Rəqəmsal Media Ekosistemində Kibertəhlükəsizlik: Qlobal Təhdidlər və Azərbaycanın Müasir Media Mühitində Təhlükəsizlik Strategiyaları

Surə Seyid
Naxçıvan Dövlət Universiteti, Naxçıvan, Azərbaycan
seyidsura@ndu.edu.az

***Xülasə*— Məqalədə rəqəmsal media platformalarında baş verən kibertəhdidlərin tipologiyası, onların cəmiyyətə və milli təhlükəsizliyə təsiri təhlil edilir. Araşdırmada Azərbaycan Respublikasında fəaliyyət göstərən internet media resurslarının kibermüdafiə səviyyəsi, "Media haqqında" yeni qanunun gətirdiyi tənzimləmələr və informasiya müharibəsi şəraitində kibertəhlükəsizliyin rolu araşdırılır. Tədqiqatın nəticələri rəqəmsal savadlılığın və texnoloji infrastrukturun təkmilləşdirilməsinin vacibliyini ortaya qoyur.**

Açar sözlər— rəqəmsal media; kibertəhlükəsizlik; internet mediası; dezinformasiya; deepfake.

I. GİRİŞ

İnformasiya texnologiyalarının sürətli inkişafı kütləvi kommunikasiya vasitələrinin rəqəmsal platformalara keçidini qaçılmaz etmişdir. Bu gün rəqəmsal media həm fərdi ünsiyyətin, həm də dövlət-vətəndaş münasibətlərinin mərkəzində dayanır. Lakin bu keçid yeni təhlükəsizlik risklərinin meydana çıxmasına səbəb olmuşdur. Kibertəhlükəsizlik rəqəmsal mediada yalnız məlumatların şifrələnməsi deyil, həm də informasiyanın manipulyasiyadan qorunması prosesi kimi başa düşülməlidir [1]. Müasir dövrdə rəqəmsal media fərdlərin və institutların əsas ünsiyyət vasitəsinə çevrilmişdir. Lakin bu platformaların mərkəzləşdirilməmiş strukturu onları kiberhücumların əsas hədəflərindən birinə çevirir. Azərbaycan kontekstində bu məsələ xüsusi əhəmiyyət kəsb edir. Ölkənin geosiyasi mövqeyi, Vətən müharibəsi və ondan sonrakı bərpa prosesi dövründə informasiya məkanına edilən kiberhücumlar bu sahədə kompleks müdafiə strategiyasının hazırlanmasını zəruriləşdirmişdir.

Rəqəmsal media ekosistemində kibertəhdidlərin tipologiyasına nəzər saldıqda qeyd etmək lazımdır ki, müasir kiberhücumlar mürəkkəb və çoxşaxəli struktura malikdir. Rəqəmsal mediada qarşılaşılan əsas təhdidləri aşağıdakı kimi qruplaşdırmaq olar (Cədvəl I):

- Sosial mühəndislik və fişinq (phishing): Media işçilərinin və istifadəçilərin etibarından istifadə edərək şifrələrin və konfidensial məlumatların ələ keçirilməsi.
- DDoS hücumları: İnternet media resurslarının (xəbər portallarının) serverlərinə həddindən artıq sorğu göndərməklə onları fəaliyyətsiz qoymaq.
- Məlumat sızması (data breach): İstifadəçi bazalarının oğurlanaraq qara bazarda satılması və ya şantaj məqsədilə istifadə edilməsi.
- Alqoritmik manipulyasiya: Sosial media alqoritmlərindən istifadə edərək saxta xəbərlərin (fake news) süni şəkildə trendə çevrilməsi [2].

CƏDVƏL I. RƏQƏMSAL MEDİA MÜHİTİNDƏ ƏSAS KİBERTƏHDİDLƏRİN NÖVLƏRİ VƏ ONLARIN MEDİA SEKTORUNA TƏSİRİ

Təhdid Növü	Cari Göstərici (2025-2026)	Media və kommunikasiya sahəsinə təsiri
Süni İntellekt (Sİ) əsaslı Fişinq	Qlobal kiberhücumların 42%-i agent tipli fərdiləşdirilmiş Sİ fişinqi ilə reallaşır.	Media işçilərinin korporativ hesablarının ələ keçirilməsi və saxta xəbər sızıntısı.
Deepfake və Sintetik Media	İnformasiya müharibələrində deepfake hücumlarının ümumi payı 10%-ə çatıb.	Reputasiyanın məqsədli şəkildə zədələnməsi, saxta bəyanatlar və ictimai rəyin manipulyasiyası.
Ransomware (Fidyə proqramları)	2026 proqnozlarına görə qlobal zərər 74 milyard dollar təşkil edir.	Yayım və media holdinqlərinin infrastrukturunun dondurulması, verilənlər bazalarının şifrələnməsi.
DDoS Hücumları	Layer 7 (tətbiq səviyyəli) hücumlarında illik 25% artım.	Xəbər saytlarının və onlayn yayım platformalarının kritik anlarda çökdürülməsi.

II. AZƏRBAYCANIN RƏQƏMSAL MEDİA MÜHİTİ VƏ KİBERTƏHLÜKƏSİZLİK SƏVİYYƏSİ

Azərbaycan Respublikasının informasiya təhlükəsizliyi siyasəti dövlət, ictimai və fərdi informasiya ehtiyatlarının qorunmasından, habelə informasiya sahəsində milli maraqların müdafiəsinə yönəlmiş tədbirlər kompleksinin həyata keçirilməsindən ibarətdir. Ölkəmizin informasiya sahəsində təhlükəsizliyinin təmin olunması üçün ölkədə informasiyanın, həmçinin dövlət informasiya ehtiyatlarının müdafiəsi sahəsində milli sistem və informasiya infrastrukturu inkişaf etdirilir və möhkəmləndirilir. Son illər informasiya-kommunikasiya texnologiyalarının (İKT) inkişaf etdirilməsi istiqamətində bir çox mühüm tədbirlər görülmüşdür. Bu kontekstdən yanaşdıqda informasiya təhlükəsizliyi sahəsində vahid dövlət siyasətinin təkmilləşdirilməsi və informasiya təhlükəsizliyinin texnoloji infrastruktur komponentlərinin yaradılması istiqamətində aparılan məqsədyönlü işlərin araşdırılması internet medianın kompleks tədqiqində zəruridir [3]. Azərbaycanda rəqəmsal media sürətlə inkişaf etsə də, təhlükəsizlik standartları bütün

DOI: 10.25045/forensic.gov.2026.81

resurslar üçün eyni səviyyədə deyil.

Texniki infrastruktur problemləri - Bir çox yerli xəbər portalları hələ də köhnəlmiş məzmunun idarəetmə sistemi (Content Management System – CMS) platformalarından istifadə edir. Bu, onların kiberhücumlar qarşısında zəif qalmasına səbəb olur. Xüsusilə regional media resurslarında SSL sertifikatlarının və müasir təhlükəsizlik divarı (firewall) sistemlərinin çatışmazlığı müşahidə olunur.

Dezinformasiya və informasiya müharibəsi - Azərbaycan internet media resursları mütəmadi olaraq xarici kiber-qrupların hədəfinə çevrilir. 2020-ci il II Qarabağ Müharibəsi dövründə dövlət saytlarına və media orqanlarına qarşı edilən hücumlar göstərdi ki, kibertəhlükəsizlik birbaşa milli təhlükəsizlik komponentidir. Bu dövrdə deepfake texnologiyası vasitəsilə hazırlanmış saxta videoların yayılması cəmiyyətdə çaşqınlıq və informasiya xaosu yaratmağa yönəlmişdi [4]. Azərbaycan Respublikasında kibertəhlükəsizliyin hüquqi bazası son illərdə əhəmiyyətli dərəcədə təkmilləşdirilmişdir.

- "Media haqqında" Azərbaycan Respublikasının Qanunu [5]: Bu qanun media subyektlərinin informasiya məkanında məsuliyyətini, o cümlədən dezinformasiyanın qarşısının alınması və istifadəçi hüquqlarının qorunması mexanizmlərini müəyyən edir.
- İnformasiya təhlükəsizliyi üzrə dövlət proqramı: Ölkə daxilində kritik informasiya infrastrukturunun qorunması üçün vahid mərkəzin (Kibertəhlükəsizlik Mərkəzi) fəaliyyətini stimullaşdırır [6].
- Azərbaycan Respublikası Prezidentinin müvafiq sərəncamları ilə təsdiq edilmiş "2025–2028-ci illər üçün Süni İntellekt Strategiyası" və "2023–2027-ci illər üçün İnformasiya Təhlükəsizliyi və Kibertəhlükəsizlik Strategiyası" bu sahədəki rəsmi inkişafın əsas sütunlarıdır [7].

"Oxford Insights" beynəlxalq tədqiqat mərkəzinin "Hökumətin Süni İntellektə Hazırlıq İndeksi" (Government AI Readiness Index) hesabatının son məlumatlarına əsasən, Azərbaycan dünyada ən kəskin və müsbət sıçrayış edən ölkə olmuşdur (Cədvəl II):

CƏDVƏL II. AZƏRBAYCANIN SÜNİ İNTELLEKTƏ HAZIRLIQ İNDEKSİ ÜZRƏ GÖSTƏRİCİLƏRİNİN DİNAMİKASI (2024–2026)

Göstərici/ Metrika	**Əvvəlki Dövr (2024)**	**Cari Göstərici (2025-2026)**	**Dinamika/ Dəyişiklik**
Qlobal Reytinq Sırası	111-ci yer	70-ci yer	+41 pillə irəliləyiş (Qlobalda ən sürətli artım)
Azərbaycanın Ümumi Balı	39.92 bal	48.96 bal	+9.04 bal artım
Cənubi və Mərkəzi Asiya Regionu (Orta bal)	-	41.40 bal	Azərbaycan regional ortalamanı xeyli üstələyir.
Cənubi Qafqazda Mövqeyi	-	I yer (BƏƏ: 32, Qazaxıstan: 51, Türkiyə: 56, Gürcüstan: 63, Ermənistan: 95)	Azərbaycan region lideridir.

Hüquqi tənzimləmə tərəfindən media subyektlərinə tələblər, onların rəqəmsal təhlükəsizlik auditindən keçməsini və jurnalistlərin kiber-gigiyena qaydalarına riayət etməsini nəzərdə tutur.

III. RƏQƏMSAL SAVADLILIQ VƏ KİBERTƏHLÜKƏSİZLİK

Kibertəhlükəsizlik zəncirinin ən zəif həlqəsi hər zaman insan amilidir. Wilson qeyd edir ki, rəqəmsal savadlılıq kiber-qalxan rolunu oynayır [8].

Azərbaycan media işçiləri üçün aşağıdakı kiber təhlükəsizlik qaydaları tətbiq edilməlidir:

- Çoxfaktorlu autentifikasiya: Bütün sosial media və idarəetmə panellərində tətbiq olunmalıdır.
- Mənbənin yoxlanılması: Gələn şübhəli keçidlərin və sənədlərin sandbox mühitində açılması.
- Kriptoqrafik alətlər: Həssas məlumatların ötürülməsi zamanı şifrələnmiş kommunikasiya kanallarından (Signal, ProtonMail və s.) istifadə.

İnformasiya texnologiyalarının gündəlik həyatın bütün sferalarına inteqrasiyası rəqəmsal mühitdə təhlükəsizlik məsələsini aktuallaşdırıb. Ənənəvi kibertəhlükəsizlik yanaşmaları daha çox texniki infrastrukturun qorunmasına yönəlsə də, statistik göstəricilər kiberhücumların böyük əksəriyyətinin (təxminən 90%-dən çoxunun) insan amili və rəqəmsal savadsızlıq səbəbindən uğurla nəticələndiyini göstərir. Rəqəmsal savadlılıq sadəcə texnoloji cihazlardan istifadə bacarığı deyil, həm də rəqəmsal məlumatın kritik qiymətləndirilməsi və risklərin idarə edilməsidir. Kibertəhlükəsizlik kontekstində bu anlayış aşağıdakı kompetensiyaları əhatə edir:

- İnformasiya gigiyenası: Şübhəli keçidlərin (links), naməlum loq fayllarının və dezinformasiyanın ayırd edilməsi.
- Verilənlərin qorunması: Güclü autentifikasiya üsullarının (məsələn, 2FA) tətbiqi və fərdi məlumatların məxfiliyinin təmini.
- Sosial mühəndislik fərqindəliyi: Psixologiyaya əsaslanan kiber-fırıldaqçılıq üsullarını tanıma bacarığı.

Müasir kiberhücumlar texniki boşluqlardan (vulnerabilities) daha çox, insanın "zəif nöqtələrinə" fokuslanır. Fişinq (phishing), vishing (səsli fırıldaqçılıq) və saxta proqram təminatları rəqəmsal savadlılıq səviyyəsi aşağı olan istifadəçiləri hədəf alır. Tədqiqatlar göstərir ki, mürəkkəb antivirus proqramlarından istifadə edən, lakin rəqəmsal savadlılığı zəif olan istifadəçi, hər hansı təhlükəsizlik aləti olmayan rəqəmsal savadlı istifadəçidən daha çox risk altındadır. Rəqəmsal savadlılıq müasir dövrdə kibertəhlükəsizliyin "insan qalxanı" rolunu oynayır. Texniki müdafiə sistemləri nə qədər mükəmməl olsa da, istifadəçinin şüurlu davranışı olmadan tam təhlükəsizlik mümkün deyildir.

IV. SÜNİ İNTELLEKT VƏ KİBERTƏHLÜKƏSİZLİYİN GƏLƏCƏYİ

Süni intellekt rəqəmsal mediada həm təhdid, həm də müdafiə vasitəsidir. Azərbaycanın rəqəmsal media resursları gələcəkdə kiberhücumları öncədən proqnozlaşdıran süni intellekt əsaslı

monitorinq sistemlərini tətbiq etməlidir. Digər tərəfdən, Sİ vasitəsilə hazırlanan dezinformasiyaların (synthetic media) aşkarlanması üçün yerli alqoritmlərin hazırlanması zəruridir.

Ənənəvi kibertəhlükəsizlik sistemləri əvvəlcədən müəyyən edilmiş qaydalara və "imzalara" (signature-based) əsaslanır. Lakin kiberhücumların dinamikası və mürəkkəbliyi artıq bu statik müdafiə mexanizmlərini üstələyir. Süni İntellekt, xüsusilə onun alt sahələri olan Maşın təlimi və Dərin təlim (Deep Learning), böyük həcmli verilənləri (Big Data) real vaxt rejimində analiz etmək qabiliyyəti ilə bu boşluğu doldurur.

Sİ kibermüdafiədə tətbiqi əsasən üç istiqamətdə qruplaşdırılır:

- Anomaliyaların aşkarlanması: Sİ sistemləri şəbəkə daxilindəki normal istifadəçi davranışlarını öyrənir. Hər hansı bir kənarlaşma (məsələn, qeyri-adi saatda böyük həcmli məlumat ötürülməsi) baş verdikdə sistem saniyələr ərzində xəbərdarlıq edir.
- Avtomatlaşdırılmış cavab tədbirləri: İnsanın müdaxiləsi olmadan, Süni İntellekt hücuma məruz qalan seqmenti izolyasiya edə və ya zərərli trafiki bloklaya bilər.
- Proqnozlaşdırıcı analitika: Keçmiş hücum verilənlərinə əsaslanaraq, gələcəkdə baş verə biləcək potensial zəif nöqtələri müəyyən edir.

Təəssüf ki, süni intellekt yalnız müdafiəçilər üçün deyil, hücumçular üçün də geniş imkanlar açır. Gələcəyin əsas kiber-təhdidləri sırasına aşağıdakılar daxildir:

- Süni intellekt tərəfindən idarə olunan Fişinq (Phishing): Sİ hədəf şəxsin sosial media yazılarını analiz edərək, onun dil üslubuna tam uyğun, hiper-fərdiləşdirilmiş və inandırıcı saxta elektron məktublar hazırlaya bilir.
- Adversarial Machine Learning (Rəqib maşın təlimi): Hakerlər müdafiə sistemindəki Sİ modelini "yanıltmaq" üçün ona xüsusi manipulyasiya olunmuş məlumatlar daxil edirlər. Bu, sistemin zərərli proqramı "təhlükəsiz" kimi qəbul etməsinə səbəb olur.
- Deepfake Texnologiyaları: Korporativ casusluqda rəhbər şəxslərin səs və ya görüntüsünün saxtalaşdırılması vasitəsilə maliyyə fırıldaqçılığı.

Azərbaycanın rəqəmsal ekosistemi qlobal kiber-təhdidlərdən sığortalanmayıb. Media resurslarının və dövlət informasiya sistemlərinin qorunmasında Sİ əsaslı həllərin tətbiqi milli təhlükəsizlik prioritetinə çevrilməlidir. Xüsusilə, dezinformasiya və saxta xəbərlər (fake news) kampaniyalarına qarşı Sİ-nin monitorinq imkanlarından istifadə olunması kritik əhəmiyyət kəsb edir.

Kibertəhlükəsizliyin gələcəyi "Süni İntellekt Sİ-yə qarşı" mübarizəsi üzərində qurulacaqdır. Müdafiə tərəfi mütləq şəkildə hücumçulardan daha sürətli öyrənən və adaptasiya olan

rəqəmsal savadlılığın vəhdətindən ibarət olmalıdır. Gələcək tədqiqatlar süni intellektin kiber-müdafiə sistemlərinə inteqrasiyasına fokuslanmalıdır.

alqoritmlər inkişaf etdirməlidir. Sİ-nin etik və hüquqi çərçivədə tətbiqi, həmçinin beynəlxalq əməkdaşlıq rəqəmsal dünyada dayanıqlığın təmin edilməsi üçün yeganə çıxış yoludur.

NƏTİCƏ

Tədqiqatlar göstərir ki, Azərbaycanın rəqəmsal media sahəsində kibertəhlükəsizlik məsələləri kompleks yanaşma tələb edir və bu sahədə konkret addımlar atılır. Mövcud vəziyyəti yaxşılaşdırmaq üçün Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi tabeliyində İnnovasiya və Rəqəmsal İnkişaf Agentliyi İsrailin texnologiya üzrə nüfuzlu ali təhsil müəssisəsi – "Technion" İnstitutu ilə birgə Azərbaycan Kibertəhlükəsizlik Mərkəzini təsis edib.

"PASHA Holding" Şirkətlər Qrupunun dəstəyi ilə ölkənin kibertəhlükəsizlik imkanlarını gücləndirmək məqsədilə yaradılan mərkəz bu sahədə yüksəkixtisaslı mütəxəssis və təlimçilərin yetişdirilməsində əsas mərkəz rolunu oynayır. 2023-cü il 28 mart tarixində fəaliyyətə başlayan Azərbaycan Kibertəhlükəsizlik Mərkəzində 3 il ərzində 1000-dən çox şəxsə təlim verilmişdir. Eyni zamanda mərkəzdə 15 təlimçinin yetişdirilməsi sayəsində gələcəkdə ölkəmizdə kibertəhlükəsizlik sahəsində mütəxəssislərin hazırlanması geniş vüsət alacaq.

Kibertəhlükəsizlik sahəsində regionda lider ölkələrdən hesab edilən İsrailin peşəkar müəllim heyəti Azərbaycana gələrək təlim iştirakçılarını ən son kibertəhlükəsizlik təhdidlərini, tendensiyaları və ən yaxşı təcrübələri əhatə edən bilik və bacarıqlarla təmin edirlər.

Mərkəzdə ən müasir texnologiya və avadanlıqlarla təchiz olunmuş sinif otaqları, təlim otaqları, simulyasiya otaqları və laboratoriyalar yaradılıb. Tələbələr həmin laboratoriyalarda tədqiqat aparır, müxtəlif kibertəhlükəsizlik məhsulları yaradırlar. [9].

Bütün bu tədbirlərlə yanaşı, rəqəmsal media ekosistemində kibertəhlükəsizlik aşağıdakı tədbirlərin həyata keçirilməsini zəruri edir:

- Vahid Media Cloud Sistemi: Yerli xəbər portallarının daha təhlükəsiz, dövlət tərəfindən qorunan bulud serverlərinə köçürülməsi.
- Mütəmadi təlimlər: Jurnalistlər və redaktorlar üçün rəqəmsal təhlükəsizlik üzrə davamlı seminarların təşkili.
- Hüquqi nəzarətin gücləndirilməsi: İstifadəçi məlumatlarının sızmasına görə media subyektlərinin məsuliyyətinin artırılması.
- Beynəlxalq əməkdaşlıq: Qlobal kiber-təhdidlərə qarşı beynəlxalq monitorinq mərkəzləri ilə inteqrasiya.

Beləliklə, rəqəmsal mediada kibertəhlükəsizliyin təmin edilməsi multidissiplinar yanaşma tələb edir. Bu proses texniki həllər, hüquqi tənzimləmə (məsələn, GDPR qaydaları) və fərdi

Azərbaycanda yaxın illərdə həyata keçirilməsi nəzərdə tutulan əsas strateji istiqamətlər Cədvəl III-də təqdim edilmişdir.

CƏDVƏL III. AZƏRBAYCANDA RƏQƏMSAL MEDİA VƏ KİBERTƏHLÜKƏSİZLİK ÜZRƏ PERSPEKTİV İNKİŞAF İSTİQAMƏTLƏRİ

İnkişaf sahəsi	Strategiya və gözlənilən nəticə
Proaktiv Kiber-Müdafiə	Hücumların hələ baş vermədən qarşısının alınması üçün ETX və XRİTDX tərəfindən **Sİ əsaslı insident təhlili sistemlərinə** tam keçid.
Milli Dil Modelləri (LLM)	Azərbaycan dili üçün kiber-maarifləndirmə və dezinformasiya ilə mübarizə apara bilən yerli süni intellekt botlarının və süzgəclərinin yaradılması.
İnsan Kapitalı və Kadrlaşma	Ali təhsil müəssisələrində "Süni İntellekt Təhlükəsizliyi" və "Kiber-Analitika" üzrə yeni ixtisaslaşma proqramlarının dövlət dəstəyi ilə genişləndirilməsi.
Milli Kiber-Dayanıqlıq	Kritik infrastruktur (enerji, su, nəqliyyat, bank) obyektlərində Sİ sistemlərinin tətbiqi zamanı informasiya təhlükəsizliyi risklərinin icbari audit rejiminin tətbiqi.

Cədvəllərdəki məlumatlar 2025–2026-cı illərin qlobal kibertəhlükəsizlik hesabatlarına (SentinelOne, CDNetworks), həmçinin Azərbaycan Respublikası Rəqəmsal İnkişaf və Nəqliyyat Nazirliyi yanında Elektron Təhlükəsizlik Xidmətinin 6 may 2026-cı il tarixli məlumatında təqdim edilən və e-Governance Academy tərəfindən hesablanan National Cyber Security Index (NCSI) göstəricilərinə əsaslanır [10].

ƏDƏBİYYAT

[1] J. Anderson, K. Lee, M. Chen, Digital media and cybersecurity: A comprehensive guide. Academic Press, 2021, 350 p.

[2] R. Smith. Information security in the digital age. Springer Nature, 2022, 280 p.

[3] S. Seyid. Internet media and information security issues in Azerbaijan // Journal of Preschool and Primary Education. Special issue, 2025, p. 83-97. DOI: 10.30546/2709-2488.2025.5025.

[4] T. Brown, L. Jones. The rise of deepfakes: Cyber threats in the age of AI. Journal of Cyber Policy. 2023, Vol. 8(2), p. 145–162. DOI: 10.1080/23738871.2023.2189011.

[5] Media haqqında Azərbaycan Respublikasının Qanunu. https://e-qanun.az/framework/49124

[6] https://mincom.gov.az/az/layiheler/azerbaycan-kibertehlukesizlik-merkezi.

[7] https://crocusoft.com/az/Blog/Details/kiberthluksizlik-strategiyalar.

[8] United Nations Office on Drugs and Crime. Comprehensive study on cybercrime. UN Publications, 2020, 312 p.

[9] S.Wilson Digital literacy as a shield against cyber attacks. Communication and Media Studies. 2020, Vol. 5(1), p. 34-48.

[10] e-Governance Academy Foundation. National Cyber Security Index (NCSI): Azerbaijan. https://ncsi.ega.ee/country/az/

Global Threats and Security Strategies in Azerbaijan's Modern Media Environment

Sura Seyid

Nakhchivan State University, Nakhchivan, Azerbaijan

seyidsura@ndu.edu.az

Abstract- This research paper analyzes the typology of cyber threats occurring on digital media platforms and their impact on society and national security. The article examines the level of cyber defense of internet media resources operating in the Republic of Azerbaijan, the regulations introduced by the new Law "On Media," and the role of cyber-hygiene in the context of information warfare. The results of the study reveal the vital importance of improving digital literacy and technological infrastructure.

Keywords- digital media; cybersecurity; internet media; disinformation; deepfake.