Recenzija

Paul Rosenzweig
Cyber Warfare. How Conflicts in Cyberspace Are Challenging America and Changing the World

Praeger, Santa Barbara, Denver, Oxford, 2013, 290 str.

Ovo je jedna od brojnih knjiga posvećenih temi ratovanja u cyber prostoru. Kao što je literatura koja bi mogla biti svrstana u kategoriju futurizma i znanstvene fantastike umnogome pridonijela osvješćivanju mogućnosti da cyber prostor postane peta domena ratovanja, tako danas činjenica da je on to doista i postao te da vlade i nevladini igrači razrađuju strategije cyber obrane i cyber napada potiče stručnjake različitih provenijencija da prikazuju dosegnute tehničke mogućnosti upotrebe i zloupotrebe interneta, da analiziraju zakonsku regulativu upotrebe cyber prostora i da predviđaju kakve će se promjene događati u virtualnom i stvarnom svijetu. Podatak da je autor ove knjige bio pomoćnik tajnika za politiku u američkom Ministarstvu domovinske sigurnosti s jedne strane navodi na pomisao o njegovoj nedvojbenoj kompetentnosti, dok, s druge, može pobuditi sumnju da će se i on, kao što su to već učinili mnogi bivši dužnosnici američkih sigurnosnih službi, pridružiti poprilično velikoj skupini onih koji namjerno proizvode inflaciju prijetnje kako bi povećali potražnju za svojim uslugama i podigli im cijenu. Kad pročita ovu knjigu, čitatelj će uvidjeti da Rosenzweig ne spada u skupinu onih koji nekritički preuveličavaju neposrednu opasnost od kataklizmičkih posljedica cyber napada na američke SCADA-sustave, na software koji upravljaju mrežom električnih dalekovoda, naftovodima i plinovodima, vodovodima i sustavima za odvodnju, uređajima u pogonima kemijske industrije i nuklearnih materijala. U knjizi se nijedanput ne spominje *cyber Pearl Harbor*, što je omiljena metafora kojom zagovornici interesa proizvođača hardwarea i softwarea za cyber sigurnost žele uvjeriti američku javnost da je *cyberwar* protiv Amerike već započeo i da je potrebna maksimalna mobilizacija svih državnih i civilnih resursa u interesu uspješne obrane. No, to nipošto ne znači da Rosenzweig na bilo koji način podcjenjuje ili zanemaruje važnost cyber prostora u obrani i promicanju američkih nacionalnih interesa. Njegova knjiga, složena na temelju njegovih članaka i izlaganja na stručnim skupovima u razdoblju od 2009. do 2012. godine, vrlo pomno ukazuje na probleme u određivanju granice između cyber kriminala i cyber rata, na probleme pravne regulacije postupaka u cyber prostoru na nacionalnoj i međunarodnoj razini, na nužnost redefiniranja pojma privatnosti u cyber prostoru, na odnos vlade i privatnog sektora u definiranju i provedbi strategije cyber sigurnosti te na načelnu nepredvidljivost smjera, brzine i sadržaja promjena u cyber prostoru.

Internet izvorno nije zamišljen kao oružje niti se pretpostavljalo da bi cyber prostor mogao postati domenom ratovanja. No, sve veća ovisnost vitalnih civilnih i vojnih sustava upravljanja većine zemalja o kompjutorskoj tehnologiji otvorila je

mogućnost da se neovlaštenim upadima u informacijske sustave utječe na te sustave s ciljem njihova ometanja ili onesposobljavanja. Kad je ubacivanje zlonamjernog koda Stuxnet u kompjutorske programe koji su upravljali centrifugama za obogaćivanje urana u iranskom postrojenju u Natanzu 2009. godine dovelo do njihova fizičkog uništenja, postalo je jasno da se manipulacijama u cyber prostoru mogu postići učinci kakvi se postižu primjenom klasičnih vrsta oružja. Tako se uz već davno uočene opasnosti krađe intelektualnog vlasništva i državnih i vojnih tajni te krađe identiteta, što bi se sve moglo svrstati u kategoriju cyber kriminala, pojavila i mogućnost upotrebe cyber prostora kao nove domene ratovanja. Izbjegavajući jasno reći ono što je u dijelu publicistike specijalizirane za teme cyber ratovanja prilično pouzdano utvrđeno, naime to da su Stuxnet kreirali američki i izraelski kompjutorski stručnjaci, Rosenzweig hipotezi o američko-izraelskoj izvedbi napada na iranska nuklearna postrojenja – pri čemu se poziva na neimenovane izvore iz Obamine administracije – dodaje onu o kineskom autorstvu nad Stuxnetom (str. 10). Pritom i te nejasnoće u vezi s autorstvom i izvedbom upotrebljava kao ilustraciju za problem atribucije, utvrđivanja počinitelja kriminalnih ili ratnih postupaka u cyber prostoru. No, i za njega, kao i za mnoštvo drugih autora koji se bave temom ratovanja u cyber prostoru, Stuxnet je definitivna potvrda mogućnosti da se manipulacijama u cyber prostoru postignu učinci identični učincima primjene klasičnog oružja. Isto tako, Stuxnet je dao snažan poticaj za razmišljanje o strategiji cyber sigurnosti s obzirom na to da bi ono što su, pretpostavlja se, Amerikanci i Izraelci već učinili drugima netko mogao učiniti Americi. Pritom bi posljedice eventualne uspješne primjene Stuxneta protiv američkih vitalnih sustava koje kontroliraju kompjutori mogao imati nesagledive ekonomske, društvene i političke posljedice usporedive s posljedicama masovnog napada cijelim spektrom klasičnog naoružanja u svim klasičnim domenama ratovanja. Uz to valja imati na umu da bi počinitelji takvih napada mogli biti neprijatelji koji su u svakom pogledu nerazmjerno slabiji od Amerike. Bio bi to izrazit primjer asimetričnog rata u kojem je nemoguće primijeniti strategiju odvraćanja ne samo stoga što bi se potencijalni počinitelj mogao skrivati iza mreže računala uključenih u izvedbu napada bez znanja njihovih vlasnika i što bi mogao računati na probleme atribucije nego i stoga što bi šteta koju bi SAD uzvratnim udarom mogao nanijeti počinitelju bila nerazmjerno manja od štete koju bi sam pretrpio.

Rosenzweig čitatelja upoznaje s pravnim dvojbama u vezi s prijetnjama koje dolaze iz cyber prostora. Jedna od njih tiče se razlike između cyber kriminala i cyber rata. Ako je riječ o krađi identiteta radi pribavljanja nepripadajuće koristi ili radi nanošenja štete časti i ugledu druge osobe, jasno je da bi ti postupci trebali biti podvedeni pod odredbe kaznenog zakonodavstva i da bi se u utvrđivanju krivnje počinitelja trebala primjenjivati sredstva kompjutorske forenzike. Čak je i nezakonito pribavljanje informacija o planovima i namjerama suparničkih vlada, kao i o stanju sustava za nacionalnu sigurnost država, zapravo, djelo cyber špijunaže, a ne ratna operacija usmjerena na uništenje neprijatelja. No, posljedice neovlaštenih upada u informacijske sustave kompanija, vlada i vojske mogu biti presudno važne

za stjecanje strateške prednosti neprijatelja, čime se aktualizira pitanje nacionalne sigurnosti i nužnog aktiviranja svih sigurnosnih komponenti, uključujući i vojnu. Ako bi neprijatelj upotrijebio botnet, mrežu kompjutora koji su angažirani u izvedbi cyber napada bez znanja njihovih vlasnika – a nezamislivo je da potencijalni napadač to ne bi učinio – i ako bi u botnet bili uključeni i kompjutori u vlasništvu američkih građana na američkom tlu, aktualne bi postale ustavne i zakonske odredbe koje onemogućuju upotrebu vojske protiv vlastitih građana. Jednako spornom mogla bi se pokazati i primjena sredstava cyber obrane koja uključuje i cyber napad na neprijateljske instalacije u slučaju da su kompjutori s kojih se izvodi napad locirani u inozemstvu, u zemljama čije se zakonodavstvo razlikuje od američkog i koje bi takve intervencije mogle smatrati ugrožavanjem svojega suvereniteta. Problemi bi mogli biti uvećani eventualnom pogreškom u atribuciji, što bi rezultiralo time da se napadne netko, pojedinac, organizacija ili država, tko zapravo nije počinio napad.

Zbog svega toga, ali i zbog mnogih drugih pravnih i političkih problema, Rosenzweig konstatira da postojeći korpus ratnoga prava ne pokriva na odgovarajući način ono što se zbiva i što bi se moglo zbivati u cyber prostoru. Isto tako upozorava da razlika između obavještajne djelatnosti, cyber špijunaže i rata nije dovoljno dobro određena. Pravne prepreke – koje proizlaze iz činjenice da je pravni sustav izgrađivan stoljećima i da je neprilagođen zahtjevima novog tehnološkog doba, ali i iz činjenice da pravnici nerijetko neopravdano prenaglašavaju pravne nejasnoće – otežavaju postizanje učinkovitosti i pravovremenosti vojnog odgovora u cyber prostoru. Da bi se izbjegle greške, Amerika želi uspostaviti sustav centraliziranog odlučivanja o pitanjima pokretanja cyber rata. Sve to dovodi Rosenzweiga do zaključka da "mi znamo da je cyber rat moguć i da nemamo ideju koja će se pravila, ako ikakva, primijeniti. To nije formula za stabilan međunarodni režim gdje prevladava vladavina zakona. To je, umjesto toga, formula za hobsovski zakon prirode" (58). Takvim zaključkom se, dakako, distancirao od *Međunarodne strategije za cyber prostor* Obamine administracije koja je "ponudila multilateralni pristup međunarodnim cyber pitanjima" (206) i koja, prema Rosenzweigovu mišljenju, nema izgleda "postići visoku prihvaćenost u mnogim državama koje ne cijene ni privatnost ni slobodu" (206). Zanimljivo bi bilo doznati Rosenzweigovu ocjenu Obamine tajne *Predsjedničke političke direktive 20* kojom je ozakonjena unilateralna upotreba DCEO-a (Defensive Cyber Effect Operations) i OCEO-a (Offensive Cyber Effect Operations). S obzirom na njegovo deklarativno prihvaćanje hobsovskog viđenja rata svih protiv sviju u cyber prostoru, pretpostavljam da bi taj dokument, koji je objavio Edward Snowden, dobio Rosenzweigovu visoku ocjenu. Poznato je, s druge strane, da je objavljivanje podataka o načinima primjene tog dokumenta izazvalo napetosti između Amerike i njezinih najbližih saveznika koji su bili podvrgnuti intenzivnom nadzoru unatoč tome što se ni po kakvim kriterijima ne bi mogli uvrstiti u kategoriju država koje ne cijene privatnost, slobodu i vladavinu zakona.

Govoreći o rizicima od otvorenog međudržavnog cyber rata, Rosenzweig je konstatirao da su oni "premda ozbiljni u smislu posljedica, relativno umjereni u smislu

izgleda da se dogode. To je, zapravo, događaj niske vjerojatnosti s mogućim velikim posljedicama" (59). No, primjeri nesimetričnog rata u okviru kojega pobunjeničke skupine, koristeći se mogućnostima koje pruža internet, onemogućuju funkcioniranje informacijskih sustava država i korporacija, sve su češći. Ponekad se s velikom vjerojatnošću može pretpostaviti da su neke hakerske skupine radile za državne naručitelje, primjerice u napadu na informacijske sustave Estonije 2007. godine i Gruzije 2008. godine kad je njihovo djelovanje očito koristilo ruskoj vladi. Utvrđeno je da su mnoge hakerske upade u baze podataka američkih kompanija iz obrambenog sektora izveli kineski hakeri, koji su vrlo vjerojatno radili po narudžbi kineskih vlasti. S visokim stupnjem pouzdanosti može se tvrditi da su izbijanje Arapskog proljeća 2011. godine i izvedba zbivanja u njemu velikim dijelom bili omogućeni intenzivnim korištenjem interneta u svrhu organizacije djelovanja prosvjednika. No, postoje hakerske skupine koje se aktivno suprotstavljaju politici američke vlade. Nakon što je WikiLeaks objavio tajne dokumente niza američkih vladinih tijela i agencija – koristeći se internetom samo za njihovo objavljivanje, ali ne i hakerskim metodama za njihovo pribavljanje – neke su kartične kompanije onemogućile plaćanje donacija za WikiLeaks putem svojih kartica. Hakerska skupina Anonymous odgovorila je hakerskim napadima na informacijske sustave tih kompanija otežavši ili kratkotrajno onemogućivši njihovo funkcioniranje. Tako je došlo do otvorenog rata između nevladinih aktera u cyber prostoru. Primjer je takva rata i hakerski upad Anonymousa u sustav meksičkog narkokartela. Kartel je Anonymouse primorao da odustanu od objavljivanja njihovih tajni izravnom prijetnjom ubojstvom pojedinih ljudi. Zanimljivu činjenicu da su hakeri Anonymousa uspjeli prodrijeti u informacijski sustav narkokartela, a da brojne američke agencije koje raspolažu nesumjerljivo većim obrambenim i napadačkim kapacitetima to nisu učinile (ili barem nisu objavile da su učinile) Rosenzweig nije komentirao.

Probleme koje simboliziraju Anonymousi on tretira u kontekstu prava na transparentnost rada državnih službi s jedne strane te prava na privatnost i anonimnost pojedinaca s druge. Interesu javnosti da dozna na što se troši novac poreznih obveznika suprotstavljaju se interesi nacionalne sigurnosti. S druge strane, mnogi protivnici vladina nadzora nad internetskim prometom pozivaju se na pravo na anonimnost i privatnost čak i onda kada su na nezakonit način došli do određenih informacija. U teško rješivom problemu suprotstavljenih interesa i sustava vrijednosti jasno je samo to da se velik broj aktera, državnih i nedržavnih, u cyber prostoru ponaša po načelu da je prihvatljivo ono što je meni u interesu, a neprihvatljivo ono što je mojem interesu suprotno. S obzirom na mogućnosti i opasnosti za interese država koje internet sa sobom nosi, Rosenzweig predviđa stanovitu vestfalizaciju cyber prostora, nametanje različitih ograničenja uvjetovanih potrebama nacionalne sigurnosti. Istodobno naglašava da trajna samoizolacija neke države nužno dovodi do tehnološkog zaostajanja, a američki sustav vrijednosti i interesi američkog biznisa isključuju mogućnost da Amerika odustane od otvorenog interneta.

Pravo na privatnost jedna je od ključnih sastavnica američkog sustava vrijednosti

zaštićenih zakonom. Internet omogućuje privatnost u smislu sudjelovanja u javnom internetskom prometu bez otkrivanja svog identiteta. Prema Rosenzweigovim shvaćanjima i stajalištima američkih administracija, to je dobro kada je riječ o zaštiti demokratskih aktivista koji se suprotstavljaju nedemokratskim vladama. Istodobno, to je izrazito loše kada je riječ o kriminalnim skupinama koje svojim aktivnostima u cyber prostoru mogu narušiti privatnost pojedinaca te vlasništvo i sigurnost različitih nedržavnih i državnih aktera. No, na pitanje o mogućim načinima povećanja razine cyber sigurnosti ne može se pronaći jednostavan odgovor. Kompanije iz sektora informacijskih i kompjutorskih tehnologija smatraju da je sigurnost privatno dobro svakog njihova korisnika, što znači da svaki vlasnik kompjutora treba osigurati sve potrebne mehanizme zaštite tako da upravo od tih kompanija kupuje odgovarajuću opremu i software. Isto tako ne odgovara im da podaci o uspješnim hakerskim napadima na njihove sustave budu objavljeni jer time gube kredibilnost, ali očekuju od države da ih upozori na mogućnost takvih napada i da otkrije njihove počinitelje. Dakle, sigurnost potrošača njihovo je privatno dobro za koje se sami moraju pobrinuti, a sigurnost privatnih kompanija opće dobro za ostvarivanje kojega se treba pobrinuti država. Svjestan ograničene vrijednosti analogija s primjerima iz drugih domena, Rosenzweig pokazuje da neprestan videonadzor cestovnog prometa ne ugrožava privatnost, ali omogućuje pronalaženje i kažnjavanje počinitelja prometnih prekršaja. Isto bi se tako nadzor podataka o internetskoj komunikaciji bez prava na uvid u njezin sadržaj bez prethodnog sudskog naloga mogao provoditi u cyber prostoru, misli Rosenzweig, premda i takva mogućnost otvara niz pravnih dvojbi. Ako se pak govori o ratu, onda se ne pretpostavlja da će svaka kompanija i svaka kuća ili ulica razvijati svoj sustav uzbunjivanja i protuzračne obrane, nego je to prvenstvena zadaća države. Zbog toga, zaključuje on, "postoji legitimna – doista nužna – uloga vlade u zaštiti interneta od krađe, špijunaže i cyber napada" (226). Budući da sigurnosni propusti u jednom dijelu internetske mreže mogu kao posljedicu imati veću izloženost rizicima, odnosno pad razine sigurnosti drugih dijelova mreže, zadaća je vlade da sigurnost interneta tretira kao opće dobro. Tu je, dakako, i zadaća nacionalne sigurnosti, ali mali su izgledi da vlada donese odgovarajuću zakonsku regulativu s obzirom na to da su zakoni, zbog dugotrajne procedure donošenja i zbog nevjerojatno brzih tehnoloških promjena, nužno zastarjeli u trenutku kad stupe na snagu. Stoga je uloga vlade ponajprije poticanje razmjene informacija i tehnoloških inovacija. I sustav američke cyber sigurnosti neadekvatan je potrebama. Rosenzweig ga je usporedio s Maginotovom linijom, sa sustavom statične obrane koja može reagirati samo na napade usmjerene izravno prema njoj. On zagovara aktivnu obranu koja će omogućiti prijelaz "s uočavanja upada nakon što su se dogodili na sprečavanje upada prije nego se dogode" (225). Dakako, autor je svjestan svih međunarodnopravnih problema povezanih s tim vidom zagovaranja prava na preventivni cyber rat.

U kratkom prikazu ne mogu se spomenuti sve teme koje je Rosenzweig obradio, na razumljiv i pregledan način prikazao i prikladno ih kontekstualizirao. Već sam upozorio da ga nespominjanje pojma *cyber Pearl Harbor* i izbjegavanje senzacionali-

stičkog uznemiravanja javnosti tvrdnjama da je pravi cyber rat već počeo svrstava u red ozbiljnijih autora koji se bave ovom izrazito aktualnom temom. Velik broj primjera i poznavanje tehnoloških mogućnosti interneta, kao i detaljno poznavanje relevantnih zakona, američke institucionalne strukture i neformalnog utjecaja pojedinih institucija ovu knjigu dodatno preporučuju kao vrijedan priručnik za snalaženje na području koje sve više postaje predmetom interesa međunarodne politike. Njegovo eksplicitno opredjeljivanje za Nacionalnu sigurnosnu agenciju kao daleko pouzdanijeg dobavljača opće cyber sigurnosti nego što je to Ministarstvo domovinske sigurnosti u kojem je radio vjerojatno je pokazatelj njegove objektivnosti u sagledavanju stanja i mogućnosti postojećeg sustava američke cyber sigurnosti. No, mislim da je jednako zanimljivo i ponešto od onog što Rosenzweig nije spomenuo ili detaljno obradio.

Naime, samo je usput spomenuo da *Cyber Intelligence Sharing and Protecting Act* (*CISPA*) nije prošao u Senatu, "djelomično zbog zabrinutosti u vezi s privatnošću i građanskim slobodama" (169). Pritom je iz konteksta jasno da on drži da je taj zakonski prijedlog trebao biti prihvaćen jer je na najbolji način osiguravao da privatne kompanije pristanu na suradnju s državnim agencijama nadležnim za cyber sigurnost, a da se ta suradnja odvija diskretno i bez uvida javnosti. Zaštita interesa biznisa je, dakako, trajna briga američke vlade i vrlo čest razlog za različite političke i vojne intervencije, ali bi interes vlade trebala biti i zaštita interesa pojedinaca te pravo javnosti na informacije od općeg interesa. Američka je javnost dugo bila zaokupljena i duboko podijeljena u vezi s tim zakonskim prijedlogom, a Rosenzweig mu je, po mom mišljenju, posvetio premalo prostora i intelektualnog napora.

Možda je od svega najzanimljivije nespominjanje sudbine jednog drugog zakonskog prijedloga koji je svojedobno mobilizirao svjetsku javnost. Riječ je o *Anti-Counterfeiting Trade Agreement* (*ACTA*), prijedlogu međunarodnog trgovinskog sporazuma koji je sponzorirala američka vlada. Dokument je predviđao uskraćivanje mogućnosti pristupa internetu bez sudske presude osobama za koje bi se utvrdilo da su putem interneta neovlašteno kopirale i distribuirale materijale koji podliježu zaštiti autorskih prava. Činjenica da Rosenzweig uopće ne spominje taj dokument tim je čudnija što su odlučujuću ulogu u kampanji protiv njegova usvajanja u nacionalnim parlamentima država diljem svijeta odigrali upravo Anonymousi, kojima on posvećuje dosta prostora. Budući da se Rosenzweig koristio analogijama da bi objasnio neke probleme u vezi s funkcioniranjem interneta, i ja ću se osloniti na analogiju. *ACTA* je, slijedeći interese američkih kompanija koje raspolažu neprocjenjivo vrijednim intelektualnim vlasništvom i autorskim pravima, trebala omogućiti da se naplaćuje prodaja tog vlasništva i onda kada prodaje zapravo nema. Ono čemu je težio taj zakonski akt moglo bi se opisati ovako: kompanija koja je proizvela i prodala karte za poker određenom građaninu očekuje da će svaki njegov partner toj kompaniji platiti određeni iznos svaki put kada bude igrao tim kartama jer taj partner nije kupio karte pa, prema tome, bez plaćanja ne bi imao pravo koristiti ih u igri. Slično je i s naplatom autorskih prava na glazbu koja bi mogla biti snimljena na praznom nosaču zvuka

kupljenom u trgovini. Koliko god to zvuči nevjerojatno, upravo takvo rješenje propisuje jedan hrvatski zakon. Taj je zakon uspio u onome u čemu *ACTA* nije uspjela: interes i korist jedne interesne skupine nametnuti kao trajnu obvezu i teret svih. Mislim da takvi primjeri navode na to da se u kontekstu rasprava o internetu vodi računa i o potrebi redefiniranja pojma intelektualnih i autorskih prava te o načinima njihove zaštite i ostvarivanja, a ne ponajprije o sve restriktivnijem definiranju građanskih prava i sloboda. Premda je njegova knjiga zanimljiva, informativna i korisna – pa je stoga preporučujem svima koje zanima problematika cyber ratovanja – ona o tim pitanjima govori jednostrano i površno. A neodgovarajuća zakonska regulativa upravo tih pitanja povod je za barem dio zbivanja koja je Rosenzweig opisao u svojoj knjizi o cyber ratovanju.

Božo Kovačević
Visoka škola međunarodnih odnosa i diplomacije Dag Hammarskjöld, Zagreb

Prikaz

Radule Knežević
Politička teorija anarhizma

Grafo Bale, Podgorica, 2013, 201 str.

Politički i ekonomski nestabilna vremena oduvijek su bila uzrokom ljudskog preispitivanja o oblicima upravljanja unutar društvene zajednice. Vremena jačanja monopola moći, propasti društvenih i moralnih vertikala te povećanog državnog intervencionizma u domeni ekonomije dovode u pitanje opstojnost postojeće društvene i ekonomske paradigme. Suprotstavljanje ugroženosti materijalne slobode pojedinca, sprečavanje kršenja ljudskih prava, dokidanje ili ograničavanje autoriteta te reguliranje odnosa moći u društvu bez prisutnosti državnog aparata temeljne su odrednice političke teorije anarhizma koje djeluju kao dio naznaka rješenja gore spomenutih problema.

Knjiga dr. sc. Radula Kneževića velik je i temeljit doprinos proučavanju anarhističke teorije od njena nastanka pa sve do vremena u kojem živimo, vremena postmoderne i postanarhizma. Kako je i sam autor naglasio u uvodnoj riječi, njegovo djelo ne teži postati priručnikom povijesti anarhizma niti želi braniti anarhističke argumente, nego ponajprije kritički razmotriti političku teoriju koja se nalazi u disbalansu između, kako kaže autor, neteoretizirane akcije i dogmatizma te aprioristićkog negiranja i etiketiranja. Knjiga nas vodi dugim putem od utemeljenja anarhističke teorije u djelima Pierrea Josepha Proudhona pa sve do današnjih dana kada anarhizam traži neke nove puteve kao odgovor i kritika na aktualne društvene, političke i ekonomske probleme. Anarhizam je oduvijek kritika, isprva kritika marksizma i socijalizma, a potom i suvremenog društva. Ovdje je bitno naglasiti da se pojmovi anarhija i anarhizam razlikuju. Anarhija je stanje nereda i kaosa, dok je anarhizam politička teorija.

Smatra se da se anarhistička misao profilirala u 18. stoljeću s nastankom moderne države i kapitalizma te povećanjem socijalne nejednakosti u društvu. No, anarhizam je prisutan u političkom mišljenju od njegovih početaka. Njegovo je korijenje u