صیانت فرهنگی و سرمایه اجتماعی
Online ISSN: 2783-249X
دوره ۲، شماره۱، بهار ۱۴۰۱
Print ISSN: 2783-3682
صفحات: ۹- ۳۹
https://ppsc.cfu.ac.ir
تاریخ دریافت: ۱۴۰۰ /۱۱/۱۷
تاریخ پذیرش: ۰۸/ ۰۱/ ۱۴۰۱

زورگویی سایبری: تعریف، تاریخچه و گونه شناسی

سید امیر قاسم تبار [۱]، سید عبدالله قاسم تبار [۲]

[۱] هیئت علمی دانشگاه فرهنگیان ، سازمان مرکزی، تهران ، ایران (نویسنده مسئول ghasemtabar.e@gmail.com)

[۲] دانشگاه فرهنگیان سازمان مرکزی، تهران ، ایران

چکیده

علیرغم پیامدهای منفی بلندمدت و گسترده زورگیری سایبری، هنوز درباره تعریف و ماهیت آن اتفاق‌نظر وجود ندارد. هدف در پژوهش حاضر ارائه تعریف، تاریخچه و گونه شناسی یا اَشکال زورگویی سایبری بود. روش پژوهش حاضر از نوع اَسنادی بود. جامعه پژوهشی تمامی منابع نوشتاری (چاپی/الکترونیکی) بین المللی در زمینه زورگویی سایبری بودند که از طریق پایگاهای اطلاعاتی خارجی قابل بازیابی و دسترسی بودند. بدین منظور با استفاده از روش نمونه برداری نظری و پس از بررسی و تحلیل منابع گردآوری شده از جامعه اسناد موجود، از میان منابعی (کتب، اسناد و مقالات) که از معیارهارهای ورود برخوردار بودند، به عنوان نمونه پژوهشی انتخاب شدند. برای تحلیل اَسناد از روش فیش برداری الکترونیکی استفاده شد. پس از بررسی و تحلیل منابع، روند تحول و شکل گیری مفهوم زورگویی سایبری تشریح شد، زورگویی سایبری تعریف شد و دوازده شکل زورگویی سایبری (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 مفهوم پردازی شد. مطالعه حاضر توانسته است اطلاعات ارزشمندی را درباره ماهیت و روشهای زورگیری سایبری برای نهادهای اجرایی و مؤثر در قانونگذاری در زمینه پشگیری از وقع جرم فراهم سازد ضمن اینکه برای روان شناسان، متخصصان تعلیم و تربیت و جامعه شناسان علاقمند به پژوهش در حوزه زورگویی سایبری نیز می تواند بسیار مفید باشد.

کلید واژه ها: زورگویی سایبری، زورگویی آنلاین، تعریف زورگویی سایبری، اَشکال زورگویی سایبری، تاریخچه زورگویی سایبری.

مقدمه

به دنبال رشد و پیشرفت فناوری اطلاعات و ارتباطات، اینترنت و فضای سایبری[۱] سکویی برای تعاملات اجتماعی بین نوجوانان تبدیل شده است که به آنها امکان می دهد بدون نظارت و محدودیت های اعمال شده 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 (انگ[۶]، ۲۰۱۵). زورگویی سایبری یعنی زورگویی از طریق اشکال الکترونیکی ارتباط مانند ایمیل، تلفن همراه، اتاق گفتگو[۷]، پیام رسانی فوری[۸]، و وب سایت ها (الویوس و لیمبر[۹]، ۲۰۱۸). پژوهش‌های متعددی شیوع زورگیری سایبری را در بین کودکان و نوجوانان مورد مطالعه قراردادند که به علت تفاوت بین پژوهش‌ها در تعریف زورگیری سایبری، روش‌شناسی پژوهش، ویژگی‌های جمعیت شناختی نمونه پژوهشی و ابزارهای گردآوری، میزان شیوع زورگیری سایبری به‌شدت متغیر اعلام شده است. برای مثال بررسی ۱۵۹ مطالعه انجام شده 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 (بروگادو، سوارس و فراگو[۱۰]، ۲۰۱۷). مطالعه بین‌المللی EU Kids Online بین سالهای ۲۰۱۹-۲۰۱۷ در بین ۲۵/۱۰۱ دانش‌آموز ۹ تا ۱۶ ساله ۱۹ کشور اروپایی نشان داد که بین ۷٪ (اسلواکی) تا ۴۰٪ (لهستان) کودکان قربانی زورگویی سایبری بودند و در بیشتر کشورها بیش از ۲۰٪ از کودکان آن را تجربه کردند (اسماهل[۱۱] و همکاران، ۲۰۲۰). مروری بر پیمایش‌های ملی انجام شده در کشورهای اروپایی نشان می‌دهد که بین ۵/۵ تا ۴۴٪ از کودکان، قربانی زورگیری سایبری شده‌اند (آتاناسیو[۱۲] و همکاران، ۲۰۱۸). پیمایش ملی انجام شده در بین ۳۳/۷۵۱ کودک ۵ تا ۱۸ سال استرالیایی در سال ۲۰۱۱ نشان داد که به‌طور میانگین ۲۲ درصد از کودکان قربانی زورگیری سایبری بوده‌اند (اسپیرز، کیلی، بیتس و کتز[۱۳]، ۲۰۱۴). همچنین بررسی ۵۸ مطالعه انجام شده در ایالات‌متحده آمریکا نشان داد که از بین کودکان ۱۰ تا ۱۹ سال، ۱ تا ۴۱ درصد قربانی زورگیری سایبری و ۳ تا ۷۲ درصد مرتکب زورگیری سایبری شده‌اند (سیلکی، فالس و

[1] Cyber space
[2] anonymity
[3] Cyberbullying
[4] Offline cyberbullying
[5] Electronic cyberbullying
[6] Ang, R. P.
[7] chat room
[8] instant messaging
[9] Olweus, D., & Limber, S. P.
[10] Brochado, S., Soares, S. & Fraga, S.
[11] Smahel, D.
[12] Athanasiou, K
[13] Spears, B., Keeley, M., Bates, S., & Katz, I.

مورینو[۱۴]، ۲۰۱۶). بر اساس نتایج پیمایش ملی در کره جنوبی، ۳۴ درصد از دانش‌آموزان پایه هفتم تا دوازدهم به‌نوعی درگیر زورگیری سایبری بوده‌اند که ۱۴/۶ از آن‌ها قربانی، ۶/۳ درصد، زورگو و ۱۳/۱ درصد نیز قربانی/ زورگو بودند (لی و شین[۱۵]، ۲۰۱۷).

مطالعات طولی انجام شده حاکی از آن است که نرخ شیوع زورگیری سایبری در بین کودکان و نوجوانان در حال افزایش است که مهم‌ترین دلیل آن افزایش استفاده از اینترنت و ابزارهای فناورانه در بین آنها است (کوالسکی[۱۶]، لیمبر و مک کورد[۱۷]، ۲۰۱۹؛ سنگوپتا و چودوری[۱۸]، ۲۰۱۱؛ مش[۱۹]، ۲۰۰۹). مطالعه انجام شده در ایران (شش جوانی، ۱۳۹۶) نیز نشان داده شد که 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 که ۷۴/۸ درصد از کودکان ۱۲ تا ۱۴ سال و ۹۳/۳ درصد از کودکان ۱۵ تا ۱۷ سال از تلفن همراه استفاده می‌کنند. این آمارها لزوم بررسی دقیق و علمی زورگیری سایبری که یکی از جدی‌ترین تهدیدات و آسیب‌های فضای مجازی برای کودکان است را مطرح می‌سازد.

شیوع بالای زورگیری سایبری در بین کودکان موجب شده است تا گروهی از مطالعات پیامدها و تأثیرات روان شناختی آن را مورد بررسی قرار دهند. یافته‌های این مطالعات نشان می‌دهد که زورگیری سایبری، پیامدهای منفی متعددی برای کودکان قربانی به دنبال دارد. این پژوهشگران تاکید می کنند که هرچند زورگیری سایبری یک بزه مجازی است، اما دارای پیامدهای منفی واقعی است (رائو، بنسل و چندران[۲۰]، ۲۰۱۸). از مهم‌ترین تأثیرات منفی زورگیری سایبری بر روی کودکان قربانی می‌توان به اضطراب (فهی[۲۱]، ۲۰۱۶)، افسردگی (هم[۲۲] و همکاران، ۲۰۱۵؛ اسپیرز، تادیو، دالی، استریتون و کارکلینز[۲۳]، ۲۰۱۵)، افکار خودکشی (یانگ، سابرامانیان، مایلز، هینانت و اندساگر[۲۴]، ۲۰۱۷؛ مسیاز، کیندریک و کاسترو[۲۵]، ۲۰۱۴)، مشکلات روان‌شناختی

[14] Selkie, E. M., Fales, J. L., & Moreno, M. A.
[15] Lee, C. & Shin, N.
[16] Kowalski, R. M.
[17] McCord, A.
[18] Sengupta, A., & Chaudhuri, A.
[19] Mesch, G. S.
[20] Rao, T. S., Bansal, D., & Chandran, S.
[21] Fahy, A. E.,
[22] Hamm, M. P.,
[23] Spears, B. A., Taddeo, C. M., Daly, A. L., Stretton, A., & Karklins, L. T.
[24] Young, R., Subramanian, R., Miles, S., Hinnant, A., & Andsager, J. L.
[25] Messias, E., Kindrick, K., & Castro, J.

درون‌سازی‌شده و برون‌سازی‌شده[۲۶] (واسدورپ و برادشو[۲۷]، ۲۰۱۵)، ناامیدی (کاسیدی، فوچر و جکسون[۲۸]، ۲۰۱۷)، کاهش سطح سلامت‌روانی (بانیک[۲۹] و همکاران، ۲۰۱۴)، کاهش عزت‌نفس (سینت[۳۰] و همکاران، ۲۰۱۴؛ ؛ پاتچین و هندوجا[۳۱]، ۲۰۱۰)، کاهش روابط اجتماعی (کروسلین و کروسلین[۳۲]، ۲۰۱۴؛ فیستل و گوانت[۳۳]، ۲۰۱۳)، نرفتن به مدرسه (فری، پیرسون و کوهن[۳۴]، ۲۰۱۵؛ راسکاوسکاس و استولتز[۳۵]، ۲۰۰۷)، و افت تحصیلی (پاتچین و هندوجا، ۲۰۰۶) ، اشاره داشت.

علیرغم پیامدهای منفی بلندمدت و گسترده زورگیری سایبری، هنوز درباره تعریف و ماهیت آن اتفاق‌نظر وجود ندارد و هر یک از پژوهشگران به شیوه های متفاواتی به مفهوم پردازی آن پرداختند (کوالسکی و همکاران ، ۲۰۱۹؛ لیمبر و همکاران، ۲۰۱۸). این امر موجب شد تا درباره انواع یا اَشکال زورگویی سایبری نیز دیدگاه متعددی مطرح شود و هر یک به شیوه های متفاوتی آن را طبقه بندی کنند (لانگوز و ساری[۳۶]، ۲۰۱۵؛ چان[۳۷] و همکاران، ۲۰۱۲؛ پای زالسکی[۳۸]، ۲۰۱۲؛ بومن[۳۹]، ۲۰۱۱؛ لی[۴۰]، ۲۰۰۷؛ ویلارد[۴۱]، ۲۰۰۵). از طرفی پدیده زورگویی سایبری در ایران کاملاً ناشناخته است. با بررسی و جستجو در پایگاه های علمی داخلی مشخص شد که هیچ مطالعه ای در داخل کشور پدیدیه زورگویی سایبری را چه به صورت نظری و چه به صورت تجربی مورد بررسی قرار نداده است. از این رو، با توجه به خلاء پژوهشی موجود در این زمینه در داخل کشور و همچنین وجود دیدگاه های نظری متفاوت و گاهاً متضاد درباره چیستی، ماهیت و گونه شناسی زورگویی سایبری در بین پژوهشگران و صاحب نظران، هدف در پژوهش حاضر آن بود تا ضمن ارائه تعریف، تاریخچه و گونه شناسی (طبقه بندی اَشکال) زورگویی سایبری، توجه پژوهشگران داخلی را نسبت به این پدید نوظهور که طبق یافته های بدست آمده از مطالعات تجربی دارای پیامدها و تاثیرات منفی متعددی است و همچنین شیوع آن نیز روز به روز در حال افزایش است، جلب نمایید.

---

[26] Externalizing/Internalizing
[27] Waasdorp, T. E., & Bradshaw, C. P.
[28] Cassidy, W., Faucher, C., & Jackson, M.
[29] Bannink, R.
[30] Cénat, J. M.
[31] Patchin, J. W., & Hinduja, S.
[32] Crosslin, K., & Golman, M.
[33] Festl, R., & Quandt, T.
[34] Frey, K. S., Pearson, C. R., & Cohen, D.
[35] Raskauskas, J., & Stoltz, A. D.
[36] Langos, C., & Sarre, R
[37] Chan, S
[38] Pyżalski, J.
[39] Bauman, S.
[40] Li, Q.
[41] Willard, N.

روش:

پژوهش حاضر از نظر هدف جزء پژوهش های کاربردی، از نظر نوع داده ها جزء پژوهش های کیفی و از نظر نحوه اجرا یک پژوهش اسنادی (سندکاوی[۴۲]) است. سند هر چیز کمّی یا ضبط شده ای است که برای مقاصد ارزیابی یا سایر اهداف تهیه شده باشد (لینکلن و گوبا[۴۳]، ۱۹۹۵). روش اسنادی، روشی کیفی است که پژوهشگر تلاش می کند تا با استفاده نظامند و منظم از داده های اسنادی به کشف، استخراج، طبقه بندی و ارزیابی مطالب مرتبط با موضوع پژوهش خود اقدام نماید[۴۴] (صادقی فسایی و عرفان‌منش، ۱۳۸۴). پینی[۴۵] و پینی (۲۰۰۴) روش اسنادی را روشی برای مقوله‌بندی، بررسی، تفسیر و شناسایی محدودیت های منابعی که غالباً به شکل اشکال مکتوب خصوصی و یا عمومی می باشند، توصیف می کنند. پژوهش اسنادی یک روش مفید رها شده‌ای است که پژوهشگران می‌توانند به شکل کاملاً مطمئنی از آن استفاده کنند، ضمن اینکه پژوهش اسنادی یک روش علمی است که مستلزم پایبندی جدی به پروتکل پژوهشی است (موگالاکوی[۴۶]، ۲۰۰۶).

جامعه پژوهشی، نمونه و روش نمونه‌برداری:

جامعه پژوهشی تمامی منابع نوشتاری (چاپی/الکترونیکی) بین المللی در زمینه زورگویی سایبری بودند که از در/ از طریق پایگاهای اطلاعاتی خارجی (همچون Science Direct، Google scholar، Springer، Taylor & Francis، SAGE، Wiley، ProQuest) قابل بازیابی و دسترسی بودند.

برای انتخاب نمونه از بین منابع و اسناد موجود از روش نمونه برداری نظری[۴۷] که یکی از روشهای اصلی نمونه برداری در روش اسنادی است (صادقی فسایی و عرفان‌منش، ۱۳۸۴)، استفاده شد. نمونه برداری نظری در طی مراحل پژوهش توسعه می یابد و نمی توان آن را از قبل طراحی کرد، زیرا اساس گروه نمونه، مفاهیم و مسائل نظری است که در طی دوره پژوهش بوجود می آید. اندیشه ها و مفاهیم نظری، گردآوری داده ها را کنترل می کند. در این روش، زمانی که هیچ اندیشه [و دانش] جدیدی بوجود نیاید، یعنی پژوهشگر به مرحله اشباع در داده‌ها برسد، نمونه برداری متوقف می شود (هومن، ۱۳۹۵). لذا در مطالعه حاضر نیز گرداوری داده های مورد نیاز از منابع تعیین شده تا آنجا ادامه یافت که پژوهشگر به مرحله اشباع اطلاعاتی رسید و احساس

---

42 . Documentary Research Method

43 . Lincoln, Y., & Guba, E

۴۴. استفاده از اصطلاح «روش کتابخانه‌ای» به جای روش اسنادی، کاملا تقلیل گرایانه است زیرا اولاً، در روش اسنادی می توان از اسناد غیر کتابخانه ای بهره برد و ثانیا، تکنیک های متعددی در روش اسنادی به کار گرفته می شود که بسیار روش مندتر از صرف خواندن چند متن قابل دسترس در کتابخانه است (صادقی فسایی وعرفان‌منش، ۱۳۸۴).

45 .Payne

46 . Mogalakwe, M.

47 . Theoretical sampling

نمود گردآوری داده های بیشتر تغییری در یافته های پژوهش ایجاد نمی کند. بر این اساس، و پس از بررسی و تحلیل منابع گردآوری شده از جامعه اسناد اشاره شده، ۷۲ مدرک (کتب، اسناد و مقالات) به عنوان نمونه پژوهشی انتخاب شدند. معیارهای ورود (در انتخاب نمونه) عبارتند بودند از حیطه جغرافیایی: سراسر دنیا؛ زبان منابع: انگلیسی؛ سال انتشار: بین سال های ۲۰۲۰-۲۰۰۰؛ نوع سند: تمامی منابع دست اول و دوم در خصوص نظریه‌ها، دیدگاه ها، رویکردها و پژوهش های نظری و مروری در زمینه زورگویی سایبری که در یک مجله و یا کتاب معتبر به چاپ رسیده اند و دارای متن کامل بودند.

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

یافته‌ها:

یافته های این پژوهش در چهار بخش اصلی ارائه شد. این چهار بخش که توضیحات آن در ذیل تشریح شد عبارتند از: ۱- تاریخچه و روند شکل گیری مفهوم زورگیری سایبری، ۲- تعریف و مفهوم شناسی زورگیری سایبری، ۳- مقایسه زورگویی سایبری با دیگر مفاهیم مرتبط، ۴- گونه شناسی زورگیری سایبری.

تاریخچه و روند شکل‌گیری مفهوم زورگیری سایبری

واژه «زورگویی» ترجمه واژه «bullying» است[۴۸]. «bullying» در اصل یک واژه آنگلوساکسون[۴۹] و یا اروپای شمالی است و ترجمه ای از واژه سوئدی «mobbning» است که اولین بار توسط یک پزشک مدرسه به نام هینیمن[۵۰] (۱۹۷۲) استفاده شد. «mobbning» یک اصطلاح کردارشناختی است که برای توصیف حمله جمعی گروهی از حیوانات به حیوانی از گونه دیگر که معمولاً بزرگتر است و دشمن طبیعی گروه است، به کار می رود (الویوس، ۲۰۱۳). پس از آن دان الویوس[۵۱] روان شناس سوئدی آن را در کتاب «پرخاشگری در مدرسه[۵۲]» (۱۹۷۳) (به سوئدی forskning om skolmobbning) به کار گرفت و پس از

[۴۸] واژه «bullying» در منابع فارسی به «قلدری» نیز ترجمه شده است. از این جهت می توان «cyberbullying »را به «قلدری سایبری» نیز ترجمه کرد.

[49] Anglo-Saxon

[50] Heinemann,

[51] Dan Olweus

[52] Aggression in school

انتشار این کتاب، مطالعه علمی پدیده زورگیری آغاز شد (اسمیت و مانکس[۵۳]، ۲۰۰۸). مطالعه علمی زورگویی بیشتر توسط روانشناسان تحولی[۵۴] و برخی جامعه شناسان صورت گرفته است (اسمیت، ۲۰۱۹).

اما اصطلاح زورگیری سایبری ابتدا در مقاله ای در روزنامه نیویورک تایمز[۵۵] در سال ۱۹۹۵ تحت عنوان «اعتیاد سایبری[۵۶]» مورد استفاده قرار گرفت. با این حال، رواج و استفاده گسترده این اصطلاح در سال ۲۰۰۳ و پس از راه اندازی وب سایت زورگویی سایبری (www.cyberbullying.ca) توسط بیل بلسی[۵۷] آغاز شد. به همین علت بسیاری از پژوهشگران، بلسی را مبدع این اصطلاح می شناسند (بومن، ۲۰۱۴). در واقع مطالعه علمی زورگیری سایبری پس از راه اندازی این وب سایت آغاز شد (بومن و بلمور[۵۸]، ۲۰۱۵) و از آن زمان پژوهش درباره زورگیری سایبری بویژه از سوی پژوهشگران رشته هایی مانند رسانه و ارتباطات، فناوری اطلاعات و مطالعات حقوقی[۵۹] روز به روز افزایش یافت (اسمیت، ۲۰۱۹). واژه زورگیری سایبری برگرفته از واژه فضای سایبری[۶۰] است که اولین بار توسط ویلیام گیبسون[۶۱] کانادایی، نویسنده داستان های تخیلی به کار گرفته شد (بومن، ۲۰۱۴).

تعریف و مفهوم شناسی زورگیری سایبری

علیرغم انجام مطالعات گسترده درباره زورگیری سایبری، هنوز درباره ماهیت، مفهوم و تعریف این پدیده نوظهور بین پژوهشگران اتفاق نظر وجود ندارد و تعاریف متعدد و متفاوتی از آن ارائه شد که در شکل زیر تعدادی از آنها ارائه شد.

زورگویی سایبری زمانی اتفاق می افتد که یک فرد از فناوری اطلاعات برای شرمساری، اذیت و آزار، ارعاب و تهدید دیگران استفاده کند و یا به نوعی به افرادی که برای چنین سوء استفاده ای هدف قرار گرفته اند، آسیب برساند (مک‌کواد، کالت و میر[۶۲]، ۲۰۰۹).
زورگیری سایبری عبارت است از آسیب عمدی و مکرری که از طریق رایانه ها، تلفن های همراه و سایر دستگاه های الکترونیکی رخ می دهد (پاتچین و هندوجا، ۲۰۱۵).

[53] Smith, P. K., & Monks, C. P.
[54] developmental psychologists
[55] New York Times
[56] Cyber addiction
[57] Bill Belsey
[58] Bellmore, A
[59] legal studies
[60] Cyberspace
[61] William Gibson
[62] McQuade, S. C., Colt, J. P., Meyer, N. B., & Meyer, N. B.

زورگیری سایبری آسیب و آذیت و آزار ناخواسته تکراری و یا تعامل تهدید کننده از طریق رسانه های ارتباطی الکترونیکی است (رافرتی و وندرون، ۲۰۱۴).

زورگویی سایبری یعنی زورگویی از طریق اشکال الکترونیکی ارتباط مانند ایمیل ها، تلفن همراه، اتاق گفتگو، پیام رسانی فوری[۶۳]، و وب سایت ها (الویوس و لیمبر، ۲۰۱۸).

زورگویی سایبری عملی است پرخاشگرانه و عمدی که توسط یک گروه یا فرد با استفاده از اشکال الکترونیکی ارتباط، به طور مکرر و در گذر زمان علیه یک قربانی که به آسانی نمی تواند از خود دفاع کند انجام می شود (اسمیت، ۲۰۰۸).

زورگویی سایبری عبارت است از استفاده از فناوری اطلاعات و ارتباطات به منظور حمایت از اعمال عمدی، تکرار شونده و با نیت زشت[۶۴]، با هدف آسیب رساندن به دیگران (آکبولت، ساهین و ارشتی[۶۵]، ۲۰۱۰).

زورگویی سایبری رفتاری است که با هدف شرمسار کردن، تهدید، آسیب رساندن و یا محروم کردن، طراحی می شود (بات[۶۶]، ۲۰۰۸).

زورگویی الکترونیکی یعنی زورگویی که در آن همسالان[۶۷] از وسایل الکترونکی برای تحقیر، توهین، تهدید، اذیت و آزار یا ترساندن دیگر همسال خود استفاده می کنند (راسکاوسکاس و استولتز ، ۲۰۰۷).

زورگیری سایبری سوءاستفاده سیستماتیک از قدرت است که با استفاده از فناوری های اطلاعات و ارتباطات (ICT) رخ می دهد (اسلانج[۶۸]، اسمیت و فریزن[۶۹]، ۲۰۱۳)

زورگویی سایبری عبارت است استفاده مکرر از فناوری برای آزار و اذیت، تحقیر یا تهدید کردن دیگران (هلادی[۷۰]، ۲۰۱۱).

زورگیری سایبری عبارت است از اقدام عمدی برای ارعاب، شرمسار کردن یا آزار و اذیت به شکل آنلاین یا دیجیتال (مارک و راتلیف[۷۱]، ۲۰۱۱) .

[63] instant messaging
[64] mean-spirited
[65] Akbulut, Y., Sahin, Y. L., & Eristi, B.
[66] Bhat, C. S.
[67] peers
[68] Slonje, R.
[69] Frisén, A.
[70] Holladay, J.
[71] Mark, L., & Ratliffe, K. T.

زورگویی سایبری رفتاری است که از طریق رسانه های الکترونیکی یا دیجیتال، افراد یا گروه هایی به طور مکرر پیام های خصمانه یا پرخاشگرانه را به منظور آسب زدن و یا ناراحت کردن برای دیگران می فرستند (اسمیت، دلباریو و توکونگا[۷۲]، ۲۰۱۰).

زورگیری سایبری هنگامی اتفاق می افتد که از نرم افزار های مبتنی بر اینترنت برای ترساندن یا توهین سیستماتیک به یک شخص مورد استفاده قرار می گیرند تا باعث تحقیر، شرمساری یا صدمه زدن به آن شخص شوند (والکنبرگ و پیتر[۷۳]، ۲۰۱۱).

زورگویی سایبری نوعی پرخاشگری است که از طریق رایانه های شخصی (به عنوان مثال پست الکترونیکی و پیام رسان فوری) یا تلفن های همراه (به عنوان مثال پیام رسان متنی) رخ می دهد (ونگ، لانوتی و نانسل[۷۴]، ۲۰۰۹).

شکل ۱. تعاریف پژوهشگران در مورد زورگویی سایبری

گروهی از پژوهشگران معتقدند که زورگیری سایبری (آنلاین یا الکترونیکی) شکل جدیدی از زورگیری سنتی[۷۵] (آفلاین[۷۶] یا حضوری[۷۷]) است (اسمیت، ۲۰۱۹؛ ولک ، لی و گای[۷۸]، ۲۰۱۷؛ اسلانچ و اسمیت، ۲۰۰۸) بنابراین باید بر اساس ویژگی های مهم زورگیری سنتی آن را تعریف نمود. رایج ترین و پذیرفته ترین تعریف از زورگیری سنتی، تعریفی است که الویوس (۱۹۹۳) از آن ارائه داد: «زمانی که یک دانش آموز به طور مکرر و در گذر زمان[۷۹] با اعمال منفی[۸۰] یک یا چند نفر دیگر مواجه می شود، [می توان گفت] آن دانش آموز مورد زورگویی قرار گرفته است یا قربانی شده است».

پژوهشگران بر اساس این تعریف سه مشخصه را برای زورگیری تعیین کرده اند که عبارتند از ۱) تکرار[۸۱]، ۲) هدفمندی[۸۲] (قصد آسیب زدن[۸۳])، و ۳) نابرابری قدرت[۸۴]. در بسیاری از مطالعات، با پذیرش این تعریف از زورگویی سنتی و در نظر گرفتن زورگویی سایبری به عنوان شکلی از زورگویی سنتی، زورگویی سایبری اینگونه تعریف شد: «عملی است پرخاشگرانه و عمدی که توسط

[72] del Barrio, C., & Tokunaga, R. S.
[73] Valkenburg, P. M., & Peter, J.
[74] Wang, J., Iannotti, R. J., & Nansel, T. R.
[75] Traditional bullying
[76] offline bullying
[77] in-person bullying
[78] Wolke, D., Lee, K., & Guy, A.
[79] over time
[80] negative actions
[81] repetition
[82] Intentionality
[83] Intent to Harm
[84] Imbalance of Power

یک گروه یا فرد با استفاده از اشکال الکترونیکی ارتباط، به طور مکرر و در گذر زمان علیه یک قربانی که به آسانی نمی تواند از خود دفاع کند، انجام می شود» (اسلانج و اسمیت، ۲۰۰۸).

در مقابل، گروه دیگری از پژوهشگران بر ویژگیهای منحصر به فرد و خاص زورگویی سایبری بویژه دو ویژگی ناشناختگی[۸۵] و عمومیت[۸۶] تاکید می کنند (توماس، اسکات و کانر[۸۷]، ۲۰۱۵؛ بیتس[۸۸]، ۲۰۱۶). 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 است برای قربانی ناشناس باقی بماند. منظور از ویژگی عمومیت نیز این است که برخلاف زورگویی سنتی که در آن شاهدان یا تماشاگران معمولاً بسیار محدود می باشند، در زورگویی سنتی، فناوری این امکان را فراهم می سازد تا افراد بسیار زیادی از سراسر جهان شاهد یا تماشاگر عمل منفی فرد مهاجم باشند. این گروه از پژوهشگران معتقدند که نمی توان بر اساس معیارهای زورگیری سنتی آن را تعریف نمود.

با این حال می توان با پذیرش این تفاوتها، از معیارهای سه گانه زورگیری سنتی برای تعریف زورگیری سایبری استفاده نمود (اسمیت، ۲۰۱۹). در ادامه ضمن توصیف این سه معیار، به تفاوت هر یک از معیارها در زورگویی سنتی و سایبری اشاره می شود و در نهایت یک تعریف از زورگویی سایبری ارائه می شود.

۱- هدفمندی: معیار هدفمندی به این موضوع اشاره دارد که تنها عمل یا رفتاری را می توان زورگویی نامید که به قصد آسیب زدن به دیگری انجام می شود. بنابراین اعمالی که بدون قصد آسیب زدن و به شکل «اتفاقی[۸۹]» رخ می دهد و یا هدف از انجام آن تنها «سرگرمی[۹۰]» است را نمی توان زورگویی دانست. معیار هدفمندی مهمترین معیار برای تعیین رفتار زورگویی سنتی و سایبری است (اسمیت و همکاران، ۲۰۱۳؛ منسینی، نوسنتینی و کالوسی[۹۱]، ۲۰۱۱). اما اینکه چگونه می توان درباره عمدی بودن یا نبودن یک رفتار قضاوت کرد، یکی از مهمترین چالش های پیش روی پژوهشگران در تعریف زورگویی است. چگونه می توان عمدی بودن یا نبود یک رفتار را مشخص کرد؟؛ معیار تعیین آسیب چیست؟: آیا باید از نگاه مرتکب یعنی «قصد آسیب رساندن» رفتار را قضاوت نمود یا از نگاه قربانی یعنی «احساس آسیب»؟.

[85] anonymity
[86] publicity
[87] Thomas, H. J., Connor, J. P., & Scott, J. G.
[88] Betts, L. R.
[89] accidental
[90] fun
[91] Menesini, E., Nocentini, A., & Calussi, P.

این مشکل در زورگویی سایبری به مراتب پیچیده تر از زورگویی سنتی است چراکه به علت غیرمستقیم بودن زورگویی سایبری تعیین نیت یک رفتار بسیار مشکل است (منسینی و نوسیتینی، ۲۰۰۹). مطالعه برن[۹۲] و فریزن (۲۰۱۱) روی نوجوانان سوئدی نشان داد که از دید شرکت کنندگان، از آنجایی که نمی توان از پشت صفحه نمایش[۹۳]، افراد را مشاهده کرد، به سختی می توان درباره قصد و نیت آنها قضاوت کرد. برای قضاوت درباره اینکه آیا یک عمل به قصد آسیب زدن به دیگری صورت گرفت یا نه، اسمیت و همکاران (۲۰۱۳) سه شاخص تعیین کردند که در صورت وجود هر سه ویژگی، می توان گفت آن رفتار به قصد آسیب انجام شد:

۱) قربانی، آسیب را تجربه کند.

۲) هدف مرتکب (زورگو)، تنها رفتار نیست بلکه آسیب است.

۳) یک فرد عاقل پیش بینی کند که چنانچه آن رفتار رخ دهد احتمالاً باعث آسیب به فرد مورد نظر (قربانی) می شود.

۲) تکرار: تکرار، معمولاً به عنوان یکی از معیارهای تعریف کننده زورگویی در نظر گرفته می شود. معیار تکرار به این معنا است که در زورگویی، رفتار یا عمل منفی بیش از یک بار اتفاق می افتد. بنابراین اعمال یا رفتاری که تنها یک بار[۹۴] رخ می دهند را نمی توان زورگویی نامید. با این حال، درباره معیار تکرار بین صاحب نظران حوزه زورگویی اتفاق نظر وجود ندارد. الویوس (۲۰۱۳) اشاره می کند که تکرار، یک معیار ضروری برای زورگویی نیست و دلیل استفاده از معیار تکرار در تعریف زورگویی این است که نشان می دهد رفتار و اعمال فرد مرتکب، به شکل تصادفی اتفاق نیفتاده است و به احتمال زیاد آن اعمال منفی به قصد آسیب انجام شده‌اند. در واقع معیار تکرار با معیار هدفمندی در ارتباط است. تکرار شدن یک عمل مضر یا آسیب زا به وضوح نشان از این واقعیت دارد که آسیب وارد شده توسط فرد مهاجم، عمدی بوده است (اسمیت و همکاران، ۲۰۱۳). از این رو، الویوس (۲۰۱۳) معیار «نسبتا تکراری[۹۵]» را پیشنهاد می دهد. در ویرایش جدید پرسشنامه زورگویی الویوس نسخه نروژی نیز، از عبارت «این موارد ممکن است به طور مکرر اتفاق بیفتد» یا «معمولاً تکرار می شوند» استفاده شد.

معیار تکرار در زورگویی سایبری ماهیت پیچیده تری دارد. یک عمل زورگویی ممکن است بر اساس نوع فناوری استفاده شده، به سرعت گسترش یابد و از کنترل اولیه خارج شود. برای مثال عکسی که تنها یکبار توسط شخص زورگو در فضای مجازی منتشر می شود، 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 بخاطر این رفتار زورگو، آسیب ببنید. بنابراین از منظر یک قربانی زورگویی سایبری، نیازی نیست

[92] Berne, S.
[93] screen
[94] one-off
[95] Some Repetitiveness

تا یک رفتار از سوی فرد زورگو بارها و بارها تکرار شود. در این ارتباط لانگوز[۹۶] (۲۰۱۲) زورگیری سایبری مستقیم[۹۷] و زورگویی سایبری غیرمستقیم[۹۸] را پیشنهاد می دهد. زورگویی سایبری مستقیم زمانی اتفاق می افتد که فرد زورگو، ارتباط الکترونیکی[۹۹] که شکل دهنده زورگویی است را مستقیماً به طرف فرد قربانی هدایت می کند. این نوع زورگویی سایبری که در فضای خصوصی سایبری[۱۰۰] رخ می دهد، شامل استفاده فرد زورگو از پیام رسان فوری، متن یا پیام های چندرسانه ای یا ایمیل، با هدف آسیب رساندن مستقیم و فوری به قربانی است. برای مثال ارسال پیام های متنی توهین آمیز برای قربانی. در مقابل، زورگویی سایبری غیرمستقیم، در فضای عمومی سایبری[۱۰۱] رخ می دهد و فرد زورگو، به جای هدایت ارتباط الکترونیکی به سمت فرد قربانی، با استفاده از سکوهای[۱۰۲] عمومی فضای مجازی مانند وب سایت های اشتراک گذاری، اتاق های گفتگو، پیام‌رسان‌هایی مانند تلگرام و شبکه‌های اجتماعی مانند یوتیوب و اینستاگرام، محتوای خود را بارگذاری می کند تا در دسترس عموم قرار گیرد. از منظر لانگوز، در زورگیری سایبری مستقیم، ضروری است تا یک رفتار منفی چندین بار رخ دهد تا منجر به آسیب شود. در نتیجه، وجود معیار تکرار در آن ضروری است. اما در زورگویی سایبری غیرمستقیم، تنها یک رفتار منفی از سوی فرد زورگو می تواند به فرد قربانی آسیب برساند چراکه در این نوع از زورگیری، رفتار بواسطه عرصه یا میدانی[۱۰۳] که در آن رخ داده است، تکرار می شود. یعنی محتوایی که در فضای عمومی سایبری قرار می گیرد می تواند برای مدت زمان بسیاری باقی بماند، توسط بسیاری از افراد دیده شود و یا توسط آنها برای دیگران به اشتراک گذاشته شود.

اسلانج و همکاران (۲۰۱۳) معتقدند که اگر رفتار یا عمل منفی از سوی همان فرد مهاجم، تکرار نشود، نمی توان آن را زورگویی نامید. با این حال دیگر محققان (یابارا، بوید، کورچ‌ماروس و آپنهایم[۱۰۴]، ۲۰۱۲) بر این باورند همانطور که نوشتن یک شایعه روی یک دیوار از سوی فرد مهاجم علیه یک قربانی، می تواند 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 اشاره شده، می توان بر اساس میزان آسیب نیز، درباره معیار تکرار، قضاوت نمود. 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

[96] Langos, C.
[97] Direct cyberbullying
[98] Indirect cyberbullying
[99] electronic communication
[100] Privet cyberspace
[101] public cyberspace
[102] Platforms
[103] arena
[104][104] Ybarra, M. L., Boyd, D., Korchmaros, J. D., & Oppenheim, J. K

قربانی متفاوت است (لانگوز، ۲۰۱۴). برای مثال تجربه تنها یکبار «زورگیری جنسی سایبری[۱۰۵]» می تواند تاثیرات منفی زیادی بر قربانی داشته باشد اما تجربه تنها یکبار «محرومیت[۱۰۶] یا طرد[۱۰۷] » ممکن است نتواند آسیب های جدی برای فرد قربانی بدنبال داشته باشد. بر این اساس، می توان گفت که معیار تکرار برای آن نوع از زورگیری سایبری که باعث آسیب جدی به قربانی می شود ضروری است اما برای نوع ملایم تر زورگیری سایبری، تکرار یک معیار ضروری برای تعریف زورگیری سایبری نیست.

با توجه به تمامی نکاتی که درباره معیار تکرار گفته شد، می توان اینگونه نتیجه گیری نمود که تکرار، یک میعار اصلی[۱۰۸] در تعریف زورگیری سایبری نیست بلکه یک معیار فرعی[۱۰۹] است (اسمیت و همکاران، ۲۰۱۳).

۳) نابرابری قدرت: معیار نابرابری در قدرت به این موضوع اشاره دارد که زورگویی سنتی یا سایبری، زمانی اتفاق می افتد که یک شخص که به نوعی از فرد قربانی قدرتمندتر است یا توانایی بیشتری دارد، قربانی را هدف قرار می دهد و به او حمله می کند (ویلانکورت[۱۱۰] و همکاران، ۲۰۰۸). بنابراین نبرد یا درگیری بین دو یا چند نفر که از هر لحاظ دارای قدرت و توانایی های برابری هستند را نمی توان زورگویی نامید و باید آن را پرخاشگری نامید (اسمیت و همکاران، ۲۰۱۳). (تفاوت زورگویی سایبری با پرخاشگری سایبری در بخشی مجزا مورد بحث قرار گرفت). نابرابری قدرت هم در زورگویی سنتی و هم در زورگویی سنتی یک معیار اصلی است و بدون نابرابری قدرت نمی توان رفتاری را زورگویی تعریف نمود. اما شیوه ها یا منابع نابرابری قدرت در بین دو نوع زورگویی سنتی و سایبری با یکدیگر متفاوت است (منسینی و همکاران، ۲۰۱۳؛ لانگوز، ۲۰۱۲). در مجموع می توان شش منبع نابرابری قدرت را در زورگویی سنتی مطرح کرد که عبارتند از:

۱- ضعیف تر بودن به لحاظ جسمی (به عنوان مثال، مورد حملات فیزیکی قرار گرفتن)

۲- ضعیف تر بودن از نظر کلامی (برای مثال مورد تمسخر قرار گرفتن)

۳- نداشتن اعتماد به نفس یا عزت نفس

۴- در اقلیت بودن یا عضویت در گروه های حاشیه ای (از نظر جنسیت، نژاد، مذهب، یا ناتوانی)

۵- نداشتن دوستان یا حمایت اجتماعی

۶- داشتن موقعیت پایین یا طرد شدن از سوی همسالان (اسمیت و همکاران، ۲۰۱۳).

---

[105] Sexual cyberbullying
[106] Exclusion
[107] Ostracism
[108] Core criteria
[109] subsidiary criteria
[110] Vaillancourt, T.

دوره ۲، شماره۱، بهار ۱۴۰۱ ، صفحات ۹-۳۹

در زورگویی سایبری ویژگیها یا شاخص های نابرابری قدرت تا حدود بسیار زیادی متفاوت است. گروهی از پژوهشگران معتقدند که داشتن مهارت و سواد بالاتر در زمینه فناوری اطلاعات و ارتباطات یکی از شاخص های اصلی نابرابری قدرت در زورگیری سایبری است (اسمیت و همکاران، ۲۰۱۳؛ وندبوش و ون کلیمپوت[۱۱۱]، ۲۰۰۸؛ یابارا و میتچل، ۲۰۰۴). نشان داده شد افرادی که اقدام به زورگویی سایبری می کنند خود را از نظر دانش و مهارت در زمینه فناوریها، بهتر از دیگران می دانند (یابارا و میتچل[۱۱۲]، ۲۰۰۴). با این حال این ویژگی همیشه نمی تواند معیاری برای نابرابری قدرت باشد چراکه برای ارتکاب به زورگویی سایبری همیشه داشتن مهارت در فناوریها الزامی نیست. نتیجه مطالعه کیفی، نوسنتینی و همکاران (۲۰۱۰) نشان داد که مهارت در زمینه استفاده از فناوریها، تنها برای نوع یا شیوه های پیچیده تر زورگویی سایبری مانند جعل هویت مورد نیاز است.

گروه دیگری از پژوهشگران پیشنهاد می دهند که نابرابری قدرت در فضای سایبری می تواند بر اساس پایگاه اجتماعی[۱۱۳] بالاتر مهاجم یا فرد زورگو در اجتماع سایبری[۱۱۴] تعریف شود (هندوجا و پاتچین، ۲۰۰۷). بعضی از پژوهشگران نیز بر این باروند که ناشناختگی به نابرابری قدرت در زورگویی سایبری کمک می کند (وندبوش و ون کلیمپوت، ۲۰۰۸). همانطور که پیش تر 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 (اسمیت، ۲۰۱۲ الف؛ توکونگا، ۲۰۱۰). در صورتی که 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 می توان گفت در صورت مشخص بودن هویت فرد مهاجم برای قربانی، تمامی ویژگی ها یا منابع نابرابری قدرت در زورگویی سنتی، برای زورگویی سایبری نیز صادق است (اسمیت و همکاران، ۲۰۱۳).

احساس درماندگی در قربانی به علت ناتوانی او در جلوگیری از رفتار منفی فرد مهاجم، یکی دیگر از جنبه های نابرابری قدرت در زورگویی سایبری است که توسط دالی، چیزالسکی و کراس[۱۱۵] (۲۰۰۹) مطرح شد. برخلاف زورگویی سنتی، در زورگویی های مبتنی بر فناوری، فرد قربانی عملاً هیچ کنترلی بر زورگویی ندارد. از این منظر، نابرابری قدرت در زورگویی سایبری بیانگر ویژگیهای فرد مهاجم نیست بلکه بیشتر ناتوانی یا نبود قدرت در هدف موردنظر یا قربانی است (دالی و همکاران، ۲۰۰۹). فرد مهاجم می تواند در هر زمان و هر مکانی به رفتار منفی خود علیه قربانی ادامه دهد. از طرفی، تعداد شاهدان در فضای مجازی به طور بالقوه بسیار بالاتر از شاهدان در زورگویی سنتی است؛ شاهدانی که ممکن است هویت بسیاری از آنها برای قربانی، ناشناس

[111] Vandebosch, H., & Van Cleemput, K.
[112] Ybarra, M. L., & Mitchell, K. J.
[113] social status
[114] virtual community
[115] Dooley, J. J., Pyzalski, J., & Cross, D.

دوره ۲، شماره۱، بهار ۱۴۰۱ ، صفحات ۹-۳۹

باشد (لانگوز، ۲۰۱۲). در این ارتباط نشان داده شد از نظر نوجوانان، آن نوع از زورگویی سایبری که شامل تعداد زیادی از شاهدان است شدیدترین نوع زورگویی سایبری است (اسلانج و اسمیت، ۲۰۰۸) که از این نوع زورگویی در ادبیات پژوهشی به «زورگویی جمعی[۱۱۶]» و «زورگویی چندگانه[۱۱۷]» نام برده می شود (اسمیت و همکاران، ۲۰۱۰). این عوامل باعث می شوند 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 منحصر به فرد زورگویی سایبری یعنی عمومی بودن زورگویی سایبری است که بر اساس طبقه بندی لانگوز (۲۰۱۲) در شکل غیر مستقیم زورگویی سایبری اتفاق می افتد.

طبق آنچه گفته شد، ویژگیها یا شاخص های نابرابری قدرت در زورگویی سایبری عبارتند از: مهارت و سواد در زمینه فناوری اطلاعات و ارتباطات، ناشناختگی، پایگاه اجتماعی در فضای سایبری، احساس درماندگی در رهایی از زورگیری. و در صورت مشخص بودن هویت فرد مهاجم برای قربانی، تمامی شاخص های نابرابری قدرت در زورگویی سنتی، برای زورگیری سایبری نیز صادق خواهد بود. بنابراین می توان نتیجه گرفت هرچند شاخص ها یا ویژگی های نابرابری قدرت در زورگیری سنتی و سایبری با یکدیگر تا حدود زیاد متفاوت می باشند، اما در هر دو شکل زورگویی، نابرابری قدرت به عنوان یک ویژگی اصلی وجود دارد و زمانی اتفاق می افتد که شخصی که به نوعی از قدرت بیشتری برخوردار است، فرد دیگری که قدرت کمتری دارد را هدف قرار می دهد و باعث احساس ناتوانی قدرت در قربانی می شود و دفاع از خود را برای قربانی مشکل می سازد.

در مقام جمع بندی این بخش، بر اساس تعاریف ارائه شده و همچنین با توجه به ویژگی های یا معیارهای تکرار، هدفمندی و عدم تعادل قدرت و همچنین دو ویژگی ناشناختگی و عمومیت که مختص زورگویی سایبری است می توان زورگیری سایبری را به این شکل 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، ارعاب، تهدید، توهین، شرمساری و یا سوءاستفاده از یک فرد ضعیف‌تری که به راحتی قادر به دفاع از خود نیست، انجام می‌شود.

مقایسه زورگویی سایبری با دیگر مفاهیم مرتبط:

زورگویی سایبری در مقایسه با زورگویی سنتی:

[116] mass bullying
[117] multiple bullying

دوره ۲، شماره۱، بهار ۱۴۰۱ ، صفحات ۹-۳۹

بر اساس تعاریف و همچنین مهمترین ویژگیهای زورگویی سنتی و سایبری، می توان دریافت که علیرغم شباهت های موجود بین آنها، زورگویی سایبری دارای ویژگیهای منحصر به فردی است که آن را از زوگویی سنتی متمایز می سازد. در این ارتباط اسمیت (۲۰۱۲ ب) معتقد است که زورگویی سایبری از هفت ویژگی منحصر به فرد برخوردار است که آن را از زورگویی سنتی متمایز می سازد. این هفت ویژگی عبارتند 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، مرتکب حداقل برای زمانی کوتاه واکنش قربانی را نمی بیند.
۴. تنوع نقش های فرد تماشاچی (شاهد) در حمله سایبری از بیشتر زورگویی های سنتی، پیچیده تر است
۵. تصور می شود یکی از انگیزه های زورگویی سنتی موقعیت یا جایگاهی است که فرد مرتکب با نشان دادن قدرت (سوءاستفاده) نسبت به دیگران، در مقابل شاهدان بدست می آورد، اما در حمله سایبری، مرتکب این فرصت را ندارد.
۶. در زورگویی سایبری مخاطبان بالقوه بیشتری وجود دارند، زیرا مرتکب در زورگویی سایبری می تواند در یک گروه همسالان - در مقایسه با گروه های کوچکی که مخاطب معمول در زورگویی سنتی هستند-، به مخاطبان زیادی دسترسی داشته باشد.
۷. فرار از زورگویی سایبری دشوار است («پناهگاه امن[۱۱۸]» وجود ندارد)، زیرا ممکن است قربانی پیام‌هایی را به تلفن همراه یا رایانه شخصی خود ارسال کند یا در هر کجا که باشد به نظرات تند 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 (کوالسکی و همکاران، ۲۰۱۹؛ بومن و بالداسار[۱۱۹]، ۲۰۱۵؛ کورکرن، مک گاکین و پرنتیس[۱۲۰]، ۲۰۱۵؛ رایت[۱۲۱]، ۲۰۱۵) معتقدند زورگیری سایبری دارای ویژگی های خاصی است که آن را از پرخاشگری سایبری جدا می سازد. این پژوهشگران معتقدند که پرخاشگری سایبری عمل عمدی مضری است که توسط شخص زورگو صورت می گیرد اما شامل تکرار و عدم تعادل قدرت نیست. همسو با این نگاه، اسمیت و همکاران (۲۰۱۳) استدلال می کنند که زورگیری سایبری دارای سه معیار یا ویژگی اصلی و محوری (هدفمندی یا

[118] safe haven
[119] Baldasare, A.
[120] Corcoran, L., Mc Guckin, C., & Prentice, G.
[121] Wright, M. F.

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 تعیین شده) و نابرابری قدرت ویژگی منحصر به فرد زورگویی سایبری است که آن را از پرخاشگری سایبری جدا می سازد. بر همین اساس پیشنهاد می دهند در پژوهش هایی که این دو معیار محوری را در تعریف خود در نظر نمی گیرند، جزء پژوهش های حوزه پرخاشگری سایبری محسوب می شوند و نه زورگویی سایبری. بنابراین از منظر این گروه، هر زورگویی سایبری نوعی پرخاشگری سایبری است اما هر پرخاشگری سایبری را نمی توان زورگویی سایبری نامید. به عبارت دیگر، زورگیری سایبری زیرمجموعه یا یکی از اشکال پرخاشگری سایبری است.

در مقابل، پژوهشگرانی چون بومن (۲۰۱۳) نگاه بدیلی را مطرح می سازند. این پژوهشگران معتقدند که از آنجایی که نمی توان بر اساس شواهد پژوهشی، درباره معیارهای زورگویی سایبری به خصوص معیار تکرار و نابرابری قدرت به طور دقیق قضاوت نمود، بهتر است در حال حاضر از مفهوم گسترده تر یعنی پرخاشگری سایبری استفاده نمود تا زمانیکه بتوان از طریق پژوهش های تجربی این معیارها دقیقا تعریف عملیاتی شوند. با این حال، مطالعه و بررسی رسانه‌ها و همچنین نشریات و منابع علمی حاکی از استفاده گسترده از واژه زورگویی سایبری به جای واژه پرخاشگری سایبری است (اسمیت و همکاران، ۲۰۱۳). افزون بر این، علیرغم مشکلات مربوط به تعیین و تعریف دقیق معیارها یا شاخص های رفتار زورگویی سایبری، همانطور که اشاره شد، می توان تا حدود بسیار زیادی این معیارها را تعریف و توصیف نمود. بنابراین به نظر می رسد نگاه اول، قابل دفاع تر باشد و بتوان به جای «پرخاشگری سایبری» از اصطلاح دقیق تر یعنی «زورگیری سایبری» استفاده کرد.

گونه‌شناسی زورگیری سایبری

در ارتباط با اشکال یا روش‌های زورگیری سایبری طبقه‌بندی‌های متفاوتی ارائه‌شده است (لانگوز و ساری، ۲۰۱۵؛ چان و همکاران، ۲۰۱۲؛ پای زالسکی، ۲۰۱۲؛ بومن، ۲۰۱۱؛ لی[۱۲۲]، ۲۰۰۷؛ ویلارد، ۲۰۰۵). در مطالعه حاضر پس از بررسی و تلفیق دسته بندی های انجام شده، دوازده شکل یا روش برای زورگیری سایبری شناسای شد که عبارتند از: آزار و اذیت سایبری[۱۲۳]، بدنام کردن[۱۲۴]،

[122] Li, Q.
[123] Harassment
[124] Denigration

دوره ۲، شماره۱، بهار ۱۴۰۱ ، صفحات ۹-۳۹

بازی سیلی خندان[۱۲۵]، اغفال سایبری[۱۲۶]، عصبانی کردن یا آتشی شدن[۱۲۷]، کمین سایبری[۱۲۸]، ظاهرسازی[۱۲۹] یا جعل‌هویت[۱۳۰]، حیله‌گری[۱۳۱]، افشاگری[۱۳۲]، کت فیشینگ[۱۳۳]، محرومیت[۱۳۴] یا طرد[۱۳۵] و زورگیری جنسی سایبری[۱۳۶]. در ادامه هر یک از اشکال زورگویی سایبری همراه با مثال بیان می شود.

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 اول: حمله متنی[۱۳۷]: ارسال صدها پیام متنی توسط یک یا تعدادی از افراد زورگو به تلفن همراه قربانی.

مثال دوم: مزاحم[۱۳۸] در بازی‌های چندنفره برخط؛ کسی که به‌طور عمدی باعث آزار و عصبانی کردن دیگران می‌شود و یا از موارد موجود در بازی به شکلی که قرار نبوده، استفاده می‌کند. هدف او بیشتر خراب کردن بازی دیگران است تا بردن بازی.

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 اول: فیلم گرفتن از زمین خوردن یک همکلاسی در زمین‌بازی و به اشتراک گذاشتن آن در فضای مجازی.

مثال دوم: 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.

---

[125] **Happy Slapping**
[126] Cyber Grooming
[127] Flaming
[128] Cyber stalking
[129] Masquerading
[130] Impersonation
[131] Trickery
[132] Outing
[133] Catfishing
[134] Exclusion
[135] Ostracism
[136] Sexual cyberbullying
[137] Text Attack
[138] Griefer

مثال: هل 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 (غیربرخط) و یا هر دو.

مثال: ارسال پیام به کودک قربانی با هر بهانه‌ای (برای مثال ارسال اشتباه پیام، پرسیدن سوال 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 به هم 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 اول: ارسال پیام‌های متنی تهدیدآمیز مانند «تو می‌میری».

مثال دوم: ارسال پیام‌های توهین‌آمیز مکرر به قربانی، از طریق رسانه‌های متعدد مانند رایانامه، تلفن همراه و شبکه‌های اجتماعی و درخواست پول برای پایان دادن به این مزاحمت‌ها.

۷. ظاهرسازی (جعل هویت): وضعیتی که در آن فرد زورگو با یک هویت جعلی (اکانت جعلی) و 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 (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 به خصوص 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 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 اول: 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[۱۳۹] می گویند.

مثال دوم: 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[۱۴۰] می گویند.

آیا فیشینگ نیز شکلی از زورگویی سایبری است؟

فیشینگ[۱۴۱]، یکی از رایج ترین تهدیدهای فضای مجازی است. اما باید توجه داشت که حمله فیشنگ را نمی توان از اشکال زورگویی سایبری دانست. در فیشینگ پیام های ایمیلی، وب سایت ها و تماس های تلفنی به شکل جعلی طراحی می شوند و برای کاربران ارسال می شوند تا با فریب دادن، آنها را به ارائه اطلاعات درباره جزئیات کارت اعتباری یا جزئیات مربوط به ورود به سیستمِ[۱۴۲] خودشان، هدایت کنند. هدف اصلی حمله فیشینگ، سود کلان پولی است (پراساد و روهوکاله[۱۴۳]،۲۰۲۰). حمله

[139] sexting
[140] Sextortion
[141] phishing
[142] Log in
[143] Prasad, R., & Rohokale, V.

فیشینگ در انواع مختلفی از جمله مهندسی اجتماعی[۱۴۴]، دستکاری لینک[۱۴۵] (پیوند)، فیشینگ نیزه[۱۴۶] ، فیشینگ کلون[۱۴۷]، فیشینگ صوتی[۱۴۸] و غیره صورت می گیرد (چودری، چودری و ریتنهوس[۱۴۹]، ۲۰۱۶). در واقع فیشنگ مانند زورگویی سایبری یکی از اشکال جرائم سایبری است که «بیشتر غیرشخصی[۱۵۰] است و هر مورد آن معمولاً «تنها برای یک بار[۱۵۱]» (و نه چندباره) اتفاق می افتد» (اسمیت، ارتباط شخصی از طریق ایمیل، ۲۱ جولای ۲۰۱۹). به عبارت دیگر، فیشینگ شکلی از دزدی هویت[۱۵۲] در بستر اینترنت است که در آن بر خلاف 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 نمی شناسد بلکه تلاش می کند تا هر فردی که می تواند را در دام و تله سایبری خود بیندازد. علاوه بر این، چنانچه اشاره شد، تکراری بودن یک عمل، یکی از ویژگیهای زورگویی سایبری است در حالیکه هر حمله فیشینگ تنها یک بار (یکباره) اتفاق می افتد.

همچنین باید توجه داشت که در کت‌فیشنگ نیز فرد مرتکب ممکن است با فریب دادن قربانی خود، برای مثال از طریق هدایت کردن او به یک وب‌گاه شبیه‌سازی‌شده بانکی، به اطلاعات مربوط به کارت اعتباری او دست یابد و بدین طریق از فرد قربانی، سوءاستفاده مالی کند اما در اینجا برخلاف فیشینگ، فرد برای کسب اطلاعات مربوط به کارت اعتباری، از روشهایی مانند ارسال وب سایت ها یا پیوندهای جعلی استفاده نمی کند بلکه بواسطه یک ارتباط دوستانه و یا عاطفی، اعتماد قربانی را جلب می کند و بدین شکل به اطلاعات مربوط به کارت اعتباری او یا هر یک از اعضای خانواده او دست می یابد.

در مقایسه فیشینگ با نوع حیله گری زورگیری سایبری باید گفت که در حیله گری، فرد مرتکب یا زورگو، اطلاعات مربوط به قربانی را برای دیگران ارسال می کند یا آن را در فضای مجازی قرار می دهد اما در فیشینگ همانطور که اشاره شد، اولاً فرد مرتکب اطلاعات قربانی را برای دیگران به اشتراک نمی گذارد. دوم اینکه، بر خلاف روش حیله گری، در فیشینگ، فرد مرتکب به دنبال گردآوری اطلاعات مربوط به حساب‌های مالی و بانکی قربانی است.

بحث و نتیجه‌گیری:

144 Social engineering
145 link manipulation
146 spear phishing
147 clone phishing
148 voice phishing
149 Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G.
150 impersonal
151 one-off
152 identity theft

پژوهش حاضر با هدف بررسی سیر تحول شکل گیری مفهوم و پدیده زورگویی سایبری، تعریف و گونه‌شناسی آن انجام شد. در این پژوهش پس از توضیح چگونگی شکل گیری مفهوم زورگویی سایبری از سال ۱۹۹۵، بر اساس تعاریف موجود دیگران پژوهشگران و نقد و بررسی شاخص ها یا معیارهای زورگویی سایبری و مقایسه آن با شکل سنتی زورگویی سایبری و همچنین مقایسه آن با دیگر مفاهیم مرتب، زورگیری سایبری به این شکل تعریف شد: زورگویی 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 رسانه‌های متفاوت (مانند وب‌گاه‌های شخصی، نشریات برخط (وبلاگ‌ها)، رایانامه، بازی‌های برخط، پیام‌رسان‌ها مانند تلگرام، واتساپ و شبکه‌های اجتماعی مانند فیس‌بوک، یوتیوب، اینستاگرام و اتاق‌های گفتگو، برای آزار و اذیت، ترساندن، تهدید، توهین، شرمساری، و یا سوءاستفاده از یک فرد (قربانی) ضعیف‌تری که به راحتی قادر به دفاع از خود نیست، انجام می‌شود. طبق این تعریف ارائه شده، می توان هفت ویژگی برای زورگویی سایبری ارائه داد: ۱) تنها اعمالی که به قصد آسیب زدن به دیگری انجام می شوند را می توان مصداق زورگویی سایبری دانست؛ اعمالی که به شکل اتفاقی و بدون قصد و نیت رخ می دهند و یا هدف از انجام آن تنها سرگرمی است را نمی توان زورگویی دانست. ۲) تکرار عمل یا رفتار تنها یک ویژگی فرعی در زورگویی سایبری است. به عبارت دیگر، برای اینکه یک رفتار را مصداق زورگویی سایبری بدانیم، تکرار رفتار از سوی فرد زورگو یا مرتکب الزامی نیست بلکه در مواقعی می توان حتی رفتاری که به قصد آسیب اما تنها برای یک بار نیز رخ می دهد را زورگویی سایبری قلمداد نمود. قصد یا نیت فرد مرتکب، قضاوت فرد قربانی و دیگران درباره شدت آسیب، و نوع زورگویی (مستقیم یا غیرمستقیم بودن) را می توان مهمترین معیارهای قضاوت در نظر گرفت. ۳) عدم تعادل قدرت یا نابرابری قدرت یک ویژگی مهم و تعریف کننده در زورگویی سایبری است. ۴) هویت فرد زورگو می تواند برای قربانی ناشناس باشد یا نباشد. ۵) زوگویی سایبری، به قصد آسیب به یک هدف یا قربانی مشخص یا از پیش تعیین شده، رخ می دهد. به عبارت دیگر، فرد قربانی از پیش برای زروگو مشخص است. ۶) زورگویی سایبری از طریق سکوها یا ابزارهای متعدد فناوری اطلاعات و ارتباطات و با استفاده از رسانه‌ها، پیام‌رسان‌ها و شبکه‌های اجتماعی رخ می دهد. ۷) زورگویی سایبری دارای اَشکال یا شیوه های متعددی است که می توان آنها را در دوازده گروه طبقه بندی کرد که عبارتند از: آزار و اذیت سایبری ، بدنام کردن ، بازی سیلی خندان ، اغفال سایبری ، عصبانی کردن یا آتشی شدن، کمین سایبری، ظاهرسازی یا جعل‌هویت، حیله‌گری، افشاگری، کت فیشینگ، محرومیت یا طرد و زورگیری جنسی سایبری.

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 سیاست‌ها و قوانین روشن برای زورگیری سایبری در بعضی از کشورها

موجب شده است تا عده‌ای از پژوهشگران از زورگیری سایبری به‌عنوان «برزخ قانونی[۱۵۳]» یاد کنند (ال‌آسام و ساماراا[۱۵۴]، ۲۰۱۶). 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 قرار گرفته و شکل‌گیری گروه‌های فساد و جرم در این فضا را به دنبال داشته است (الهیاری و مجیدی‌پرست، ۱۳۹۳). یکی از اصول مهم و خاص جرم‌انگاری در جرائم سایبری، اصل دقت است. اصل دقت در تعریف جرائم سایبری بیانگر این موضوع است که قانونگذار باید اعمال ممنوع را به تفصیل بیان کرده، با ارائه تعاریف دقیق از اعمال غیرقانونی و تعیین اوصاف حقوق ماهوی و محدودهٔ آن، از ابهام و کلی‌گویی خودداری نمایید (حسنی، ۱۳۸۹ نقل از صفاری‌فرد خوزانی، ۱۳۹۹). تحقق‌بخشیدن به این اصل مهم در حوزه زورگیری سایبری، و تعریف دقیق «ضابطه رفتار» و همچنین «ضابطه کیفر»، مستلزم آن است که قانونگذار با ماهیت، و همچین اَشکال یا شیوه‌های زورگیری سایبری، شناخت همه‌جانبه و کاملی داشته باشد. 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 پشگیری از وقع جرم فراهم سازد ضمن اینکه برای روان شناسان، متخصصان تعلیم و تربیت و جامعه شناسان علاقمند به پژوهش در حوزه زورگویی سایبری نیز می تواند بسیار مفید باشد.

در مطالعه حاضر برای تعریف و گونه شناسی زورگویی سایبری تنها از منابع مکتوبی که به زبان انگلیسی منتشر شده اند، استفاده شد اما به توجه به نقش متغیرهای فرهنگی در تعریف و تعیین ویژگیهای تعریف کننده زورگویی سایبری، باید این محدودیت را در پژوهش حاضر مدنظر قرار داد. با توجه به این محدودیت، پیشنهاد می شود پژوهش های 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 نمود، ارزشمند است، با این حال تنها از طریق انجام پژوهش های تجربی با رویکردهای متعدد (کمی، کیفی و ترکیبی) و گردآوری داده های تجربی می توان ماهیت، ویژگی ها، میزان شیوع، عوامل پیش بینی کننده و کنترل کننده زورگویی سایبری را در ایران شناخت و برای پیشگیری و کنترل آن راهکارهای عملی و اثربخش ارائه داد.

[153] legal limbo

[154] El Asam, A., & Samara, M.

دوره ۲، شماره۱، بهار ۱۴۰۱ ، صفحات ۹-۳۹

فهرست منابع

۱) شش جوانی، حمیدرضا. (۱۳۹۶). کودکان و تلفن همراه: پژوهشی درباره رفتارهای مصرفی کودکان. تهران: مرکز پژوهش های صنایع فرهنگی و خلاق.

۲) صادقی فسایی، سهیلا. و عرفان منش، ایمان. (۱۳۸۴). مبانی روش شناختی پژوهش اسنادی در علوم اجتماعی، مورد مطالعه: تاثیرات مدرن شدن بر خانواده ایرانی .راهبرد فرهنگ، ۸ (۲۹) ۹۱-۶۱.

۳) صفاری فرد خوزانی، محسن. (۱۳۹۹). سیاست کیفری حاکم بر جرایم سایبری با چشم انداز کیفر شناسی. تهران: چاپ و نشر ایران

۴) اله یاری، طلعت.، مجیدی پرست، سجاد. (۱۳۹۳). گونه شناسی باندهای جرم و فساد در فضای مجازی. پژوهش نامه مددکاری اجتماعی، ۲، ۱۳۲-۱۵۰.

۵) هومن، حیدرعلی. (۱۳۹۵). شناخت روش علمی در علوم رفتاری. تهران: سمت

6) 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.

7) Ang, R. P. (2015). Adolescent cyberbullying: A review of characteristics, prevention and intervention strategies. Aggression and violent behavior, 25, 35-42.

8) Athanasiou, K., Melegkovits, E., Andrie, E. K., Magoulas, C., Tzavara, C. K., Richardson, C., ... & Tsitsika, A. K. (2018). Cross-national aspects of cyberbullying victimization among 14–17-year-old adolescents across seven European countries. BMC public health, 18(1), 800.

9) 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.

10) 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.

11) 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.

12) Bauman, S. (2014). Cyberbullying: What counsellors need to know? John Wiley & Sons.

13) Berne, S., & Frisén, A. (2011, August). Adolescents' view on how different criteria define cyberbullying. In Symposium at the European Conference on Developmental Psychology (Vol. 25).

14) Betts, L. R. (2016). Cyberbullying: Approaches, consequences and interventions. Springer.

15) Bhat, C. S. (2008). Cyber bullying: Overview and strategies for school counsellors, guidance officers, and all school personnel. Journal of Psychologists and Counsellors in Schools, 18(1), 53-66.

16) Brochado, S., Soares, S. & Fraga, S. (2017). A scoping review on studies of cyberbullying prevalence among adolescents. Trauma, Violence, & Abuse 18 (5), 523-531.

17) Brochado, S., Soares, S. & Fraga, S. (2017). A scoping review on studies of cyberbullying prevalence among adolescents. Trauma, Violence, & Abuse 18 (5), 523-531,

18) 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.

19) 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.

20) 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.

21) 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.

22) 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.

23) Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing attacks and defenses. International Journal of Security and Its Applications, 10(1), 247-256.

24) 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.

25) 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.

26) 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

27) El Asam, A., & Samara, M. (2016). Cyberbullying and the law: A review of psychological and legal challenges. Computers in Human Behavior, 65, 127-141.

28) 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

29) 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.

30) 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.

31) 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.

32) 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.

33) Langos, C. (2012). Cyberbullying: The challenge to define. Cyberpsychology, Behavior, and Social Networking, 15(6), 285-289.

34) Langos, C. (2014). Regulating cyberbullying: a South Australian perspective. Flinders LJ, 16, 73.

35) Langos, C., & Sarre, R. (2015). Responding to cyberbullying: The case for family conferencing. Deakin L. Rev., 20, 299.

36) Lee, C. & Shin, N. (2017). Prevalence of cyberbullying and predictors of cyberbullying perpetration among Korean adolescents. Computers in Human Behavior, 68,352-358.

37) Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. Computers in human behavior, 23(4), 1777-1791.

38) Lincoln, Y. S., & Guba, E. (1995). Paper presented at the Annual Meeting of The American Educational Research Association. In Emerging Criteria for Quality in Qualitative and Interpretive Research.

39) Mark, L., & Ratliffe, K. T. (2011). Cyber worlds: New playgrounds for bullying. Computers in the Schools, 28(2), 92-116.

40) McQuade, S. C., Colt, J. P., Meyer, N. B., & Meyer, N. B. (2009). Cyber bullying: Protecting kids and adults from online bullies. ABC-CLIO.

41) Menesini, E., & Nocentini, A. (2009). Cyberbullying definition and measurement: Some critical considerations. Zeitschrift für Psychologie/Journal of Psychology, 217(4), 230-232.

42) 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.

43) 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.

44) Mesch, G. S. (2009). Parental mediation, online activities and cyberbullying. Cyberpsychology & Behavior, 12, 387-393.

45) 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.

46) Mogalakwe, M. (2006). The use of documentary research methods in social research. African Sociological Review, 10, (1), 221-230.

47) 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.

48) Olweus, D. (1993). Bullying at school: What we know and what we can do. Cambridge, MA: Blackwell Publishers, Inc.

49) Olweus, D. (2013). School bullying: Development and some important challenges. Annual review of clinical psychology, 9, 751-780.

50) Olweus, D., & Limber, S. P. (2018). Some problems with cyberbullying research. Current opinion in psychology, 19, 139-143.

51) O'Neill, B., & Dinh, T. (2015). Mobile technologies and the incidence of cyberbullying in seven European countries: Findings from Net Children Go Mobile. Societies, 5(2), 384-398.

52) 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.

53) Patchin, J. W., & Hinduja, S. (2010). Cyberbullying and self-esteem. Journal of school health, 80(12), 614-621.

54) Payne, G., & Payne, J. (2004). Key concepts in social research. Sage.

55) Prasad, R., & Rohokale, V. (2020). Cyber Security: The Lifeline of Information and Communication Technology. Springer International Publishing.

56) Pyżalski, J. (2012). From cyberbullying to electronic aggression: Typology of the phenomenon. Emotional and behavioural difficulties, 17(3-4), 305-317.

57) Rafferty, R., & Vander Ven, T. (2014). I hate everything about you: A qualitative examination of cyberbullying and on-line aggression in a college sample. Deviant behavior, 35(5), 364-377.

58) Rao, T. S., Bansal, D., & Chandran, S. (2018). Cyberbullying: A virtual offense with real consequences. Indian journal of psychiatry, 60(1), 3.

59) Raskauskas, J., & Stoltz, A. D. (2007). Involvement in traditional and electronic bullying among adolescents. Developmental psychology, 43(3), 564.

60) Selkie, E. M., Fales, J. L., & Moreno, M. A. (2016). Cyberbullying Prevalence Among US Middle and High School–Aged Adolescents: A Systematic Review and Quality Assessment. Journal of Adolescent Health, 58(2), 125–133.

61) 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.

62) Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying?. Scandinavian journal of psychology, 49(2), 147-154.

63) Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. Computers in human behavior, 29(1), 26-32.

64) 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

65) 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.

66) 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.

67) Smith, P. K. (2012). Cyberbullying: Challenges and opportunities for a research program—A response to Olweus (2012). European journal of developmental psychology, 9(5), 553-558.

68) 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.

69) Smith, P. K., & Monks, C. P. (2008). Concepts of bullying: Developmental and cultural aspects. APublic HEALTH CONCERN, 3.

70) 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.

71) 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.

72) 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.

73) 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.

74) 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.

75) 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.

76) Valkenburg, P. M., & Peter, J. (2011). Online communication among adolescents: An integrated model of its attraction, opportunities, and risks. Journal of adolescent health, 48(2), 121-127.

77) Vandebosch, H., & Van Cleemput, K. (2008). Defining cyberbullying: A qualitative research into the perceptions of youngsters. CyberPsychology & Behavior, 11(4), 499-503.

78) Waasdorp, T. E., & Bradshaw, C. P. (2015). The overlap between cyberbullying and traditional bullying. Journal of Adolescent Health, 56(5), 483-488.

79) Wang, J., Iannotti, R. J., & Nansel, T. R. (2009). School bullying among adolescents in the United States: Physical, verbal, relational, and cyber. Journal of Adolescent health, 45(4), 368-375.

80) Willard, N. (2005). Cyberbullying and cyber threats. Washington: US Department of Education.

81) Wolke, D., Lee, K., & Guy, A. (2017). Cyberbullying: a storm in a teacup?. European child & adolescent psychiatry, 26(8), 899-908.

82) 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.

83) 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.

84) 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.

85) 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.

صیانت فرهنگی و سرمایه اجتماعی

دوره ۲، شماره۱، بهار ۱۴۰۱ ، صفحات ۹-۳۹

Cyberbullying: Definition, History and Typology

Seyyed Amir Qasim Tabar [1], Sayyed Abdullah Qasim Tabar [2]

[1] Faculty of Farhangian University, Central Organization, Tehran, Iran (corresponding author ghasemtabar.e@gmail.com)

[2] Central Organization Farhangian University, Tehran, Iran

Abstract

Despite the long-term and far-reaching negative consequences of cyberbullying, there is still no consensus on its definition and nature. The aim of the present study was to provide a definition, history and typology or forms of cyberbullying. The method of the present study was documentary. The research pupulation was all international written (print / electronic) sources on cyberbullying that could be retrieved and accessed through databases. For this purpose, using theoretical sampling method and after reviewing and analyzing the sources collected from the existing document community, among the sources (books, documents and articles) that met the inclusion criteria, were selected as a research sample. Electronic note taking method was used to analyze the documents. After reviewing and analyzing the sources, the evolution and formation of the concept of cyberbullying was explained, cyberbullying was defined and twelve forms of cyberbullying (Harassment, Denigration, Happy Slapping, Cyber Grooming, Flaming, Cyber stalking, Masquerading or Impersonation, Trickery, Outing, Catfishing, Exclusion, Ostracism, Sexual cyberbullying) were identified, defined and conceptualized. The present study has been able to provide valuable information about the nature and methods of cyberbullying for executive bodies and effective legislation in the field of crime prevention, while also for psychologists, educators and sociologists interested in research in the field of cyberbullying. It can be very useful.

Keywords: Cyberbullying, Online Bullying, Definition of Cyberbullying, Forms of Cyberbullying, History of Cyberbullying