سال دهم/ زمستان ۱۴۰۰

زورگویی سایبری: تعریف، تاریخچه و گونه شناسی

• سید امیر قاسم تبار[۱]، سید عبدالله قاسم‌تبار[۲]، عاطفه سهرابی[۳]

DOR: 20.1001.1.38552322.1400.10.41.16.1

چکیده

علی‌رغم تأثیرات گسترده زورگیری سایبری، هنوز درباره تعریف و ماهیت آن اتفاق‌نظر وجود ندارد. هدف پژوهش حاضر ارائه تعریف، تاریخچه و گونه‌شناسی زورگویی سایبری است. روش پژوهش حاضر از نوع اسنادی است. جامعه پژوهشی تمامی منابع نوشتاری (چاپی/الکترونیکی) بین‌المللی در زمینه زورگویی سایبری بود که از طریق پایگاه‌های اطلاعاتی خارجی قابل بازیابی و دسترسی بودند. بدین منظور با استفاده از روش نمونه‌برداری نظری و پس از بررسی و تحلیل منابع گردآوری‌شده از جامعه اسناد موجود، از میان منابعی (کتاب‌ها، اسناد و مقالات) که از معیارهای ورود برخوردار بودند، به‌عنوان نمونه پژوهشی انتخاب شدند. برای تحلیل اسناد از روش فیش‌برداری الکترونیکی استفاده شد. پس از بررسی و تحلیل منابع، روند تحول و شکل‌گیری مفهوم زورگویی سایبری تعریف شد و دوازده شکل آن (آزار و اذیت سایبری، بدنام کردن، بازی سیلی خندان، اغفال سایبری، عصبانی کردن یا آتشی شدن، کمین سایبری، ظاهرسازی یا جعل هویت، حیله‌گری، افشاگری، کت فیشینگ، محرومیت یا طرد و زورگیری جنسی سایبری) شناسایی، تعریف و مفهوم‌پردازی شد. مطالعه حاضر توانست درباره ماهیت و روش‌های زورگیری سایبری برای نهادهای اجرایی و مؤثر در قانون‌گذاری در زمینه پیشگیری از وقوع جرم اطلاعات فراهم سازد. همچنین این اطلاعات برای روان‌شناسان، متخصصان تعلیم و تربیت و جامعه‌شناسان علاقه‌مند به پژوهش در حوزه زورگویی سایبری نیز می‌تواند بسیار مفید باشد.

واژگان کلیدی: زورگویی سایبری، زورگیری جنسی سایبری، اغفال سایبری، قلدری آنلاین، کت فیشینگ

---

۱ استادیار گروه علوم‌تربیتی، دانشگاه فرهنگیان، تهران، ایران؛ Ghasemtabar.e@gmail.com
۲ استادیار گروه تکنولوژی آموزشی دانشگاه خوارزمی، تهران، ایران؛ ghasemtabar@khu.ac.ir
۳ کارشناسی علوم سیاسی، دانشگاه خوارزمی، تهران، ایران؛ Atefehsohrabi712@yahoo.com

مقدمه

به دنبال رشد و پیشرفت فناوری اطلاعات و ارتباطات، اینترنت و فضای سایبری[۱] محملی برای تعاملات اجتماعی نوجوانان شده است و به آن‌ها امکان می‌دهد بدون نظارت و محدودیت‌های اعمال‌شده از سوی بزرگسالان، و همچنین تا حدودی ناشناختگی[۲] (ناشناس ماندن)، دست به رفتارهای پرخطر از جمله زورگیری سایبری[۳] (آنلاین[۴]/ الکترونیکی[۵]) بزنند (Ang, 2015). زورگویی سایبری یعنی زورگویی از طریق اشکال الکترونیکی ارتباط مانند ایمیل، تلفن همراه، اتاق گفتگو[۶]، پیام‌رسانی فوری[۷]، و وب سایت‌ها (Olweus & Limber, 2018). پژوهش‌های متعددی شیوع زورگیری سایبری را بین کودکان و نوجوانان مورد مطالعه قراردادند که به علت تفاوت بین پژوهش‌ها در تعریف زورگیری سایبری، روش‌شناسی پژوهش، ویژگی‌های جمعیت‌شناختی نمونه پژوهشی و ابزارهای گردآوری، میزان شیوع زورگیری سایبری به‌شدت متغیر اعلام‌شده است. برای مثال بررسی ۱۵۹ مطالعه انجام‌شده در خصوص شیوع زورگیری سایبری نشان داد که میزان قربانیان زورگیری سایبری بین ۱ تا ۶۱/۱ درصد و ارتکاب به زورگیری بین ۳ تا ۳۹ درصد متغیر است (Brochado, Soares & Fraga, 2017). مطالعه بین‌المللی EU Kids Online بین سال‌های ۲۰۱۹-۲۰۱۷ بین ۲۵۱۰۱ دانش‌آموز ۹ تا ۱۶ ساله ۱۹ کشور اروپایی نشان داد که بین ۷ (اسلواکی) تا ۴۰ درصد (لهستان) کودکان قربانی زورگویی سایبری بودند و در بیشتر کشورها بیش از ۲۰ درصد از کودکان آن را تجربه کردند (Smahel & et al, 2020).

مطالعات طولی انجام شده حاکی از آن است که نرخ شیوع زورگیری سایبری بین کودکان و نوجوانان در حال افزایش است. مهم‌ترین دلیل آن افزایش استفاده از اینترنت و ابزارهای فناورانه بین آن‌هاست (Kowalski, Limber & McCord, 2019; Sengupta & Chaudhuri, 2011; Mesch, 2009). مطالعه انجام شده در ایران (شش‌جوانی، ۱۳۹۶) نیز نشان داد ۶۶/۳ درصد از کودکان ۱۲ تا ۱۴ سال و ۸۹/۳ درصد از کودکان ۱۵ تا ۱۷ سال از اینترنت استفاده می‌کنند. این مطالعه همچنین نشان داد ۷۴/۸ درصد از کودکان ۱۲ تا ۱۴ سال و ۹۳/۳ درصد از کودکان ۱۵ تا

---

1 Cyber space
2 anonymity
3 Cyberbullying
4 Offline cyberbullying
5 Electronic cyberbullying
6 chat room
7 instant messaging

۱۷ سال از تلفن همراه استفاده می‌کنند. این آمارها لزوم بررسی دقیق و علمی زورگیری سایبری را که یکی از جدی‌ترین آسیب‌های فضای مجازی برای کودکان است، مطرح می‌کند. پژوهشگران تأکید می‌کنند هرچند زورگیری سایبری یک بزه مجازی است، اما پیامدهای منفی واقعی دارد (Rao, Bansal & Chandran, 2018). از مهم‌ترین تأثیرات منفی زورگیری سایبری بر کودکان قربانی می‌توان به اضطراب (Fahy, 2016)، افسردگی (Hamm & et al, 2015; Spears, Taddeo, Daly, Stretton & Karklins, 2015)، افکار خودکشی (Young, Subramanian, Miles, Hinnant & Andsager, 2017; Messias, Kindrick & Castro, 2014)، مشکلات روان‌شناختی درون‌سازی‌شده و برون‌سازی‌شده[1] (Waasdorp & Bradshaw, 2015)، ناامیدی (Cassidy, Faucher & Jackson, 2017)، کاهش سطح سلامت‌روانی (Bannink & et al, 2014)، کاهش عزت‌نفس (Cénat & et al, 2014; Patchin & Hinduja, 2010)، کاهش روابط اجتماعی (Crosslin & Golman, 2014; Festl & Quandt, 2013)، نرفتن به مدرسه (Frey, Pearson & Cohen, 2015; Raskauskas & Stoltz, 2007) و افت تحصیلی (Patchin & Hinduja, 2006) اشاره داشت.

علی‌رغم پیامدهای منفی بلندمدت و گسترده زورگیری سایبری، هنوز درباره تعریف و ماهیت آن اتفاق‌نظر وجود ندارد و پژوهشگران به شیوه‌های متفاوتی به مفهوم‌پردازی آن پرداختند (Kowalski & et al, 2019; Limber & et al, 2018). این امر موجب شد تا درباره انواع زورگویی سایبری نیز دیدگاه متعددی مطرح شود و هر یک به شیوه‌های متفاوتی آن را طبقه‌بندی کنند (Langos & Sarre, 2015; Chan & et al, 2012; Pyżalski, 2012; Bauman, 2011; Li, 2007; Willard, 2005). از طرفی پدیده زورگویی سایبری در ایران کاملاً ناشناخته بود. در پایگاه‌های علمی داخلی هیچ مطالعه‌ای پدیده زورگویی سایبری را به‌صورت نظری یا تجربی بررسی نکرده بود. ازاین‌رو، با توجه به خلاء پژوهشی موجود در این زمینه در کشور و همچنین وجود دیدگاه-های نظری متفاوت و گاهی متضاد درباره چیستی، ماهیت و گونه شناسی زورگویی سایبری در بین پژوهشگران و صاحب‌نظران، هدف در پژوهش حاضر آن بود تا ضمن ارائه تعریف، تاریخچه و گونه شناسی زورگویی سایبری، توجه پژوهشگران داخلی را نسبت به این پدید نوظهور که طبق یافته‌های به‌دست‌آمده از مطالعات تجربی دارای پیامدها و تأثیرات منفی متعددی است و همچنین شیوع آن نیز روزبه‌روز در حال افزایش است، جلب کند.

---

1 Externalizing/Internalizing

روش

پژوهش حاضر ازنظر هدف پژوهشی کاربردی، ازنظر نوع داده‌ها پژوهشی کیفی و ازنظر نحوه اجرا یک پژوهش اسنادی (سندکاوی[1]) است. روش اسنادی، روشی کیفی است که پژوهشگر تلاش می‌کند تا با استفاده نظام‌مند از داده‌های اسنادی به کشف، استخراج، طبقه‌بندی و ارزیابی مطالب مرتبط با موضوع پژوهش خود اقدام کند (صادقی‌فسایی و عرفانمنش، ۱۳۸۴).

جامعه پژوهشی تمامی منابع نوشتاری (چاپی/الکترونیکی) بین‌المللی در زمینه زورگویی سایبری بودند که از طریق پایگاه‌های اطلاعاتی خارجی[2] قابل بازیابی و دسترسی بودند. برای جستجو و یافتن مطالعات و منابع مرتبط با موضوع پژوهش، از کلیدواژه‌های متعددی استفاده شد. به‌منظور گردآوری منابع درباره تاریخچه و تعریف زورگویی سایبری از کلیدواژه‌های متعددی استفاده شد.[3] همچنین با توجه به اینکه یکی از اهداف اصلی مطالعه حاضر گونه شناسی زورگویی سایبری بود، بدین منظور از کلیدواژه‌های[4] مرتبط با آن استفاده شد.

برای انتخاب نمونه از بین منابع و اسناد موجود از روش نمونه‌برداری نظری[5] که یکی از روش‌های اصلی نمونه‌برداری در روش اسنادی است (صادقی فسایی و عرفانمنش، ۱۳۸۴)، استفاده شد. پس از بررسی و تحلیل منابع گردآوری‌شده از جامعه اسناد اشاره‌شده، ۷۲ مدرک (کتب، اسناد و مقالات) به‌عنوان نمونه پژوهشی انتخاب شدند. معیارهای ورود (در انتخاب نمونه) عبارت‌اند بودند از حیطه جغرافیایی: سراسر دنیا؛ زبان منابع: انگلیسی؛ سال انتشار: بین سال‌های ۲۰۲۰-۲۰۰۰؛ نوع سند: تمامی منابع دست‌اول و دوم در خصوص نظریه‌ها، دیدگاه‌ها، رویکردها و پژوهش‌های نظری و مروری در زمینه زورگویی سایبری که در یک مجله و یا کتاب معتبر به چاپ رسیده‌اند و دارای متن کامل بودند.

---

1 Documentary Research Method

۲همچون Science Direct، Google scholar، Springer، Taylor & Francis، SAGE، Wiley، ProQuest

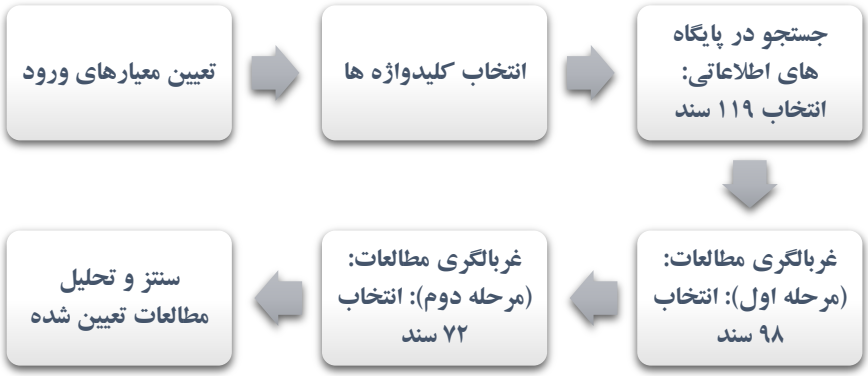
3 cyberbullying, online cyberbullying, electronic cyberbullying, cyber threats, cyber-aggression, bullying in students, cyber harassment, online harassment, cyberbullying define, nature of cyberbullying, cyberbullying assessment.

4 cyberbullying typology, cyberbullying types, cyberbullying forms, sexting, sextortion impersonation, trickery, outing, catfishing, exclusion, ostracism, sexual cyberbullying, text attack, harassment, denigration, happy slapping, cyber grooming, flaming, cyber stalking, masquerading, phishing, identity theft.

5 Theoretical sampling

برای اطمینان از اینکه پژوهش‌هایی که در مرحله جستجو شناسایی و انتخاب شده بودند (۱۱۹ پژوهش)، از معیارهای ورود می‌باشند، در یک فرایند غربالگری دومرحله‌ای[1]، داوری و گزینش شدند. بدین‌صورت که ابتدا چکیده گزارش پژوهش‌های انتخاب‌شده بررسی و در مرحله بعد، از بین پژوهش‌های باقی‌مانده (۹۸ پژوهش)، جهت بررسی دقیق‌تر و عمیق‌تر، متن کامل پژوهش‌ها مورد مداقه قرار گرفت. پس از اتمام مرحله غربالگری، ۷۲ پژوهش برای تحلیل باقی ماند. در شکل ۱ مراحل انجام پژوهش نشان داده شد.

روش تحلیل منابع: برای تحلیل اسناد از روش فیش‌برداری الکترونیکی که از یکی از روش‌های تحلیل و بررسی منابع در پژوهش اسنادی است (صادقی فسایی و عرفانمنش، ۱۳۸۴) استفاده شد. فیش‌برداری به معنای استخراج عبارت، جمله یا پاراگرافی از یک متن و نوشتن آن در فیش مطالعه است (صادقی فسایی و عرفانمنش، ۱۳۸۴).



شکل ۱. مراحل انجام پژوهش

یافته‌ها

یافته‌های این پژوهش در چهار بخش اصلی ارائه شد. این چهار بخش که توضیحات آن در ذیل تشریح شد عبارت‌اند از: ۱- تاریخچه و روند شکل‌گیری مفهوم زورگیری سایبری، ۲- تعریف و مفهوم‌شناسی زورگیری سایبری، ۳- مقایسه زورگویی سایبری با دیگر مفاهیم مرتبط، ۴- گونه‌شناسی زورگیری سایبری.

---

1 Two stage screening

تاریخچه و روند شکل‌گیری مفهوم زورگیری سایبری

واژه «زورگویی» ترجمه واژه «bullying» است[۱]. «bullying» در اصل یک واژه آنگلوساکسون[۲] و یا اروپای شمالی است و ترجمه‌ای از واژه سوئدی «mobbning» است که اولین بار توسط یک پزشک مدرسه به نام هینیمن[۳] (۱۹۷۲) استفاده شد. «mobbning» یک اصطلاح کردارشناختی است که برای توصیف حمله جمعیِ گروهی از حیوانات به حیوانی از گونه دیگر که معمولاً بزرگ‌تر است و دشمن طبیعی گروه است، به‌کار می‌رود (Olweus, 2013). پس‌ازآن دان الویوس (Dan Olweus) روانشناس سوئدی آن را در کتاب «پرخاشگری در مدرسه[۴]» (۱۹۷۳) (به سوئدی forskning om skolmobbning) به کار گرفت و پس از انتشار این کتاب، مطالعه علمی پدیده زورگیری آغاز شد (Smith & Monks, 2008). مطالعه علمی زورگویی بیشتر توسط روانشناسان تحولی[۵] و برخی جامعه‌شناسان صورت گرفته است (Smith, 2019).

اما اصطلاح زورگیری سایبری ابتدا در مقاله‌ای در روزنامه نیویورک‌تایمز[۶] در سال ۱۹۹۵ تحت عنوان «اعتیاد سایبری[۷]» مورد استفاده قرار گرفت. بااین‌حال، رواج و استفاده گسترده این اصطلاح در سال ۲۰۰۳ و پس از راه‌اندازی وبسایت زورگویی سایبری (www.cyberbullying.ca) توسط بیل بلسی (Bill Belsey) آغاز شد. به همین علت بسیاری از پژوهشگران، بلسی را مبدع این اصطلاح می‌شناسند (Bauman, 2014). درواقع مطالعه علمی زورگیری سایبری پس از راه‌اندازی این وبسایت آغاز شد (Bauman & Bellmore, 2015) و از آن زمان پژوهش درباره زورگیری سایبری به‌ویژه از سوی پژوهشگران رشته‌هایی مانند رسانه و ارتباطات، فناوری اطلاعات و مطالعات حقوقی[۸] روزبه‌روز افزایش یافت (Smith, 2019). واژه زورگیری سایبری برگرفته از واژه فضای سایبری[۹] است که اولین بار توسط ویلیام گیبسون (William Gibson) کانادایی، نویسنده داستان‌های تخیلی به کار گرفته شد (Smith, 2014).

۱واژه «bullying» در منابع فارسی به «قلدری» نیز ترجمه‌شده است. ازاین‌جهت می‌توان «cyberbullying» را به «قلدری سایبری» نیز ترجمه کرد.

2 Anglo-Saxon
3 Heinemann,
4 Aggression in school
5 developmental psychologists
6 New York Times
7 Cyber addiction
8 legal studies
9 Cyberspace

تعریف و مفهوم شناسی زورگیری سایبری

علی‌رغم انجام مطالعات گسترده درباره زورگیری سایبری، هنوز درباره ماهیت، مفهوم و تعریف این پدیده نوظهور بین پژوهشگران اتفاق‌نظر وجود ندارد و تعاریف متعدد و متفاوتی از آن ارائه شد (Olweus & Limber, 2018; Patchin & Hinduja, 2015; Slonje, Smith & Frisén, 2013; Smith, 2014). گروهی از پژوهشگران معتقدند که زورگیری سایبری (آنلاین یا الکترونیکی) شکل جدیدی از زورگیری سنتی[1] (آفلاین[2] یا حضوری[3]) است (Smith, 2019; Wolke, Lee & Guy, 2017; Slonje & Smith, 2008). بنابراین باید براساس ویژگی‌های مهم زورگیری سنتی آن را تعریف کرد. رایج‌ترین و پذیرفته‌ترین تعریف از زورگیری سنتی، تعریفی است که الویوس (۱۹۹۳) از آن ارائه داد: «زمانی که یک دانش‌آموز به‌طور مکرر و در گذر زمان[4] با اعمال منفی[5] یک یا چند نفر دیگر مواجه می‌شود، [می‌توان گفت] آن دانش‌آموز مورد زورگویی قرارگرفته است یا قربانی شده است».

پژوهشگران براساس این تعریف سه مشخصه را برای زورگیری تعیین کرده‌اند که عبارت‌اند از ۱) تکرار[6]، ۲) هدفمندی[7] (قصد آسیب زدن[8])، و ۳) نابرابری قدرت[9]. در بسیاری از مطالعات، با پذیرش این تعریف از زورگویی سنتی و در نظر گرفتن زورگویی سایبری به‌عنوان شکلی از زورگویی سنتی، زورگویی سایبری این‌گونه تعریف شد: «عملی است پرخاشگرانه و عمدی که توسط یک گروه یا فرد با استفاده از اشکال الکترونیکی ارتباط، به‌طور مکرر و در گذر زمان علیه یک قربانی که به‌آسانی نمی‌تواند از خود دفاع کند، انجام می‌شود» (Slonje & Smith, 2008).

در مقابل، گروه دیگری از پژوهشگران بر ویژگی‌های منحصربه‌فرد و خاص زورگویی سایبری به‌ویژه دو ویژگی ناشناختگی[10] و عمومیت[11] تأکید می‌کنند (Thomas, Connor & Scott, 2015; Betts, 2016). ویژگی ناشناختگی به این اشاره دارد که برخلاف زورگویی سنتی که هدف یا قربانی از هویت فرد زورگو مطلع است، در زورگویی سایبری، هویت فرد مهاجم ممکن

---

1 Traditional bullying
2 offline bullying
3 in-person bullying
4 over time
5 negative actions
6 repetition
7 Intentionality
8 Intent to Harm
9 Imbalance of Power
10 anonymity
11 publicity

است برای قربانی ناشناس باقی بماند. منظور از ویژگی عمومیت نیز این است که برخلاف زورگویی سنتی که در آن تعداد شاهد[1] یا تماشاگر[2] معمولاً بسیار معدود است، در زورگویی سنتی، فناوری این امکان را فراهم می‌سازد تا افراد بسیار زیادی از سراسر جهان شاهد یا تماشاگر عمل منفی فرد مهاجم باشند. این گروه از پژوهشگران معتقدند که نمی‌توان براساس معیارهای زورگیری سنتی آن را تعریف کرد.

بااین‌حال می‌توان با پذیرش این تفاوت‌ها، از معیارهای سه‌گانه زورگیری سنتی برای تعریف زورگیری سایبری استفاده کرد (Smith, 2019). در ادامه ضمن توصیف این سه معیار، به تفاوت هر یک از معیارها در زورگویی سنتی و سایبری اشاره می‌شود و در نهایت یک تعریف از زورگویی سایبری ارائه می‌شود.

۱- هدفمندی: معیار هدفمندی به این موضوع اشاره دارد که تنها عمل یا رفتاری را می‌توان زورگویی نامید که به‌قصد آسیب زدن به دیگری انجام می‌شود. بنابراین اعمالی که بدون قصد آسیب زدن و به شکل «اتفاقی[3]» رخ می‌دهد و یا هدف از انجام آن تنها «سرگرمی[4]» است را نمی‌توان زورگویی دانست. معیار هدفمندی مهم‌ترین معیار برای تعیین رفتار زورگویی سنتی و سایبری است (Smith & et al, 2013; Menesini, Nocentini & Calussi, 2011). اما اینکه چگونه می‌توان درباره عمدی بودن یا نبودن یک رفتار قضاوت کرد، یکی از مهم‌ترین چالش‌های پیشروی پژوهشگران در تعریف زورگویی است. چگونه می‌توان عمدی بودن یا نبود یک رفتار را مشخص کرد؟؛ معیار تعیین آسیب چیست؟: آیا باید از نگاه فرد زورگو یعنی «قصد آسیب رساندن» رفتار را قضاوت کرد یا از نگاه قربانی یعنی «احساس آسیب»؟. اسمیت و همکاران (۲۰۱۳) برای قضاوت درباره اینکه آیا یک عمل به‌قصد آسیب زدن به دیگری صورت گرفت یا نه، سه شاخص تعیین کردند که در صورت وجود هر سه ویژگی، می‌توان گفت آن رفتار به‌قصد آسیب انجام شد: ۱- قربانی، آسیب را تجربه کند؛ ۲- هدف فرد زورگو، تنها رفتار نیست بلکه آسیب است؛ ۳- یک فرد عاقل پیش‌بینی کند که چنانچه آن رفتار رخ دهد احتمالاً باعث آسیب به فرد موردنظر (قربانی) می‌شود.

۲) تکرار: تکرار، معمولاً به‌عنوان یکی از معیارهای تعریف‌کننده زورگویی در نظر گرفته می‌شود. معیار تکرار به این معنا است که در زورگویی، رفتار یا عمل منفی بیش از یک‌بار اتفاق

---

1 Witness
2 bystander
3 accidental
4 fun

میافتد. بنابراین اعمال یا رفتاری که تنها یک‌بار[1] رخ می‌دهند را نمی‌توان زورگویی نامید. بااین‌حال، درباره معیار تکرار بین صاحب‌نظران حوزه زورگویی اتفاق‌نظر وجود ندارد. الویوس (۲۰۱۳) اشاره می‌کند که تکرار، یک معیار ضروری برای زورگویی نیست و دلیل استفاده از معیار تکرار در تعریف زورگویی این است که نشان می‌دهد رفتار و اعمال فرد مرتکب، به شکل تصادفی اتفاق نیفتاده است و به‌احتمال‌زیاد آن اعمال منفی به‌قصد آسیب انجام‌شده‌اند. درواقع معیار تکرار با معیار هدفمندی در ارتباط است. تکرار شدن یک عمل مضر یا آسیب‌زا به‌وضوح نشان از این واقعیت دارد که آسیب وارد شده توسط فرد مهاجم، عمدی بوده است (Smith & et al, 2013). ازاین‌رو، الویوس (۲۰۱۳) معیار «نسبتاً تکراری[2]» را پیشنهاد می‌دهد. در ویرایش جدید پرسشنامه زورگویی الویوس نسخه نروژی نیز، از عبارت «این موارد ممکن است به‌طور مکرر اتفاق بیفتد» یا «معمولاً تکرار می‌شوند» استفاده شد.

معیار تکرار در زورگویی سایبری ماهیت پیچیده‌تری دارد. یک عمل زورگویی ممکن است براساس نوع فناوری استفاده‌شده، به‌سرعت گسترش یابد و از کنترل اولیه خارج شود. برای مثال عکسی که تنها یک‌بار توسط شخص زورگو در فضای مجازی منتشر می‌شود، ممکن است توسط بسیاری از افراد دیده شود و یا توسط دیگران برای سایر افراد به اشتراک گذاشته شود و بدین شکل فرد قربانی بارها و بارها به خاطر این رفتار زورگو، آسیب بینند. بنابراین از منظر یک قربانی زورگویی سایبری، نیازی نیست تا یک رفتار از سوی فرد زورگو بارها و بارها تکرار شود. اسلانج و همکاران (۲۰۱۳) معتقدند که اگر رفتار یا عمل منفی از سوی همان فرد مهاجم، تکرار نشود، نمی‌توان آن را زورگویی نامید. بااین‌حال دیگر محققان (Ybarra, Boyd, Korchmaros & Oppenheim, 2012) بر این باورند همان‌طور که نوشتن یک شایعه روی یک دیوار از سوی فرد مهاجم علیه یک قربانی، می‌تواند مصداق یک زورگویی سنتی باشد، بارگذاری یک عکس و یا قراردادن یک شایعه در فضای مجازی و به اشتراک گذاشتن آن توسط دیگران نیز نوعی زورگویی سایبری است.

افزون بر موارد اشاره‌شده، می‌توان براساس میزان آسیب نیز، درباره معیار تکرار، قضاوت کرد. چنانچه در ادامه و در بخش روش‌ها یا اَشکال زورگویی سایبری خواهیم دید، زورگویی سایبری دارای اَشکال متعددی است که میزان آسیب هر یک از آن‌ها بر قربانی متفاوت است

---

1 one-off
2 Some Repetitiveness

(Langos, 2014). برای مثال تجربه تنها یک‌بار «زورگیری جنسی سایبری[1]» می‌تواند تأثیرات منفی زیادی بر قربانی داشته باشد اما تجربه تنها یک‌بار «محرومیت[2] یا طرد[3]» ممکن است نتواند آسیب‌های جدی برای فرد قربانی به دنبال داشته باشد. بر این اساس، می‌توان گفت که معیار تکرار برای آن نوع از زورگیری سایبری که باعث آسیب جدی به قربانی می‌شود ضروری است، اما برای نوع ملایم‌تر زورگیری سایبری، تکرار یک معیار ضروری برای تعریف زورگیری سایبری نیست. با توجه به‌تمامی نکاتی که درباره معیار تکرار گفته شد، می‌توان این‌گونه نتیجه‌گیری کرد که تکرار، یک معیار اصلی[4] در تعریف زورگیری سایبری نیست بلکه یک معیار فرعی[5] است (Smith & et al, 2013).

۳) نابرابری قدرت: معیار نابرابری در قدرت به این موضوع اشاره دارد که زورگویی سنتی یا سایبری، زمانی اتفاق می‌افتد که یک شخص که به‌نوعی از فرد قربانی قدرتمندتر است یا توانایی بیشتری دارد، قربانی را هدف قرار می‌دهد و به او حمله می‌کند (Vaillancourt & et al, 2008). بنابراین نبرد یا درگیری بین دو یا چند نفر که از هر لحاظ دارای قدرت و توانایی‌های برابری هستند را نمی‌توان زورگویی نامید و باید آن را پرخاشگری نامید (Smith & et al, 2013). (تفاوت زورگویی سایبری با پرخاشگری سایبری در بخشی مجزا موردبحث قرار گرفت). نابرابری قدرت هم در زورگویی سنتی و هم در زورگویی سنتی یک معیار اصلی است و بدون نابرابری قدرت نمی‌توان رفتاری را زورگویی تعریف نمود. اما شیوه‌ها یا منابع نابرابری قدرت در بین دو نوع زورگویی سنتی و سایبری با یکدیگر متفاوت است (Menesini & et al, 2013; Langos, 2014). در مجموع می‌توان شش منبع نابرابری قدرت را در زورگویی سنتی مطرح کرد که عبارت‌اند از ۱- ضعیف‌تر بودن به لحاظ جسمی؛ ۲- ضعیف‌تر بودن ازنظر کلامی؛ ۳- نداشتن عزت‌نفس؛ ۴- در اقلیت بودن یا عضویت در گروه‌های حاشیه‌ای (ازنظر جنسیت، نژاد، مذهب، یا ناتوانی)؛ ۵- نداشتن دوستان یا حمایت اجتماعی؛ ۶- داشتن موقعیت پایین یا طرد شدن از سوی همسالان (Smith & et al, 2013).

در زورگویی سایبری ویژگی‌ها یا شاخص‌های نابرابری قدرت تا حدود بسیار زیادی متفاوت است. گروهی از پژوهشگران معتقدند که داشتن مهارت و سواد بالاتر در زمینه فناوری اطلاعات

---

1 Sexual cyberbullying
2 Exclusion
3 Ostracism
4 Core criteria
5 subsidiary criteria

و ارتباطات یکی از شاخص‌های اصلی نابرابری قدرت در زورگیری سایبری است (Smith & et al, 2013; Vandebosch & Van Cleemput, 2008; Ybarra & Mitchell, 2004). نشان داده شد افرادی که اقدام به زورگویی سایبری می‌کنند خود را ازنظر دانش و مهارت در زمینه فناوری‌ها، بهتر از دیگران می‌دانند (Ybarra & Mitchell, 2004). با این‌حال، این ویژگی همیشه نمی‌تواند معیاری برای نابرابری قدرت باشد چراکه برای ارتکاب به زورگویی سایبری همیشه داشتن مهارت در فناوری‌ها الزامی نیست. مطالعه نوسنتینی و همکاران (۲۰۱۰) نشان داد که مهارت در زمینه استفاده از فناوری‌ها، تنها برای نوع یا شیوه‌های پیچیده‌تر زورگویی سایبری مانند جعل هویت مورد نیاز است.

گروه دیگری از پژوهشگران پیشنهاد می‌دهند که نابرابری قدرت در فضای سایبری می‌تواند براساس پایگاه اجتماعی[1] بالاتر مهاجم یا فرد زورگو در اجتماع سایبری[2] تعریف شود (Hinduja & Patchin, 2008). بعضی از پژوهشگران نیز بر این باروند که ناشناختگی به نابرابری قدرت در زورگویی سایبری کمک می‌کند (Vandebosch & Van Cleemput, 2008). همان‌طور که پیش‌تر اشاره شد منظور از ناشناختگی این است که در زورگویی سایبری، هویت فرد مهاجم ممکن است برای قربانی ناشناس باقی بماند که البته در غالب موارد این‌گونه است (Smith, 2012). درصورتی‌که قربانی از هویت فرد مهاجم یا زورگو مطلع باشد، شهامت تلافی کردن یا دفاع از خود را نخواهند داشت و احتمال کمتری وجود دارد که واکنش اثربخشی از خود نشان دهد. در این صورت می‌توان گفت در صورت مشخص بودن هویت فرد مهاجم برای قربانی، تمامی ویژگی‌ها یا منابع نابرابری قدرت در زورگویی سنتی، برای زورگویی سایبری نیز صادق است (Smith & et al, 2013).

احساس درماندگی در قربانی به علت ناتوانی او در جلوگیری از رفتار منفی فرد مهاجم، یکی دیگر از جنبه‌های نابرابری قدرت در زورگویی سایبری است (Dooley, Pyzalski & Cross, 2009). برخلاف زورگویی سنتی، در زورگویی‌های مبتنی بر فناوری، فرد قربانی عملاً هیچ کنترلی بر زورگویی ندارد. از این منظر، نابرابری قدرت در زورگویی سایبری بیانگر ویژگی‌ها فرد مهاجم نیست بلکه بیشتر ناتوانی یا نبود قدرت در هدف موردنظر یا قربانی است (Dooley & et al, 2009). فرد مهاجم می‌تواند در هر زمان و هر مکانی به رفتار منفی خود علیه قربانی ادامه دهد. از طرفی، تعداد شاهدان در فضای مجازی به‌طور بالقوه بسیار بالاتر از شاهدان در زورگویی

---

1 social status
2 virtual community

سنتی است؛ شاهدانی که ممکن است هویت بسیاری از آن‌ها برای قربانی، ناشناس باشد (Langos, 2014). دراین‌ارتباط نشان داده شد ازنظر نوجوانان، آن نوع از زورگویی سایبری که شامل تعداد زیادی از شاهدان است شدیدترین نوع زورگویی سایبری است (پ(Slonje & Smith, 2008) که از این نوع زورگویی در ادبیات پژوهشی به «زورگویی جمعی[1]» و «زورگویی چندگانه[2]» نام‌برده می‌شود (Smith & et al, 2010). این عوامل باعث می‌شوند تا قربانی خود را در فرار یا رهایی از رفتارهای منفی فرد مهاجم درمانده ببیند. در واقع این جنبه از نابرابری قدرت ناشی از یکی از ویژگی منحصربه‌فرد زورگویی سایبری یعنی عمومی بودن زورگویی سایبری است که براساس طبقه‌بندی لانگوز (۲۰۱۲) در شکل غیرمستقیم زورگویی سایبری اتفاق میافتد.

طبق آنچه گفته شد، ویژگی‌ها یا شاخص‌های نابرابری قدرت در زورگویی سایبری عبارت‌اند از: مهارت و سواد در زمینه فناوری اطلاعات و ارتباطات، ناشناختگی، پایگاه اجتماعی در فضای سایبری، احساس درماندگی در رهایی از زورگیری. در صورت مشخص بودن هویت فرد مهاجم برای قربانی، تمامی شاخص‌های نابرابری قدرت در زورگویی سنتی، برای زورگیری سایبری نیز صادق خواهد بود. بنابراین می‌توان نتیجه گرفت هرچند شاخص‌ها یا ویژگی‌های نابرابری قدرت در زورگیری سنتی و سایبری با یکدیگر تا حدود زیاد متفاوت می‌باشند، اما در هر دو شکل زورگویی، نابرابری قدرت به‌عنوان یک ویژگی اصلی وجود دارد و زمانی اتفاق میافتد که شخصی که به‌نوعی از قدرت بیشتری برخوردار است، فرد دیگری که قدرت کمتری دارد را هدف قرار می‌دهد و باعث احساس ناتوانی قدرت در قربانی می‌شود و دفاع از خود را برای قربانی مشکل می‌سازد.

براساس تعاریف ارائه شده و همچنین با توجه به ویژگی‌ها یا معیارهای تکرار، هدفمندی و عدم تعادل قدرت و همچنین دو ویژگی ناشناختگی و عمومیت که مختص زورگویی سایبری است می‌توان زورگیری سایبری را اینگونه تعریف نمود: زورگیری سایبری عمل یا رفتاری است که با قصد قبلی توسط یک یا گروهی از افراد از طریق ابزارهای فناوری اطلاعات و ارتباطات (مانند رایانه خانگی، لپ‌تاپ، تبلت، گوشی هوشمند) و با استفاده از رسانه‌ها (مانند وب‌گاه‌های شخصی، نشریات برخط یا وبلاگ‌ها، رایانامه، بازی‌های برخط)، پیام‌رسان‌ها (مانند تلگرام، واتساپ) و شبکه‌های اجتماعی (مانند فیس‌بوک، یوتیوب، اینستاگرام، اتاق‌های گفتگو)، برای آزار و اذیت،

---

1 mass bullying
2 multiple bullying

ارعاب، تهدید، توهین، شرمساری و خجالت و یا سوءاستفاده از یک فرد ضعیف‌تری که به‌راحتی قادر به دفاع از خود نیست، انجام می‌شود. طبق تعریف ارائه شده، می‌توان هفت ویژگی برای زورگویی سایبری ارائه داد: ۱) تنها اعمالی که به‌قصد آسیب زدن به دیگری انجام می‌شوند را می‌توان مصداق زورگویی سایبری دانست؛ ۲) تکرار عمل یا رفتار تنها یک ویژگی فرعی در زورگویی سایبری است. قصد یا نیت فرد مرتکب، قضاوت فرد قربانی و دیگران درباره شدت آسیب، و نوع زورگویی (مستقیم یا غیرمستقیم بودن) را می‌توان مهم‌ترین معیارهای قضاوت در نظر گرفت؛ ۳) عدم تعادل قدرت یا نابرابری قدرت یک ویژگی مهم و تعریف‌کننده در زورگویی سایبری است؛ ۴) هویت فرد زورگو می‌تواند برای قربانی ناشناس باشد یا نباشد؛ ۵) زورگویی سایبری، به‌قصد آسیب به یک هدف یا قربانی مشخص یا از پیش تعیین‌شده، رخ می‌دهد؛ ۶) زورگویی سایبری از طریق سکوها یا ابزارهای متعدد فناوری اطلاعات و ارتباطات و با استفاده از رسانه‌ها، پیام‌رسان‌ها و شبکه‌های اجتماعی رخ می‌دهد؛ ۷) زورگویی سایبری دارای اشکال یا شیوه‌های متعددی است. (توضیحات آن در بخش اَشکال زورگویی سایبری ارائه شد).

زورگویی سایبری در مقایسه با زورگویی سنتی

براساس تعاریف و همچنین مهم‌ترین ویژگی‌های زورگویی سنتی و سایبری، می‌توان دریافت که علی‌رغم شباهت‌های موجود بین آن‌ها، زورگویی سایبری دارای ویژگی‌های منحصربه‌فردی است که آن را از زورگویی سنتی متمایز می‌سازد. در این ارتباط اسمیت (۲۰۱۲) معتقد است که زورگویی سایبری از هفت ویژگی منحصربه‌فرد برخوردار است که آن را از زورگویی سنتی متمایز می‌سازد. این هفت ویژگی عبارت‌اند از: ۱- زورگویی سایبری تا حدودی مستلزم داشتن تخصص در فناوری است؛ ۲- زورگویی سایبری در درجه اول غیرمستقیم است نه چهره به چهره، بنابراین فرد مرتکب یا زورگو ممکن است ناشناس باشد؛ ۳- معمولاً در زورگویی سایبری، فرد زورگو حداقل برای زمانی کوتاه واکنش قربانی را نمی‌بیند؛ ۴- تنوع نقش‌های فرد تماشاگر (شاهد) در حمله سایبری از بیشتر زورگویی‌های سنتی، پیچیده‌تر است؛ ۵- تصور می‌شود یکی از انگیزه‌های زورگویی سنتی موقعیت یا جایگاهی است که فرد مرتکب با نشان دادن قدرت (سوءاستفاده) نسبت به دیگران، در مقابل شاهدان به دست می‌آورد، اما در حمله سایبری، مهاجم این فرصت را ندارد؛ ۶- در زورگویی سایبری مخاطبان بالقوه بیشتری وجود دارند، زیرا مرتکب در زورگویی سایبری می‌تواند در یک گروه همسالان - در مقایسه با گروه‌های کوچکی که مخاطب معمول در زورگویی سنتی هستند-، به مخاطبان زیادی

دسترسی داشته باشد؛ ۷- فرار از زورگویی سایبری دشوار است («پناهگاه امن[1]» وجود ندارد)، زیرا ممکن است قربانی پیام‌هایی را به تلفن همراه یا رایانه شخصی خود ارسال کند یا در هرکجا که باشد به نظرات تند در وبسایت دسترسی پیدا کند.

زورگیری سایبری و مقایسه آن با پرخاشگری سایبری

در ارتباط با مقایسه زورگیری سایبری با پرخاشگری سایبری دو نگاه وجود دارد. گروهی از پژوهشگران (Kowalski & et al, 2019; Bauman & Baldasare, 2015; Corcoran, Mc Guckin & Prentice, 2105; Wright, 2015) معتقدند زورگیری سایبری دارای ویژگی‌های خاصی است که آن را از پرخاشگری سایبری جدا می‌سازد. این پژوهشگران معتقدند که پرخاشگری سایبری عمل عمدی مضری است که توسط شخص زورگو صورت می‌گیرد اما شامل تکرار و عدم تعادل قدرت نیست. همسو با این نگاه، اسمیت و همکاران (۲۰۱۳) استدلال می‌کنند که زورگیری سایبری دارای سه معیار یا ویژگی اصلی و محوری (هدفمندی یا قصد آسیب، وجود یک هدف مشخص، عدم تعادل قدرت) و یک معیار فرعی (تکرار) است. این پژوهشگران معتقدند که از بین سه معیار اصلی، معیار هدفمندی یا قصد آسیب بین پرخاشگری سایبری و زورگویی سایبری مشترک است اما دو معیار دیگر یعنی وجود یک هدف مشخص (قربانی از پیش تعیین‌شده) و نابرابری قدرت، ویژگی منحصربه‌فرد زورگویی سایبری است که آن را از پرخاشگری سایبری متمایز می‌سازد. بر همین اساس پیشنهاد می‌دهند در پژوهش‌هایی که این دو معیار محوری را در تعریف خود در نظر نمی‌گیرند، جزء پژوهش‌های حوزه پرخاشگری سایبری محسوب می‌شوند و نه زورگویی سایبری. بنابراین از منظر این گروه، هر زورگویی سایبری نوعی پرخاشگری سایبری است، اما هر پرخاشگری سایبری را نمی‌توان زورگویی سایبری نامید.

در مقابل، پژوهشگرانی چون بومن (۲۰۱۳) نگاه بدیلی را مطرح می‌سازند. این پژوهشگران معتقدند که ازآنجایی‌که نمی‌توان براساس شواهد پژوهشی، درباره معیارهای زورگویی سایبری به‌خصوص معیار تکرار و نابرابری قدرت به‌طور دقیق قضاوت کرد، بهتر است در حال حاضر از مفهوم گسترده‌تر یعنی پرخاشگری سایبری استفاده کرد تا زمانی که بتوان از طریق پژوهش‌های تجربی، این معیارها دقیقاً تعریف عملیاتی شوند. با اینحال، مطالعه و بررسی رسانه‌ها و همچنین نشریات و منابع علمی حاکی از استفاده گسترده از واژه زورگویی سایبری به‌جای واژه پرخاشگری سایبری است (Smith & et al, 2010). افزون بر این، علیرغم مشکلات

---

1 safe haven

مربوط به تعیین و تعریف دقیق معیارها یا شاخص‌های رفتار زورگویی سایبری، همان‌طور که اشاره شد، می‌توان تا حدود بسیار زیادی این معیارها را تعریف و توصیف نمود. بنابراین به نظر می‌رسد نگاه اول، قابل دفاع‌تر باشد و بتوان به‌جای «پرخاشگری سایبری» از اصطلاح دقیق‌تر یعنی «زورگیری سایبری» استفاده کرد.

گونه شناسی زورگیری سایبری

در ارتباط با اشکال یا روش‌های زورگیری سایبری طبقه‌بندی‌های متفاوتی ارائه‌شده است (Langos & Sarre, 2015; Chan & et al, 2012; Pyżalski, 2012: Bauman, 2011: Li, 2007; Willard, 2005). در مطالعه حاضر پس از بررسی و تلفیق دسته‌بندی‌های انجام شده، دوازده شکل یا روش برای زورگیری سایبری شناسای شد که عبارت‌اند از: آزار و اذیت سایبری[۱]، بدنام کردن[۲]، بازی سیلی خندان[۳]، اغفال سایبری[۴]، عصبانی کردن یا آتشی شدن[۵]، کمین سایبری[۶]، ظاهرسازی[۷] یا جعل هویت[۸]، حیله‌گری[۹]، افشاگری[۱۰]، کت فیشینگ[۱۱]، محرومیت[۱۲] یا طرد[۱۳] و زورگیری جنسی سایبری[۱۴]. در ادامه هر یک از اشکال زورگویی سایبری همراه با مثال تعریف می‌شود.

۱. آزار و اذیت: ارسال پیام‌های توهین‌آمیز و آزارنده به شکل مکرر برای یک کودک (قربانی) توسط یک یا گروهی از افراد زورگو که عموماً در محیط‌های مجازی عمومی (مانند اتاق‌های گفتگو، گروه‌ها) و یا شخصی (مانند رایانامه شخصی؛ پیامک متنی به تلفن همراه) اتفاق می‌افتد. مثال: حمله متنی[۱۵]: ارسال صدها پیام متنی توسط یک یا تعدادی از افراد زورگو به تلفن همراه قربانی.

---

1 Harassment
2 Denigration
3 Happy Slapping
4 Cyber Grooming
5 Flaming
6 Cyber stalking
7 Masquerading
8 Impersonation
9 Trickery
10 Outing
11 Catfishing
12 Exclusion
13 Ostracism
14 Sexual cyberbullying
15 Text Attack

۲. بدنام کردن: تحقیر و توهین دیگران به کمک فناوری. یا به‌عبارت‌دیگر، به اشتراک گذاشتن اطلاعات غیرواقعی، تحقیرآمیز و توهین‌آمیز درباره یک قربانی برای دیگران و یا ارسال آن برای قربانی. مثال: طراحی یک عکس تحریف‌شده از کودک (برای مثال زشت کردن صورت با فتوشاپ) و ارسال کردن آن برای قربانی یا دیگران در فضای مجازی.

۳. بازی سیلی خندان: کتک زدن، سیلی زدن، حمله کردن یا پرتاب یک شی به سمت قربانی (آشنا یا غریبه) و فیلم گرفتن هم‌زمان از آن و سپس ارسال یا اشتراک‌گذاری آن در فضای مجازی. مثال: هُل دادن کودک قربانی داخل جوی آب درحالی‌که توسط فرد زورگو یا یکی از دوستان او، از این صحنه فیلم گرفته می‌شود و سپس به اشتراک گذاشتن آن در فضای مجازی.

۴. اغفال سایبری: ایجاد یک ارتباط دوستانه و مبتنی بر احترام با کودک از طریق ابزارهای فناوری اطلاعات و ارتباطات با هدف سوءاستفاده جنسی از کودک به‌صورت مجازی (برخط) و یا به شکل ملاقات حضوری (غیر برخط) و یا هر دو. مثال: ارسال پیام به کودک قربانی با هر بهانه‌ای (برای مثال ارسال اشتباه پیام، پرسیدن سؤال و مانند این موارد)، به‌تدریج زمینه‌چینی برای دوستی و کسب اعتماد کودک و درنهایت ارسال پیام‌هایی با محتوای جنسی با هدف کسب لذت جنسی.

۵. عصبانی کردن (آتشی شدن): تعاملات و مشاجره‌های کوتاه خصمانه، دردناک و توهین‌آمیز بین دو یا چند نفر که در محیط‌های مجازی معمولاً عمومی مثل گروه‌ها یا اتاق‌های گفتگو اتفاق می‌افتد. مثال: ارسال پیام‌هایی مانند «تو یک ابلهی» «حالم ازت بهم می‌خورد»، «برو بمیر»، «خیکی زشت».

۶. کمین سایبری: مزاحمت‌های مکرر فرد زورگو برای تهدید، کنترل و یا آزار و اذیت با استفاده از دستگاه‌های ارتباطی الکترونیکی یا هرگونه وسیله با قابلیت اتصال به اینترنت. ابزارها و رسانه‌هایی که برای تعقیب سایبری استفاده می‌شوند بسیار متعددند که ازجمله آن‌ها می‌توان به رایانامه، اتاق‌های گفتگو، وبلاگ‌ها و وب‌گاه‌ها، ابزارهای نظارتی، GPS، دوربین، ابزارهای شنود، ویروس و برنامه‌های رایانه‌ای اشاره داشت. در مقایسه با «آزار و اذیت سایبری»، تهدید یا آزار و اذیت فرد زورگو در کمین سایبری بسیار جدی‌تر است، به‌گونه‌ای که زندگی قربانی مختل شده و یا باعث سلب امنیت و آسایش او می‌شود. مثال: ارسال پیام‌های متنی تهدیدآمیز مانند «تو می‌میری».

۷. ظاهرسازی (جعل هویت): وضعیتی که در آن فرد زورگو با یک هویت جعلی (اکانت[1] جعلی) یا با اطلاعات هویتی فرد دیگر (قربانی)، جهت ارسال پیام‌های نامناسب یا توهین‌آمیز برای یک یا گروهی از افراد استفاده می‌کند. مثال: ارسال رایانامه‌های توهین‌آمیز به دیگران با استفاده از اکانت جعلی (یا اطلاعات هویتی) کودک قربانی.

۸. کت فیشینگ: ایجاد یک پروفایل برخط جعلی و فریب دادن قربانی برای ایجاد یک ارتباط عاطفی دروغین با هدف سوءاستفاده مالی، جنسی و به‌خصوص عاطفی از قربانی. مثال: ساخت اکانت جعلی در وب‌گاه‌های دوست‌یابی به‌منظور سوءاستفاده عاطفی از قربانی.

۹. حیله‌گری: در این روش فرد زورگو/ متجاوز، با ایجاد ارتباط عاطفی و در نهایت با جلب اعتماد قربانی، او را متقاعد می‌سازد تا اطلاعات محرمانه، خصوصی و یا شرم‌آور را برای او ارسال کند. سپس اطلاعات را در فضای مجازی برای دیگران به اشتراک می‌گذارد (در فیشینگ[2] اشتراک‌گذاری وجود ندارد و عموماً درباره گردآوری اطلاعات مربوط به حساب‌های مالی است). مثال: درخواست ارسال عکس و یا فیلم‌های خصوصی از قربانی و سپس به اشتراک گذاشتن آن‌ها در فضای مجازی.

۱۰. افشاگری: حالتی است که کودک قربانی، اطلاعات شخصی خود را به خاطر ارتباط عاطفی و یا اعتمادی که به فرد زورگو دارد، در اختیار او قرار می‌دهد و این اطلاعات توسط فرد زورگو برای دیگران به اشتراک گذاشته می‌شود. در زورگویی سایبری به روش افشاگری، برخلاف روش حیله‌گری، این اطلاعات با میل خود قربانی برای فرد زورگو ارسال می‌شود نه به درخواست او. مثال: به اشتراک گذاشتن عکس‌ها یا فیلم‌های خصوصی قربانی در فضای مجازی بعد از پایان یافتن یک ارتباط عاطفی.

۱۱. محرومیت (طرد): حذف عمدی قربانی از یک گروه یا بازی برخط یا هرگونه شبکه‌های اجتماعی. مثال: حذف یک همکلاسی (قربانی) از یک گروه مجازی.

۱۲. زورگیری سایبری جنسی: رفتار جنسی تهاجمی یا اجباری به کمک رسانه‌های الکترونیکی نسبت به یک کودک قربانی.

مثال: ارسال پیام‌های تصویری یا متنی با محتوای جنسی برای تحریک جنسی کودک قربانی علی‌رغم مخالفت کودک قربانی. به این شکل از زورگیری سایبری جنسی، پیامک جنسی[3] می-

---

1 account
2 phishing
3 sexting

گویند یا تهدید کردن قربانی در اشتراک گذاشتن عکس نیمه برهنه وی در صورت عدم رضایت به رابطه جنسی. به این شکل از زورگیری سایبری جنسی، اخاذی جنسی[1] می‌گویند.

آیا فیشینگ نیز شکلی از زورگویی سایبری است؟

حمله فیشنگ را نمی‌توان از اشکال زورگویی سایبری دانست. در فیشینگ پیام‌های ایمیلی، وب‌سایت‌ها و تماس‌های تلفنی به شکل جعلی طراحی می‌شوند و برای کاربران ارسال می‌شوند تا با فریب دادن، آن‌ها را به ارائه اطلاعات درباره جزئیات کارت اعتباری یا جزئیات مربوط به ورود به سیستمِ[2] خودشان، هدایت کنند. هدف اصلی حمله فیشینگ، سود کلان پولی است (Prasad & Rohokale, 2020). در واقع فیشنگ مانند زورگویی سایبری یکی از اشکال جرائم سایبری است که «بیشتر غیرشخصی[3] است و هر مورد آن معمولاً «تنها برای یک بار[4]» (و نه چندباره) اتفاق میافتد» (Smith، ارتباط شخصی از طریق ایمیل، ۲۱ جولای ۲۰۱۹). به‌عبارت‌دیگر، فیشینگ شکلی از دزدی هویت[5] در بستر اینترنت است که در آن برخلاف زورگویی سایبری الزاماً هدف (قربانی) مشخصی وجود ندارد و فرد مرتکب به دنبال کلاهبرداری مالی از فرد خاصی نیست و الزاماً قربانی خود را از پیش نمی‌شناسد. علاوه بر این، چنانچه اشاره شد، تکراری بودن یک عمل، یکی از ویژگی‌های زورگویی سایبری است در حالیکه هر حمله فیشینگ تنها یک بار اتفاق می‌افتد.

در مقایسه فیشینگ با نوع حیله‌گری زورگیری سایبری باید گفت که در حیله‌گری، فرد مرتکب یا زورگو، اطلاعات مربوط به قربانی را برای دیگران ارسال می‌کند یا آن را در فضای مجازی قرار می‌دهد، اما در فیشینگ همان‌طور که اشاره شد، اولاً فرد مرتکب اطلاعات قربانی را برای دیگران به اشتراک نمی‌گذارد. دوم اینکه، برخلاف روش حیله‌گری، در فیشینگ، فرد مرتکب به دنبال گردآوری اطلاعات مربوط به حساب‌های مالی و بانکی قربانی است.

بحث و نتیجه‌گیری

زورگیری سایبری یکی از رایج‌ترین اشکال جرائم سایبری است که در اکثر کشورهای جهان از جمله انگلستان، فنلاند، آمریکا، ژاپن، و استرالیا دارای قوانین روشن و دقیق است. نبود

---

1 Sextortion
2 Log in
3 impersonal
4 one-off
5 identity theft

سیاست‌ها و قوانین روشن برای زورگیری سایبری در بعضی از کشورها موجب شده است تا عده‌ای از پژوهشگران از زورگیری سایبری به‌عنوان «برزخ قانونی[1]» یاد کنند (El Asam & Samara, 2016). فضای مجازی با توجه به ناشناخته بودن بسیاری از اجزای آن برای عامه مردم به عاملی برای افزایش فرصت‌های جنایی بدل گشته است. این ویژگی توسط مجرمان مجازی مورد سوءاستفاده قرارگرفته و شکل‌گیری گروه‌های فساد و جرم در این فضا را به دنبال داشته است (الهیاری و مجیدی پرست، ۱۳۹۳). در این راستا، مطالعه حاضر توانسته است اطلاعات ارزشمندی را درباره ماهیت و روش‌های زورگیری سایبری برای نهادهای اجرایی و مؤثر در قانون‌گذاری در زمینه پیشگیری از وقوع جرم فراهم سازد ضمن اینکه برای روان‌شناسان، متخصصان تعلیم و تربیت و جامعه‌شناسان علاقه‌مند به پژوهش در حوزه زورگویی سایبری نیز می‌تواند بسیار مفید باشد.

در مطالعه حاضر برای تعریف و گونه شناسی زورگویی سایبری تنها از منابع مکتوبی که به زبان انگلیسی منتشرشده‌اند، استفاده شد اما به توجه به نقش متغیرهای فرهنگی در تعریف و تعیین ویژگی‌های تعریف‌کننده زورگویی سایبری، باید این محدودیت را در پژوهش حاضر مدنظر قرار داد. با توجه به این محدودیت، پیشنهاد می‌شود پژوهش‌های آتی با استفاده از رویکردهای کیفی در پژوهش، معنا و مفهوم زورگویی سایبری را نظر نوجوانان و جوانان ایرانی مورد بررسی قرار دهند. از طرفی، مطالعه حاضر پدیده زورگویی سایبری را تنها از منظر نظری مورد بررسی قرار داده است. هرچند این پژوهش از این نظر که پدیده زورگویی سایبری را به جامعه پژوهشی کشور معرفی کرد، ارزشمند است، بااین‌حال تنها از طریق انجام پژوهش‌های تجربی با رویکردهای متعدد (کمی، کیفی و ترکیبی) و گردآوری داده‌های تجربی می‌توان ماهیت، ویژگی‌های، میزان شیوع، عوامل پیش‌بینی‌کننده زورگویی سایبری را در ایران شناخت و برای پیشگیری و کنترل آن راهکارهای عملی و اثربخش ارائه داد.

---

1 legal limbo

منابع

- ششجوانی، حمیدرضا. (۱۳۹۶). کودکان و تلفن همراه: پژوهشی درباره رفتارهای مصرفی کودکان. تهران: مرکز پژوهش‌های صنایع فرهنگی و خلاق.
- صادقی فسایی، سهیلا. و عرفان منش، ایمان. (۱۳۸۴). مبانی روش‌شناختی پژوهش اسنادی در علوم اجتماعی، مورد مطالعه: تأثیرات مدرن شدن بر خانواده ایرانی. راهبرد فرهنگ، ۸ (۲۹) ۹۱-۶۱.
- الهیاری، طلعت.، مجیدی پرست، سجاد. (۱۳۹۳). گونه شناسی باندهای جرم و فساد در فضای مجازی. پژوهشنامه مددکاری اجتماعی، ۲، ۱۵۰-۱۳۲.
- Akbulut, Y., Sahin, Y. L., & Eristi, B. (2010). Development of a scale to investigate cybervictimization among online social utility members. Contemporary Educational Technology, 1(1), 46-59.
- Ang, R. P. (2015). Adolescent cyberbullying: A review of characteristics, prevention and intervention strategies. Aggression and violent behavior, 25, 35-42.
- Bannink, R., Broeren, S., van de Looij–Jansen, P. M., de Waart, F. G., & Raat, H. (2014). Cyber and traditional bullying victimization as a risk factor for mental health problems and suicidal ideation in adolescents. PloS one, 9(4), e94026.
- Bauman, S. (2011). Cyberbullying: What counsellors need to know?. John Wiley & Sons.
- Bauman, S. & Baldasare, A. (2015). Cyber aggression among college students: Demographic differences, predictors of distress, and the role of the university. Journal of College Student Development, 56, 317-30.
- Bauman, S. (2014). Cyberbullying: What counsellors need to know? John Wiley & Sons.
- Betts, L. R. (2016). Cyberbullying: Approaches, consequences and interventions. Springer.
- Brochado, S., Soares, S. & Fraga, S. (2017). A scoping review on studies of cyberbullying prevalence among adolescents. Trauma, Violence, & Abuse 18 (5), 523-531,
- Cassidy, W., Faucher, C., & Jackson, M. (2017). Adversity in university: Cyberbullying and its impacts on students, faculty and administrators. International journal of environmental research and public health, 14(8), 888.
- Cénat, J. M., Hébert, M., Blais, M., Lavoie, F., Guerrier, M., & Derivois, D. (2014). Cyberbullying, psychological distress and self-esteem among youth in Quebec schools. Journal of affective disorders, 169, 7-9.

- Chan, S., Khader, M., Ang, J., Tan, E., Khoo, K., & Chin, J. (2012). Understanding happy slapping. International Journal of Police Science & Management, 14(1), 42-57.
- Corcoran, L., Guckin, C. M., & Prentice, G. (2015). Cyberbullying or cyber aggression?: A review of existing definitions of cyber-based peer-to-peer aggression. Societies, 5(2), 245-255.
- Crosslin, K., & Golman, M. (2014). Maybe you don't want to face it–College students' perspectives on cyberbullying. Computers in Human Behavior, 41, 14-20.
- Dooley, J. J., Pyżalski, J., & Cross, D. (2009). Cyberbullying versus face-to-face bullying: A theoretical and conceptual review. Zeitschrift für Psychologie/Journal of Psychology, 217(4), 182–188
- El Asam, A., & Samara, M. (2016). Cyberbullying and the law: A review of psychological and legal challenges. Computers in Human Behavior, 65, 127-141.
- Fahy, A. E., Stansfeld, S. A., Smuk, M., Smith, N. R., Cummins, S., & Clark, C. (2016). Longitudinal Associations between Cyberbullying Involvement and Adolescent Mental Health. Journal of Adolescent Health, 59(5), 502–509
- Festl, R., & Quandt, T. (2013). Social relations and cyberbullying: The influence of individual and structural attributes on victimization and perpetration via the internet. Human communication research, 39(1), 101-126.
- Frey, K. S., Pearson, C. R., & Cohen, D. (2015). Revenge is seductive, if not sweet: Why friends matter for prevention efforts. Journal of Applied Developmental Psychology, 37, 25-35.
- Hamm, M. P., Newton, A. S., Chisholm, A., Shulhan, J., Milne, A., Sundar, P., ... & Hartling, L. (2015). Prevalence and effect of cyberbullying on children and young people: A scoping review of social media studies. JAMA pediatrics, 169(8), 770-777.
- Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. Deviant behavior, 29(2), 129-156.
- Kowalski, R. M., Limber, S. P., & McCord, A. (2019). A developmental approach to cyberbullying: Prevalence and protective factors. Aggression and violent behaviour, 45, 20-32.
- Langos, C. (2012). Cyberbullying: The challenge to define. Cyberpsychology, Behavior, and Social Networking, 15(6), 285-289.
- Langos, C. (2014). Regulating cyberbullying: a South Australian perspective. Flinders LJ, 16, 73.
- Langos, C., & Sarre, R. (2015). Responding to cyberbullying: The case for family conferencing. Deakin L. Rev., 20, 299.
- Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. Computers in human behavior, 23(4), 1777-1791.

- Menesini, E., Nocentini, A., & Calussi, P. (2011). The measurement of cyberbullying: Dimensional structure and relative item severity and discrimination. Cyberpsychology, Behavior and Social Networking, 14(5), 267–274.
- Menesini, E., Nocentini, A., Palladino, B. E., Scheithauer, H., Schultze-Krumbholz, A., Frisen, A., ... & Blaya, C. (2013). Definitions of cyberbullying. In P. K. Smith & G. Steffgen (Eds.), Cyberbullying through the new media: Findings from an international network (pp. 23-36). New York: Psychology Press.
- Mesch, G. S. (2009). Parental mediation, online activities and cyberbullying. Cyberpsychology & Behavior, 12, 387-393.
- Messias, E., Kindrick, K., & Castro, J. (2014). School bullying, cyberbullying, or both: correlates of teen suicidality in the 2011 CDC Youth Risk Behavior Survey. Comprehensive psychiatry, 55(5), 1063-1068.
- Nocentini, A., Calmaestra, J., Schultze-Krumbholz, A., Scheithauer, H., Ortega, R., & Menesini, E. (2010). Cyberbullying: Labels, behaviours and definition in three European countries. Australian Journal of Guidance and Counselling, 20(2), 129.
- Olweus, D. (1993). Bullying at school: What we know and what we can do. Cambridge, MA: Blackwell Publishers, Inc.
- Olweus, D. (2013). School bullying: Development and some important challenges. Annual review of clinical psychology, 9, 751-780.
- Olweus, D., & Limber, S. P. (2018). Some problems with cyberbullying research. Current opinion in psychology, 19, 139-143.
- Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. Youth violence and juvenile justice, 4(2), 148-169.
- Patchin, J. W., & Hinduja, S. (2010). Cyberbullying and self-esteem. Journal of school health, 80(12), 614-621.
- Patchin, J. W., & Hinduja, S. (2015). Measuring cyberbullying: Implications for research. Aggression and Violent Behavior, 23, 69-74.
- Prasad, R., & Rohokale, V. (2020). Cyber Security: The Lifeline of Information and Communication Technology. Springer International Publishing.
- Pyżalski, J. (2012). From cyberbullying to electronic aggression: Typology of the phenomenon. Emotional and behavioural difficulties, 17(3-4), 305-317.
- Rao, T. S., Bansal, D., & Chandran, S. (2018). Cyberbullying: A virtual offense with real consequences. Indian journal of psychiatry, 60(1), 3.
- Raskauskas, J., & Stoltz, A. D. (2007). Involvement in traditional and electronic bullying among adolescents. Developmental psychology, 43(3), 564.

- Sengupta, A., & Chaudhuri, A. (2011). Are social networking sites a source of online harassment for teens? Evidence from survey data. Children and Youth Services Review, 33(2), 284-290.
- Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying?. Scandinavian journal of psychology, 49(2), 147-154.
- Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. Computers in human behavior, 29(1), 26-32.
- Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. Retrieved from: http://eprints.lse.ac.uk/103294/1/EU_Kids_Online_2020_March2020.pdf
- Smith, P. K. (2012 a). Cyberbullying and cyber aggression. In: Jimerson, S. R., Nickerson, A. B., Mayer, M. J., Furlong, M. J. (eds) Handbook of school violence and school safety: International research and practice, (2nd ed.) (pp. 93–103). New York, NY: Routledge.
- Smith, P. K. (2012 b). Cyberbullying: Challenges and opportunities for a research program—A response to Olweus (2012). European Journal of Developmental Psychology, 9(5), 553–558.
- Smith, P. K. (2019). Research on cyberbullying: strengths and limitations. In Narratives in Research and Interventions on Cyberbullying among Young People (pp. 9-27). Springer, Cham.
- Smith, P. K., & Monks, C. P. (2008). Concepts of bullying: Developmental and cultural aspects. APublic HEALTH CONCERN, 3.
- Smith, P. K., del Barrio, C., & Tokunaga, R. S. (2013). Definitions of bullying and cyberbullying: How useful are the terms? In S. Bauman, D. Cross, & J. Walker (Eds.), Routledge monographs in mental health. Principles of cyberbullying research: Definitions, measures, and methodology (pp. 26-40). New York, NY, US: Routledge/Taylor & Francis Group.
- Smith, P. K., Slonje, R. (2010) Cyberbullying: The nature and extent of a new kind of bullying, in and out of school. In: Jimerson, S. R., Swearer, S. M., Espelage, D. L. (eds) Handbook of bullying in schools: An international perspective, New York, NY: Routledge, pp. 249–262.
- Spears, B. A., Taddeo, C. M., Daly, A. L., Stretton, A., & Karklins, L. T. (2015). Cyberbullying, help-seeking and mental health in young Australians: Implications for public health. International journal of public health, 60(2), 219-226.
- Thomas, H. J., Connor, J. P., & Scott, J. G. (2015). Integrating traditional bullying and cyberbullying: challenges of definition and measurement in adolescents–a review. Educational psychology review, 27(1), 135-152.
- Vaillancourt, T., McDougall, P., Hymel, S., Krygsman, A., Miller, J., Stiver, K., & Davis, C. (2008). Bullying: Are researchers and children/youth talking about

the same thing?. International Journal of Behavioral Development, 32(6), 486-495.

- Vandebosch, H., & Van Cleemput, K. (2008). Defining cyberbullying: A qualitative research into the perceptions of youngsters. CyberPsychology & Behavior, 11(4), 499-503.
- Waasdorp, T. E., & Bradshaw, C. P. (2015). The overlap between cyberbullying and traditional bullying. Journal of Adolescent Health, 56(5), 483-488.
- Willard, N. (2005). Cyberbullying and cyber threats. Washington: US Department of Education.
- Wolke, D., Lee, K., & Guy, A. (2017). Cyberbullying: a storm in a teacup?. European child & adolescent psychiatry, 26(8), 899-908.
- Wright, M. F. (2015). Adolescents' cyber aggression perpetration and cyber victimization: The longitudinal associations with school functioning. Social Psychology of Education, 18(4), 653-666.
- Ybarra, M. L., & Mitchell, K. J. (2004). Online aggressor/targets, aggressors, and targets: A comparison of associated youth characteristics. Journal of child Psychology and Psychiatry, 45(7), 1308-1316.
- Ybarra, M. L., Boyd, D., Korchmaros, J. D., & Oppenheim, J. K. (2012). Defining and measuring cyberbullying within the larger context of bullying victimization. Journal of Adolescent Health, 51(1), 53-58.
- Young, R., Subramanian, R., Miles, S., Hinnant, A., & Andsager, J. L. (2017). Social representation of cyberbullying and adolescent suicide: A mixed-method analysis of news stories. Health communication, 32(9), 1082-1092.