Asimetrična krizna komunikacija kao sigurnosno ograničenje u kibernetičkoj obrani uz djelomično dijeljenje informacija

Izvorni znanstveni rad, DOI 10.22522/cmr202601116, primljeno 31. ožujka 2026.
Rad je licenciran pod CC BY-NC-ND 4.0 / This work is licensed under CC BY-NC-ND 4.0
UDK: 007:005.7

Zlatan Morić, v. pred.
Sveučilište Algebra Bernays (Zagreb, Hrvatska)
eMail: zlatan.moric@algebra.hr

Sažetak

Kibernetička obrana u nacionalno-sigurnosnom kontekstu odvija se u uvjetima trajne informacijske asimetrije, pravnih ograničenja i klasifikacijskih režima koji onemogućuju potpuno i simetrično dijeljenje informacija među akterima. Unatoč tome, postojeći modeli krizne komunikacije često polaze od normativnih pretpostavki transparentnosti, brzine i informacijske simetrije. Ovaj rad uvodi koncept asimetrične krizne komunikacije kao analitički okvir za razumijevanje komunikacijskih procesa u kibernetičkoj obrani uz djelomično dijeljenje informacija. Rad se temelji na konceptualno-analitičkom pristupu i scenarijskoj analizi realistične kibernetičke krize koja uključuje heterogene aktere s različitim mandatima i režimima zaštite podataka. Analiza pokazuje da informacijska asimetrija, fragmentacija značenja i koordinacijska latencija ne predstavljaju nužno komunikacijske neuspjehe, već legitimne sigurnosne kompromise. Time se krizna komunikacija pozicionira kao aktivni mehanizam upravljanja sigurnosnim rizikom, a ne samo kao sredstvo prijenosa informacija, čime se doprinosi realističnijem razumijevanju kibernetičke obrane.

Ključne riječi: asimetrična krizna komunikacija, kibernetička obrana, nacionalna sigurnost, krizno odlučivanje

1. Uvod

Kibernetička obrana u suvremenim sigurnosnim okruženjima sve se češće odvija u uvjetima trajne krize, pri čemu granice između izvanrednih i redovitih operativnih stanja postaju nejasne. Za razliku od klasičnih kriznih situacija koje su vremenski ograničene i jasno definirane, kibernetičke prijetnje karakterizira kontinuirana prisutnost, visoka razina neizvjesnosti te potreba za donošenjem odluka uz ograničene i fragmentirane informacije. U takvom kontekstu koordinacija između različitih dionika kibernetičke obrane – uključujući državna tijela, oružane snage, privatni sektor i akademsku zajednicu – postaje ključni preduvjet zaštite nacionalne sigurnosti.

U literaturi o kriznoj komunikaciji komunikacija se tradicionalno promatra kroz prizmu transparentnosti, pravodobnog dijeljenja informacija i uspostave zajedničkog razumijevanja situacije. Međutim, takve pretpostavke uvelike proizlaze iz konteksta organizacijskog upravljanja i reputacijskih kriza, gdje je potpuna razmjena informacija često moguća i poželjna. U kibernetičkoj obrani, osobito kada su u pitanju informacije od značaja za nacionalnu sigurnost, takav pristup suočava se s ozbiljnim ograničenjima. Informacije relevantne za razumijevanje prijetnje i donošenje odluka često su klasificirane, pravno zaštićene ili institucionalno ograničene, što onemogućuje njihovo potpuno i simetrično dijeljenje među uključenim akterima.

Komunikacija se stoga u kibernetičkoj obrani odvija u uvjetima trajne informacijske asimetrije i djelomičnog dijeljenja podataka. Takva ograničenja ne proizlaze nužno iz nedostatka suradnje, već iz potrebe zaštite osjetljivih izvora, metoda i operativnih sposobnosti. Istodobno, djelomično dijeljenje informacija otežava razvoj zajedničke predodžbe situacije, usklađivanje prioriteta i pravodobno donošenje odluka. Komunikacija time prestaje biti neutralni prijenos informacija te postaje strukturni čimbenik koji oblikuje koordinaciju i učinkovitost kibernetičke obrane.

Unatoč rastućem interesu za kriznu komunikaciju, postojeća literatura rijetko analizira komunikacijske procese u nacionalno-sigurnosnom kontekstu, osobito u situacijama u kojima je informacijska asimetrija institucionalno uvjetovana. U sigurnosnim studijama komunikacija se često tretira kao tehničko ili organizacijsko pitanje, dok komunikacijska istraživanja rijetko uzimaju u obzir operativna i pravna ograničenja sigurnosnih sustava. Posljedično, nedostaje analitičkih okvira koji bi omogućili razumijevanje komunikacije u uvjetima djelomičnog dijeljenja informacija.

Polazeći od istraživačkog pitanja na koji način djelomično dijeljenje informacija i sigurnosna ograničenja oblikuju kriznu komunikaciju u kibernetičkoj obrani, rad uvodi koncept asimetrične krizne komunikacije. Cilj je konceptualizirati komunikaciju u takvim uvjetima kao strukturno stanje, a ne komunikacijski neuspjeh, te pokazati kako informacijska asimetrija, fragmentacija značenja i koordinacijska latencija utječu na donošenje odluka u kriznim situacijama. Time se predlaže teorijski pomak od normativnih modela krizne komunikacije prema sigurnosno utemeljenom analitičkom okviru.

2. Krizna komunikacija u kontekstu kibernetičke sigurnosti

Krizna komunikacija predstavlja jedno od središnjih područja istraživanja u komunikacijskim znanostima, organizacijskim studijama i istraživanjima upravljanja rizicima. Klasični radovi definiraju kriznu komunikaciju kao proces razmjene informacija i značenja tijekom izvanrednih događaja s ciljem ograničavanja štete, obnove povjerenja i omogućavanja nastavka djelovanja organizacija i institucija (Coombs, 2021; Heath & O'Hair, 2010; Sellnow & Seeger, 2020). U tim pristupima komunikacija se promatra kao ključni upravljački instrument, a uspješan krizni odgovor povezuje se s pravodobnošću, transparentnošću i konzistentnošću poruka. U posljednjem desetljeću, s porastom kibernetičkih prijetnji i incidenata, krizna komunikacija sve se češće razmatra i u kontekstu kibernetičke sigurnosti (Mott, Nurse, & Baker-Beall, 2023; Tinonetsana, Rawjee, & Govender, 2025). Međutim, prijenos dominantnih komunikacijskih modela u ovu domenu pokazao se problematičnim, budući da kibernetičke krize imaju obilježja koja ih bitno razlikuju od organizacijskih ili reputacijskih kriza. Kibernetički incidenti često su dugotrajni, tehnički složeni, transnacionalni i odvijaju se u uvjetima visoke neizvjesnosti, pri čemu su informacije fragmentirane i dostupne različitim akterima u nejednakoj mjeri (Dupont, Shearing, Bernier, & Leukfeldt, 2023; Ruohonen, Rindell, & Busetti, 2025).

2.1. Dominantni pristupi kriznoj komunikaciji

Situacijska teorija krizne komunikacije (SCCT) i srodni organizacijski modeli polaze od pretpostavke da se krizne situacije mogu klasificirati prema razini odgovornosti te da komunikacijske strategije treba prilagoditi percepciji krize i očekivanjima dionika (Coombs, 2021). U tim okvirima transparentnost i otvorenost komunikacije smatraju se ključnim preduvjetima za učinkovito upravljanje krizom (Sellnow & Seeger, 2020). Brojna empirijska istraživanja potvrđuju da nedostatak informacija, zakašnjela komunikacija ili kontradiktorne poruke mogu dodatno eskalirati krizu i narušiti povjerenje (Heath & O'Hair, 2010).

Primjena ovih modela na kibernetičke incidente najčešće se odnosi na povrede podataka, ransomware[1] napade ili prekide digitalnih usluga u organizacijskom kontekstu (Du, Xu, & Vasarhelyi, 2024; Tinonetsana et al., 2025). Ti radovi primarno analiziraju komunikaciju prema korisnicima, javnosti i regulatorima, s naglaskom na objavu informacija, pravnu usklađenost i reputacijske učinke. Međutim, rijetko obuhvaćaju komunikacijske procese unutar sigurnosnog sustava, gdje su odluke izravno povezane s nacionalnom sigurnošću.

Ključno ograničenje ovih pristupa jest implicitna pretpostavka informacijske simetrije ili barem mogućnosti njezina postupnog postizanja. U kibernetičkoj obrani takva pretpostavka često nije ostvariva zbog pravnih, klasifikacijskih i sigurnosnih ograničenja koja definiraju granice razmjene informacija (Ruohonen et al., 2025; Serini, 2024).

1 Ransomware predstavlja vrstu napada koji od žrtve zahtijeva otkupninu za povrat podataka ili njihovo neobjavljivanje.

2.2. Krizna komunikacija i kibernetička sigurnost

Literatura kibernetičke sigurnosti sve više prepoznaje da učinkovito upravljanje incidentima i krizama zahtijeva koordinaciju između heterogenih aktera, uključujući nacionalne CSIRT-ove, operatore kritične infrastrukture, regulatorna tijela i sigurnosno-obavještajne institucije (Anderson et al., 2021; Wu, 2023). U tom kontekstu komunikacija se često promatra kao preduvjet za dijeljenje obavještajnih podataka o kibernetičkim prijetnjama (CTI) i uspostavu kolektivne situacijske svjesnosti (Abraham, Bélanger, & Daultrey, 2025; Fang, Tang, & Guo, 2025).

Empirijska istraživanja i sustavni pregledi ukazuju da dijeljenje CTI-ja može povećati otpornost organizacija i smanjiti vrijeme reakcije na incidente (Alkalabi, Simpson, & Morarji, 2021; Rantos et al., 2020). Međutim, brojni autori ističu da praksa razmjene informacija ostaje ograničena pravnim nejasnoćama, zabrinutostima oko odgovornosti, troškovima koordinacije i nedostatkom povjerenja među akterima i sektorima (Abraham et al., 2025; Chang & Huang, 2023; Reittinger, Grill, & Pernul, 2026). Ovi nalazi upućuju na to da komunikacija u kibernetičkoj sigurnosti nije isključivo tehničko pitanje interoperabilnosti, već složen institucionalni i upravljački problem.

Istodobno, istraživanja incidentnog odgovora naglašavaju da se donošenje odluka u kibernetičkim krizama odvija pod snažnim vremenskim pritiskom i uz ograničenu dostupnost pouzdanih informacija (Groenendaal, Barjas, & Helsloot, 2021; Hayes, Bearman, Butler, & Owen, 2021; Lakshmi, Naseer, Maynard, & Ahmad, 2021). Koncepti interpretacije i situacijske svjesnosti koriste se za opisivanje procesa kroz koje akteri interpretiraju parcijalne signale i donose odluke u uvjetima neizvjesnosti (Dupont et al., 2023; Patterson, Nurse, & Franqueira, 2023). Međutim, većina tih radova implicitno pretpostavlja da je cilj postići što potpuniju predodžbu situacije (situational awareness), dok se manje pažnje posvećuje analizi uvjeta u kojima je potpuna informacijska predodžba institucionalno nedostižna.

2.3. Ograničenja dijeljenja informacija u sigurnosnom kontekstu

U području nacionalne sigurnosti ograničenja dijeljenja informacija predstavljaju strukturno obilježje sustava. Informacije relevantne za kibernetičku obranu često su klasificirane, povezane s obavještajnim izvorima ili osjetljivim tehničkim sposobnostima, što ograničava njihovu dostupnost izvan uskog kruga ovlaštenih aktera (Ruohonen et al., 2025; Serini, 2024). Dodatna ograničenja proizlaze iz pravnih okvira, uključujući zaštitu osobnih podataka i regulatorne obveze, koje dodatno kompliciraju razmjenu informacija tijekom kibernetičkih kriza (Cremer et al., 2022). Sigurnosna literatura upozorava da takva ograničenja, iako nužna za zaštitu nacionalnih interesa, mogu imati izravne posljedice na koordinaciju i donošenje odluka (ENISA, 2024; Hodgson, Clark-Ginsberg, Haldeman, Lauland, & Mitch, 2022). U europskom kontekstu razvoj mehanizama za kibernetičko krizno upravljanje, poput EU-CyCLONe, ilustrira napetost između potrebe za koordiniranom razmjenom informacija i obveze zaštite osjetljivih podataka (EU Parlament, 2022; General Secretariat of the Council, 2025).

U operativnoj provedbi odgovora na incidente standardizirani okviri služe usklađivanju aktivnosti i očekivanja različitih aktera, ali ne uklanjaju komunikacijska ograničenja koja proizlaze iz mandata i klasifikacijskih režima. Promjene u praksama odgovora na incidente stoga zahtijevaju jasno definirane pragove eskalacije, odgovornosti i komunikacijske procedure kako bi se odluke mogle donositi dosljedno i u uvjetima neizvjesnosti. Sličan pristup naglašen je i u preporukama za prilagodbu praksi odgovora na incidente prema NIST CSF 2.0, koje ističu važnost strukturiranih "playbookova" i standardiziranih indikatora rizika koji se mogu dijeliti bez otkrivanja osjetljivih informacija (Morić, Dakić, Kapulica, & Redžepagić, 2025).

Djelomično dijeljenje informacija ne znači samo kvantitativno smanjenje dostupnih podataka, već i kvalitativnu fragmentaciju značenja. Različiti akteri raspolažu različitim dijelovima situacijske slike, pri čemu nedostatak konteksta otežava uspostavu zajedničkog razumijevanja (Dupont et al., 2023; Lakshmi et al., 2021). Ipak, većina istraživanja ova ograničenja tumači kao operativne izazove koje je moguće ublažiti poboljšanjem procesa ili tehnologije, a ne kao trajno sigurnosno obilježje sustava.

Noviji konceptualni pristupi dodatno proširuju klasične modele kibernetičkih incidenata naglašavanjem faza koje prethode samom napadu. U tom kontekstu, uvođenje tzv. "pre-chain" faze unutar Cyber Kill Chain[2] modela ukazuje na važnost pripreme, kontekstualnog razumijevanja i organizacijskih preduvjeta koji oblikuju kasniji tijek incidenta. Takvi pristupi ističu da se ključne odluke, ograničenja i odnosi povjerenja često uspostavljaju prije nego što incident postane tehnički vidljiv, čime se komunikacijski i institucionalni obrasci formiraju unaprijed (Kopal et al., 2025). Ova perspektiva pruža relevantan temelj za analizu krizne komunikacije kao strukturnog procesa koji započinje prije same eskalacije incidenta.

2.4. Istraživački jaz

Sinteza postojeće literature ukazuje na nekoliko ključnih praznina. Prvo, krizna komunikacija u kibernetičkoj sigurnosti dominantno se analizira iz organizacijske, reputacijske ili regulatorne perspektive, dok su komunikacijski procesi unutar nacionalno-sigurnosnog sustava nedovoljno istraženi (Mott et al., 2023; Tinonetsana et al., 2025). Drugo, iako sigurnosna literatura prepoznaje postojanje ograničenja dijeljenja informacija, komunikacijske posljedice tih ograničenja rijetko se sustavno analiziraju (Ruohonen et al., 2025; Serini, 2024). Treće, velik dio postojećih radova implicitno polazi od ideala informacijske simetrije, čak i kada priznaje da je ona u praksi teško ostvariva. Takav pristup ograničava razumijevanje stvarnih uvjeta u kojima se odvija kibernetička obrana, gdje je djelomično dijeljenje informacija trajno stanje, a ne privremena anomalija (ENISA, 2024; Hodgson et al., 2022). Posljedično, nedostaju analitički okviri koji bi omogućili proučavanje komunikacije kao sigurnosnog ograničenja koje izravno utječe na koordinaciju, prioritizaciju i donošenje odluka tijekom kibernetičkih kriza.

2 Cyber Kill Chain je model koji opisuje faze kibernetičkog napada, od početnog izviđanja i pripreme napada do iskorištavanja ranjivosti i ostvarivanja cilja napada.

Ovaj rad adresira navedeni istraživački jaz uvođenjem koncepta asimetrične krizne komunikacije, kojim se krizna komunikacija analizira kao strukturni sigurnosni čimbenik u kibernetičkoj obrani, a ne kao pomoćna organizacijska funkcija.

3. Djelomično dijeljenje informacija kao sigurnosni zahtjev

U kibernetičkoj obrani djelomično dijeljenje informacija ne može se razumjeti kao komunikacijski nedostatak koji proizlazi iz loših procesa, nedostatka kapaciteta ili slabog međuinstitucionalnog povjerenja. Naprotiv, riječ je o normativno i operativno utemeljenom sigurnosnom zahtjevu koji proizlazi iz same prirode nacionalno-sigurnosnih informacija, pravnog okvira njihova korištenja te odgovornosti institucija koje njima raspolažu. U tom smislu, djelomično dijeljenje informacija nije anomalija kriznog stanja, već trajna strukturna značajka kibernetičke obrane, koja postaje osobito izražena tijekom kriznih situacija. Za razliku od organizacijskih ili reputacijskih kriza, u kojima se ograničavanje informacija često promatra kao privremena i neželjena mjera, u području nacionalne sigurnosti ograničenja razmjene informacija predstavljaju instrument zaštite sustava. Potpuna transparentnost u takvom kontekstu ne samo da je neizvediva, već bi u mnogim slučajevima predstavljala izravni sigurnosni rizik, jer bi mogla dovesti do kompromitacije obavještajnih izvora, metoda detekcije, operativnih sposobnosti ili međunarodnih obveza države (Ruohonen et al., 2025; Serini, 2024).

3.1. Sigurnosno osjetljive informacije kao posebna kategorija

Kako bi se razumjela nužnost djelomičnog dijeljenja informacija, potrebno je razlikovati sigurnosno osjetljive informacije od ostalih podataka koji se pojavljuju u kibernetičkim incidentima. Takve informacije ne obuhvaćaju samo formalno klasificirane dokumente, već i tehničke, operativne i analitičke podatke čije bi nekontrolirano dijeljenje moglo povećati sigurnosni rizik. U kibernetičkoj obrani to uključuje, primjerice, podatke o neotkrivenim ranjivostima, naprednim indikatorima kompromitacije, forenzičke nalaze o taktikama napadača, obavještajne procjene o namjeri protivnika te informacije o vlastitim sposobnostima detekcije i odgovora.

Dijeljenje takvih podataka podliježe različitim ograničenjima, uključujući režime klasifikacije, nacionalna zakonodavstva, pravila zaštite osobnih podataka i međunarodne obveze (Cremer et al., 2022). Ta ograničenja nisu proizvoljna, već su ugrađena u institucionalni dizajn sigurnosnog sustava. Različiti akteri – poput nacionalnih CSIRT-ova, sigurnosno-obavještajnih agencija, regulatornih tijela i operatora kritične infrastrukture – djeluju unutar različitih mandata, što određuje kojim informacijama mogu pristupiti i koje informacije smiju dijeliti. Posljedično, potpuna situacijska predodžba nije dostupna nijednom pojedinačnom akteru, niti je takva razina dijeljenja informacija u praksi dopuštena.

3.2. Djelomično dijeljenje informacija i fragmentacija značenja

Djelomično dijeljenje informacija u kibernetičkoj obrani ima posljedice koje nadilaze smanjenje količine dostupnih podataka. Njegov ključni učinak jest fragmentacija značenja među akterima uključenima u krizni odgovor. Ona nastaje kada različiti akteri raspolažu različitim informacijskim fragmentima te kada isti informacijski signali dobivaju različita značenja ovisno o kontekstu, mandatu i dostupnim dopunskim informacijama (Dupont et al., 2023; Lakshmi et al., 2021). U takvim uvjetima komunikacija prestaje biti neutralni prijenos činjenica i postaje proces selektivne konstrukcije značenja unutar sigurnosnih ograničenja. Umjesto potpune informacijske slike, zajedničko razumijevanje situacije formira se kroz djelomično preklapajuće interpretacije koje mogu, ali i ne moraju, biti dovoljno usklađene za donošenje odluka.

Istraživanja odgovora na kibernetičke incidente često naglašavaju važnost dijeljenja kontekstualnih informacija radi smanjenja neizvjesnosti i koordinacije djelovanja (Groenendaal et al., 2021; Patterson et al., 2023). Međutim, u nacionalno-sigurnosnom kontekstu takvo dijeljenje često nije moguće. Akteri su stoga prisiljeni donositi odluke na temelju parcijalnih i nesinkroniziranih interpretacija situacije, što dodatno povećava kompleksnost kriznog upravljanja.

Kako bi se razlikovale posljedice ograničenog dijeljenja podataka od fragmentacije značenja, Tablica 1 prikazuje analitičko razgraničenje između vrsta sigurnosno relevantnih informacija, ograničenja njihova dijeljenja i komunikacijskih učinaka koji iz toga proizlaze. Prikaz pokazuje da djelomično dijeljenje informacija ne rezultira samo smanjenom dostupnošću podataka, nego i strukturnim ograničenjima u uspostavi zajedničkog razumijevanja situacije među akterima kibernetičke obrane.

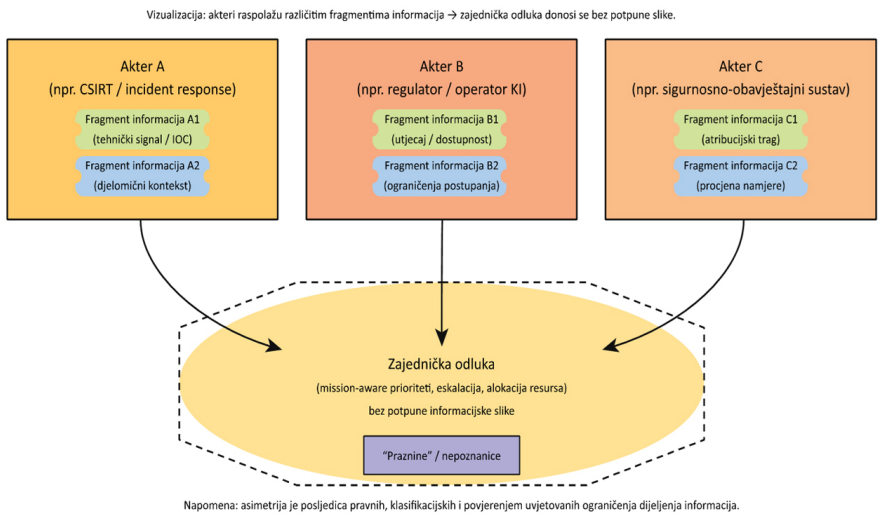
TABLICA 1. Razlikovanje informacija i značenja u kibernetičkoj obrani (izrada autora)

Vrsta informacije	Sigurnosno ograničenje	Posljedica za dijeljenje	Posljedica za zajedničko razumijevanje
Tehnički detalji ranjivosti (npr. zero-day)	Zaštita operativnih sposobnosti i sprječavanje eksploatacije	Dijeljenje ograničeno na mali broj ovlaštenih aktera	Ostali akteri razumiju postojanje prijetnje, ali ne i njezin tehnički uzrok
Indikatori kompromitacije (IOC)	Rizik otkrivanja detekcijskih metoda	Dijeljenje selektivno i vremenski ograničeno	Djelomična sposobnost povezivanja incidenata u širu predodžbu
Forenzički nalazi	Zaštita istrage i dokaznog materijala	Dijeljenje apstrahiranih ili agregiranih rezultata	Ograničeno razumijevanje tijeka i razmjera napada

Obavještajne procjene o napadaču	Zaštita izvora i metoda	Nedijeljenje ili visoka razina apstrakcije	Različite interpretacije namjere i sposobnosti napadača
Informacije o vlastitim obrambenim kapacitetima	Sprječavanje prilagodbe protivnika	Nedostupnost izvan zatvorenog kruga institucija	Nemogućnost pune procjene ukupne razine rizika
Pravne i regulatorne procjene	Povjerljivost postupaka i pravna odgovornost	Dijeljenje u formalnim okvirima i s odgodom	Asinkrono razumijevanje dopuštenih opcija djelovanja

Prikazane razlike potvrđuju da se komunikacijski izazovi u kibernetičkoj obrani ne mogu svesti na dostupnost informacija, već proizlaze iz strukturne nemogućnosti potpunog usklađivanja značenja među akterima koji djeluju unutar različitih sigurnosnih i institucionalnih ograničenja. Iako Tablica 1 analitički razgraničuje vrste informacija i njihove komunikacijske učinke, u praksi se problem očituje kroz paralelnu izgradnju djelomičnih situacijskih predodžbi u različitim institucijama i sektorima. Slika 1 prikazuje obrazac u kojem akteri raspolažu različitim fragmentima informacija, dok se zajednička odluka donosi bez potpune informacijske slike, što povećava rizik divergentnih interpretacija i prioriteta.

SLIKA 1. Asimetrija informacija i fragmentacija značenja



Izvor: autor

Ovakva fragmentacija ne predstavlja iznimku, već očekivanu posljedicu sigurnosnih ograničenja dijeljenja informacija, zbog čega se koncept asimetrične krizne komunikacije u nastavku rada uvodi kao prikladniji okvir za analizu odlučivanja u kibernetičkoj obrani.

3.3. Asimetrična krizna komunikacija: konceptualna razrada

Na temelju prethodne analize, rad definira asimetričnu kriznu komunikaciju kao stanje u kojem je koordinirano donošenje sigurnosno relevantnih odluka nužno ostvariti u uvjetima trajne informacijske asimetrije uzrokovane pravnim, klasifikacijskim i institucionalnim ograničenjima dijeljenja informacija. Ne radi se o privremenom poremećaju komunikacijskih procesa, već o strukturnom obilježju sigurnosnog sustava. Za razliku od normativnih modela krizne komunikacije koji polaze od pretpostavke da asimetriju informacija treba smanjiti ili ukloniti, u kibernetičkoj obrani asimetrija predstavlja polazišnu točku. Ključno pitanje stoga nije kako postići potpunu informacijsku simetriju, već kako omogućiti donošenje odluka u njezinoj trajnoj odsutnosti. Takav pomak zahtijeva i redefiniranje kriterija uspješne komunikacije u sigurnosnom kontekstu.

Kako bi se koncept asimetrične krizne komunikacije jasnije pozicionirao u odnosu na dominantne teorijske pristupe, Tablica 2 prikazuje usporedbu ključnih analitičkih dimenzija normativnih komunikacijskih modela i pristupa koji polazi od strukturne informacijske asimetrije u kibernetičkoj obrani.

TABLICA 2. Normativna vs. asimetrična krizna komunikacija

Dimenzija	**Normativni komunikacijski modeli**	**Asimetrična krizna komunikacija**
Temeljna pretpostavka	Informacijska simetrija je poželjan i ostvariv cilj	Informacijska asimetrija je trajno stanje
Uloga komunikacije	Smanjenje neizvjesnosti kroz dijeljenje informacija	Upravljanje sigurnosnim ograničenjima
Odnos prema transparentnosti	Transparentnost kao ključ uspjeha	Selektivna i kontrolirana transparentnost
Uloga povjerenja	Povjerenje omogućuje šire dijeljenje informacija	Povjerenje određuje granice dijeljenja
Kriterij uspješnosti	Potpunost i brzina razmjene informacija	Donošenje odluka unatoč ograničenjima
Izvor komunikacijskih problema	Nedostatak informacija ili loši procesi	Strukturna sigurnosna ograničenja
Uloga pravnog okvira	Sekundarni ili implicitni čimbenik	Primarni čimbenik komunikacije

Dimenzija	Normativni komunikacijski modeli	Asimetrična krizna komunikacija
Odnos prema nacionalnoj sigurnosti	Često implicitno ili marginalno	Eksplicitno središnji
Analitički fokus	Organizacija i reputacija	Koordinacija i odlučivanje

U asimetričnoj kriznoj komunikaciji uspjeh se ne mjeri količinom razmijenjenih informacija, već sposobnošću sustava da, unatoč ograničenjima, omogući dovoljno zajedničkog razumijevanja za koordinirano djelovanje. Time se komunikacija pozicionira kao sigurnosno ograničenje koje oblikuje dinamiku kriznog odgovora, a ne kao varijabla koju je moguće optimizirati neovisno o širem institucionalnom kontekstu.

3.4. Sigurnosne posljedice i racionalnost kompromisa

Djelomično dijeljenje informacija i asimetrična krizna komunikacija imaju izravne sigurnosne posljedice koje se manifestiraju kroz kašnjenja u koordinaciji, nesklad u prioritizaciji i odgode u donošenju odluka (Hodgson et al., 2022; Mott et al., 2023). Važno je, međutim, razlikovati posljedice od neuspjeha. U mnogim slučajevima, ti učinci ne predstavljaju znak disfunkcionalnosti sustava, već racionalne sigurnosne kompromise donesene radi zaštite osjetljivih informacija. Drugim riječima, sporiji ili fragmentiraniji odgovor ne mora nužno biti rezultat loše komunikacije, već posljedica svjesnog ograničavanja informacija kako bi se spriječila eskalacija rizika. Takvi kompromisi često ostaju nevidljivi u analizama koje komunikaciju promatraju isključivo kroz prizmu učinkovitosti ili brzine, bez uzimanja u obzir sigurnosnih ograničenja unutar kojih se odluke donose.

3.5. Implikacije za analitičke okvire i dizajn sustava

Prepoznavanje djelomičnog dijeljenja informacija kao sigurnosnog zahtjeva zahtijeva promjenu analitičkih okvira koji se koriste za proučavanje krizne komunikacije u kibernetičkoj sigurnosti. Evaluacija komunikacijskih procesa ne može se temeljiti na kriterijima transparentnosti ili potpunosti, već na sposobnosti sustava da podrži donošenje odluka u uvjetima informacijske asimetrije. To podrazumijeva razvoj komunikacijskih mehanizama koji omogućuju prijenos apstrahiranog, ali odlučivanju relevantnog značenja, bez otkrivanja osjetljivih detalja. Takvi mehanizmi moraju biti usklađeni s pravnim i institucionalnim ograničenjima te integrirani u šire okvire kibernetičke obrane. Upravo ova perspektiva omogućuje konceptualizaciju komunikacije kao strukturnog sigurnosnog čimbenika, čime se postavlja temelj za empirijsku analizu u nastavku rada.

4. Metodološki pristup i istraživački kontekst

Rad koristi kvalitativni, konceptualno-analitički pristup s ciljem razumijevanja komunikacijskih ograničenja u kibernetičkoj obrani, osobito u uvjetima djelomičnog dijeljenja informacija i asimetrične krizne komunikacije. Odabrani metodološki okvir proizlazi iz prirode istraživačkog problema, koji se ne odnosi na mjerenje učestalosti komunikacije, već na analizu strukturnih ograničenja i njihovih sigurnosnih posljedica. Budući da se komunikacijski procesi u nacionalno-sigurnosnom kontekstu odvijaju unutar strogo definiranih pravnih i institucionalnih okvira, velik dio relevantnih informacija nije javno dostupan niti pogodan za kvantitativnu analizu. Kvalitativni pristup stoga omogućuje identifikaciju obrazaca i kompromisa koji oblikuju donošenje odluka u kibernetičkim krizama.

Krizni scenarij razvijen je kao analitička sinteza obrazaca identificiranih u znanstvenoj i regulatornoj literaturi, javno dostupnim izvješćima te stručnim raspravama održanim tijekom međunarodnog Simpozija kibernetička obrana u kolovozu 2025. godine. Na simpoziju su sudjelovali predstavnici akademske zajednice, industrije i javnog sektora koji su raspravljali o tipičnim izazovima komunikacije i koordinacije u kibernetičkim krizama pod sigurnosnim i pravnim ograničenjima. Scenarij ne predstavlja rekonstrukciju konkretnog incidenta, već konceptualno modeliranje ponavljajućih komunikacijskih obrazaca u uvjetima djelomičnog dijeljenja informacija, čime se osigurava analitička relevantnost bez izlaganja osjetljivih ili klasificiranih podataka.

4.1. Istraživački dizajn

Istraživanje je strukturirano kao analitička studija utemeljena na konceptualnom modeliranju i scenarijskoj analizi, pri čemu se empirijski uvidi koriste za ilustraciju i provjeru teorijskih tvrdnji razvijenih u prethodnim poglavljima. Ovakav dizajn omogućuje povezivanje teorijskih koncepata krizne komunikacije s praktičnim izazovima kibernetičke obrane, bez potrebe za izlaganjem osjetljivih operativnih podataka.

Analiza se oslanja na tri komplementarna izvora podataka:

- sekundarna analiza znanstvene i regulatorne literature, korištena za identifikaciju dominantnih obrazaca i institucionalnih ograničenja
- analitička interpretacija realističnog kibernetičkog kriznog scenarija, temeljena na javno dostupnim opisima incidenata, vježbi i institucionalnih praksi sa simpozija
- strukturirana konceptualna analiza komunikacijskih tokova, usmjerena na identifikaciju točaka informacijske asimetrije i fragmentacije značenja

Takva kombinacija omogućuje analizu komunikacijskih procesa bez potrebe za pristupom klasificiranim podacima, uz zadržavanje visoke razine analitičke relevantnosti za sigurnosni kontekst.

4.2. Istraživački kontekst

Istraživački kontekst rada obuhvaća kibernetičku obranu u nacionalnom i nadnacionalnom okruženju, s posebnim naglaskom na europski sigurnosni okvir. Analiza uključuje institucionalne aranžmane koji povezuju državna tijela, nacionalne CSIRT-ove, regulatore, operatore kritične infrastrukture i sigurnosno-obavještajni sustav.

Ovaj kontekst karakteriziraju:

- višerazinski upravljački mehanizmi,
- heterogeni akteri s različitim mandatima,
- pravna i klasifikacijska ograničenja dijeljenja informacija,
- potreba za donošenjem odluka pod vremenskim pritiskom

Takvi uvjeti čine kibernetičku obranu posebno pogodnim područjem za proučavanje asimetrične krizne komunikacije, budući da se komunikacijski procesi odvijaju u uvjetima trajne informacijske nejednakosti.

4.3. Operacionalizacija asimetrične krizne komunikacije

Kako bi se koncept asimetrične krizne komunikacije analitički primijenio, u radu se koristi skup kvalitativnih analitičkih dimenzija koje omogućuju prepoznavanje i usporedbu komunikacijskih obrazaca u kriznim situacijama. Te dimenzije uključuju:

- razinu informacijske asimetrije među akterima,
- stupanj fragmentacije značenja u interpretaciji situacije,
- vrijeme potrebno za usklađivanje prioriteta (koordinacijska latencija),
- način na koji sigurnosna ograničenja utječu na komunikacijske odluke

Umjesto kvantifikacije, naglasak je stavljen na identifikaciju uzročno-posljedičnih veza između ograničenja dijeljenja informacija i sigurnosnih učinaka u kriznom odgovoru. Time se omogućuje analiza komunikacije kao strukturnog čimbenika koji oblikuje donošenje odluka, a ne kao varijable koju je moguće promatrati izolirano.

4.4. Ograničenja istraživanja

Odabrani metodološki pristup ima određena ograničenja koja je potrebno jasno naznačiti. Prvo, oslanjanje na javno dostupne izvore i analitičke scenarije znači da se ne mogu izravno analizirati stvarni klasificirani komunikacijski tokovi. Drugo, kvalitativna priroda analize ne omogućuje statističku generalizaciju nalaza. Međutim, ta ograničenja ne umanjuju znanstvenu vrijednost rada, budući da je cilj istraživanja teorijsko i konceptualno objašnjenje fenomena koji je zbog svoje prirode teško kvantificirati. Upravo jasno definirana ograničenja doprinose transparentnosti i metodološkoj dosljednosti rada. Budući da je istraživanje konceptualno-analitičko, rad ne nastoji kvantitativno mjeriti učinke komunikacijskih obrazaca, već ih analizira kao strukturne uvjete donošenja odluka u kibernetičkim krizama.

4.5. Etika i istraživačka odgovornost

Rad ne uključuje podatke koje bi mogle ugroziti nacionalnu sigurnost ili otkriti osjetljive operativne detalje. Analiza se temelji isključivo podacima koji nisu klasificirani, čime se osigurava usklađenost s etičkim načelima istraživanja u području sigurnosti.

5. Analiza komunikacijskih ograničenja u kibernetičkoj krizi

Koncept asimetrične krizne komunikacije razvijen u prethodnom poglavlju u nastavku se operacionalizira kroz realističan, ali analitički kontroliran krizni scenarij. Analitički fokus nije na deskripciji incidenta, već na prikazu kako strukturna ograničenja dijeljenja informacija proizvode ponavljajuće obrasce djelovanja: trajnu informacijsku asimetriju, fragmentaciju značenja, odgode u usklađivanju prioriteta te komunikacijske odluke oblikovane sigurnosnim kompromisima. Analiza je strukturirana prema dimenzijama iz poglavlja 4.3. Scenarij je oblikovan na temelju obrazaca identificiranih u stručnim raspravama i iskustvima sudionika međunarodnog simpozija Kibernetička obrana održanog u kolovozu 2025. te služi kao reprezentativni model komunikacijskih izazova u kibernetičkim krizama.

5.1. Scenarij: prekogranični incident u kritičnoj infrastrukturi s pravnim i klasifikacijskim ograničenjima

Scenarij obuhvaća incident koji pogađa operatora kritične infrastrukture (KI) čiji poremećaji imaju potencijal prekograničnog učinka. Incident se manifestira kroz degradaciju dostupnosti i anomalije u upravljačkim sustavima, uz indikacije kompromitacije na IT i OT sloju. U ranoj fazi nije jasno radi li se o izoliranom incidentu, koordiniranom napadu ili složenijem hibridnom djelovanju.

U odgovor su uključeni sljedeći akteri, koji imaju različite mandate i različite informacijske "vidike":

- Akter A: nacionalni CSIRT / tehnički timovi (primarno tehnički uvid: IOC, telemetrija, forenzika; fokus: detekcija, ograničavanje širenja, oporavak)
- Akter B: operator KI (operativni uvid: stanje usluge, kontinuitet, sigurnost procesa; fokus: stabilizacija i kontinuitet)
- Akter C: regulator / nadležno tijelo (pravni uvid: obveze prijave, pragovi eskalacije, koordinacija; fokus: usklađenost i sistemski rizik)
- Akter D: sigurnosno-obavještajni sustav (obavještajni uvid: indikacije namjere i mogućeg aktera; fokus: nacionalna sigurnost; ograničenja: zaštita izvora i metoda)

Ključno obilježje scenarija jest da se relevantni podaci ne mogu slobodno dijeliti: dio je klasificiran, dio je pravno osjetljiv (npr. osobni podaci / poslovne tajne), dio je operativno osjetljiv (metode detekcije, sposobnosti odgovora). Zbog toga se komunikacija odvija uz djelomično dijeljenje informacija kao legitimnog sigurnosnog zahtjeva.

Iako su svi uključeni akteri usmjereni prema zajedničkom cilju stabilizacije sustava i ograničavanja štete, njihova uloga u kriznom odgovoru definirana je različitim mandatima, odgovornostima i režimima zaštite informacija. Kako bi se pokazalo da informacijska asimetrija u takvom okruženju ne nastaje slučajno, već proizlazi iz strukturnih obilježja sustava kibernetičke obrane, u Tablici 3 prikazani su ključni akteri, njihovi primarni mandati te tipični informacijski "vidici" kojima raspolažu tijekom kriznog odgovora.

TABLICA 3. Akteri, mandati i tipični informacijski "vidici" u kriznom odgovoru

Akter	Primarni mandat	Tipični informacijski "vidici"	Strukturna ograničenja dijeljenja informacija
Nacionalni CSIRT / tehnički timovi	Detekcija, analiza i tehnički odgovor na incident	Tehnički indikatori kompromitacije, forenzički tragovi, telemetrija sustava	Zaštita metoda detekcije, osjetljivost tehničkih detalja
Operator kritične infrastrukture	Očuvanje kontinuiteta usluge i sigurnosti procesa	Operativni učinci incidenta, stanje sustava, utjecaj na usluge	Poslovne tajne, sigurnost procesa, reputacijski i regulatorni rizici
Regulatorno / nadležno tijelo	Nadzor, pravna usklađenost i sistemska stabilnost	Informacije o prijavi incidenta, razini rizika, međusektorskim učincima	Pravna povjerljivost, proceduralna ograničenja
Sigurnosno-obavještajni sustav	Zaštita nacionalne sigurnosti i procjena prijetnji	Indikacije namjere, atribucijski signali, širi sigurnosni kontekst	Zaštita izvora i metoda, klasifikacijski režimi
Ostala državna tijela (po potrebi)	Koordinacija, javne politike, krizno upravljanje	Agregirane procjene utjecaja i preporuke	Ograničen pristup tehničkim i obavještajnim detaljima

Prikazana raspodjela mandata i informacija pokazuje da informacijska asimetrija u kriznom odgovoru nije rezultat nedostatka suradnje, već strukturna posljedica legitimnih sigurnosnih, pravnih i institucionalnih ograničenja.

5.2. Dimenzija 1: Razina informacijske asimetrije

U prikazanom scenariju informacijska asimetrija ne pojavljuje se kao iznimka, već kao strukturno obilježje kriznog odgovora. Već u ranoj fazi incidenta vidljivo je da relevantne informacije nisu ravnomjerno raspodijeljene među akterima te da ne postoji institucionalni mehanizam koji bi omogućio njihovo potpuno objedinjavanje bez narušavanja sigurnosnih i pravnih ograničenja. Time se potvrđuje teza iz poglavlja 3 da djelomično dijeljenje informacija u kibernetičkoj obrani predstavlja očekivano stanje.

Informacijska asimetrija pritom ne proizlazi samo iz količine dostupnih podataka, nego i iz razlika u vrsti i interpretabilnosti informacija. Nacionalni CSIRT i tehnički timovi raspolažu detaljnim tehničkim tragovima i forenzičkim nalazima, ali bez potpunog uvida u širi sigurnosni kontekst. Sigurnosno-obavještajni sustav može imati indikacije o namjeri ili pozadini napadača, ali ne nužno i o tehničkom razmjeru incidenta. Operator kritične infrastrukture najjasnije vidi operativne posljedice za kontinuitet usluge, ali ne i njihove uzroke.

Takva raspodjela informacija proizlazi iz razdvajanja mandata i odgovornosti, a ne iz nedostatka koordinacije. Informacijska asimetrija stoga nije samo pitanje pristupa podacima, nego i dopuštenja za njihovo dijeljenje te institucionalnog konteksta u kojem se informacije interpretiraju i koriste. U analitičkom smislu, u scenariju se mogu identificirati tri međusobno povezane razine informacijske asimetrije:

Asimetrija pristupa, koja proizlazi iz činjenice da različiti akteri imaju pristup različitim skupovima podataka. Nacionalni CSIRT raspolaže tehničkim indikatorima kompromitacije i forenzičkim tragovima, sigurnosno-obavještajni sustav indikacijama namjere i mogućeg aktera, dok operator kritične infrastrukture ima detaljan uvid u operativni učinak incidenta na sustav.

Asimetrija dopuštenja, koja se pojavljuje i u situacijama kada akter posjeduje relevantnu informaciju, ali je ne može dijeliti zbog klasifikacijskih režima, pravnih ograničenja ili potrebe zaštite operativnih sposobnosti i izvora. Ova razina asimetrije posebno je izražena u odnosima između tehničkih i obavještajnih aktera.

Asimetrija konteksta, koja nastaje kada isti podatak ima različito značenje ovisno o institucionalnom i operativnom okviru u kojem se tumači. Primjerice, indikator kompromitacije bez dodatnog konteksta ne omogućuje regulatoru procjenu sistemskog rizika, dok obavještajna procjena bez tehničke potvrde ne mora biti dovoljna za operativnu eskalaciju.

Asimetrija nije posljedica loše komunikacije, već rezultat legitimnog razdvajanja mandata, odgovornosti i režima zaštite podataka unutar sustava kibernetičke obrane. Ovakvo razumijevanje informacijske asimetrije ključno je za daljnju analizu, jer pokazuje zašto komunikacijski izazovi u kibernetičkim krizama ne mogu biti adekvatno objašnjeni normativnim modelima koji polaze od pretpostavke informacijske simetrije.

5.3. Dimenzija 2: Fragmentacija značenja i divergentne interpretacije incidenta

Strukturna informacijska asimetrija ne ostaje ograničena na dostupnost podataka, već utječe na način na koji akteri interpretiraju značenje incidenta. U analiziranom scenariju djelomično dijeljenje informacija dovodi do paralelnih interpretacija iste krizne situacije kroz različite institucionalne i operativne perspektive. Fragmentacija značenja pritom ne označava pogrešno razumijevanje među akterima, već razilaženje u legitimnim interpretacijama koje proizlaze iz različitih mandata, odgovornosti i informacija kojima raspolažu. Drugim riječima, različite interpretacije nisu nužno znak komunikacijskog neuspjeha, nego očekivan ishod djelovanja u uvjetima trajne informacijske asimetrije.

U scenariju se to očituje kroz razvoj različitih radnih hipoteza o prirodi incidenta. Nacionalni CSIRT, oslanjajući se na tehničke indikatore i forenzičke nalaze, incident primarno interpretira kao operativni sigurnosni problem koji zahtijeva brzu tehničku reakciju. Operator kritične infrastrukture fokusira se na stabilizaciju sustava i kontinuitet usluge, dok sigurnosno-obavještajni sustav incident promatra kroz prizmu moguće šire sigurnosne prijetnje. Ove interpretacije nisu proizvoljne, već racionalne unutar konteksta svakog aktera.

Ključno je da se takve interpretacije ne mogu jednostavno uskladiti dodatnim dijeljenjem informacija. Potpuno usklađivanje zahtijevalo bi razmjenu kontekstualnih podataka koji su često klasificirani ili pravno osjetljivi. Fragmentacija značenja stoga predstavlja strukturno ograničenje kriznog odgovora, a ne problem koji se može riješiti optimizacijom komunikacijskih procedura.

Ove razlike u interpretaciji izravno utječu na prioritete, procjenu rizika i odluke o eskalaciji. Tehnička interpretacija incidenta naglašava brzinu reakcije i oporavak sustava, dok sigurnosna interpretacija može potaknuti oprez, provjeru atribucije i sprječavanje eskalacije. Takva razilaženja ne moraju dovesti do otvorenog konflikta, ali mogu produljiti proces donošenja odluka i povećati koordinacijsku latenciju čak i kada su komunikacijski kanali formalno uspostavljeni.

Analitički gledano, fragmentacija značenja predstavlja poveznicu između informacijske asimetrije i sigurnosnih učinaka kriznog odgovora. Dok informacijska asimetrija opisuje raspodjelu podataka, fragmentacija značenja objašnjava kako ta raspodjela utječe na interpretaciju i odlučivanje. Kako bi se te razlike učinile vidljivima, Tablica 4 prikazuje dominantne radne hipoteze ključnih aktera uključenih u krizni odgovor te njihove prioritete i sigurnosne implikacije.

TABLICA 4. Radne hipoteze aktera i implikacije na prioritete

Akter	Dominantna radna hipoteza	Primarni prioritet	Potencijalni sigurnosni rizik fragmentacije značenja
Nacionalni CSIRT / tehnički timovi	Incident je primarno tehnički sigurnosni problem	Brza detekcija, izolacija i sanacija	Podcjenjivanje šireg sigurnosnog konteksta
Operator kritične infrastrukture	Incident ugrožava kontinuitet usluge i sigurnost procesa	Stabilizacija sustava i kontinuitet rada	Fokus na kratkoročni oporavak nauštrb dugoročnog rizika
Regulatorno / nadležno tijelo	Incident predstavlja potencijalni sistemski rizik	Pravodobna prijava i usklađenost s propisima	Administrativna odgoda operativnih odluka
Sigurnosno-obavještajni sustav	Incident može biti dio šire namjerne kampanje	Sprječavanje eskalacije i zaštita izvora	Odgoda tehničkih mjera zbog potrebe verifikacije
Ostala državna tijela	Incident zahtijeva koordinirani međuresorni odgovor	Usklađivanje politika i komunikacija	Nejasni prioriteti zbog ograničenog uvida

Prikazane razlike u radnim hipotezama pokazuju da fragmentacija značenja izravno utječe na definiranje prioriteta i očekivanja u kriznom odgovoru, čime se postavlja temelj za razumijevanje zašto usklađivanje odluka u uvjetima asimetrične krizne komunikacije zahtijeva dodatno vrijeme i koordinacijski napor.

5.4. Dimenzija 3: Vrijeme potrebno za usklađivanje prioriteta (koordinacijska latencija)

Fragmentacija Fragmentacija značenja među akterima neposredno utječe na vrijeme potrebno za usklađivanje prioriteta i donošenje zajedničkih odluka. U kontekstu asimetrične krizne komunikacije taj vremenski odmak ne predstavlja samo operativni problem, već sigurnosni fenomen koji proizlazi iz donošenja odluka uz djelomično dijeljenje informacija i različite interpretacije situacije. U analiziranom scenariju koordinacijska latencija ne proizlazi iz nedostatka komunikacijskih kanala ili volje za suradnjom, nego iz potrebe za iterativnim usklađivanjem značenja. Budući da akteri raspolažu parcijalnim informacijama i različitim radnim hipotezama, postizanje minimalnog konsenzusa zahtijeva dodatne komunikacijske cikluse u kojima se informacije postupno apstrahiraju i prevode u oblik prihvatljiv širem krugu sudionika.

Jedan od ključnih mehanizama koji produljuju proces usklađivanja jest apstrakcija informacija. Sigurnosno osjetljivi podaci rijetko se mogu dijeliti u izvornom obliku, već se prenose kao zaključci ili indikacije bez potpunog konteksta. Takav pristup smanjuje rizik kompromitacije izvora i metoda, ali istodobno povećava neizvjesnost primatelja koji često zahtijevaju dodatna pojašnjenja prije djelovanja.

Drugi mehanizam odnosi se na rizik pogrešne eskalacije. U uvjetima informacijske asimetrije akteri su svjesni da odluke donesene na temelju parcijalnih ili pogrešno interpretiranih informacija mogu dovesti do neopravdane eskalacije ili kompromitacije osjetljivih sposobnosti. Zbog toga se često primjenjuje oprezniji pristup u kojem se odluke odgađaju dok se ne postigne dovoljna razina pouzdanosti.

Koordinacijsku latenciju dodatno oblikuju različiti institucionalni pragovi eskalacije. Tehnički akteri mogu incident smatrati hitnim operativnim problemom, dok regulatorna ili sigurnosno-obavještajna tijela zahtijevaju dodatne potvrde prije šire koordinacije ili političke eskalacije. Takvi pragovi proizlaze iz zakonskih i institucionalnih obveza, ali otežavaju brzo usklađivanje prioriteta.

U ovom radu koordinacijska latencija ne tumači se kao pokazatelj neučinkovitosti komunikacije, nego kao sigurnosno racionalan kompromis. Sporiji proces donošenja odluka često predstavlja svjesni izbor kojim se nastoji smanjiti rizik pogrešne reakcije u uvjetima visoke neizvjesnosti. Time koordinacijska latencija postaje ključni indikator asimetrične krizne komunikacije, jer proizlazi iz napetosti između potrebe za brzom reakcijom i obveze zaštite osjetljivih informacija. Razumijevanje te napetosti omogućuje realističniju evaluaciju kriznog odgovora u kibernetičkoj obrani. Kako bi se ovaj fenomen analitički prikazao, Tablica 5 prikazuje ključne uzroke produljenog usklađivanja prioriteta, njihovu manifestaciju u komunikacijskim procesima te sigurnosne posljedice koje iz njih proizlaze. Takav prikaz omogućuje razlikovanje između komunikacijskih kašnjenja koja su posljedica neefikasnosti i onih koja proizlaze iz legitimnih sigurnosnih kompromisa.

TABLICA 5. Koordinacijska latencija: uzroci, manifestacije i sigurnosne posljedice

Uzrok koordinacijske latencije	**Manifestacija u komunikaciji**	**Sigurnosna posljedica**	**Potencijalno ublažavanje bez narušavanja ograničenja**
Apstrakcija osjetljivih informacija	Dijeljenje sažetih procjena bez detaljnog konteksta	Povećana neizvjesnost u donošenju odluka	Standardizirani apstrahirani indikatori rizika
Zaštita izvora i metoda	Ograničeno objašnjavanje razloga procjene	Odgoda eskalacijskih odluka	Povjerljivi briefinzi za ovlaštene donositelje odluka
Različiti institucionalni pragovi eskalacije	Nesinkronizirane odluke o razini odgovora	Fragmentirana koordinacija	Prethodno definirani pragovi eskalacije
Pravna i regulatorna ograničenja	Odgoda dijeljenja informacija do pravne provjere	Kašnjenje zajedničkog odgovora	Krizni pravni protokoli
Rizik pogrešne atribucije	Oprez u komunikaciji o namjeri napadača	Konzervativniji odgovor	Scenarijsko planiranje bez eksplicitne atribucije

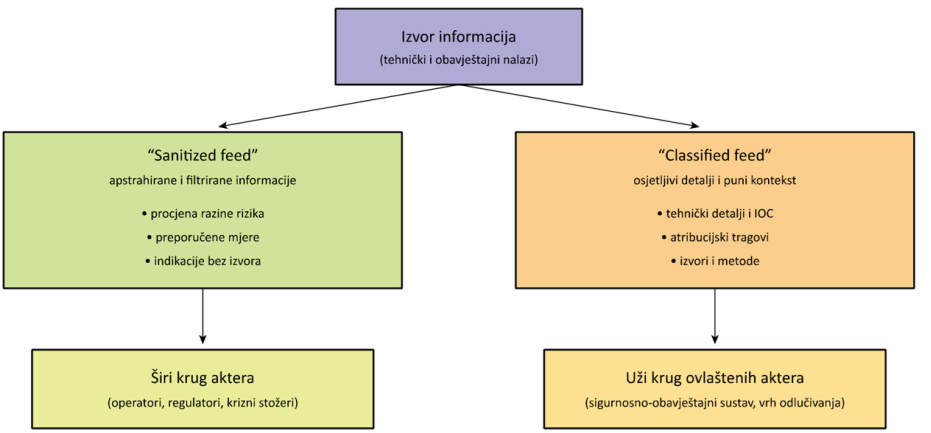
Prikazani uzroci i učinci koordinacijske latencije potvrđuju da se sporiji tempo usklađivanja odluka u kibernetičkim krizama ne može jednostavno tumačiti kao nedostatak učinkovitosti. Naprotiv, u uvjetima asimetrične krizne komunikacije koordinacijska latencija često predstavlja sigurnosno racionalan odgovor na potrebu zaštite osjetljivih informacija i izbjegavanja pogrešne eskalacije.

5.5. Dimenzija 4: Utjecaj sigurnosnih ograničenja na komunikacijske odluke

U prethodnim pod poglavljima pokazano je kako informacijska asimetrija i fragmentacija značenja proizvode koordinacijsku latenciju u kibernetičkim krizama. Međutim, akteri u kriznom odgovoru nisu pasivni nositelji tih ograničenja. Sigurnosna ograničenja aktivno se ugrađuju u komunikacijske odluke, koje postaju dio strategije upravljanja krizom. U analiziranom scenariju komunikacija nije usmjerena prema maksimalnom dijeljenju informacija, već prema kontroliranom prijenosu značenja koji omogućuje donošenje odluka bez izlaganja osjetljivih podataka. Time sigurnost postaje temeljni kriterij oblikovanja komunikacijskih poruka, kanala i vremenskih okvira.

Takav pristup često dovodi do paralelnih komunikacijskih tokova u kojima se ista sigurnosna situacija prenosi različitim akterima u različitim oblicima. Slika 2 prikazuje razlikovanje između "sanitized feeda", namijenjenog širem krugu sudionika kriznog odgovora, i "classified feeda", koji je ograničen na uži krug ovlaštenih aktera.

SLIKA 2. "Sanitized feed" vs. "classified feed": dva paralelna komunikacijska toka



Napomena: paralelni tokovi omogućuju odlučivanje bez potpune transparentnosti, ali institucionaliziraju informacijsku asimetriju.

Izvor: autor

Ovakvi paralelni tokovi pokazuju da informacijska asimetrija nije samo nuspojava sigurnosnih ograničenja, već njihova institucionalizacija kroz komunikacijsku praksu. Time komunikacija postaje aktivni mehanizam upravljanja sigurnosnim rizikom.

U scenariju se pritom izdvajaju tri dominantna obrasca. Prvi je apstrakcija komunikacijskog sadržaja, pri čemu se umjesto sirovih tehničkih ili obavještajnih podataka dijele procjene rizika ili preporuke za djelovanje. Drugi je segmentacija komunikacije prema principu "need-to-know", gdje različiti akteri primaju različite verzije informacija prilagođene njihovim mandatima. Treći je temporalno upravljanje komunikacijom, odnosno odgađanje dijeljenja određenih informacija dok se ne razjasne njihovi sigurnosni ili politički učinci.

Komunikacijske odluke u kibernetičkoj krizi stoga predstavljaju balans između brzine, sigurnosti i legitimnosti. Brzina reakcije i transparentnost ne mogu se promatrati izolirano od sigurnosnih posljedica, pa akteri oblikuju komunikaciju tako da optimiziraju donošenje odluka unutar postojećih sigurnosnih ograničenja.

5.6. Obrasci asimetrične krizne komunikacije

Analiza kriznog scenarija kroz dimenzije informacijske asimetrije, fragmentacije značenja, koordinacijske latencije i sigurnosno uvjetovanih komunikacijskih odluka omogućuje identifikaciju ponavljajućih obrazaca asimetrične krizne komunikacije koji su dosljedno prepoznati u analiziranom scenariju i potvrđeni kroz stručne rasprave u međunarodnom okruženju. Ovi obrasci ne proizlaze iz specifičnosti pojedinog incidenta, već iz strukturnih obilježja sustava u kojem se krizni odgovor odvija pod pravnim, institucionalnim i sigurnosnim ograničenjima.

Prvi obrazac odnosi se na trajnu informacijsku asimetriju među akterima. U svim fazama kriznog odgovora niti jedan akter ne raspolaže potpunom situacijskom slikom, već isključivo fragmentima informacija koji su u skladu s njegovim mandatom i razinom ovlasti. Ova asimetrija nije privremeni nedostatak koji se može ukloniti dodatnim dijeljenjem podataka, već stabilno stanje proizvedeno razdvajanjem funkcija, klasifikacijskim režimima i zaštitom osjetljivih sposobnosti.

Drugi obrazac je fragmentacija značenja, koja nastaje kada se parcijalne informacije interpretiraju kroz različite institucionalne perspektive. Akteri razvijaju legitimne, ali divergentne radne hipoteze o prirodi incidenta, što dovodi do različitih procjena rizika i prioriteta. Fragmentacija značenja time postaje ključna poveznica između informacijske asimetrije i konkretnih učinaka na donošenje odluka, jer oblikuje način na koji se informacije prevode u djelovanje.

Treći obrazac odnosi se na koordinacijsku latenciju kao sigurnosno uvjetovan fenomen. Produljeno vrijeme usklađivanja prioriteta ne proizlazi primarno iz neučinkovitosti komunikacije, već iz potrebe za opreznim donošenjem odluka u uvjetima visoke neizvjesnosti i ograničenog dijeljenja informacija. Koordinacijska latencija stoga ne predstavlja nužno slabost sustava, već često reflektira svjesni kompromis između brzine reakcije i smanjenja rizika pogrešne eskalacije.

Četvrti obrazac odnosi se na aktivno oblikovanje komunikacijskih odluka kao odgovora na sigurnosna ograničenja. Komunikacija se ne odvija kao neutralan prijenos informacija, već kao selektivni proces apstrakcije, segmentacije i vremenskog upravljanja sadržajem. Uspostava paralelnih komunikacijskih tokova, poput "sanitized" i "classified" feedova, institucionalizira informacijsku asimetriju i omogućuje donošenje odluka bez potpune transparentnosti, ali uz povećanu potrebu za povjerenjem i koordinacijom.

Zajedno promatrani, ovi obrasci potvrđuju da se krizna komunikacija u kibernetičkoj obrani ne može adekvatno analizirati kroz normativne modele koji polaze od pretpostavke informacijske simetrije i potpune transparentnosti. Umjesto toga, asimetrična krizna komunikacija pojavljuje se kao strukturno stanje u kojem komunikacija djeluje kao mehanizam upravljanja sigurnosnim ograničenjima, a ne samo kao sredstvo za razmjenu informacija.

6. Rasprava i implikacije

Nalazi analize kriznog scenarija razmatraju se u odnosu na postojeću literaturu o kriznoj komunikaciji i kibernetičkoj sigurnosti. Polazeći od teze da je asimetrična krizna komunikacija strukturno obilježje kibernetičke obrane, a ne devijacija od normativnih modela, rad omogućuje reinterpretaciju pojava koje se u dosadašnjim istraživanjima često tumače kao komunikacijski nedostaci ili organizacijski neuspjesi.

6.1. Doprinos teoriji krizne komunikacije

U literaturi krizne komunikacije dominantni modeli često polaze od pretpostavke da su informacijska simetrija, transparentnost i brza razmjena informacija ključni preduvjeti učinkovitog kriznog odgovora. Rezultati ovog istraživanja pokazuju da takve pretpostavke imaju ograničenu primjenjivost u kibernetičkoj obrani, osobito kada su u pitanju podaci osjetljivi za nacionalnu sigurnost.

Rad stoga proširuje teoriju krizne komunikacije uvođenjem koncepta asimetrične krizne komunikacije, koji polazi od trajne informacijske nejednakosti među akterima. U tom okviru komunikacijski problemi ne tumače se prvenstveno kao posljedica nedostatka informacija ili slabe koordinacije, nego kao rezultat legitimnih sigurnosnih, pravnih i institucionalnih ograničenja. Time se fokus pomiče s normativnog pitanja kako bi komunikacija trebala izgledati na analitičko pitanje kako funkcionira u realnim sigurnosnim uvjetima.

Poseban doprinos rada jest razlikovanje informacijske asimetrije i fragmentacije značenja. Dok se informacijska asimetrija odnosi na raspodjelu podataka među akterima, fragmentacija značenja objašnjava kako se ti podaci interpretiraju i prevode u odluke. Ova distinkcija omogućuje precizniju analizu situacija u kojima formalna razmjena informacija postoji, ali zajedničko razumijevanje i dalje izostaje.

Prepoznati komunikacijski obrasci pojavljuju se i u raspravama stručnjaka iz različitih nacionalnih i sektorskih okvira, što upućuje na njihovu širu primjenjivost.

6.2. Reinterpretacija učinkovitosti krizne komunikacije

Nalazi rada dovode u pitanje uobičajene kriterije evaluacije učinkovitosti krizne komunikacije. U normativnim modelima kašnjenja u donošenju odluka, selektivno dijeljenje informacija i fragmentirana komunikacija često se tumače kao znakovi neučinkovitosti. Analiza u ovom radu pokazuje da takvi fenomeni u kibernetičkoj obrani mogu predstavljati sigurnosno racionalne kompromise, a ne komunikacijske neuspjehe. Primjerice, koordinacijska latencija ne proizlazi nužno iz slabosti komunikacijskih procesa, već iz potrebe za opreznim donošenjem odluka kako bi se izbjegla pogrešna eskalacija ili kompromitacija osjetljivih informacija. Stoga se učinkovitost krizne komunikacije u sigurnosnom kontekstu ne može procjenjivati isključivo brzinom ili količinom razmijenjenih informacija, nego sposobnošću sustava da donosi prihvatljive odluke u uvjetima neizbježnih ograničenja. Kako bi se jasnije prikazala razlika između normativnih pristupa kriznoj komunikaciji i sigurnosno utemeljenog pristupa predloženog u ovom radu, Tablica 6 uspoređuje ključne kriterije učinkovitosti.

TABLICA 6. Usporedba normativnih i sigurnosno utemeljenih kriterija učinkovitosti krizne komunikacije

Dimenzija	Normativni kriteriji	Sigurnosno utemeljeni kriteriji (ovaj rad)
Temeljna pretpostavka	Informacijska simetrija je dostižan cilj	Informacijska asimetrija je trajno stanje
Uloga transparentnosti	Maksimalna transparentnost povećava učinkovitost	Selektivna transparentnost smanjuje sigurnosni rizik
Brzina komunikacije	Brzina je ključni pokazatelj uspjeha	Brzina se balansira s oprezom i verifikacijom
Dijeljenje informacija	Šire dijeljenje poboljšava koordinaciju	Djelomično dijeljenje štiti izvore i sposobnosti
Koordinacijska latencija	Kašnjenje ukazuje na neučinkovitost	Latencija može biti sigurnosno racionalna
Kriterij uspješnosti	Količina i brzina razmijenjenih informacija	Kvaliteta odluka pod ograničenjima
Uloga povjerenja	Povjerenje je posljedica transparentnosti	Povjerenje zamjenjuje potpunu transparentnost
Odnos prema sigurnosti	Sigurnost implicitna ili sekundarna	Sigurnost kao primarni dizajnerski kriterij

Konceptualni pomak dodatno je prikazan na Slici 3, koja ilustrira prijelaz od normativnog komunikacijskog ideala – obilježenog transparentnošću, brzinom i informacijskom simetrijom – prema pristupu u kojem se odluke donose uz sigurnosna ograničenja, selektivno dijeljenje informacija i prihvaćanje asimetrije.

SLIKA 3. Pomak od normativne prema sigurnosno utemeljenoj kriznoj komunikaciji

Izvor: autor

Vizualizirani pomak naglašava da učinkovitost krizne komunikacije u kibernetičkoj obrani proizlazi iz sposobnosti sustava da donosi legitimne i sigurnosno prihvatljive odluke u uvjetima trajnih informacijskih ograničenja.

6.3. Implikacije za praksu kibernetičke obrane

Nalazi ovog rada upućuju na potrebu za realističnim dizajnom komunikacijskih mehanizama u kibernetičkoj obrani, utemeljenim na pretpostavci trajne informacijske asimetrije. U praksi to znači integriranje komunikacijskog dizajna u planove odgovora na incidente kroz unaprijed definirane pragove eskalacije i standardizirane, apstrahirane indikatore rizika koji su sigurni za dijeljenje među heterogenim akterima. Takav pristup omogućuje koordinaciju i donošenje odluka čak i kada potpuna informacijska predodžba nije dostupna svim sudionicima. Operativno se to može provoditi kroz strukturirane playbookove i procedure promjene aktivnosti usklađene s okvirima poput NIST CSF 2.0, koji naglašavaju upravljanje procesima i očekivanjima, a ne maksimalno dijeljenje svih informacija (Morić et al., 2025). Rezultati također ističu važnost paralelnih komunikacijskih tokova, poput “sanitized” i “classified” feedova, koji omogućuju dijeljenje relevantnih informacija uz očuvanje sigurnosnih ograničenja. U takvom okruženju povjerenje među akterima postaje ključni mehanizam koordinacije jer djelomično nadomješta nemogućnost potpune transparentnosti. Ovakav pristup može smanjiti nesporazume i neusklađena očekivanja te pridonijeti stabilnijem upravljanju kibernetičkim krizama.

6.4. Implikacije za buduća istraživanja

Nalazi ovog rada otvaraju nekoliko smjerova za daljnja istraživanja krizne komunikacije u kibernetičkoj obrani. Prvo, koncept asimetrične krizne komunikacije može se empirijski testirati kroz komparativne studije različitih nacionalnih, sektorskih ili institucionalnih okvira kako bi se utvrdilo u kojoj mjeri identificirani obrasci predstavljaju opće obilježje kibernetičke obrane u sigurnosno osjetljivim okruženjima.

Drugi smjer odnosi se na operacionalizaciju ključnih analitičkih dimenzija – informacijske asimetrije, fragmentacije značenja i koordinacijske latencije – kroz razvoj kvalitativnih ili hibridnih evaluacijskih okvira. Takvi pristupi mogli bi omogućiti sustavniju analizu kriznih odgovora bez potrebe za pristupom klasificiranim podacima.

Posebno važna tema za buduća istraživanja jest uloga povjerenja u uvjetima trajne informacijske nejednakosti. Budući da potpuna transparentnost u kibernetičkoj obrani često nije moguća, povjerenje među akterima postaje ključni mehanizam koordinacije, osobito u višerazinskim i prekograničnim oblicima suradnje.

Naposljetku, predloženi konceptualni okvir može se primijeniti i na druge sigurnosno osjetljive domene u kojima je djelomično dijeljenje informacija strukturna nužnost, poput obrambenih sustava, kriznog upravljanja u zdravstvu ili zaštite kritične infrastrukture. Takva proširenja omogućila bi daljnju provjeru i razvoj koncepta asimetrične krizne komunikacije u različitim kontekstima kompleksnih kriza.

7. Zaključak

Krizna komunikacija u kibernetičkoj obrani u ovom radu promatra se kroz prizmu djelomičnog dijeljenja informacija i strukturnih sigurnosnih ograničenja. Polazeći od pretpostavke da potpuna informacijska transparentnost u nacionalno-sigurnosnom kontekstu nije ostvariva niti nužno poželjna, uvodi se koncept asimetrične krizne komunikacije kao analitički okvir za razumijevanje komunikacijskih procesa tijekom kibernetičkih kriza. Analiza pokazuje da informacijska asimetrija, fragmentacija značenja i koordinacijska latencija ne predstavljaju nužno komunikacijske neuspjehe, nego često racionalne posljedice sigurnosnih, pravnih i institucionalnih ograničenja.

Znanstveni doprinos rada ogleda se u pomaku od normativnih modela krizne komunikacije prema sigurnosno utemeljenom razumijevanju komunikacije kao instrumenta upravljanja rizikom. Time se krizna komunikacija u kibernetičkoj obrani pozicionira kao strukturni element sigurnosnog sustava, a ne samo kao organizacijska ili reputacijska funkcija.

U praktičnom smislu, predloženi okvir može poslužiti institucijama uključenima u upravljanje kibernetičkim incidentima, poput nacionalnih CSIRT-ova, regulatornih tijela i operatora kritične infrastrukture. Umjesto pretpostavke potpune informacijske simetrije, pristup naglašava upravljanje informacijskom asimetrijom kroz jasno definirane pragove eskalacije i paralelne komunikacijske tokove koji omogućuju donošenje odluka uz očuvanje sigurnosnih ograničenja.

Rad time otvara prostor za daljnja istraživanja koja mogu empirijski ispitati ulogu komunikacije u sigurnosno osjetljivim kriznim kontekstima i doprinijeti razvoju realističnijih modela kibernetičke obrane.

Literatura

- Abraham, C., Bélanger, F., & Daultrey, S. (2025). Promoting research on cyber threat intelligence sharing in ecosystems. *Journal of cybersecurity*, *11*(1). https://doi.org/10.1093/CYBSEC/TYAF016
- Alkalabi, W., Simpson, L., & Morarji, H. (2021). Barriers and incentives to cybersecurity threat information sharing in developing countries: A case study of saudi arabia. *ACM international conference proceeding series*. https://doi.org/10.1145/3437378.3437391
- Anderson, P., Beauvois, F., Blanco Bouza, S., Karkala, S., Kourtis, G., Michota, A., … Stupka, V. (2021, January). CSIRT–law enforcement cooperation. ENISA. Retrieved from https://www.enisa.europa.eu/publications/csirt-law-enforcement-cooperation
- Chang, K., & Huang, H. (2023). Exploring the management of multi-sectoral cybersecurity information-sharing networks. *Government information quarterly*, *40*(4), 101870. https://doi.org/10.1016/J.GIQ.2023.101870
- Coombs, W. Timothy. (2021). Ongoing Crisis communication: planning, managing, and responding (6th ed.). Thousand Oaks, CA: SAGE Publications, Inc. Retrieved from https://uk.sagepub.com/en-gb/eur/ongoing-crisis-communication/book270207
- Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance. Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/S41288-022-00266-6
- Du, H. W., Xu, J., & Vasarhelyi, M. A. (2024). Systematic review of cybersecurity disclosure research. *Lecture notes in computer science*, *15179 LNCS*, 247–262. https://doi.org/10.1007/978-981-97-7798-3_21
- Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers & security*, *132*, 103372. https://doi.org/10.1016/J.COSE.2023.103372
- ENISA. (2024, February). Best practices for cyber crisis management. ENISA. https://doi.org/10.2824/767828
- EU Parlament. (2022). DIREKTIVA (EU) 2022/2555. Retrieved from https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32022L2555
- Fang, J., Tang, Y., & Guo, M. (2025). Comprehensive review of cyber threat intelligence sharing: challenges and methodologies. *Proceedings of the 4th Asia-Pacific Artificial Intelligence and Big Data Forum, AIBDF 2024*, *7*, 455–461. https://doi.org/10.1145/3718491.3718565
- General Secretariat of the Council. (2025). *Council recommendation on an eu blueprint for cyber crisis management*. Brussels. Retrieved from https://data.consilium.europa.eu/doc/document/ST-9794-2025-INIT/en/pdf
- Groenendaal, J., Barjas, S., & Helsloot, I. (2021). Cyber incident response decision making: What can be learned from experienced Cyber Incident Response Consultants? A preliminary investigation. *The Hague: The Hague University of Applied Sciences*. Retrieved from https://www.dehaagsehogeschool.nl/sites/hhs/files/documents/onderzoeksrapport-cyber-incident-decision-making-digi.pdf
- Hayes, P., Bearman, C., Butler, P., & Owen, C. (2021). Non-technical skills for emergency incident management teams: A literature review. *Journal of contingencies and crisis management*, *29*(2), 185–203. https://doi.org/10.1111/1468-5973.12341
- Heath, R. L., & O'Hair, H. D. (2010). Handbook of risk and crisis communication. 1–683. https://doi.org/10.4324/9780203891629
- Hodgson, Q. E., Clark-Ginsberg, A., Haldeman, Z., Lauland, A., & Mitch, I. (2022). Managing response to significant cyber incidents: comparing event life cycles and incident response across cyber and non-cyber events. https://doi.org/10.7249/RRA1265-4
- Kopal, R., Alikavazović, B., & Morić, Z. (2025). From context to action: establishing a pre-chain phase within the cyber kill chain. *Journal of cybersecurity and privacy*, *6*(1), 5. https://doi.org/10.3390/jcp6010005
- Lakshmi, R., Naseer, H., Maynard, S., & Ahmad, A. (2021). Sensemaking in cybersecurity incident response: the interplay of organizations, technology and individuals. https://doi.org/10.48550/arXiv.2107.02941
- Morić, Z., Dakić, V., Kapulica, A., & Redžepagić, J. (2025). Best practices for incident response changes with NIST CSF 2.0. *2025 10th International conference on cloud computing and big data analytics (ICCCBDA)*, 546–553. IEEE. https://doi.org/10.1109/ICCCBDA64898.2025.11030516
- Mott, G., Nurse, J. R. C., & Baker-Beall, C. (2023). Preparing for future cyber crises: lessons from governance of the coronavirus pandemic. *Policy design and practice*, *6*(2), 160–181. https://doi.org/10.1080/25741292.2023.2205764
- Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & security*, *132*, 103309. https://doi.org/10.1016/J.COSE.2023.103309
- Rantos, K., Spyros, A., Papanikolaou, A., Kritsas, A., Ilioudis, C., & Katos, V. (2020). Interoperability challenges in the cybersecurity information sharing ecosystem. *Computers 2020, Vol. 9, Page 18*, *9*(1), 18. https://doi.org/10.3390/COMPUTERS9010018

- Reittinger, T., Grill, J., & Pernul, G. (2026). Share and benefit: incentives for cyber threat intelligence sharing. *International journal of information security 2025 25:1*, *25*(1), 37-. https://doi.org/10.1007/S10207-025-01165-2
- Ruohonen, J., Rindell, K., & Busetti, S. (2025). From cyber security incident management to cyber security crisis management in the European Union. *Computers & security*, *159*, 104689. https://doi.org/10.1016/J.COSE.2025.104689
- Sellnow, T. L., & Seeger, M. W. (2020). Theorizing crisis communication. *Wiley-Blackwell*.
- Serini, F. (2024). Collective cyber situational awareness in EU. A political project of difficult legal realisation? *Computer law & security review*, *55*, 106055. https://doi.org/10.1016/J.CLSR.2024.106055
- Tinonetsana, F., Rawjee, V., & Govender, J. (2025). Crisis communication during cyber attacks: A situational crisis communication theory perspective. *International journal of research in business and social science (2147- 4478)*, *14*(8), 43–51. https://doi.org/10.20525/ijrbs.v14i8.4379
- Wu, Y. (2023). National cybersecurity crisis management frameworks. *ACM international conference proceedings*. https://doi.org/10.1145/3625469.3625487

Asymmetric Crisis Communication as a Security Constraint in Cyber Defense with Partial Information Sharing

Abstract

Cyber defence within a national security framework functions amid enduring information asymmetry, regulatory limitations, and classification protocols that hinder comprehensive and equitable information exchange among stakeholders. Nonetheless, existing models of crisis communication frequently rely on normative assumptions of transparency, expediency, and informational symmetry. This research presents the notion of asymmetric crisis communication as an analytical framework for comprehending communication processes in cyber defence amid partial information dissemination. The research employs a conceptual-analytical methodology alongside a scenario-based examination of a plausible cyber crisis featuring diverse entities with varying mandates and data protection frameworks. The research indicates that information asymmetry, fragmentation of meaning, and coordination lag do not inherently signify communication failures, but instead represent valid security trade-offs. Crisis communication is thus framed as an active instrument of security risk management, rather than simply a conduit for information dissemination, enhancing the comprehension of cyber defence.

Keywords: asymmetric crisis communication, cyber defence, national security, crisis decision-making