ECESM NEWSLETTER **CYBER VOCABULARY** **Broj: 05; Oktobar 2016.**

Poštovani čitaoci,

sa velikim zadovoljstvom vam predstavljamo peti broj časopisa «Sajber bezbjednost za sve», koji izdaje Centar za edukaciju u oblasti sajber bezbjednosti u Crnoj Gori (engl. Montenegrin cyber security educational center – MCEC), osnovan u okviru Tempus projekta «Unaprijeđenje sistema obrazovanja u oblasti sajber bezbjednosti u Crnoj Gori» (engl. Enhancment of Cyber Educational System of Montenegro – ECESM).

Ovaj broj časopisa je specifičan po svojoj strukturi, odnosno formi riječnika pojmova o sajber bezbjednosti.Riječnik pojmova i termina o sajber bezbjednosti prevashodno je zasnovan na prevodu engleskih termina na naš jezik.

Tokom svog dugogodišnjeg rada i istraživanja u oblasti sajber bezbjednosti, često smo se sami susretali sa teškoćama da neke termine iz oblasti sajber bezbjednosti prevedemo na naš jezik, a sam kvalitet prevoda je nerijetko bio nezadovoljavajući. Mnoge riječi iz ove oblasti nemaju adekvatnu riječ u crnogorskom jeziku, te zahtjevaju opisan prevod.

Cilj i svrha ovog riječnika je da približi pojmove sajber bezbjednosti svima koji su na bilo koji način bave ovom problematikom ili su upućeni na nju iz različitih razloga. To mogu biti: novinari, studenti, učenici, profesori, naučni radnici, ali i svi građani koji žele da steknu i unaprijede svoja znanja u oblasti sajber bezbjednosti.

ECESM uređivački odbor

Sadržaj:

ENHANCEMENT OF CYBER EDUCATIONAL SYSTEM OF MONTENEGRO

This project has been funded with support from the European Commission. The publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

A

Aktivni napad (*engl. Active Attack)*

Napad na računarski sistem izvršen namjerno od stranog izvora prijetnji, prilikom koga se na sistem pokušavaju promijeniti informacije, sistem, njegova sredstva, podaci, operacije, ili generisanje lažnih podataka u sistemu. Aktivni napad se obično dešava kada je veći broj računara programiran tako da istovremeno pokušava da pristupi istom računarskom sistemu i istrajan je u daljim pokušajima u toku napada. Ove vrste napada su zlonamjerne i mogu dovesti do velikih gubitaka za žrtve. Primjeri ovakve vrste napada uključuju: posrednika u sredini, lažno predstavljanje i sesije otmice.

Aktivnosti oružanih snaga u informacionom prostoru *(engl. Activities of the Armed Forces in information space)*

Podrazumijevaju korištenje informacionih resursa od strane oružanih snaga u oružanom konfliktu, koji se usmjerava na rukovođenje (menadžment) i koristi informacije u svim oblicima i na svim nivoima da bi se ostvarila odlučujuća vojna prednost, za rješavanje zadataka odbrane i sigurnosti.

B

Bezbjednosni izazovi u sajber prostoru *(engl. Security Challenges in Cyberspace)*

Bezbjednosni izazovi za državu uključuju kategorije sajber kriminala usmjerene protiv kritičnih informacionih sistema države ili u svrhu dobijanja tajnih informacija, ekonomske sabotaže i drugih politički motivisanih sredstava. Takođe, na nižem nivou, djela protiv sajber bezjbednosti koji ugrožavaju pristup informacijama i pravilno funkcionisanje informacionih sistema.

Bezbjednost informacija *(engl. Information Security)*

Bezbjednost informacija znači obezbjeđivanje povjerljivosti (definisanje načina nivoa pristupa informacijama, putem strukturisanih i zaštićenih ovlašćenja), integriteta (zaštita tačnosti i kompletnosti informacija i definisanje načina ko, kako, gde i na koji način generiše i obrađuje informaciju, sa pozicije bezbednosti) i dostupnosti informacija (omogućavanje pravovremene dostupnosti informacijama, osobama sa ovlašćenjima, u vremenu kada je to potrebno i na mestu gde je to predviđeno).

Bezbjednost računara *(engl. Computer Security)*

Bezbjednost računara se bavi nadzorom, praćenjem i spriječavanjem raznih opasnosti koje mogu prouzrokovati nestabilnost, prestanak rada ili bilo kakvu vrstu štete na softveru, pa i hardveru

računara. Za cilj ima da obezbijedi dostupnost i pravilno funkcionisanje računara i računarskog sistema. Ovaj pojam podrazumijeva mjere i kontrole koje obezbjeđuju povjerljivost, integritet i dostupnost informacionog sistema imovine, uključujući hardver, softver i informacije koje se obrađuju, čuvaju i saopštavaju. Bezbjednost informacija i bezbjednost računara često se koriste alternativno, iako su u vezi sa neznatno različitim aspektima u oblasti sajber bezbjednosti.

D

Domen informacija *(engl. Information Domain)*

Potreba za integracijom, odnosno dijeljenjem i zajedničkim korišćenjem heterogenih informacija u aplikacijama jedan je od najznačajnijih problema koji je prisutan u različitim domenima. Prisutan je trodjelni koncept za razmjenu informacija, nezavisno od informacionih sistema i bezbjednosnih domena koje identifikuje:

1. dijeljenja učesnika kao pojedinih članova informacije,
2. sadrži informacije dijeljenih objekata i
3. daje bezbjednosne politike, kojima se identifikuju uloge i privilegije članova koje je potrebno zaštiti za informacione objekte.

Dominacija informacione operacije *(engl. Information Operations Dominance)*

Dominacija informacione operacije je bazirana na zaštiti i odbrani informacija i informacionih sistema, koje obezbeđuju njihovu raspoloživost, integritet, autentičnost, povjerljivost i neporicivost. Ovo je doprinijelo velikoj mogućnosti u informacionim operacijama, što je dovelo do kontrolnog položaja.

Državni akteri *(engl. State Actors)*

Državni akteri su dobro uspostavljeni i organizovani za obavljanje najsavremenije prijetnje u sajber prostoru sa ciljem eksploatacije računara, informacionih i komunikacionih mreža, za prikupljanje obavještajnih podataka o Vladi, vojsci, industrijskih i ekonomskih ciljeva, i protivnika i njihovih režima. Oni sakupljaju obavještajne podatke i informacije koje se mogu koristiti za širenje laži i ometanje kritičnih usluga. Ponekad instalirani skriveni zlonamjerni softver na sistemu može da se prilagodi promjenljivim ciljevima napadača, leži skriven u okviru sistema i spreman je za eksploataciju u toku povećane napetosti ili sukoba.

E

Elektronska informaciona infrastruktura *(engl. Electronic Information Infrastructure)*

Uslov elektronskog informacionog sistema u kojem je njena zaštita zatvorena, sveobuhvatna, kontinuirana i u srazmjeri sa rizicima u pogledu povjerljivosti, integriteta i dostupnosti podataka; upravljanje takvim elektronskim informacionim sistemom, kao i integritet i dostupnost elektronskih elemenata informacionog sistema. Informaciona infrastruktura u svom najširem smislu uključuje žične i bežične (radijske) komunikacije. Ova infrastruktura omogućava brzo, jednostavno i jeftino skladištenje informacija, povraćaj, prenos i obradu digitalizovanih podataka u formi govora, podataka, videa, animacija, itd.

Elektronske komunikacione mreže *(engl. Electronic Communication Network)*

Prenosni sistemi, rasklopni i usmjeravani uređaji, uključujući elemente mreže koji se ne koriste i druge resurse koji omogućavaju da prenose signale u mreži uz pomoć kablova, radio talasa, optičkih ili drugih elektromagnetnih sredstava, bez obzira na informacije koje prenose.

Elektronski napad *(engl. Elektronic Attack)*

Odjeljenje za elektronsko ratovanje uključuje korišćenje elektromagnetne energije, u režiji energije ili protiv radijacionog oružja za napad kadrova, prostorija, opreme ili sa namjerom degradiranja, neutralizacije ili uništavanja neprijateljske borbene sposobnosti i ima oblik požara. Elektronski napad predstavlja napad koji se postiže upotrebom elektromagnetne visoke energije ili elektromagnetnog impulsa, čime dolazi do preopterećenja strujnog kola računara ili mikrotalasnog radio-prenosa.

Elektronski ratni incident *(engl. Electronic Warfare Incident)*

Vojna akcija koja eksploatiše elektromagnetnu energiju da obezbijedi bezbjednosna upozorenja i postigne ofanzivne i defanzivne efekte.
Incident kao negativni mrežni događaj u informacionom sistemu ili mreži ili opasnost od nastanka takvog događaja.

Elektronsko ratovanje *(engl. Electronic Warfare)*

U vojnoj nauci i vojnim doktrinama, oblast elektromagnetnog spektra se izuzetno detaljno proučava, a tim područjem ratovanja se bavi zasebna disciplina – elektronsko ratovanje. Elektronsko ratovanje po Združenoj komandi američke vojske obuhvata aktivnosti pri kojima se upotrebljavaju sve vrste elektromagnetnih talasa na svim frekvencijama, poput radio, mikrotalasnih, usmerenih talasa i preklapa se sa mrežnim ratovanjem koje uključuje radio mreže, satelitske veze, taktičke digitalne informatičke veze (TADIL), telemetriju, digitalne podatke, telekomunikacijske i bežične komunikacijske mreže i sisteme. U nekimm vojnim doktrinama ona je samostalna vojna disciplina za podršku osnovnim snagama, dok je u doktrini NATO zemalja deo šire oblasti – informacionih operacija. U suštini, elektrensko ratovanje je svaka vojna akcija koja uključuje upotrebu elektromagnetne energije i usmjerena je da kontroliše elektromagnetni spektar ili da napadne neprijatelja.

G

Globalna informaciona infrastruktura *(engl. Global Information Infrastructure)*

Svjetski rasprostranjen međusobni informacioni sistem svih zemalja, međunarodnih i multinacionalnih organizacija i međunarodnih komercijalnih komunikacija.

Globalna informaciona mreža *(engl. Global Information Grid(GIG))*

Globalno povezan skup informacionih mogućnosti za prikupljanje, obradu, skladištenje, širenje i upravljanje informacijama o potražnji za vojnicima u borbi, kreatorima politike i pomoćnom osoblju. GIG uključuje u vlasništvo i zakup komunikacije i računarskih sistema i usluga, softvera (uključujući i aplikacije), podatke, službe bezjbednosti, druge povezane usluge i sistem nacionalne bezbjednosti. Neglobalna informacona mreža uključuje samostojeće, samostalne ili ugrađene IT mreže koje nijesu i neće biti povezane sa mrežom preduzeća.

I

ICT-informaciono komunikacione tehnologije *(engl. ICT-Information and communications technology)*

ICT predstavljaju bilo koje uređaje za komunikacije ili aplikacije, uključujući radio, televiziju, mobilne telefone, satelitske sisteme, računare, mreže hardvera i softver i druge usluge, kao što su video konferencije.
Upućuje na tehnologije koje ljudi koriste da dijele, distribuiraju, prikupljaju informacije i da komuniciraju putem računara i računarskih mreža; aplikacije računara i telekomunikacione opreme za skladištenje, preuzimanje, prenos i manipulisanje podacima.

ICT prijetnje *(engl. ICT Threats)*

Izvori ovih prijetnji obuhvataju kako državne tako i nedržavne aktere. Pored toga, pojedinci, grupe ili organizacije, uključujući i kriminalne organizacije, mogu da djeluju kao zastupnici države u vođenju zlonamjernih ICT akcija. Potencijal za razvoj i širenje sofisticiranih zlonamjernih alata i tehnika, kao što je bot-mreža, od strane države ili nedržavnih aktera može dodatno povećati rizik od pogrešne atribucije i nenamjerne eskalacije. Odsustvo zajedničkog shvatanja o prihvatljivom stanju ponašanja u vezi sa korišćenjem informacionih i komunikacionih tehnologija povećava rizik za međunarodni mir i bezbjednost. Terorističke grupe koriste ICT za komunikaciju, prikupljanje informacija, regrutovanje, organizovanje, koordiniranje planova i napada, promovišu svoje ideje i akcije i traže sredstva. Ako takve grupe stiču alate napada, mogu da obavljaju i remete ICT aktivnosti. Države su zabrinute da bi ugrađivanje štetnih skriveneih funkcija u ICT moglo da se koristi na način koji bi uticao na sigurno i pouzdano korišćenje ICT i lanac snabdijevanja ICT za proizvodima i uslugama, erodiranje povjerenja u trgovini i štete nacionalnoj bezbjednosti.

Incident *(engl. Incident)*

Incident označava događaj, činjenje ili nečinjenje koje dovodi ili može dovesti do neovlašćenog pristupa informacionom sistemu ili elektronske komunikacione mreže, prekida ili promjena rada (uključujući i preuzimanje kontrole) informacionog sistema ili elektronske komunikacione mreže, uništenje, oštećenje, brisanje ili promjena elektronskih informacija, uklanjanje ili ograničavanje mogućnosti za korišćenje elektronskih informacija i takođe, da da povoda ili da može dovesti do prisvajanja, objavljivanja, širenja ili bilo koje druge upotrebe nejavne elektronske informacije od strane lica ovlašćenog za to.

Informacija *(engl. Information)*

Uključuje tekstualne podatke, slike, zvučne kodove, kompjuterske programe, softvere i baze podataka. Informacija obuhvata podatke, poruke, tekst, slike, zvuk, glas, kodove, računarske programe, softver i baze podataka ili mikro film ili kompjuterski generisane mikro utikače. Generalno, informacija je sve što je u stanju da prouzrokuje da ljudski um promijeni svoje mišljenje o trenutnom stanju u stvarnom svijetu. Formalno, a posebno u nauci i inženjerstvu, informacija je ono što doprinosi smanjenju neizvjesnosti stanja sistema u ovom slučaju, neizvjesnost se obično izražava u objektivno mjerljive forme. Obično, to se radi pomoću Šenonove entropije. Ipak, ova formula za neizvjesnost podrazumijeva vjerovatnoće i može biti subjektivna. Ako je tako, formalno mjerenje se mora okvalifikovati u zavisnosti od subjektivne vjerovatnoće i neizvjesnost mora biti zamijenjena mišljenjem ili ličnom procjenom – nesigurnosti. Informacija mora da se razlikuje od bilo kog medija koji je sposoban da je nosi. Fizički medijum (kao što je magnetni disk) može nositi logičan medijum (podaci, kao što su binarni ili tekst simbola). Sadržaj informacije bilo kog fizičkog objekta ili logičkih podataka, ne može se mjeriti ili raspravljati o njoj dok se ne sazna opseg mogućnosti koja je postojala prije i nakon što su je dobili. Informacija leži u smanjenju neizvjesnosti usljed prijema predmeta ili podataka, a ne u veličini ili složenosti predmeta ili samih podataka. Pitanja oblika, funkcije i semantičkog uvoza podataka su relevantni samo za informaciju pošto oni doprinose smanjenju neizvjesnosti. Informacija ima posledice na bezbjednost, politiku, kulturu i ekonomiju, kao i u nauci i inženjerstvu. Stepen do kojeg se podaci koriste kao ekonomska roba je jedan od definisanja karakteristika "post-industrijskog društva", otuda fraza "informaciono društvo".

Informaciono okruženje *(engl. Information Environment)*

Agregat pojedinaca, organizacija i/ili sistema koji prikupljaju, obrađuju ili šire informacije, takođe uključene u same informacije. Informaciono okruženje unutar njegove sfere, takođe podrazumijeva kreiranje svih tipova komunikacionih infrastruktura, zajednica, skladišta, prodavnica, servisa, itd., kao i digitalne duplikacije našeg vidljivog svijeta.

Informaciona bezbjednost *(engl. Information Security)*

Informaciona bezbjednost podrazumijeva stanje povjerljivosti, integriteta i dostupnosti informacija. Informaciona bezbjednost je usmjerena na podatake, bez obzira na njihovu formu: elektronske, štampane i druge oblike podataka. Međunarodna informaciona bezbjednost bi trebalo da bude bazirana na postojećem međunarodnom pravu (ius ad bellum), koji definiše kako da se suprotstavi prijetnjama međunarodnom miru i bezbjednosti, kao i međunarodnog humanitarnog prava (jus in bello), koje se odnosi na sredstva i metode ratovanja; zaštite država od strana koje nisu u sukobu i lica i imovine koji jesu ili mogu biti pogođene sukobom.
Set nacionalnih i međunarodnih institucija koje regulišu aktivnosti različitih aktera globalnog informacionog prostora. Ovaj sistem je dizajniran da se suprotstavi prijetnjama strateške stabilnosti i

jednakom strateškom partnerstvu da promoviše globalni informacioni prostor. Kao uslov bezbjednosti svojih nacionalnih interesa u informacionom prostoru, određuje izbalansiranu kombinaciju interesa pojedinaca, društva i države.

Informaciona bezbjednost oružanih snaga *(engl. Information Security of the Armed Forces)*

Uslov bezbjednosti informacionih resursa koji pripadaju oružanim snagama su od uticaja za napad u informacionom prostoru.

Informaciona infrastruktura *(engl. Information Infrastructure)*

Skup tehničkih alata i sistema formiranja, stvaranja, transformacije, prenosa, korišćenja i čuvanja informacija. Informaciona infrastruktura obuhvata svu infrastrukturu u određenoj organizaciji, koja na bilo kakav način utiče na ključna svojstva povjerljivosti, dostupnosti ili integriteta podataka u okviru koje podaci nastaju, obrađuju se ili čuvaju.

Informaciona operacija *(engl. Information Operation)*

Informaciona operacija definiše se kao koordinisana primjena aktivnosti koje se preduzimaju protiv informacija i informacionih sistema neprijatelja, uz čuvanje vlastitih. Osnovni ciljevi su: uticaj, prekidanje ili nanošenje neispravnosti protivničkom "ljudskom" ili automatizovanom sistemu za rukovođenje. Centralne aktivnosti informacionih operacija su: psihološke operacije, vojno obmanjivanje, zaštita operacija, elektronsko ratovanje i računarsko-mrežne operacije.

Informacione tehnologije *(engl. Information Technology)*

Informacione tehnologije su jedne od kritičnih sektora u sajber prostoru. One su nastale kao jedne od najznačajnijih za rast ekonomije, ovaj sektor je takođe pozitivno uticao na živote svih ljudi kroz direktne i indirektne raznovrsne doprinose socioekonomskih parametara kao što su: zapošljavanje, životni standard i različitosti između ostalih. Vlada predstavlja ključni vodič za povećanje usvajanja ICT proizvoda i IT omogućavanja usluga u javnim službama (vlada za usluge građanima, identifikaciju građana, sistemi javne distribucije), zdravstvo (telemedicina, daljinske konsultacije, mobilne klinike), obrazovanje (e-učenje, virtualne učionice, itd.) i finansijske usluge mobilnog bankarstva, itd. Takve inicijative su omogućile povećano usvajanje informacionih tehnologija u zemlji kroz sektorske reforme i nacionalne programe koji su doveli do stvaranja IT infrastrukture velikih razmjera sa korporativnim/privatnim učešćem.

Informacioni alati *(engl. Information Tools)*

Informacione tehnologije, sredstva i metode koje se koriste za potrebe informacionog rata i sajber terorizma.

Informacioni prostor *(engl. Information Space)*

Informacioni prostor predstavlja montažu informacija, informacione infrastrukture, entiteta koji se bave sakupljanjem, formiranjem, širenjem i korišćenjem informacija, kao i sistem upravljanja odnosa s javnošću koje proističu iz ovih komunikacija.
Može se definisati i kao površina aktivnosti koje se odnose na formiranje, stvaranje, transformaciju, prenos, korišćenje i skladištenje informacija koje, između ostalog, utiču na pojedinca i društvenu svijest, informacione infrastrukture i sam izvor informacija.

Informacioni sukob *(engl. Information Conflict)*

Napeta situacija između ili van nacionalnih država ili organizovanih grupa, gdje se informacione operacije dovode do odmazde

Informacioni rat *(engl. Information War)*

Stanje eskaliranja informacionog sukoba izmedju država u kojima državni akteri izvode informacione operacije za političko-vojne svrhe.
Konfrontacija između dvije ili više Vlada u informacioni prostor sa ciljem da ošteti sistem, procese i resurse, kritičnih duplikata.

Informacioni resursi *(engl. Information Resources)*

Informacioni resursi koji su predmet kontrolnih aktivnosti su definisani kao ljudi, aplikacije, informaciona infrastruktura, kao i odgovarajuće informacije i njihovi tokovi.

Informacioni sistem *(engl. Information System)*

Diskretni skup informacionih resursa organizovanih za prikupljanje, obradu, održavanje, korišćenje, dijeljenje, širenje ili raspolaganje informacijama. Informacioni sistem je integrisani skup komponenti za sakupljanje, snimanje, čuvanje, obradu i prenošenje informacija. Osnovne komponente informacionih sistema čine hardver i softver računara, baze podataka, telekomunikacioni sistemi i tehnologije, ljudski resursi i procedure, tj. metodologije procesovanja i prenošenja informacija.

Informacioni sistemi sigurnosti (engl. Information System Security)

Zaštita informacionih sistema od neovlašćenog pristupa ili izmjene podataka, bilo u skladištenju, obradi ili tranzitu, a protiv uskraćivanja usluga ovlašćenim korisnicima, uključujući i one mjere koje su neophodne za detekciju, dokumentovanje i kontru takvih prijetnji.

Informaciono bezbjednosna arhitektura *(engl. Information Security Architecture)*

Ugrađeni, sastavni dio poslovne arhitekture koja opisuje strukturu i ponašanje za preduzeća, bezbjednosne procese, informacione bezbjednosti sistema, kadrovske i organizacione podjedince, pokazujući svoje usklađivanje sa misijom preduzeća i strateškim planovima.

Informaciono oružje *(engl. Information Weapon)*

Informacione tehnologije, sredstva i metode koji se koriste za svrhe vođenja informacionog rata. Informacije i telekomunikacioni sistemi mogu postati oružje kada su dizajnirani ili korišćeni da izazovu štetu infrastrukturi neke države. Na primjer, napadaju nacionalne mreže sa stranim softverom ili iz izvora unutar države, ali promovisani ili zamišljeni iz inostranstva; radio i televizijske emisije imaju za cilj da poremete društveni poredak i institucionalni okvir koji proističe iz Ustava druge države u kojima se ovi signali šalju; aktivnosti namijenjene da ometaju, oštete ili se parališu za emitovanje drugih država, itd. Načini i sredstva koja se koriste sa ciljem oštećenja informacionih resursa, procesa i sistema države, vršeći negativan uticaj, kroz informisanje, odbrambene, administrativne, političke, socijalne, ekonomske i druge vitalne sisteme država, kao i masovno psihološka manipulacija populacije u cilju destabilizacije društva i države.

Informaciono ratovanje *(engl. Information Warfare)*

Iako se termini sajber ratovanje, sajber odbrana ili sajber napad često koriste u svakodnevnom govoru, širok vojni koncept koji se koristi u tom cilju je informaciono ratovanje, termin koji pokriva širok spektar operacija.

1. Akcije usmjerene na postizanje superiornosti informacija izvršavanjem mjera da se iskoristi, korumpira, uništi, ošteti ili destabilizuje informacija neprijatelja i njegova funkcija;
2. Preduzete mjere za zaštitu nečijih izvora informacija i telekomunikacionih sistema;
3. Iskorišćavanje djelovanja nečijih izvora informacija i telekomunikacionih sistema za postizanje ciljeva i interesa, na primjer, sajber ratovanja (informaciono ratovanje u odbrani u vojnom kontekstu), ili "Internet rat" (informaciono ratovanje u širem društvenom kontekstu).

Informaciono tehnološki incident *(engl. Information Technology Security Incident)*

Štetni događaj ili prekršaj, zbog kojeg su ugroženi integritet, dostupnost ili tajnost informacionih tehnologija.

Internet bezbjednost *(engl. Internet Security)*

U tehničkom smislu, odnosi se na zaštitu Internet servisa i srodnih ICT sistema i mreža, kao i proširenje mrežne bezbjednosti u organizacijama i domovima, kao obezbjeđivanje svrhe bezbjednosti. Bezbjednost na Internetu obezbjeđuje i dostupnost i pouzdanost Internet servisa. Međutim, u političkom kontekstu, Internet bezbjednost se često izjednačava sa onim što je takođe poznato kao bezbjedno korišćenje Interneta. Prema nekim definicijama, Internet bezbjednost uključuje globalni režim koji se bavi stabilnošću Internet koda i hardvera, kao i sporazume o krivičnom gonjenju ilegalnih sadržaja.

K

Kompjuterski sistem *(engl. Computer System)*

Jedan ili više međusobno povezanih računara sa pripadajućim softverom i perifernim uređajima. To može uključivati senzore i/ili (programsko sposobne logične) kontrolere, povezane preko računarske mreže. Kompjuterski sistemi mogu biti opšte namjene ili specijalizovani. (1)

Elektronski, magnetni, optički, elektrohemijski ili drugi uređaj za brzu obradu ili grupa međusobno povezanih ili srodnih uređaja koji obavljaju funkcije logike, aritmetike ili skladištenja, i obuhvata svako skladište ili komunikacije podataka objekata u direktnoj vezi ili zajedno sa takvim uređajem ili uređajima. (2)

Kritična infrastruktura *(engl. Critical Infrastructure)*

Uključuje elektronske informacije i komunikacione sisteme, usluge i informacije sadržane u ovim sistemima i uslugama. Informacioni i komunikacioni sistemi i usluge se sastoje od svih hardvera i

softvera koji procesuju, prodaju i prenose informacije ili bilo koju kombinaciju svih ovih elemenata. Obrada uključuje kreiranje, pristup, modifikaciju i uništavanje podataka. Skladištenje obuhvata štampane, magnetne, elektronske, kao i sve ostale vrste medija. Komunikacije uključuju dijeljenje i distribuciju informacija. Na primjer: računarskih sistema; kontrolnih sistema (na primjer, supervizorska kontrola i prikupljanje podataka); mreža, kao što je Internet i sajber usluge (na primje, upravljanje službama bezbjednosti) su dio sajber infrastrukture. (1)

Informaciona infrastruktura je ključna komponenta državne kritične infrastrukture, koja obuhvata sljedeće sektore: energetika i komunalne usluge, komunikacije i informacione tehnologije, finansije, zdravstvo, hranu, vodu, prevoz, Vladu i proizvodnju. Izazovi obezbjeđenja informacione infrastrukture su isti u svim sektorima, od kojih se procjenjuje da je do 90% u privatnom vlasništvu koji njima i upravljaju. Kritična infrastruktura se odnosi na infrastrukturu čiji bi poremećaj, propust ili uništenje imalo ozbiljne implikacije za društvo, privatni sektor i državu. To uključuje, na primjer, kontrolu i upravljački uređaj za snabdijevanje energijom ili telekomunikacijama. Popis kritične infrastrukture će biti sastavljen od strane nacionalne strategije za zaštitu kritične infrastrukture. (2)

Kritična infrastruktura informacija *(engl. Critical Information Infrastructure)*

Kritična infrastrukturna informacija podrazumijeva elektronsku komunikacionu mrežu, informacioni sistem ili grupu informacionih sistema, gdje incident koji se javlja prouzrokuje ili može prouzrokovati tešku štetu nacionalnoj bezbjednosti, nacionalnoj ekonomiji ili socijalnom blagostanju. (1)

Kritična infrastrukturna informacija podrazumijeva element ili sistem elemenata kritične infrastrukture u sektoru komunikacionih i informacionih sistema u okviru oblasti sajber bezbjednosti. Može se odnosi na sve IT sisteme koji podržavaju ključna dobra i usluge u okviru nacionalne infrastrukture. Uključuju sve operacije i kontrole kritičnih nacionalnih sektora kao što su zdravstvo, voda, prevoz, komunikacije, energija, hrana, finansije i hitne službe. (2)

Kritična nacionalna informaciona infrastruktura *(engl. National Critical Information Infrastructure)*

Označava sve ICT sisteme, sisteme za prenos podataka, baze podataka, mreže (uključujući i ljude, zgrade, objekate, postrojenja i procese), koji su od fundamentalnog značaja za efikasno funkcionisanje države.

Kritična sajber infrastruktura *(engl. Critical Cyber Infrastructure)*

Sajber infrastruktura koja je od suštinskog značaja za vitalne službe, za javnu bezbjednost, ekonomsku bezbjednost, nacionalnu i međunarodnu bezbjednosti i stabilnosti za održivost i obnovu kritične sajber infrastrukture.

Kritične sajber usluge *(engl. Critical Cyber Services)*

Sajber usluge koje su od vitalnog značaja za očuvanje javne, ekonomske, nacionalne i međunarodne bezbjednosti.

Kritični sajber prostor (*engl. Critical Cyberspace)*

Sajber infrastrukture i sajber usluge koje su od vitalnog značaja za očuvanje javne bezbjednosti, ekonomske stabilnosti, nacionalne bezbjednosti i međunarodne stabilnosti.

Krizne situacije *(engl. Crisis Situation)*

Faza eskalacije sukoba koju odlikuje upotreba vojne sile pri njenom rješavanju.

Kultura Informacione bezbjednosti *(engl. Information Security (culture))*

Država treba da podstiče razvoj jedne kulture informacionog društva, kroz podizanje svijesti među svojim građanima i subjektima u privatnom sektoru. Oni imaju slobodan pristup uslugama informacionog društva i informacijama o odgovornom ponašanju i korišćenju informacionih tehnologija. Građani moraju biti zaštićeni od zlonamjernih uticaja sajber napada koji mogu negativno uticati na kvalitet njihovog života i njihovo povjerenje u državu.

M

Međusobnost *(engl. Interoperability)*

Međusobnost je osnovni uslov za moderne informacione sisteme. Posebno se tumači na različitim nivoima međusobnosti informacionih sistema, naročito prilikom pregleda mijenja fokus međusobnosti istraživačkih tema, posljednja dostignuća i nove izazove u nastajanju globalne informacione infrastrukture. Ona dijeli istraživanja u tri generacije, i raspravlja o nekim dostignućima iz prošlosti. Na kraju se raspravlja potreba za postizanje semantičke međusobnosti i ključne komponente rješenja su uvedene. Za potrebe ovog standarda, međusobnost omogućava bilo kom Vladinom objektu ili informacionom sistemu, bez obzira na PIN (verifiacija ličnog identiteta) izdavaoca, da provjeri identitet vlasnika kartice pomoću akreditiva na kartici.

Međunarodni informacioni terorizam *(engl. International Information Terrorism)*

Upotreba telekomunikacija, informacionih sistema, resursa i uticaj na takve sisteme ili sredstva u međunarodnom informacionom prostoru za terorističke svrhe.

Metode sajber ratovanja *(engl. Methods of Cyber Warfare)*

Sajber taktike, tehnike i procedure kojima se sprovode neprijateljstva.

Mrežna bezbjednost *(engl. Network Security)*

Važna je za kritične infrastrukture koje često nijesu direktno povezane na Internet.

Mrežne operacije *(engl. Network Operations)*

Organizaciona stanica sposobnih za među komunikaciju, ali ne nužno na istom kanalu.

N

Napad *(engl. Attack)*

Bilo koja vrsta zlonamjernih aktivnosti koja pokušava prikupiti, poremetiti, odbiti, degradirati ili uništiti informacione resurse sistema ili same podatke. (1)

Napadači, takođe mogu djelovati u ime trećih osoba koje žele steći prednost. Napad može biti poznat ili nepoznat. Poznati napad znači da je otkrivena šema ili paket napada. Iako šema ili paket napada nijesu otvoreni kod nepoznatog napada, to se odnosi na ponašanje vezano uz pogoršanje situacije na mreži. Preduzete aktivnosti zaobilaze ili iskorišćavaju nedostatke u sigurnosnim mehanizmima na sistemu. Direktnim napadom sistema oni iskorišćavaju nedostatke u temeljnim algoritmima, načelima ili svojstvima sigurnosnih mehanizama. Direktni napadi se izvode kad se žele zaobići mehanizmi ili kad sistem koristi neodgovarajuće mehanizme. (2)

Napad na računarske mreže *(engl. Computer Network Attack)*

Akcije preduzete kroz upotrebu računarskih mreža da poremete, poriču, degradiraju ili unište informacije stanovnika u računaru i računarskih mreža, ili računara i samih mreža. Napad na računarske mreže je vrsta sajber napada.

Napadač *(engl. Attacker)*

Svaka osoba koja svjesno iskorišćava ranjivosti sistema u tehničkim i netehničkim sigurnosnim kontrolama kako bi ukrala ili ugrozila informacione sisteme i mreže, ili da kompromituje dostupnost legitimnim korisnicima informacionog sistema i mrežnih resursa. Pojedinac, grupa, organizacija ili Vlada mogu da vrše napad. Stranka djeluje zlonamjerno radi kompromitovanja informacionog sistema.

Napadačke sajber prostorne operacije *(engl. Offensive Cyberspace Operations)*

Sajber prostorene operacije namijenjene su da projektuji moć primjenom sile u/ili kroz sajber prostor.

Napredna konstantna prijetnja *(engl. Advanced Persistent Threat)*

Protivnik koji posjeduje sofisticirane nivoe stručnosti i značajna sredstva koja mu omogućavaju da stvori uslove za postizanje svojih ciljeva koristeći raznovrsne vektore napada (na primjer: sajber, fizički i obmane). Ovi ciljevi obično uključuju uspostavljanje i širenje uporišta u informacione tehnologije, infrastrukture ciljanih organizacija za potrebe informacije, podrivanja ili ometanja kritičnih aspekata misije, programa ili organizacije ili samo pozicioniranje za obavljanje ovih ciljeva u buducnosti.
Napredna konstantna prijetnja:

- ostvaruje svoje ciljeve u više navrata tokom dužeg vremenskog perioda,
- prilagođava se naporima branitelja i braniteljki da se odupre i
- odlučna je da održi nivo interakcije koji je neophodan da izvrši svoje ciljeve.

Grupa, kao što je strana vlada, sa mogućnošću i namjerom da kontinuirano i efikasno ciljaju specifični entitet, često sprovode špijunažu ili operacione napade.

Nedržavni akteri *(engl. Non-State Actors)*

Organizovani i neorganizovani kriminalci posluju u sivoj ekonomiji, eksploatišući slabosti u pojedinačnim, korporativnim i vladinim sistemima informacione infrastrukture. Koristili su različite tehnologije i metode psihologije da manipulišu korisnika i angažuju visoko sofisticirane sajber alate da zaraze, otmu i kontrolišu vrijedne informacije za kriminalne svrhe. Finansijska motivacija je obično vodilja ovim nedržavnim akterima. Oni nanose ogromnu finansijsku štetu svojim žrtvama. Njihovo djelovanje oštećuje ugled država i nanosi ogromnu štetu finansijskom sistemu države.

O

Odbrambena sajber prostorna operacija *(engl. Defensive Cyberspace Operation)*

Pasivna i aktivna sajber prostorna operacija namijenjena da očuva sposobnost da iskoristi prijateljske sajber prostorne sposobnosti i zaštiti podatake, mreže, u središtu sposobnosti, kao i drugih određenih sistema.

Odbrambene sajber prostorne operacije *(engl. Defensive Cyberspace Operations)*

Namjerno, ovlašćene defanzivne mjere i aktivnosti preduzete izvan mreže da štite i brane sajber sposobnosti Ministarstva odbrane ili drugih određenih sistema.

Odbrana računarske mreže *(engl. Computer Network Defense)*

Akcije preduzete da se odbrani od neovlašćenih aktivnosti u okviru računarskih mreža. Obuhvata praćenje, analiziranje, otkrivanje, ometanje, odgovor i restauraciju aktivnosti neovlašćenih aktivnosti koje se sprovode protiv računarskih mreža i IT sistema.

Online napad *(engl. Online Attack)*

Napad na protokol provjere identiteta, na kom napadač preuzima ulogu tužioca sa ovjerivačem istine ili aktivno mijenja kanal za potvrdu identiteta. Cilj napada može biti da se dobije ovjereni pristup ili da se nauče tajne provjere identiteta.

Osiguranje informacija *(engl. Information Assurance)*

Mjere koje štite i brane informacije i informacione sisteme obezbeđujući njihovu dostupnost, integritet, provjeru identiteta, povjerljivost i neporecivost. Ove mjere uključuju obezbjeđivanje za obnovu informacionih sistema u koji su uključene zaštita, otkrivanje i sposobnosti za reagovanje.

P

Pasivna sajber odbrana *(engl. Passive Cyber Defence)*

Mjere za otkrivanje i ublažavanje sajber upada i efekta sajber napada koji ne uključuju pokretanje preventivno, preče ili suprotstavljanje operaciji protiv izvora. Primjeri pasivnih mjera sajber odbrane su: protivpožarne zakrpe, anti virus softveri i digitalni forenzički alati.

Pasivni napad *(engl. Passive Attack)*

Napad protiv protokola za provjeru autentičnosti u kojoj napadač presrijeće podatke koji se kreću duž mreže između tužioca i verifikatora, ali ne izmjenjuje podatke (tj. prisluškivanje). Napad ne mijenja sistem ili podatke.

Prijetnja *(engl. Threat)*

Svaka okolnost ili događaj sa potencijalom da negativno utiče na organizacione poslove (uključujući misije, funkcije, slike ili ugled), organizaciona sredstva ili pojedince kroz informacioni sistem putem neovlašćenog pristupa, razaranja, otkrivanja, modifikacije informacija i/ili izvornih servisa. Takođe, potencijal za izvorne prijetnje uspješno koristi ranjivost informacionog sistema.

Prijetnja silom (sajber) *(engl. Threat of Force [Cyber])*

Sajber operacije ili prijetnja sajber operacijama sastavljene od nezakonite prijetnje silom, kada su zaprijećene akcije, ukoliko postoji nezakonita upotreba sile.

Protivmjera *(engl. Countermeasure)*

Akcije, uređaji, procedure, tehnike koje ispunjavaju ili se protive opasnosti, ranjivosti, eliminisanju ili sprječavanju napada, smanjenjem štete može da izazove, otkrije ili izvještava, tako da korektivne akcije mogu biti donijete.

Protivnik *(engl. Adversary)*

Pojedinac, grupa, organizacija ili Vlada koja vodi ili ima namjeru da sprovede štetne aktivnosti.

R

Računarska mreža *(engl. Computer Network)*

Informacijska struktura se koristi da dozvoli računaru razmjenu podataka. Infrastruktura može biti žična ili kao Wi-Fi ili kombinacija ova dva.

Računarska mrežna eksploatacija *(engl. Computer Network Exploitation)*

Omogućavanje operacija i sposobnosti prikupljanje obaveštajnih podataka sprovedena kroz upotrebu računarskih mreža za prikupljanje podataka iz ciljnih ili protivničkih automatizovanih informacionih sistema ili mreža. (1)

Operacije koje se sprovode u sajber prostoru da bi se izvukle informacije od ciljanih informaciono-komunikacionih mreža ili računarskih sistema. Ovo su obavještajne aktivnosti ili akcije spremne za izvršenje sajber napada. (2)

Računarske mrežne operacije *(engl. Computer Network Operations)*

Složeni proces planiranja, koordinacije, usklađivanja i razvoja akcije u sajber prostoru zaštite, kontrole i korišćenja računarske mreže da se dobiju informacije superiorno, dok se neutrališe neprijateljska sposobnost. Sastoji se od računarske mreže napada, računarske mreže odbrane i srodnih računarskih mreža eksploatacija koji omogućavaju operacije.

S

Sajber *(engl. Cyber)*

Riječ "sajber" je skoro uvijek prefiks za jedan mandat ili modifikator složenice, nego što je samostalna riječ. Njegov zaključak obično se odnosi na obrađene elektronske informacije (podatke), informacione tehnologije, elektronske komunikacije (prenos podataka) ili informacionih i računarskih sistema. Sam potpun termin složenice može biti napravljen da ima stvarno značenje. Riječ sajber se generalno vjeruje da potiče iz starogrčkog glagola kybereō (kibereo) što bi značilo "upravljati, voditi, kontrolisati", koji se odnose ili karakterišu na kulturu računara, informacione tehnologije i virtuelne realnosti.

Sajber bezbjednosni incident *(engl. Cyber Security Incident)*

Sajber incident podrazumijeva sigurnosne informacione sisteme, bezbjednost usluga, povrede ili integritet elektronskih komunikacionih mreža koje proizilaze iz bezbjednosti sajber događaja.

Sajber sigurnost *(engl. Cyber Safety)*

Sajber sigurnost je u vezi zaštite pojedinaca, naročito djece, od online rizika kao što su: izloženost uvredljivog sadržaja, sajber - maltretiranje na mreži. Mjere sajber bezbjednosti Vlade uključuju sprovođenje zakona, filtriranje i obrazovanje.

Sajber bezbjednost *(engl. Cyber security)*

Skup alata, politika, koncepata bezbjednosti, bezbjednosnih garancijja, smjernica, pristupa upravljanja rizicima, akcija, obuke, najbolje prakse, osiguranja i tehnologije koje mogu da se koriste za zaštitu životne sredine, sajber organizacije i korisničke imovine. Organizacija i korisnička sredstva uključuju povezane računarske uređaje, osoblje, infrastrukturu, aplikacije, servise telekomunikacionih

sistema, kao i ukupnost prenosa i/ili sačuvanih podataka u sajber okruženju. Sajber bezbjednost nastoji da osigura postizanje i održavanje bezbjednosnih karakteristika organizacije i korisničkih sredstva protiv nadležnih bezbjednosnih rizika u sajber okruženju. Opšti ciljevi bezbjednosti obuhvataju sledeće: povjerljivost, integritet (što može uključivati autentičnost i neporecivost) i dostupnost

Sajber događaj *(engl. Cyber Event)*

Sajber bezbjednosni događaj označava događaj koji može izazvati kršenje sigurnosti informacija u informacionim sistemima i bezbjednost usluga ili povrede bezbjednosti i integriteta elektronskih komunikacionih mreža.

Sajber domen *(engl. Cyber Domain)*

Sajber domen znači domen elektronske informacije (podatka) za obradu, koja se sastoji od jednog ili više informacionih tehnologija/infrastrukture. Obrada informacija (podataka) znači sakupljanje, čuvanje, organizovanje, korištenje, prenos, otkrivanje, pohranjivanje, izmjenu, kombinovanje, zaštitu, uklanjanje, rušenje i druge slične akcije na informaciji (podacima).

Sajber eksploatacija *(engl. Cyber Exploitation)*

Iskoristivšćavanje prilike u sajber prostoru da se postigne objekat.

Sajber elektromagnetne aktivnosti *(engl. Cyber Electromagnetic Activities)*

Aktivnosti preduzete da zadrže i iskoriste prednost nad protivnicima i neprijateljima u sajber prostoru i elektromagnetnom spektru, istovremeno negirajući i ponižavajuću protivnika i neprijatelja upotrebom iste zaštitne misije komandnog sistema.

Sajber entitet *(engl. Cyber Entity)*

Bilo koja posebna stvar ili akter koji postoji u sajber infrastrukturi.

Sajber imovina *(engl. Cyber Asset)*

Sajber entiteti sa vrijednošću.

Sajber incident *(engl. Cyber Incident)*

Incident označava neki događaj, činjenje ili nečinjenje koje daje povoda ili može da dovede do neovlašćenog pristupa informacionom sistemu ili elektronskoj komunikacionoj mreži, prekida ili promjene operacije (uključujući i preuzimanje kontrole) uništenje, oštećenje, brisanje ili promjenu elektronskih informacija, uklanjanje ili ograničavanje mogućnosti za korišćenje elektronskih informacija, što dovodi ili može dovesti do prisvajanja, objavljivanja, širenja ili bilo koje druge upotrebe nejavne elektronske informacije od strane ovlašćenih lica. (1)

Akcije preduzete kroz upotrebu računarskih mreža koje rezultiraju stvarnom ili potencijalno negativnom efektu na informacioni sistem i/ili informacije koje u njoj žive. (2)

Sajber incident od nacionalnog značaja *(engl. Cyber Ralated Incident of National Significance)*

Sajber incident od nacionalnog značaja može biti bilo koji oblik, organizovan u sajber napad, nekontrolisana ekspoloatacija, kao što su kompjuterski virusi, crvi ili bilo koji od zlonamjerskih softvera kod prirodne katastrofe sa značajnim posledicama, sajber ili drugih srodnih incidenata koji mogu izazvati veliku štetu na informacione infrastrukture ključnih sredstava. Sajber indicent velikih razmjera može preplaviti Vlade, javna i privatna sredstava i sektor usluga od ometanja fukcionisanja do kritičnih informacionih sistema. Komplikacije takvog obima mogu da ugroze živote, ekonomiju i nacionalnu bezbjednost.

Sajber infiltriranje *(engl. Cyber Exfiltration)*

Tip sajber operacije koja uključuje kopiranje ili uklanjanje bilo kakvih podataka.

Sajber infrastruktura *(engl. Cyber Infrastructure)*

Uključuje elektronske informacione i komunikacione sisteme, usluge i informacije sadržane u ovim sistemima i uslugama. Informacioni i komunikacioni sistemi i usluge se sastoje od svih hardvera i softvera u tom procesu, skladište i prenose informacije ili bilo koju kombinaciju svih ovih elemenata. Obrada uključuje kreiranje, pristup, modifikaciju i uništavanje podataka. Skladištenje obuhvata štampane, magnetne, elektronske, kao i sve ostale vrste medija. Komunikacije uključuju dijeljenje i distribuciju informacija. Na primjer: računarskih sistema, kontrolnih sistema (na primjer: supervizorska kontrola i prikupljanje podataka), mreža kao što je Internet i sajber usluge (na primjer: primijenjeni servisi bezbjednosti) su dio sajber infrastrukture. (1)

Agregacija ljudi, procesa i sistema koji sačinjavaju sajber prostor. (2)

Sajber inteligencija *(engl. Cyber Intelligence)*

Aktivnosti koje se preduzimaju koristeći sve "inteligencijske" izvore u prilog sajber bezbjednosti, da mapira opšte sajber prijetnje, da prikupi sajber namjere i mogućnosti potencijalnih protivnika, analiziraju i komuniciraju, da se identifikuju, lociraju i dodjeljuju izvori sajber napada.

Sajber izviđanje *(engl. Cyber Reconnaissance)*

Upotreba sajber mogućnosti da se dobije informacija o aktivnostima, izvorima informacija ili mogućnostima sistema.

Sajber kontramjere *(engl. Cyber Countermeasures)*

Kontramjere znače da bi akti Agencije za nacionalnu bezbjednost trebalo da zaštite informacione sisteme ili usluge i elektronske komunikacione mreže od prijetnje u oblasti sajber bezbjednosti ili da djeluje u rješavanju već postojećih sajber bezbjednosnih incidenata. Zaštitna kontramjera opšte prirode na osnovu već riješenih sajber bezbjendosnih analiza incidenata u cilju povećanja zaštite informacionih sistema ili usluga ili elektronskih komunikacionih mreža.

Sajber kontranapad *(engl. Cyber Counter-Attack)*

Upotreba sajber oružja sa namerom da naudi određenom cilju kao odgovoru na napad.

Sajber kriminal *(engl. Cyber Crime)*

Sajber kriminal je kriminalna aktivnost sprovedena pomoću računara i Interneta, često finansijski motivisana. Sajber kriminal uključuje, između ostalih aktivnosti, krađu identiteta, prevare i Internet prevare. Sajber kriminal se razlikuje od drugih oblika zlonamjernih sajber aktivnosti, koje imaju političke, vojne ili špijunske motive. Sajber kriminal obuhvata ilegalne napade iz sajber prostora putem ICT sistema, koji su definisani u krivičnim ili administrativnim zakonima. Termin stoga pokriva sva krivična djela počinjena uz pomoć informacionih tehnologija i komunikacionih mreža i obuhvata Internet kriminal. Sajber kriminal obično se odnosi na širok spektar različitih kriminalnih aktivnosti u kojima su kompjuteri i informacioni sistemi uključeni bilo kao osnovno sredstvo ili kao primarni cilj. Sajber kriminal se sastoji od tradicionalnih djela (na primjer: prevara, falsifikovanje i krađe identiteta), djela sadržanih u vezi (na primjer: online distribuciju dječje pornografije ili izazivanje rasne mržnje) i krivična djela jedinstvena samo za računare i informacione sisteme (na primjer: napad na informacione sisteme, poricanje usluga i malvezacije).

Ova krivična djela mogu se grubo podijeliti u tri kategorije:

a) Univerzalna, državna i javna djela, koja predstavljaju prijetnju po nacionalnu i javnu bezbjednost (uključujući i pozive da sruše postojeći poredak, pokušaja da devalvira suverenitet ili da ugrozi nezavisnost i nacionalne interese, terorističke propagande, šovinizam, ksenofobiu, svi oblici ekstremizma i diskriminacija na nacionalnoj, rasnoj, vjerskoj, polnoj i drugim osnovama);

b) Univerzalna civilna djela koja predstavljaju prijetnju individualnih prava i sloboda (uključujući kršenja individualnih prava i sloboda, upotreba kompromitovanih materijala, vršenja pritiska na pojedince, diskreditovanje pojedinaca, širenje povjerljivih informacija, korišćenje tuđih Internet usluga, falsifikata dokumenata i autorskih prava);

c) Tradicionalna djela, koja ugrožavaju temelje morala i pristojnosti (uključujući pornografiju, pedofiliju i druge oblike seksualne perverzije, narkomanije i alkoholizma).

Sajber kriminalitet/sajber kriminal *(engl. Cybercriminality/cybercrime)*

Djelo uvredljivog korišćenja automatizacije ili automatskog pružanja ugrožavanja informacionih sistema ili registrovanih izvora informacija, da ugrozi informacione sisteme ili registrovane informacije.

Sajber napad *(engl. Cyber Attack)*

Sajber napad je informacioni napad u sajber prostoru usmjeren protiv jednog ili više drugih informacionih sistema i usmjerena na oštećenje informacione bezbjednosti. Ciljevi informacione bezbjednosti, povjerljivosti, integriteta i dostupnosti mogu svi ili pojedinačno biti ugroženi. Sajber napadi usmjereni protiv tajnosti informacionih sistema, koje su pokrenule ili upravljaju strane obavještajne službe, zovu se sajber špijunaža. Sajber napadi protiv integriteta i dostupnosti informacionih sistema se nazivaju sajber sabotaže. (1)

Sajber napadi se izvode na računarima, mrežama i podacima. Oni imaju za cilj da ometaju integritet podataka ili funkcionisanje infrastrukture kao i ograničavanje ili prekidanje njihove dostupnosti. Oni takođe traže da ugroze povjerljivost ili autentičnost informacija putem neovlašćenog čitanja, brisanja ili izmjene podataka, veze ili preopterećenja usluga servera, informacioni kanali su špijunirani i nadzirani, a obrađeni sistemi su ciljano izmanipulisani. (2)

Termin sajber napad se može odnositi na bilo šta od malih e-mail prevara do sofisticiranih napada velikih razmjera sa različitim političkim i ekonomskim motivima. Veliki napadi mogu da imaju veliki broj međusobno povezanih ciljeva kao što su: dobijanje neovlašćenog pristupa povjerljivim informacijama; uzrokovanje prekida IT infrastrukture; ili nanošenje fizičkog poremećaja (na primjer, industrijskim sistemima). (3)

Sajber napad (posledice) *(engl. Cyber-attack (Consequences))*

Sajber napadi povećavaju mogućnost otkrivanja podataka, manipulacije podacima, gubitak podataka i diverzantske sisteme.

Sajber napadi *(engl. Cyber Attacks)*

Sajber napadi usmjereni protiv javnosti, kao i privatnog sektora su sve češći i sofisticiraniji. Oni mogu da izazovu posebno neuspjeh komunikacije, energije i transportne mreže, transportnih procesa i industrijskih i finansijskih sistema, što dovodi do velike materijalne štete. Oružani snage u zavisnosti od informacionih i komunikacionih sistema mogu da utiču na sposobnost odbrane države. Drugi problem usko povezan sa sajber napadom je politička i ekonomska špijunaža.

Sajber odbrambena sposobnost *(engl. Cyber Defensive Capability)*

Sposobnost da efikasno zaštiti i odbiju sajber eksploatacije ili sajber napade, kao i napade koji se mogu kategorizovati kao sajber zastrašivanje.

Sajber odbrambene kontramjere *(engl. Cyber Defensive Countermeasure)*

Raspoređivanje određenih sajber odbrambenih sposobnosti da poraze ili preusmjere sajber napad.

Sajber odbrana *(engl. Cyber Defence)*

Skup svih tehničkih i netehničkih mjera koje omogućavaju državi da brani sajber informacione sisteme koji se smatraju kritičnim. Sposobnost država da spriječe i suprotstave se bilo kakvoj prijetnji ili incidentu koji je kibernetički u prirodi i koji utiče na nacionalni suverenitet. Primjena efikasnih mjera zaštite da dobiju odgovarajući nivo sajber bezbjednosti kako bi se garantovala odbrana i funkcionalnost. Ovo se postiže primjenom odgovarajućih mjera zaštite kako bi se smanjio bezbjednosni rizik na prihvatljiv nivo. Sajber odbrana se sastoji od sledećih zadataka: zaštite, odgovaranja i obnove.

Sajber ofanziva *(engl. Cyber Offensive)*

Ofanzivni kapacitet uključuje manipulaciju ili narušavanje mreža i sistema s ciljem ograničavanja ili eliminisanja protivnikove operativne mogućnosti. Ova sposobnost može da traži da se garantuje slobodna akcija u sajber domenu. Sajber napad može biti pokrenut da odbije napad (aktivna odbrana), ili da podrže operativnu akciju.

Sajber ofanzivna mogućnost *(engl. Cyber Offensive Capabiltiy)*

Postojanje mogućnosti da se pokrene sajber napad koji može da se koristi kao sajber zastrašivanje.

Sajber operacija *(engl. Cyber Operation)*

Organizovanje aktivnosti u sajber prostoru da se okupe, pripreme, šire ili obrađuju informacije sa ciljem da se postigne pogodak.

Sajber operacije *(engl. Cyber Operations)*

Upotreba sajber sposobnosti gdje je primarna svrha da se postignu ciljevi u/ili kroz sajber prostor. Takve operacije uključuju rad kompjuterske mreže i aktivnosti za rad i odbranu globalne informacione mreže.

Sajber oružje *(engl. Cyber Weapon)*

Softver, firmware ili hardver projektovan ili primijenjen da prouzrokuju štetu kroz sajber domen.

Sajber prijetnja *(engl. Cyber Threat)*

Sajber prijetnje znače mogućnost djelovanja ili incident u sajber domenu koji kada se materijalizuje, ugrožava neku operaciju zavisnu od sajber svijeta. Sajber prijetnje su informacione prijetnje koje, kada se materijalizuju, ugrožavaju ispravno ili namjereno funkcionisanje informacionog sistema. Mogućnost zlonamjernog pokušaja da se ošteti ili poremeti računarska mreža ili sistem.

Sajber prijetnje *(engl. Cyber Threats)*

Neki od primjera sajber prijetnji pojedincima, preduzećima i Vladi su gradski identitet, fišing, socijalni inženjering, haktivizam, sajber terorizam, složene prijetnje usmjerene na mobilne uređaje i smart telefone, kompromitovani digitalni sertifikati, napredne postojeće prijetnje, poricanje usluga, bot mreže, lanac snabdijevanja napada, curenje podataka, itd. Zaštita informatičke infrastrukture i očuvanje povjerljivosti, integriteta i dostupnosti informacija u sajber prostoru je suština sigurnosti u sajber prostoru.

Sajber prodor *(engl. Cyber Penetration)*

Neovlašćeni ulazak u sajber entitet.

Sajber prostor *(engl. Cyberspace)*

Sajber prostor je virtuelni prostor svih IT sistema povezanih na nivou podataka na globalnom nivou. Osnova za sajber prostor je Internet kao univerzalna i javno dostupna veza i transportna mreža, koja može biti dopunjena i proširena preko drugih mreža. U običnom govoru, sajber prostor se odnosi na globalne mreže različitih nezavisnih informacionih infrastruktura, telekomunikacionih mreža i računarskih sistema. U socijalnoj sferi korišćenje ove globalne mreže omogućava pojedincima da komuniciraju, razmjenjuju ideje, šire informacije, daju socijalnu pomoć, angažuju u poslovanju, kontolišu akcijama, stvaraju umjetnost i medijske poslove, igraju igrice, učestvuju u političkim diskusijama i mnogo više. Sajber prostor je postao zajednički naziv za sve stvari vezane za Internet i za različite Internet kulture. Mnoge zemlje imaju umrežene ICT i nezavisne mreže koje rade preko ovog medija kao komponente svoje "nacionalne kritične infrastrukture". Sajber prostor označava fizički i nefizički teren stvoren i/ili sastavljen od nekih ili od svega sljedećeg: računara, računarskih sistema, mreža i njihovih kompjuterskih programa, kompjuterskih podataka, podataka sadržaja,

podataka o saobraćaju i korisnicima.

Sajber prostor je interaktivno okruženje koje uključuje korisnike, mreže, kompjuterske tehnologije, softver, procese, informacije u tranzitu ili skladištenja, aplikacija, usluga i sistema koji se mogu direktno ili indirektno povezati sa Internetom, telekomunikacionim i računarskim mrežama. Sajber prostor nema fizičke granice.

Sajber prostorna inteligencija *(engl. Cyberspace Intelligence)*

Mjere za identifikaciju, prodiranje ili neutralisanje inostranih operacija koje koriste sajber, znače kao primarna metodologija trgovinske vještine, kao i zbirka napora stranih obaveštajnih službi koji koriste tradicionalne metode da se utvrde sajber sposobnosti i namjere.

Sajber prostorna operacija *(engl. Cyberspace Operations)*

Operativna prednost preko i iz sajber prostora za obavljanje poslova u datom trenutku i u datom domenu bez previsokih uplitanja.

Sajber prostorna superiornost *(engl. Cyberspace Superiority)*

Stepen dominacije u sajber prostoru jedne sile koja omogućava bezbjedno i pouzdano vođenje poslovanja od strane te sile, i njihovog povezanog zemljišta, klime, morskih i svemirskih snaga u datom vremenu i mjestu bez previsokih miješanja protivnika.

Sajber ranjivosti *(engl. Cyber Vulnerability)*

Imovina sajber entiteta koja je podložna eksploataciji.

Sajber rat *(engl. Cyber War)*

Sajber rat se odnosi na jedan vid rata u virtuelnom prostoru, sredstvima koja su uglavnom povezana sa informacionim tehnologijama. U širem smislu, to podrazumijeva podršku vojnih kampanja u tradicionalnom operativnom prostoru tj. kopnenih, vodenih, vazdušnih i svemirskih - putem mjera preduzetih u virtuelnom prostoru. Generalno, termin se takođe, odnosi na visokotehnološki rat u informatičkom dobu na osnovu opsežne kompjuterizacije, elektronizacije i umrežavanja gotovo svih vojnih sektorskih pitanja.

Sajber ratnici *(engl. Cyber Warrior)*

Stručna lica direktno angažovana u sajber ratovanju.

Sajber ratovanje *(engl. Cyberwarfare)*

Upotreba sajber sposobnosti dovoljnog obima, tokom određenog perioda velikom brzinom, da se dođe do određenih ciljeva u sajber prostoru; ove akcije se smatraju kao prijetnja za ciljane države.

Sajber ratovanja *(engl. Cyber Warfare)*

Sajber napadi koji su ovlašćeni od strane državnih aktera protiv sajber infrastrukture u konekciji sa Vladinom kampanjom.

Sajber sistem *(engl. Cyber System)*

Jedan ili više međusobno povezanih računara namijenjen za udruženo povezivanje sa pripadajućim softverom i perifernim uređajima. To može uključivati senzore i/ili (Programmable Logic) kontrolere, povezane preko računarske mreže. Kompjuterski sistemi mogu biti opšte namjene (na primjer, laptop) ili specijalizovanih.

Sajber snage *(engl. Cyber Forces)*

Sajber sredstva organizovana za obavljanje poslova sajber operacija.

Sajber sukob *(engl. Cyber Conflict)*

Napeta situacija između i/ili među nacionalnim državama i/ili organizovanim grupama kojima nepoželjni sajber napadi dovode do odmazde.

Sajber svijest *(engl. Cyber Awareness)*

Svijest se odnosi na bezbjednosnu svijest svih lica koja dijele odgovornost za informacionu bezbjednost. Razumijevanje i motivacija su neophodni kako bi se osiguralo da su bezbjednosna pravila posmatrana i sprovedena na stalnoj osnovi.

Sajber špijunaža *(engl. Cyber Espionage)*

Sajber napadi imaju za cilj da ukradu osjetljive informacije i podatke iz finansijskih, državnih i komunalnih infrastrukturnih ciljeva. Ovi napadi mogu da ciljaju na intelektualnu svojinu ili osjetljive informacije o organizacijama ili Vladama. Sajber špijunaža se definiše kao korišćenje agensa u cilju dobijanja informacija o planovima ili aktivnostima strane države ili konkurentske kompanije. Nije neuobičajeno da se kompanije ili Vlada suočavaju sa pokušajima neovlašćenog pristupa svojim računarskim sistemima preko Interneta. Mnoge zemlje koriste špijunske alate za podsticanje njihovog ekonomskog razvoja zasnovane na naprednim tehnologijama. Informaciono komunikacione tehnologije, prisutni temelji razvoja i implementacije drugih tehnologija, kako u civilnim tako i u vojnim sektorima, su postali primarni cilj za špijunažu.

Sajber terorizam *(engl. Cyber Terrorism)*

Sajber terorizam je definisan kao politički motivisani zločini državnih i/ili nedržavnih aktera protiv računara, mreža i podataka koji se nalaze u njemu. Cilj je da se izazove ozbiljno ili dugoročno narušavanje javnog života ili da prouzrokuje ozbiljnu štetu ekonomskoj aktivnosti sa namjerom ozbiljnog zastrašivanja stanovništva, forsiranja javnih vlasti ili međunarodne organizacije da sprovede, toleriše ili izostavi akt ili duboko uznemire ili unište političke, ustavne, ekonomske ili socijalne temelje države ili međunarodne organizacije. Ovi akti predstavljaju organizovanu sajber sabotažu (napade) izazvane od strane političko-fundamentalističke grupe ili pojedinačnih počinilaca i usmjereni su protiv država, organizacija ili preduzeća. Politički motivisano korišćenje računara i informacionih tehnologija u cilju nanošenja teških poremećaja ili širenja straha.

Terorističke mreže se takođe pokreću da ugrade sajber operacije u svoje strateške doktrine. Među brojnim aktivnostima, oni koriste Internet da podrži svoja zapošljavanja, prikupljanja sredstava i propagandne aktivnosti. Teroristi su svjesni potencijala za korišćenje zavisnosti Zapadnog svijeta od sajber sistema kao ranjivost da se eksploatiše. Na primjer, sada postoje onlajn resursi koji pružaju

savjete teroristima kako da brane svoje sajtove, dok pokreću sajber napade na svoje neprijatelje. Pored toga, veliki broj terorističkih grupa, uključujući i Al-Kaidu, izrazili su namjeru da pokrenu sajber napade protiv zapadnih država. Iako stručnjaci sumnjaju da teroristi trenutno imaju sposobnost da nanesu ozbiljnu štetu preko sajber napada, oni priznaju da će ovaj kapacitet vjerovatno razvijati tokom vremena.

Sajber usluge *(engl. Cyber Services)*

Niz razmjene podataka u sajber prostoru za direktnu ili indirektnu korist ljudi.

Sajber vježba *(engl. Cyber Exercise)*

Planirani događaj tokom kojeg organizacija simulira sajber prekid za razvoj ili test sposobnosti, kao što je sprječavanje, otkrivanje, ublažavanje, odgovor na ili oporavljanje od prekida.

Sajber zastrašivanje *(engl. Cyber Deterrent)*

Deklarisani mehanizam koji se pretpostavlja u efikasnom obeshrabljivanju sajber sukoba ili prijetećih sajber aktivnosti.

Sajber životna sredina *(engl. Cyber Environment)*

Ovo uključuje korisnike, mreže, uređaje, sve programe, procese, informacije u skladištenju ili tranzitu, aplikacije, usluge i sisteme koji se mogu direktno ili indirektno povezati na mrežama.

Sfera informacija *(engl. Information Sphere)*

Formirani sistem faktora ako društveni život njegove aktivnosti utiče na državne, političke, ekonomske, odbrambene i ostale svoje bezbjednosne komponente.

Slučajni insajderi *(engl. Unintentional Insiders)*

Oni sa ovlašćenim pristuomp na mrežu, sistem, ili informacije organizacije. Slučajni insajderi mogu predstavljati prijetnju zbog nezlonamjernog činjenja ili nečinjenja koje nanosi štetu ili utiče na povjerljivost, integritet ili dostupnost mreže, sistema ili informacije.

Superiornost informacija *(engl. Information Superiority)*

Imati bolje informacije ili više informacija.

T

Teroristično korišćenje Interneta *(engl. Terrorist Use of the Internet)*

Terorističke mreže takođe ugrađuju sajber operacije u svoje strateške doktrine. Među brojnim aktivnostima oni koriste Internet da podrži njihovo zapošljavanje, prikupljanje sredstava i propagandne aktivnosti. Teroristi su svjesni potencijala za korišćenje i Zapadnu svjetsku zavisnost od sajber sistema, kao i ranjivost da se eksploatiše. Na primjer, sada postoje onlajn resursi koji pružaju savjete teroristima kako da brane svoje sajtove dok pokreću sajber napade na svoje neprijatelje. Pored toga, veliki broj terorističkih grupa, uključujući Al-Kaidu, izrazili su namjeru da pokrenu sajber napade protiv zapadnih država. Iako stručnjaci sumnjaju da teroristi trenutno imaju sposobnost da nanesu ozbiljnu štetu preko sajber napada, oni priznaju da će ovaj kapacitet vjerovatno razviti tokom vremena.

Terorizam *(engl. Terrorism)*

Različiti oblici sajber terorizma: presijecanje, DoS napadi, uskraćivanja usluga, logičkih bombi, trojanaca, crva, virusa, HERF pištolja, itd.

Testiranje pasivne bezbjednosti *(engl. Passive Security Testing)*

Sigurnost testiranja koje ne podrazumijeva bilo kakvu direktnu interakciju sa ciljevima, kao što je slanje paketa u metu.

U

Unutrašnje prijetnje *(engl. Insider Threat)*

Tzv. insajder prijetnje predstavljaju značajan izazov. Insajder prijetnje uključuju potpunu zaposlenost ili nemarno kršenje bezbjednosnih procedura na radnom mjestu. U tom kontekstu, opasnost od nemara predstavlja poseban izazov - zaposleni mogu nenamjerno pustiti neovlašćene osobe na radnom mjestu držeći vrata strancima, ili mogu preuzeti programe sa sumnjivim sadržajima. Ako zaposleni ne poštuju bezbjednosne procedure, to povećava rizik od neovlašćenog pristupa internim mrežama i samim tim osjetljivim informacijama.

Upotreba sile (sajber) *(engl. Use of Force [Cyber])*

Sajber operacija predstavlja upotrebu sile kada se njen obim i efekti mogu porediti sa ne sajber operacijama podiže na nivo upotrebe sile.

V

Vanredno sajber stanje *(engl. Cyber Emergency)*

Državno sajber vanredno stanje znači stanje tokom kojeg je bezbjednost informacija u informacionim sistemima ili usluga ili elektronskih komunikacionih mreža ozbiljno ugrožena i interesi države mogu tako biti prekršeni ili ugroženi.

Važne mreže *(engl. Important Network)*

Važne mreže predstavljaju elektronske komunikacione mreže pružanja direktnog međunarodnog povezivanja javnih komunikacionih mreža ili pružanje direktne veze sa kritičnim informacionim infrastrukturama.

Važni informacioni sistemi (*engl. Important Information System)*

Važni informacioni sistemi znače informacioni sistem kojim upravlja jedna od javne vlasti, koja nije kritično informacijska infrastruktura i koje mogu ugroziti ili primjetno ograničiti obavljanje javne uprave u slučaju povrede sigurnosti informacija.

Vojni sukob u informacionom prostoru (*engl. Military Conflict in Information Space)*

Oblik međudržavnih ili unutar državnih sukoba, koristeći informaciona oružja.

Z

Zaštita kritične infrastrukture (*engl. Critical Infrastructure Protection)*

Akcije preduzeti da spriječi, otkloni ili ublaži rizike koji proističu iz ranjivosti kritične infrastrukture imovine.

Zatvorena akcija sajber operacije *(engl. Close Action [Cyber] Operation*)

Sajber operacija zahtijeva fizičku blizinu ciljanog sistema.

Značenje sajber ratovanja *(engl. Means of Cyber Warfare)*

Sajber oružje i njihovi povezani sajber sistemi.

Životna sredina-operacije *(engl. Environment of Operation)*

Fizički, tehnički i organizacioni ambijent u kome informacioni sistem funkcioniše, uključujući ali se ne ograničavajući na: misije/poslovnih funkcija; misije/poslovnih procesa; prostorne prijetnje; ranjivosti; preduzeća i informacije bezbjednosne arhitekture; osoblja; objekata; lanaca snabdijevanja odnosa; informacione tehnologije; organizaciono upravljanje i kultura; akvizicija i nabavka procesa; organizacione politike i procedure; organizacione pretpostavke, ograničenja, tolerancija rizika i prioriteti/kompromisi. Fizička okolina u kojoj je informacioni sistem proces, prodavnica i prenosi informacije.

IMPRESSUM

Online časopis: **»Sajber bezbjedonosne instrukcije za sve«**

Godina 2, broj 5, Oktobar 2016.

Izdaje: Centar za edukaciju u oblasti sajber bezbjednosti u Crnoj Gori MCEC

web: http://imtm.me/mcec.php

e-mail: newsletter.ecesm@gmail.com