neposredno komunikacijo z aktualnimi raziskovalnimi trendi v razvitem svetu. Po knjigi bosta posegali akademska in strokovna javnost, predvsem visokošolski učitelji in študenti obramboslovja, politologije, sociologije, komunikologije in (družboslovne) informatike ter odločevalci v strukturah nacionalne in mednarodne varnosti. Zaradi pojasnjevanja vpliva informacijsko-komunikacijske tehnologije na varnost posameznika, bo knjiga zanimiva tudi za obveščeno laično javnost.

Marjan Malešič

VSEBINA

PRVI DEL

UVOD	9
-------------------	---

DRUGI DEL

DRUŽBENE IMPLIKACIJE UPORABE INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE

Informacijsko-komunikacijska tehnologija (IKT) – opredelitev	16
Tehnične osnove informacijske družbe	18
Uporaba IKT (interneta) in vpliv države	21
Informacijska revolucija in globalizacija	23
Informacijsko-komunikacijske tehnologije kot družbenotehnična omrežja	27

TRETJE DEL

SODOBNO OBRAVNAVANJE VARNOSTI

■ TEORETIČNE PERSPEKTIVE OBRAVNAVANJA VARNOSTI	34
Realizem	34
Liberalizem	37
Konstruktivizem	41
Teorija mednarodnih odnosov in varnosti na Kitajskem	48
Varnostne teorije v sodobnem varnostnem okolju – perspektive in izzivi	52
■ RAZVOJ SODOBNE VARNOSTNE PARADIGME	55
■ KONCEPTI NACIONALNE VARNOSTI	66
Skupnosti kot oblike zagotavljanja varnosti držav	67
■ DRUŽBENA VARNOST	74
■ KONCEPT GLOBALNE VARNOSTI	80
Globalizacija kot varnostni izziv	80
Globalna družba kot družba skupnega tveganja	88
■ KONCEPT ČLOVEKOVE VARNOSTI	93

■ KONCEPT OMREŽNE IN INFORMACIJSKE VARNOSTI	105
■ UPORABA INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE V NEKATERIH VARNOSTNIH MEHANIZMIH	109
■ SKLEP	116

ČETRTI DEL

VARNOSTNE IMPLIKACIJE UPORABE INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE

■ INFORMACIJSKO-KOMUNIKACIJSKA TEHNOLOGIJA IN NACIONALNA (DRŽAVNA) VARNOST	118
ZDA	118
<i>Razvoj konceptov</i>	118
<i>Spremembe v obrambnem sistemu</i>	127
<i>Zaščita kritične informacijske infrastrukture – nov izziv nacionalnovarnostnega sistema ZDA</i>	138
Kitajska	141
<i>Kitajski pogled na informacijsko bojevanje</i>	145
<i>Uporaba IKT v Ljudski osvobodilni armadi</i>	147
<i>Avtoritarno-centralistični model zaščite kritične informacijske infrastrukture</i>	152
Nemčija	154
<i>Konceptualna zasnova uporabe IKT v obrambnem sistemu</i>	154
<i>Uporaba IKT v Bundeswehru</i>	156
<i>Zaščita kritične informacijske infrastrukture</i>	160
Švedska	165
<i>Razvoj koncepta</i>	165
<i>Spremembe v obrambnem sistemu – na omrežju temelječa obramba</i>	168
<i>Zaščita kritične informacijske infrastrukture v konceptu totalne obrambe</i>	170
Švica	173
<i>Obravnavanje varnostnih implikacij uporabe IKT</i>	174
<i>Reforme nacionalnovarnostnega in obrambnega sistema</i>	179
<i>Vseobsežna zaščita kritične (informacijske) infrastrukture</i>	181
Primerjalna analiza držav	184
■ NEDRŽAVNE ORGANIZACIJE IN STRUKTURE	200

■ POSAMEZNIK KOT REFERENČNI OBJEKT VARNOSTNIH IMPLIKACIJ UPORABE INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE.....	202
■ SKLEP.....	211

PETI DEL

**VLOGA UPORABE INFORMACIJSKO-KOMUNIKACIJSKE
TEHNOLOGIJE V SODOBNIH KONFLIKTIH
(študija primera Iraka)**

■ NEENAKOMEREN INFORMACIJSKI RAZVOJ – OSNOVA ZA SODOBNE ASIMETRIČNE KONFLIKTE	218
Revolucija v vojaških zadevah	218
■ UPORABA INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE V AMERIŠKO-IRAŠKEM KONFLIKTU 2003–2004.....	221
Uporaba IKT v pripravljalni fazi konflikta	223
Druga faza: operacija Iraška svoboda	230
<i>Implementacija koncepta omreženih oboroženih sil</i>	230
<i>Operativna in taktična raven izvajanja informacijskega bojevanja</i>	235
Tretja faza: prevlada (uspešne) asimetrične strategije nad informacijsko in tehnološko dominantnim nasprotnikom ter učinkovitostjo omreženih oboroženih sil?.....	238
Analiza učinkovitosti uporabe IKT v ameriško-iraškem konfliktu.....	242
■ SKLEP.....	247

ŠESTI DEL

SKLEPNE MISLI	253
----------------------------	------------

LITERATURA	261
STVARNO IN IMENSKO KAZALO.....	283

*Nove ideje sprova zavračajo in trdijo, da so nesmisel.
Nato jih obravnavajo kot samoumevne in trivialne.
Na koncu pa pravijo: »Saj so vendar naše!«*

William James

1842–1910

Profesor filozofije, Univerza v Harvardu

PRVI DEL

UVOD

Razvoj informacijsko-komunikacijske tehnologije (IKT) in njena uporaba v sodobnih družbah sta doživela revolucionaren razmah. Telekomunikacije, satelitske povezave in računalniška omrežja so velik del sveta povezala v prepleteno celoto – informacijsko družbo, ki je danes že splošno sprejet aksiom tako v znanstveni kot tudi javni-politični sferi. Uporaba IKT že dolgo ni več omejena zgolj na raziskovalne, akademske ter obrambno-vojaške okvire, pač pa je postala temelj delovanja vseh pomembnejših družbenih podsistemov (nacionalnovarnostnega, upravno-političnega, znanstveno-raziskovalnega in izobraževalno-socializacijskega, gospodarskega, medijskega ter telekomunikacijskega idr.), hkrati pa je korenito spremenila delovanje posameznika, družbenih skupin in institucij.¹ Kot taka je postala **cilj in sredstvo za doseganje njihovih interesov** tudi na področju varnosti. Temeljne družbene spremembe, ki jih je povzročila uporaba IKT, lahko pojasnimo na primeru ekonomskega, organizacijskega in vojaškega podsistema, pri tem pa je pomembno identificirati naslednje procese (Waltz, 1998):

1. **Produkcija (proizvodnja)** se vse bolj spreminja v ustvarjanje – bistveno je pridobivanje in oblikovanje informacij na osnovi zbiranja podatkov ter njihovo kontekstualiziranje v znanje in razumevanje. Na vseh družbenih področjih postajata znanje in razumevanje ključna strateška elementa in osnova informacijske moči.
2. **Neotipljive vrednote** – uporaba IKT je spremenila tudi družbene vrednote, katerih širjenje je vse manj materialno in temelječe na realnem okolju. Navidezna resničnost (ang. virtual reality) postaja vse pomembnejše okolje za družbeno delovanje posameznika kot tudi družbenih podsistemov.
3. **Demasifikacija in specializacija** – agrarne in industrijske družbe so temeljile na kvantiteti, medtem ko se informacijske družbe gibljejo v smeri vse večje specializacije in delitve dela, kar zahteva kontinuirano usposabljanje in izobraževanje oz. pridobivanje znanja. Družbe in njihovi podsistemi postajajo vse bolj temelječi na znanju.
4. **Organizacija (upravljanje in vodenje)** – organizacije z informacijskimi mrežami se bodo preoblikovale iz strukture, kjer se informacije pretakajo po hierarhični lestvici v vertikalni smeri, v mreže z informacijskim pretokom v vse smeri (poudarek na horizontalni smeri).

¹ Podobno razmišlja v članku tudi Valeri (2000), ko izpostavlja pomen mednarodnega (so)delovanja pri oblikovanju tistih varnostnih mehanizmov v informacijskih družbah, ki so primarno usmerjeni v zaščito informacijske infrastrukture.

5. **Infrastruktura** – fizična infrastruktura (geografske lokacije enot, fizična namestitvev materialov, fizična alokacija virov) vse bolj odstopa prostor infrastrukturi, ki temelji bolj na koristnosti informacij kot na fizični lokaciji, sposobnosti in ranljivosti (informacijska infrastruktura).
6. **Pospešitev procesa in premagovanje fizičnega prostora** – ključne spremembe družbenih procesov se odvijajo hitreje, v kolikor se IKT uporablja pri proizvodnji outputa. Izredne spremembe pa so se dogodile tudi pri premagovanju fizičnega prostora, kajti IKT je povzročila pravo revolucijo v zaznavi časa in prostora.

Uporaba IKT je tako postala vir sprememb družbenega okolja, ogrožanja sodobnih družb kot tudi varnostih akterjev. Značilnosti, kot so **nizki vstopni stroški** (za razliko od izdelave visoko tehnoloških oborožitvenih sistemov so vstopni stroški pri IKT vse nižji, kar ji omogoča disperzijo med družbene skupine ali države z manjšo finančno zmogljivostjo), **nejasnost tradicionalnih razmejitev** (informacijska in telekomunikacijska tehnologija – internet – je zameglila oz. presegla geografske, birokratske in jurisdikcijske meje kot tudi razsežnosti obravnavanja varnosti v tradicionalnem državocentričnem (realističnem) smislu), **povečana možnost vplivanja na zaznavo stvarnosti** (nove informacijske tehnike bistveno povečujejo moč manipulativnih aktivnosti), **možnost uporabe** v oboroženih silah na strateški kot tudi taktični in operativni ravni oz. nacionalnovarnostnih sistemih v celoti ter **geografsko-prostorska neomejenost**, povzročajo ne samo spremembe tradicionalnih varnostnih akterjev in njihovega delovanja, temveč omogočajo tudi pojav novih. Zato bomo varnostne implikacije uporabe IKT preučili na temelju sodobne varnostne teorije, temelječe na treh najpomembnejših teoretičnih znanstveno-raziskovalnih paradigmah: realizmu, liberalizmu in konstruktivizmu. Le na ta način bomo lahko varnost v informacijskih družbah preučili holistično v najširšem pomenu, znotraj katerega lahko pomembno oz. potencialno učinkovanje uporabe IKT identificiramo v naslednjih 4 točkah:

- IKT kot pomemben vstavljen del (ang. imbedded technology) sodobnih konvencionalnih oborožitvenih in podpornih sistemov je v veliki meri spremenila njihovo uporabo, zmogljivosti in način delovanja.
- Uporaba novih (IKT) tehnologij omogoča oblikovanje nadaljnjih zmogljivosti in doktrinarnih pristopov za povečanje učinkovitosti vojskovanja v konvencionalnem prostoru (vojskovanje, temelječe na digitaliziranem poveljniško – nadzornem sistemu).
- Oblikovanje novega prostora in dimenzij za izvajanje konfliktov in bojevanja (kibernetski prostor, informacijska sfera).
- Oblikovanje novih vrednot, tako v smislu njene ofenzivne kot defenzivne uporabe (Campen in Dearth, 2001).

Kljub temu da so omenjene značilnosti IKT splošno sprejeti postulati, izhajajoči iz družbene integriranosti IKT, in predpostavke, da njen aplikativni del teži k univerzalnosti, njeni vplivi na področju varnosti ne vodijo nujno k univerzalnim zakonitostim. Ob tem se nam zastavlja

vprašanje ali so univerzalne tehnološke lastnosti IKT značilne tudi za varnostno področje, kar izpostavlja tehnološki determinizem ali pa je okolje uporabe oz. človeški dejavnik bistvena determinanta, ki vodi do tehnološkega relativizma. V natančnejši analizi, kjer smo varnostne implikacije razdelili na neposredne (uporaba IKT – zaznava varnosti) in posredne (uporaba IKT v tradicionalnih varnostnih instrumentih in mehanizmih – varnostni akterji), pa smo ugotovili, da vendarle obstajajo pomembne razlike tako znotraj sodobnih družb, ki jih lahko označimo za informacijske ali omrežne, kot tudi med družbami oz. državami, kjer informacijski sektor še ni prevladujoč, je pa vsekakor v velikem vzponu. Uporaba in razvoj IKT posebej v neposrednem varnostnem smislu sta očitno izrazito družbeno determinirana in odvisna od družbenega konteksta, v aplikativnem smislu pa še posebej od človeškega dejavnika (posameznikovo uporabo IKT določajo njegove vrednote, primarna, sekundarna in terciarna socializacija ter kulturni in družbeni okvir, v katerem deluje). Tako nas pogled na posamezne države opozori na bistvene razlike, ki jih uporaba IKT povzroča na področju varnosti. Znotraj držav, ki so na podoben kvalitativni stopnji informacijske razvitosti, opazimo zelo različno zaznavo IKT kot vira družbenega ogrožanja, prav tako pa so različni tudi odzivi in uporaba IKT v nacionalnovarnostnih sistemih. Medtem ko nekatere države IKT obravnavajo predvsem kot nov vir družbene moči oz. kot sredstvo za povečevanje tradicionalnih oz. za vzpostavitev novih oblik moči² (ZDA, Kitajska), pa druge v skladu s prevladujočimi nacionalnovarnostnimi politikami in strateškimi usmeritvami (npr. koncept totalne obrambe v nevtralnih Švici in Švedski s poudarkom na t. i. »mehki« moči) razvijajo predvsem zaščito kritične informacijske infrastrukture kot defenzivni oz. obrambni varnostni mehanizem, IKT pa uporabljajo tudi za krepitev tradicionalnih elementov nacionalnovarnostnih sistemov (obrambnega in varnostnega sistema), ki so sicer pretežno defenzivno naravnani. Po drugi strani pa se v državah z izrazitim nesorazmerjem med ekonomsko, politično in vojaško močjo nesorazmerje kaže tudi v varnostnih implikacijah uporabe IKT, predvsem v spremembah varnostnega sistema kot odgovora na ogrožanje njihovih ekonomskih in političnih interesov (Nemčija), medtem pa članstvo v varnostnih in obrambnih integracijah zahteva prilagajanje tudi obrambnega dela nacionalnovarnostnega sistema vodilnim državam na področju uporabe in razvoja IKT. Zato je oblikovanje novih strateških premis in doktrin, katerih jedro predstavlja IKT in njena uporaba ter njihovo izvajanje v

² Rothkopf (1998: 325) trdi, da bodo ZDA svojo prevlado v svetu ohranile le v primeru, če bodo spoznale spremenjeno naravo moči v svetovnem okolju in se ji prilagodile. Tudi Wenger in Dunn (2003: 10–15) izpostavljata nove vire družbene moči, kot so informacije, tehnologije in fleksibilne institucije, ki naj bi v primerjavi s tradicionalnimi viri (vojaška moč, ozemlje ter naravni viri) pridobivali na pomenu. Tovrstnim ugotovitvam pa se odkrito pridružuje tudi ameriška vlada, ko načrtuje uporabo IKT za doseganje ameriških strateških interesov posebej v času t. i. globalnega boja proti terorizmu.

omenjenih državah, zelo različno (npr. razvoj koncepta neomejenega in informacijskega bojevanja, informacijskih operacij, zaščite kritične informacijske infrastrukture ter omreženih oboroženih sil). V tem okviru je potrebno natančneje analizirati tiste notranje in zunanje družbene dejavnike, ki vplivajo na diferenciranost varnostnih implikacij uporabe IKT v posameznih državah oz. družbah glede vpliva na varnostne akterje in odziva (v obliki varnostnih instrumentov in mehanizmov) na zaznavanje IKT kot varnostnega problema v širšem smislu, še posebej pa je pomembno preučevanje vloge, ki jo imajo (novi) varnostni akterji v spremenjenih družbenih, mednarodnih in tehnoloških razmerah. Ključna je namreč ugotovitev, kako se tradicionalne organizacije, kot je npr. totalitarno in hierarhično strukturirana vojaška organizacija, prilagajajo sodobnim izzivom in nalogam, popolnoma drugačnim od tistih, ki jih postavlja javnost, oz. na katere je vojaška organizacija pripravljena in zahtevajo organizacijske, funkcionalne in institucionalne spremembe tako znotraj vojaškega podsistema kot sistema nacionalne varnosti v celoti. Po drugi strani pa je potrebno določiti tudi vlogo in pomen novih varnostnih akterjev, katerih delovanje je pomembno določila ravno uporaba IKT. Primer je nedvomno tudi študija konflikta v Iraku, kjer se je sprva pretežno konvencionalni spopad med dvema državnima akterjema preoblikoval v izrazito asimetrično bojevanje, v katerem so zlasti na iraški strani glavno vlogo prevzeli novi akterji v sodobnem varnostnem okolju (nedržavne organizacije ter posamezniki, ki jih v zahodnih državah imenujejo islamski fundamentalisti oz. teroristi). Čeprav zaradi specifičnosti sodobnih konfliktov uporaba IKT kot odločilni dejavnik, ki bi vplival na izid sodobnih konfliktov, ni povsod prisotna, pa se je delovanje vpletenih akterjev pomembno spremenilo, prav tako pa se je bistveno spremenila tudi zaznava konfliktov.

Razmerje med tehnološko in družbeno determiniranostjo uporabe IKT je bilo torej glavno vodilo, ki nas je usmerjalo v raziskovalnem procesu, pa naj gre za primerjalno analizo varnostnih implikacij, ki jih je uporaba IKT povzročila v posameznih državah, ali pa za študijo primera konflikta v Iraku, kjer smo poskušali ugotoviti, kakšna je njena vloga pri izidu sodobnih konfliktov. Po drugi strani pa smo poskušali oblikovati celovit teoretični model, ki bi na temelju sodobnih varnostnih paradigem omogočal razumevanje vplivov, ki jih je na področju varnosti povzročila tako revolucionarna tehnologija kot je IKT. Veljavnost modela bo vsekakor pokazal čas, že sedaj pa nas v pravilnost nastavkov prepričujejo številni primeri iz kibernetike sveta, ki je obenem tudi naša empirična stvarnost.

DRUGI DEL

**DRUŽBENE IMPLIKACIJE
UPORABE INFORMACIJSKO-
KOMUNIKACIJSKE
TEHNOLOGIJE**

Informacijsko-komunikacijska tehnologija (IKT) – opredelitev

IKT opredeljujejo številne znanosti, tako družboslovne kot naravoslovne. Za lažje razumevanje nadaljnje razprave in zaradi narave razvoja in uporabe v skoraj vseh družbenih sferah in podsistemih, je potrebna široka opredelitev IKT. Nanaša se torej na zbiranje, obdelavo in prikaz podatkov, prav tako pa vključuje tudi komunikacijski element, ki omogoča prenos podatkov.³ Tehnologije za obdelavo podatkov obsegajo tako združevanje podatkov in njihovo analizo kot tudi podporo pri odločevalskem procesu (Alberts, 1996; Wilson, 1998). Označuje prodor moderne elektronske, predvsem računalniške in komunikacijske tehnologije v metode obdelave informacij. Izvor termina sega v 70. leta 20. stoletja (Bosch, 2000: 86–87), bistveno pri njegovem širšem razumevanju pa je, da ne govorimo samo o tehnično-infrastrukturnem strojnem vidiku in napravah. Upoštevati moramo predvsem vidik programske opreme, ki daje napravam uporabno vrednost, in človeški dejavnik, ki programsko in strojno opremo seveda uporablja. Programski in strojni vidik je torej nujno povezati z uporabo pri doseganju zelenih ciljev (tehnološka aplikabilnost oz. družbena uporabnost). Zato lahko IKT opredelimo kot sposobnost, znanje, spretnost oz. tehniko, da predvsem z uporabo strojev in naprav, ki omogočajo informacijske dejavnosti, dosežemo zelene učinke. Taka splošna opredelitev nam omogoča, da informacijske dejavnosti in procese opredeljujemo in preučujemo v vseh družbenih podsistemih. V tem smislu vse pogosteje govorimo o kritični informacijski infrastrukturi⁴ (Wenger in drugi, 2002, Westrin, 2001) kot ključnem elementu delovanja sodobnih družb, ki pa je lahko partikularna (aplicirana le v določenem družbenem podsistemu), nacionalna/državna (na ravni države) in globalna, povezana predvsem z razmahom interneta, telekomunikacij, satelitskih povezav, medijev... (FM 100-6). Vse bolj razvita informacijska tehnologija, svetovni trendi v smeri globalnih standardov, vse večje zahteve potrošnikov ter naraščajoče mednarodno tekmovanje so tisti ključni

³ Eriksson (1999) trdi, da je ravno komunikacijski vidik IKT odločilno vplival na prehod iz industrijskih v omrežne-informacijske družbe.

⁴ Nacionalno kritično infrastrukturo opredeli tudi Wik (2001), ki jo umesti med električno, telekomunikacijsko in računalniško (internet) omrežje. Tako naj bi zajemala področja, kot so preskrba z električno energijo, transport, sistem notranje varnosti v širšem smislu, sistem vojaškega vodenja in poveljevanja, vladne službe, množične medije, finančni in bančni sistem ter industrijsko proizvodnjo.