PRAVNO UREĐENJE BEZBEDNOSTI INFORMACIONE KRITIČNE INFRASTRUKTURE

Tatjana Bugarski
Pravni fakultet u Novom Sadu, Univerzitet u Novom Sadu;
t.bugarski@pf.uns.ac.rs

Milana Pisarić
Pravni fakultet u Novom Sadu, Univerzitet u Novom Sadu;

Korespondencija: mpisaric@pf.uns.ac.rs

Apstrakt: Mrežni i informacioni sistemi i usluge, kao informaciona kritična infrastruktura, imaju značajnu ulogu u savremenom društvu, pa je njihova pouzdanost i bezbednost od važnosti za ključne društvene i ekonomske aktivnosti. Ipak, njihovom postojanju i pravilnom funkcionisanju prete određeni bezbednosni rizici u sajber prostoru, koji su sve većih razmera, učestalosti i uticaja. Tako ovi sistemi mogu postati meta sajber napada, odnosno nedozvoljenih radnji koje se preduzimaju sa namerom prouzrokovanja štete i/ili prekida njihovog rada. Ovakvi incidenti mogu ugroziti društvene i ekonomske aktivnosti, koji zavise od informacione kritične infrastrukture. Zbog toga je neophodno posvetiti pažnju sajber bezbednosti. Pri tome, upravljanje rizicima u sajber prostoru mora biti takvo da se ne ugrozi pravna sigurnost. U tom smislu od izuzetne važnosti je način na koji se propisuju smernice za procenu rizika po sajber bezbednost. Dobar primer regulative predstavlja Direktiva Evropske unije o bezbednosti mrežnih i informacionih sistema. Direktiva predviđa da se određene organizacije obavežu da preduzmu odgovarajuće i proporcionalne mere bezbednosti, te da uoče, procene i uzmu u obzir rizike po sajber bezbednost sa kojima se suočavaju, kako bi se smetnje po pružanje usluga sprečile i svele na minimum. Cilj Direktive je da se propisivanjem tavih obaveza obezbedi da informaciona kritična infrastruktura bude zaštićena od prekida koji bi mogli biti od uticaja po ključne ekonomske i društvene aktivnosti. Predmet rada je analiza obaveze zaštite i infor-

misanja koje Direktiva o bezbednosti mrežnih i informacionih sistema propisuje za pružaoce digitalnih usluga.

Ključne reči: kritična infrastruktura, sajber bezbednost, bezbednost podataka, upravljanje rizikom, NIS Direktiva.

1. UVOD

Sajber prostor predstavlja kompleksno okruženje koje je rezultat interakcije ljudi, softvera i usluga na Internetu koja se ostvaruje uz pomoć tehnoloških uređaja i mreža sa kojom su uređaji povezani. Zaštita sajber prostora postala je još izazovnija sa sve većom međupovezanošću njegovih komponenata i sve većom zavisnošću od njegove pouzdanosti, integriteta, i dostupnosti. Život u savremenim uslovima zavisi od niza usluga, koje se pružaju u okviru različitih delatnosti, kao što su energetika, saobraćaj, finansije i zdravstvo, a koje se oslanjaju ne samo na fizičku, nego i na digitalnu infrastrukturu, koja istovremeno omogućava komunikaciju i interakciju. Polazeći od toga da se pod kritičnom infrastrukturom podrazumevaju sistemi koji pružaju osnovne funkcije i usluge koje podržavaju društvene i ekonomske sisteme, mrežni i informacioni sistemi i usluge mogu se označiti kao informaciona kritična infrastruktura, a zaštita njene pouzdanosti, integriteta i dostupnosti kao mrežna i informaciona bezbednost (Network and Information Security: NIS), odnosno sajber bezbednost.

Postojanju i pravilnom funkcionisanju informacione kritične infrastrukture prete određeni bezbednosni rizici u sajber prostoru, koji su sve većih razmera, učestalosti i uticaja. Broj i pojavni oblici sajber napada neprestano rastu, pri čemu su sve više sofisticirani i usmereni na različita područja ranjivosti u informacionoj kritičnoj infrastrukturi. Može se očekivati da će tokom naredne decenije postati sve teže proceniti i protumačiti rizike sajber bezbednosti usled povećane složenosti pejzaža pretnji i aktera napada, te širenje mogućih meta napada. Pri tome, potencijalna šteta od napada na informacione sisteme višestruko se povećava zbog međuzavisnosti fizičke i digitalne infrastrukture, pa ovi napadi mogu dovesti do poremećaja, čak i do prekida u pružanju ključnih usluga. Takođe, poremećaji u jednom sektoru mogu imati neposredan učinak na operacije u drugima: napad na proizvodnju električne energije može uzrokovati kolaps telekomunikacija, bolnica ili banaka a napad na digitalnu infrastrukturu mogao

bi dovesti do poremećaja u elektroenergetskim mrežama ili finansijskom sektoru. Zbog svega navedenog zaštita sajber bezbednosti postalo je pitanje od strateške važnosti za državu.

Kako bi država pravilno reagovala na potrebu očuvanja sajber bezbednosti, nužno je da raspolaže strategijom za osiguravanje visokog nivoa bezbednosti mrežnih i informacionih sistema na svojoj teritoriji. Takođe,od izuzetne važnosti je da se postojeći okvir za zaštitu i otpornost kritične infrastrukture nadogradi, u korak s pojavom novih rizika po sajber bezbednost, propisivanjem odgovarajućih mera, ne samo za zaštitu fizičke, nego i informacione kritične infrastrukture i izgradnju otpornosti. Istovremeno, usled transnacionalne prirode mrežnih i informacionih sistema, poremećaj u njihovom radu, može uticati i na druge države, pa bezbednost informacione kritične infrastrukture, iako ključna za svaku pojedinu državu, ima i prekograničnu dimenziju. S obzirom na to da Republika Srbija ima status kandidata za članstvo u Evropskoj uniji, pažnju je potrebno posvetiti regulatornom okviru sajber bezbednosti ove regionalne organizacije.

2. NIS DIREKTIVA

Iako je još 2008. na nivou Unije usvojena Direktivao kritičnoj infrastrukturi,[1]prvi izvor prava o sajber bezbednosti predstavljaDirektiva o bezbednosti mrežnih i informacionih sistema (NIS Direktiva).[2]Kako su do tada države članice imale različite nivoe pripravnosti, što je dovelo do postojanja rascepkanog pristupa ovom problemu, nivo bezbednosti mrežnih i informacionih sistema je bio narušen, čemu je doprinela i nemogućnost uspostavnja nadnacionalne efikasne saradnje. Za stvaranje delotvornog odgovora na izazove sajber bezbednosti bio je potreban pristup na nivou Unije u smislu zajedničkih minimal-

[1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union L 345/75, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008L0114&from=hr.

[2]Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the European Union L 194/1,https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=HR.

nih zahteva za izgradnju kapaciteta i planiranje, razmenu informacija, saradnju i zajedničke zahteve bezbednosti za pružaoce ključnih usluga i pružaoce digitalnih usluga.Kao prvi korak u tom pravcu prepoznato je usvajanje nacionalne strategije za bezbednost mrežnih i informacionih sistema u kojoj bi se odredili strateški ciljevi i konkretna politička aktivnost koju treba preduzeti.

Usvajanje NIS Direktive doprinelo je poboljšanju kapaciteta sajber bezbednosti na nivou država članica jer se od njih zahtevalo donošenje nacionalnih strategija i imenovanje tela zaduženog za sajber bezbednost. Takođe, unapređena je saradnja između država članica uspostavljanjem različitih foruma za olakšavanje razmene strateških i operativnih informacija. Što je još važnije, povećana je otpornost na sajber rizike javnih i privatnih subjekata u sedam ključnih sektora (energetika, saobraćaj, bankarstvo, infrastruktura finansijskog tržišta, zdravstvo, snabdevanje vodom za piće i digitalna infrastruktura) i u primeni tri digitalne usluge (internet tržišta, pretraživači interneta i usluge računarstva u oblaku) jer se od država članica zahtevalo da obezbede da pružaoci ključnih usluga i pružaoci digitalnih usluga utvrde zahteve sajber bezbednosti i prijavljuju incidente.

Ipak, evaluacijom funkcionisanja NIS Direktive za potrebe procenenjenog učinka, utvrđeni su određeni problemi, prvenstveno nizak nivo sajber otpornosti preduzeća koja posluju u EU, a potom i neujednačena otpornost u državama članicama i sektorima i nizak nivo informisanosti o stanju, odnosno nedostatak zajedničkog odgovora na krizu. Naime, Komisija je analizirajući relevantnost NIS Direktive, njenu dodatu vrednost, usklađenost, delotvornost i učinkovitost, zaključila sledeće: a) područje primene NIS Direktive je ograničeno u pogledu obuhvaćenih sektora, s obzirom na to da se poslednjih godina povećala digitalizacija i stepen međupovezanosti, usled čega Direktiva ne obuhvata sve digitalizovane sektore koji pružaju ključne usluge ekonomiji i društvu u celini; b) nedovoljno je jasno da li se Direktiva odnosi i na pružaoce ključnih usluga, jer njene odredbe ne daju jasnu sliku o nacionalnoj nadležnosti nad pružaocima digitalnih usluga, usled čega pojedini subjekti nisu obuhvaćeni obavezom uvođenja mera bezbednosti i obavezom prijavljivanja incidenata; c) državama je ostavljeno preširoko diskreciono pravo prilikom utvrđivanja zahteva bezbednosti i izveštavanja o incidentima za pružaoce ključnih usluga, što je dovelo da različitog postupanja u pojedinim državama članicama; d) sistem nadzora i sprovođenja Direktive NIS nije efikasan; e) razlikuju se finansijski i ljudski resursi a time i stepen zrelosti u

postupanju sa rizicima sajber bezbednosti i otpornosti između država članica; f) ne postoji sistemski mehanizam za razmenu informacija između država članica, što negativno utiče na efikasnost mera sajber bezbednosti.

Zbog toga je Evropski parlament u rezoluciji od 12. marta 2019. Pozvao Komisiju da proceni da li je potrebno dodatno proširiti područje primene NIS Direktive na druge kritične sektore i usluge koji nisu obuhvaćeni posebnim zakonodavstvom.[3] Sredinom 2020. Evropska komisija je među strateškim prioritetima za bezbednost Unije na prvom mestu navela stvaranje bezbednog okruženja otpornog na promene u budućnosti, pre svega u vidu zaštite i otpornosti kritične infrastrukture, odnosno sajber bezbednosti.[4] U tom pravcu su bili predviđeni sledeći koraci: usvajanje odgovarajućih propisa o zaštiti i otpornosti kritične infrastrukture, revizija Direktive o mrežnim i informacionim sistemima i usvajanje strategije za sajber bezbednost. Tokom 2020. Komisija je iznela predlog nove Strategije za sajber bezbednost, kao ključne komponente Strategije oblikovanja digitalne budućnostiUnije,[5]predlog Plana za obnovu Unije[6] i predlog Strategije za bezbednost Unije.[7]Takođe, u cilju jačanja fizičke i sajber otpornosti kritičnih entiteta i mreža Komisija je iznela predlog Direktive o merama za visoki zajednički nivo sajber bezbednosti u Uniji (revidirana NIS Direktiva) i predlog nove Direktive o otpornosti kritičnih entiteta.[8]Savet EU je pozdravio planove Komisije da obezbedi doslednu primenu pravila za tržišne operatere i omogući bezbednu, pouzdanu i prikladnu razmenu informacija o pretnjama i incidentima, između ostalog i kroz reviziju NIS Direktive, te da se na taj način doprinese-

[3] European Parliament resolution of 12 March 2019 on security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them (2019/2575(RSP)), https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.html.

[4] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy COM/2020/605 final, 24.7.2020, https://eur-lex.europa.eu/legal content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605#

[5]Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, 16.12.2020 JOIN(2020) 18 final, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164.

[6]Recovery Plan for Europe, https://ec.europa.eu/info/strategy/recovery-plan-europe_en.

[7]Communication from the Commission on the EU Security Union Strategy, 24.7.2020 COM(2020) 605 final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&from=EN.

[8] Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities, 16.12.2020, https://ec.europa.eu/home-affairs/system/files/2020-12/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf.

poboljšanju sajber otpornosti i delotvornije odgovori na sajber napade.

3. REVIZIJA NIS DIREKTIVE

Direktivom bi se države članice obavezale da: (a) usvoje nacionalnu strategiju za sajber bezbednost i da imenuju nadležne organe, jedinstvene kontaktne tačke i CSIRT-ove; (b) propišu obaveze upravljanja rizicima sajber bezbednosti i izveštavanja o njima za ključne subjekte koji su navedeni u Prilogi I i važne subjekte koji su navedeni u Prilogu II; (c) razmenjuju informacije o sajber bezbednosti. Direktiva bi se primenjivala na određene javne ili privatne ključne subjekte koji posluju u sektorima koji su navedeni u Prilogu I (energetika, saobraćaj, bankarstvo, infrastruktura finansijskog tržišta, zdravstvo, voda za piće, otpadne vode, digitalna infrastruktura, javna uprava i svemir) i određene važne subjekte koji posluju u sektorima koji su navedeni u Prilogu II (poštanske i kurirske usluge, upravljanje otpadom, izrada, proizvodnja i distribucija hemikalija, proizvodnja, prerada i distribucija hrane, proizvodnja i pružaoci digitalnih usluga). Mikrosubjekti i mali subjekti u smislu Preporuke Komisije 2003/361/EZ od 6. maja 2003. bili bi izuzeti iz područja primene Direktive, osim pružalaca mreža elektronske komunikacije ili javno dostupnih usluga elektronske komunikacije, pružalaca usluga poverenja, registara naziva domena i javnih Uprava.

Tako se u članovovima 5-11 predloga Direktive utvrđuje nacionalni okvir za sajber bezbednost. U tom smislu od država članica bi se zahtevalo da usvoje nacionalnu strategiju za sajber bezbednost, kojom bi se utvrdili strateški ciljevi i odgovarajuće mere politike i regulatorne mere radi postizanja i održavanja visokog nivoa sajber bezbednosti. Direktivom bi se uspostavio i okvir za koordinisano otkrivanje ranjivosti, pa bi se od država članica zahtevalo da imenuju CSIRT-ove koji bi delovali kao pouzdani posrednici i time olakšali interakciju između subjekata koji podležu obavezi obaveštavanja i proizvođača ili pružalaca proizvoda i usluga informaciono- komunikacione tehnologije. Takođe, ENISA bi se obavezala da razvije i vodi evropski registar ranjivosti za otkrivene ranjivosti. Pored toga, od država se očekuje da uspostave nacionalne okvire za upravljanje sajber krizama, između ostalog i kroz imenovanje nadležnih organa koji bi bili odgovorni za upravljanje sajber incidentima i sajber krizama velikih razmera. Takođe, države bi se obavezale da imenuju jedan ili više organa koji bi bio nadležan za sajber bezbednost a koji bi vršio nadzor u skladu sa

članovima 28-34 Direktive, kao i jedinstvenu kontaktnu tačku za sajber bezbednost, koja bi vršila funkciju povezivanja kako bi se omogućila prekogranična saradnja između nadležnih organa drugih država članica.

U pogledu obaveze upravljanja rizicima sajber bezbednosti i izveštavanja o njima (članovi 17-23) od država članica bi se zahtevalo da propišu da upravljačka tela svih subjekata koji su obuhvaćeni područjem primene Direktive odobravaju mere upravljanja rizicima sajber bezbednosti koje bi preduzimali odgovarajući subjekti, kao i da učestvuju u posebnom osposobljavanju o sajber bezbednosti. Obaveza odobravanje mera podrazumeva osmišljavanje i primenu odgovarajućih i srazmernih tehničkih i organizacionih mera za upravljanje rizicima sajber bezbednosti koji prete bezbednosti mrežnih i informacionih sistema. Takođe, ovi subjekti bili bi dužni da obaveštavaju nacionalne nadležne organe ili CSIRT-ove o svakom značajnijem sajber incidentu usmerenom protiv usluge koju pružaju.

U predlogu Direktive se insistira na prekograničnoj saradnji (članovi 12-16). Naime, predviđa se osnivanje grupe za saradnju u svrhu podsticanja i olakšavanja strateške saradnje i razmene informacija između država članica, kao i unapređenja međusobnog poverenja. Zbog toga bi se formirala mreža CSIRT-ova, u cilju olakšanja i ubrzanja operativne saradnje, kao i Evropska mreža organizacija za vezu za sajber krize (EU-CyCLONe), radi pružanja podrške koordinisanom upravljanju sajber incidentima i sajber krizama velikih razmera i obezbeđenja redovne razmene informacija između država članica i institucija EU. Takođe, ENISA bi se obavezala da u saradnji sa Komisijom izdaje dvogodišnje izveštaje o stanju sajber bezbednosti u Uniji. Što se tiče razmene informacija (čl. 26-27) predviđa se da bi države članice utvrđivale pravila po kojima se subjektima omogućava da učestvuju u razmeni u okviru posebnih mehanizama razmene informacija o sajber bezbednosti u skladu sa članom 101 UFEU. Osim toga, države članice bi mogle da omoguće i subjektima koji nisu obuhvaćeni područjem primene Direktive da dobrovoljno prijavljuju ozbiljne incidente, sajber pretnje ili izbegnute incidente.

4. ZAKLJUČAK

Uprkos značajnim dostignućima, NIS Direktiva ima određena ograničenja, kako je to analiza njene primene pokazala. Naime, s ubrzanom digitalnom transformacijom društva proširen je pejzaž pretnji i novih

izazova, što zahteva prilagođen i inovativni odgovor država. Upravo zbog toga je predlog revidirane NIS Direktive usmeren ka prevazilaženju prepreka postojećeg legislativnog okvira i iznalaženju odgovarajućeg odgovora s ciljem podizanja nivoa sajber bezbednosti u Uniji. Naime, i pored postojećih mera na nivou Unije i na nacionalnom nivou koje imaju za cilj da podrže zaštitu kritičnih infrastruktura u Uniji, subjekti koji upravljaju tom infrastrukturom nisu uvek adekvatno opremljeni za rešavanje trenutnih i očekivanih budućih rizika za njihovo poslovanje koji mogu dovesti do poremećaja u pružanju usluga koje su neophodne za obavljanje vitalnih društvenih funkcija ili ekonomskih aktivnosti. Ovo je posledica dinamičnog pejzaža pretnji sa evoluirajućim hibridnim i terorističkim pretnjama i rastućom međuzavisnošću između infrastruktura i sektora, kao i povećanim fizičkim rizikom usled prirodnih katastrofa i klimatskih promena. Štaviše, relevantni sektori i tipovi subjekata nisu dosledno prepoznati kao kritični u svim državama članicama, a na nivou Unije ne postoji jedinstvena lista sektora kritične infrastrukture. Umesto toga, različiti pravni akti pokrivaju različite sektore. Pri tome, određene kritične infrastrukture imaju panevropsku dimenziju, kao što su Evropska organizacija za bezbednost vazdušne plovidbe, Eurocontrol i Union's Global Satellite Navigation System, Galileo. Pored toga, subjekti uključeni u pružanje osnovnih usluga podležu različitim zahtevima nametnutim zakonima država članica. Činjenica da neke države članice imaju manje stroge bezbednosne zahteve za ove subjekte ne samo da stvara različite nivoe otpornosti, već i negativno utiče na održavanje vitalnih društvenih funkcija ili ekonomskih aktivnosti širom Unije, i dovodi do nelojalne konkurencije i prepreka za pravilno funkcionisanje unutrašnjeg tržišta. Slični tipovi entiteta se smatraju kritičnim u nekim državama članicama, ali ne u drugim, a oni koji su identifikovani kao kritični podležu različitim zahtevima u različitim državama članicama. Ovo rezultira dodatnim i nepotrebnim administrativnim opterećenjem za kompanije koje posluju preko granica, posebno za kompanije aktivne u državama članicama sa strožijim zahtevima. Revizijom NIS Direktive, novi okvir Unije će stoga imati efekat izjednačavanja uslova za kritične subjekte širom Unije što će doprineti povećanom stepenu zaštite informacione kritične infrastrukture.

Reference

1. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the

assessment of the need to improve their protection, Official Journal of the European Union L 345/75, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008L0114&from=hr

2. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the European Union L 194/1, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=HR

3. European Parliament resolution of 12 March 2019 on security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them (2019/2575(RSP)), https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.html

4. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy COM/2020/605 final, 24.7.2020, https://eur-lex.europa.eu/legal content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605#

5. Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, 16.12.2020 JOIN(2020)18 final, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164.

6.Recovery Plan for Europe, https://ec.europa.eu/info/strategy/recovery-plan-europe_en.

7. Communication from the Commission on the EU Security Union Strategy, 24.7.2020 COM (2020) 605 final, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&from=EN.

8. Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities, 16.12.2020, https://ec.europa.eu/home-affairs/system/files/2020-12/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf

LEGAL REGULATION OF INFORMATION CRITICAL INFRASTRUCTURE SECURITY

Tatjana Bugarski
The Faculty of Law, University in Novi Sad
t.bugarski@pf.uns.ac.rs

Milana Pisarić
The Faculty of Law, University in Novi Sad
Correspondence: mpisaric@pf.uns.ac.rs; Tel.: +381-21-485-3073

Abstract: Network and information systems and services, as an information critical infrastructure, play a significant role in modern society, so their reliability and security are important for key social and economic activities. However, their existence and proper functioning are threatened by certain security risks in cyberspace, which are of increasing size, frequency, and impact. Thus, these systems may become the target of cyberattacks, i.e. unauthorized actions that are taken with the intention of causing damage and/or interrupting their functioning. Consequently, such incidents may jeopardize social and economic activities, which depend on information-critical infrastructure. That is why it is necessary to pay attention to cyber security. In doing so, risk management in cyberspace must be such as not to jeopardize legal certainty. In that sense, the way in which the guidelines for cyber security risk assessment are prescribed is extremely important. A good example of regulation is the European Union Directive on the Security of Network and Information Systems (NIS Directive). The Directive stipulates that certain organizations are obliged to take appropriate and proportionate security measures and to identify, assess and take into account the cyber security risks they face, in order to prevent and minimize interference with the provision of services. The aim of the Directive is to ensure that information critical infrastructure is protected from disruptions that could affect key economic and social activities by prescribing such obligations. The subject of this paper is the analysis of the protection and information obligations

that the NIS Directive prescribes for digital service providers, as well as the analysis of the proposed revision of the Directive.

Keywords: information critical infrastructure, cyber security, data security, risk management, NIS Directive.