A Model for an Aggression Discovery Through Person Online Behavior

Germanas Budnikas

A MODEL FOR AN AGGRESSION DISCOVERY THROUGH PERSON ONLINE BEHAVIOR

Germanas Budnikas

Faculty of Economics and Informatics in Vilnius, University of Bialystok, Lithuania
german.budnik@uwb.edu.pl

Faculty of Informatics, Kaunas University of Technology, Lithuania

Abstract. Reports on aggression acts are quite often in modern community. Its bigger part actively uses Internet resources. The paper considers a hypothesis on a presence of the relationship between real world aggressive behavior and behavior in Internet. The presented model assumes a conduction of aggression tests and monitoring web user online behavior. Gathered data serves as a training data set required for machine learning, which will let to classify an aggression through a person online behavior.

Keywords: online behavior, tracking, aggression, machine learning.

1 Introduction

One of the problems of nowadays community is aggressive behavior of its members. "Aggression is a forceful behavior, action, or attitude that is expressed physically, verbally, or symbolically. It may arise from innate drives or occur as a defense mechanism. It is manifested by either constructive or destructive acts directed toward oneself or against others" [1].

Aggressive behavior leads to negative outcomes and has a direct impact on a welfare of the society. These facts are continuously evidenced by mass media reports. Investigation of aggression at persons of all ages is important. This paper deals with aggression discovery model at adolescent persons of 17-18 years old through their online behavior.

The following is an outline of online activities that have a relationship to aggressive behavior found in psychological literature:

- Usage of violent media that includes viewing action films, playing violent computer games, and visiting violence-oriented Internet sites [2,3],
  ─ Playing violent game [4,5].
- Listening to aggressive music [6,7]. Some research have discovered that aggressive lyrics are more significant in forecasting hostile behavior than just an aggressive tone [7, 8].
- Cyber bullying [9, 10].

adfa, p. 1, 2011.

In other words, activities and interactions with the following Internet based resources can be associated with an aggressive behavior if it possess a violent content:

- Internet sites,
- Online games,
- Forums, posts in social media,
- Online music and video.

In order to be able to perceive a kind of activities performed onsite – violent and aggressive or friendly, it is vital to be able to track web user online actions with its content. Next, these data can be used for classification of a behavior.

Some recent works in online behavior tracking, classification of common patterns and prediction are outlined further (see Table 1) with respect to (w.r.t.) four parts: outcomes to be achieved, monitored online activities, experiment and used methods and techniques.

Table 1. Some recent works in the field (Source: self-made)

	Work by Gutschmidt [11]
Goals/outcomes:	To find significant behavioral differences between web task categories.
Monitored activity:	Mouse pointing, clicking, scrolling.
Experiment (data source, time):	Users documented a kind of task they implemented during browsing – fact-finding, information gathering, just browsing (45 users, 1 month).
Methods:	Descriptive analysis, mean value comparison and correlation analysis, testing hypotheses with mean value comparisons, machine learning methods, descriptive statistics of behavioral attributes, discriminant analysis.
	Work by Xian *et al* [12]
Goals/outcomes:	To predict undesirable network behaviors; to find a relationship between network services and types of services provided; to find trends and types of services provided in the same period.
Monitored activity:	Specific patterns and rules in network user behavior; time of using campus network; times and trends of using types of services provided; network use in different periods.
Experiment (data source, time):	Web site classification based on Open Directory Project (ODP) (ODP catalogue, information from calendar, class, institute, user's IP address, log data of router, DNS catalogue, E-card log data; 1 month).
Methods:	Data mining, statistical analysis.
	Work by Canali *et al* [13]
Goals/outcomes:	Risk prediction based on user web browsing behavior only (probability of visiting malicious web pages).
Monitored activity:	74 features grouped in: how much a user surfs the web; how diversified is the set of websites visited by a user; which website categories the user is mostly interested in; computer type; how popular are the websites visited by the user; how stable is the set of visited pages.
Experiment (data source, time):	Antivirus software on each of user computers that monitors user activity (160.000 users, 3 months).
Methods:	A correlation analysis (to see if any of the browsing factors is correlated with the probability of visiting malicious web pages); machine learning techniques to provide a prediction model that can be used to estimate the risk class of a given user.

Work by Ho *et al* [14]	
Goals/outcomes:	Model for interpreting online dialogues; classification of anomalous online behavior w.r.t. predefined model.
Monitored activity:	Online user social interaction through emails, blogs, online conversation.
Experiment (data source, time):	Analysis of dialogs in computer-mediated communication environments.
Methods:	Attribute assignment to certain words or actions; dyadic attribute model; computational analysis.

Work by Vachirapanang *et al* [15]	
Goals/outcomes:	To classify online game addiction level among adolescents; to find relationship between the playing data recorded and game addiction risk conditions and risk behaviors.
Monitored activity:	Game-playing periods and frequency, game-playing times, text-based chatting, mouse clicks and keyboard typing during the game.
Experiment (data source, time):	Real-time interaction-based behavior data from a program agent installed in PC (20 users, 2 months).
Methods:	Semi-structured interviews; constructing the user model using Waikato Environment for Knowledge Analysis (WEKA); validation method by decision tree; backpropagation neural networks.

Main objective of the paper is to propose a model that could enable to verify an existence of a relation between an aggression and person online activities in virtual environments using techniques of computer processing and recognition.

A research hypothesis – collected data about person behavior in virtual environments will permit to state about patterns of an aggressive behavior.

Need and *actuality* of the suggested investigation topic are defined by:

- Actual issues influenced by aggressive behavior of persons,
- Announced in the end of 2014 and actual call of Defense Advanced Research Projects Agency in the field of *Detection and computational analysis of psychological signals* [16],
- Recent works in the field of classification and interpretation of a behavior in virtual environments [11,12,13,14,15],
- Existence of theoretical [17] and practical [18] techniques for implementation of behavioral change. This fact permits to consider a possibility to influence aggressive persons online that can be discovered using the model proposed in the given paper.

The paper is structured in the following manner. Section 2 describes general schema of the model proposed in the paper and gives details on implementing the model too. Differences and similarities of the proposed model to the works in the alike topic are presented in the succeeding section. Conclusion summaries the proposed approach.

2 Model construction

2.1 General schema

In order to recognize a kind of aggressive behavior in virtual environments like those that were mentioned in the Introduction section – web portals, online games and social media, a supervised machine learning can be applied. A training data set for such a system is composed in two steps.

At the first one, respondents are assigned with unique identifiers and are interviewed using psychological aggression questionnaires[1]. An outcome of the interviews is a division of respondent groups into subgroups with respect to their aggression types or non-aggression property. Additionally, each respondent possesses some psychological portrait drawn by conclusions of filled-out questionnaires in terms of discovered additional aggression types.

At the second step, respondents are asked to log to a dedicated web portal that contains elements of the following types (see first layer at Figure 1):

- Online game,
- Online chat, forum, text,
- Image gallery,
- Hyperlinks,
- Media clips (sound and video).

Web portal collects data about web user interactions with or within a specific portal element. For example, it is possible to monitor user actions undertaken during online game, either to collect user votes on images of different categories. All these data joined with the data from the first step produce a training set (see second layer at Figure 1), which is used by a supervised machine learning. The later technique permits to develop a model for an aggression type discovery (see third layer at Figure 1). Additionally, as each respondent might been classified by additional aggression types, like proactive and reactive aggression [20], another classification and analysis experiments with the training data set are possible in order to define a behavioral pattern w.r.t. aggression types discovered during the first step. While building a model for machine learning, initial experiments are to be performed using representative training set that are generated using the special technique [23] based on *k*-nn and genetic algorithms.

---

[1] As stated in [19], efficiency of the revised version of the inventory of psychological aggression syndrome IPSA-II [20] increases in case of application of additional inventories. Two more questionnaires might be applied – the aggression questionnaire by Buss & Perry [21] and multi-scale inventory of aggression by Choynowski [22]. Mentioned questionnaires cover aggression types analyzed in the paper, i.e. physical, verbal, without physical or verbal contact and inward aggression [19], and may discover additional aggression types like proactive and reactive aggression.

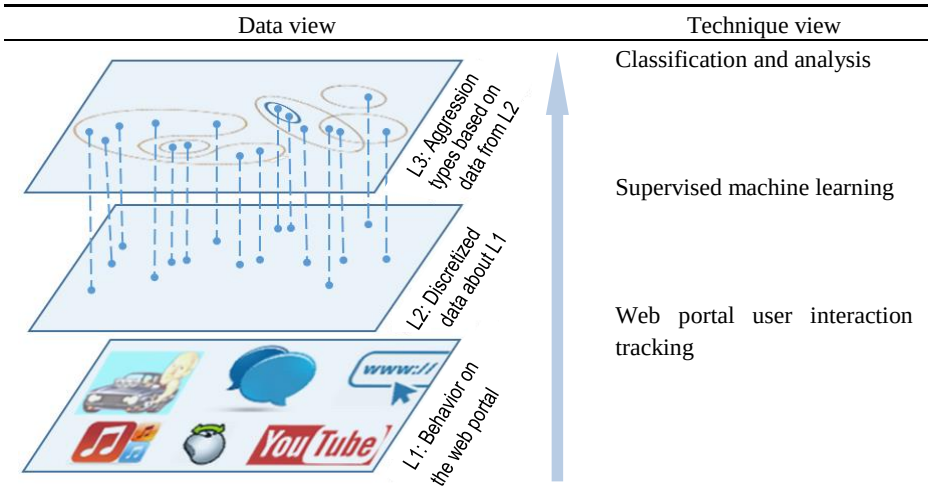

Fig. 1. General schema of the proposed model (Source: self-made)

Next sub-section explains model implementation issues in more detail.

2.2 Details on model implementation

A key functional point in the proposed approach is a monitoring of web user onsite behavior. Such data gathering is quite popular and useful for achievement of stated goals [11], [24].

User behavior with web portal elements is context specific and needs to be represented in such a general form to compose a joint training data set. Such representation is offered in a form of a semantic network, presented in Figure 2. Here, in the Figure 2, an action category is defined with respect to the characteristic property of the applied aggression type as shown in Table 2.

Table 2. Characteristic properties of aggression types considered in the work (Source: self-made using [1], [19])

Aggression type			
Physical	Verbal	Without physical or verbal contact	Inward
° beating, ° pushing, ° spitting ° destruction of property, ° forcing to perform some activities.	° insults, ° threats, ° black-mailing.	° grimaces, ° hostile gestures, ° isolation – limitation of actions (e.g. blocking in the rooms).	° destructive behavior directed against oneself.

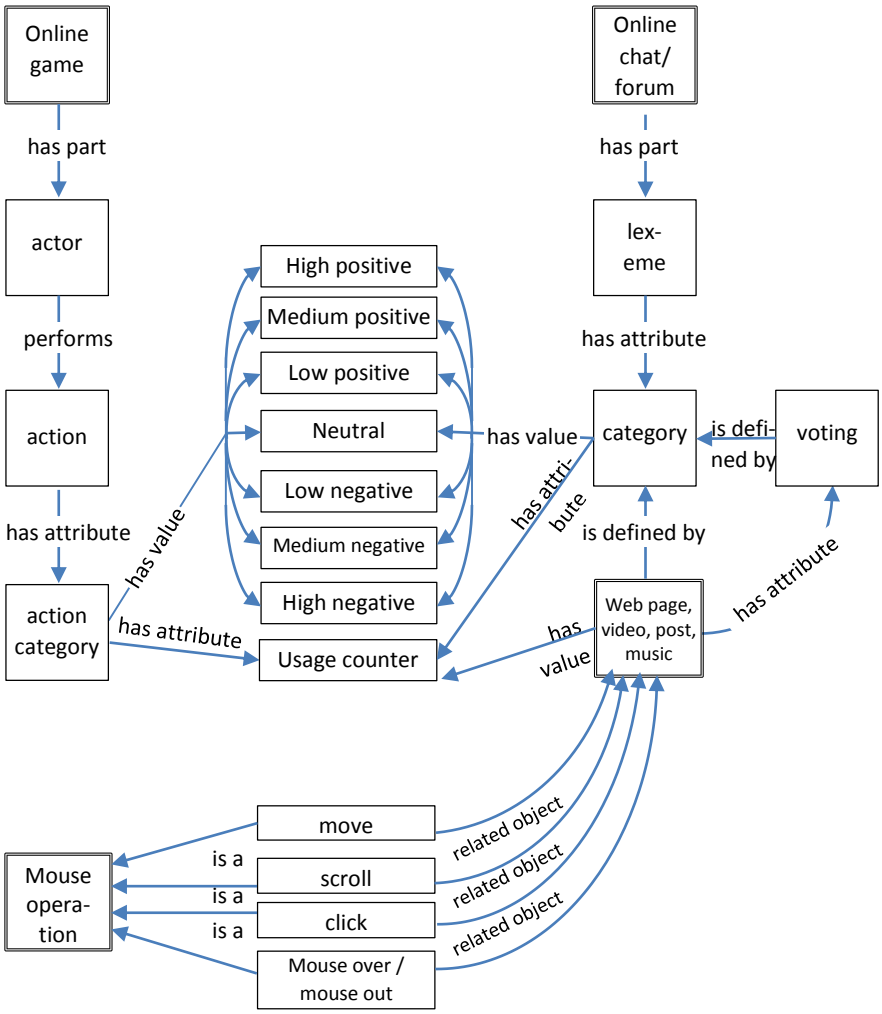

Fig. 2. Discretization of different activities on the web portal for composition of a training data (Source: self-made)

The semantical network shows how user behavior in web portal elements is discretized into pieces of data, which are used for an analysis. The model foresees a creation of an online role-playing game (RPG), which players interact between themselves and with game bots by actions enlisted in Table 2. As seen from the Figure 2, action category may have negative or positive values[2]. A number of application of actions belonging to certain categories is recorded in corresponding usage counters. An online chat consists of exchange of predefined lexemes that are of a certain category and its usage

[2] In order to evaluate a certain aggression type, its two marginal behaviors must present – an aggressive and a friendly.

counters are employed in the analysis too. A number of visited web pages and/or read web posts of a certain category is evaluated during the analysis as well. Web pages and/or web posts may be assessed by certain category votes. In addition, as it was mentioned in the review (see Table 1), mouse operations have to be taken into account.

Another important issue in this approach is assignment of categories for those web portal elements, which content is continuously updated or has a bigger volume – text and video clips. Following table briefly outlines techniques to be applied for categorization of big volumes of text and video content (see Table 3).

Table 3. Suggested categorization techniques for text and video information sources (Source: self-made)

Web portal content type(s)	Suggested categorization technique
° text (song lyrics, chat post, news feeds), ° hyperlinks to web sites.	Text categorization using aggressive feature selection [25] permits a solution of text categorization problem that are characterized by many redundant features using classification technique C4.5.
° video clips.	Multimodal and ontology-based fusion approaches of audio and visual processing for violence detection in movies [26] uses multimodal approach that provides binary decisions on the existence of violence or not, and employs machine learning techniques and an ontological and reasoning techniques, that combine the audio-visual cues with violence and multimedia ontologies.

The approach presented above outlines a model construction based on training data. However, in order to successfully use the model in practice, the following must be taken into consideration. Recent research [27,28] has shown a correlation between demographic variables like sex and location, thus, these parameters must be derived from behavioral data too. Location data may be obtained by querying IP address location function, while mining gender information from visited web pages and read texts is possible using Support Vector Machine Regression technique [29,30] as described in [31].

Data about user online behavior can be gathered from a website by means of Event Tracking method (a part of Google Analytics Tracking Code) that enables recording user interaction with website elements, such as embedded AJAX page element, page gadgets, Flash-driven element and so on which are the parts of online game.

Planned period of data collection is influenced by a desired model accuracy and is equal to minimum two months duration in case of daily use of the web portal. Collected data from the web portal will be analyzed by methods that were outlined in Table 1.

3 Related works

A review of the related works is given in Table 4 with respect to the three criteria – research model, differences and similarities with the topics presented in this paper.

Table 4. Review of the related works (Source: self-made)

Goals	Model	Similarities	Differences
Work by Law *et al* [32]			
to investigate reactive and proactive online aggression.	completion of self-reported questionnaires.	use of aggression test inventories.	three is no tracking of online behavior; there is no machine learning (ML).
Work by France *et al* [33]			
to identify prevention efforts to impact reasons for cyberbullying.	completion of self-reported questionnaires.	online survey on web portal elements similar to ones listed in Sec. 2.1.	the same as previous.
Work by Canali *et al* [13]			
to test an aggression in an online game.	completion of self-reported questionnaires before and after playing the game	use of aggression test inventories, use of game.	the same as previous.
Work by Ho *et al* [14]			
to interpret online dialogues; to classify anomalous online behavior w.r.t. predefined model.	online RPG game, provocation of online user communication and behavior	interpretation of texts, behavior tracking.	used techniques for text classification.
Work by Bidel *et al* [34]			
to investigate various statistical ML models for the categorization and tracking of user navigation behaviors in rich hypermedia systems.	questionnaire based generation of data related to user behavior on the web; application of various ML methods.	tracking of user behavior on the web; behavior models and behavior categorization are similar to discovering different behaviors w.r.t. aggression types.	application area; scope and depth of analyzed web media.

Conclusions and Discussion

Pros and cons of the suggested model are discussed in this section. Although the paper does not contain experimental part – only the model has been proposed, some assumptions can be made on the applicability of the proposed model. It may serve as a basis for:

- development of machine learning techniques for an analysis of a relationship between behavior in virtual environments and properties of aggressive behavior,
- succeeding investigations of dependencies between other psychological patterns and actual person behavior in virtual environments,
- enabling a selection and classification of persons, who should be covered by actions of prophylactic either therapeutic nature with respect to discovered aggression types,

- development of behavior impact methods using virtual environments similar to [17,18].

Weaknesses of the suggested approach are twofold – issues of implementation and scalability. Creation of the web portal to be so interesting and continuously updating in order adolescents would use it in a natural way during all period of investigations is a challenging task. An agreement with the existing popular web resource might be a solution. Another issue is that the suggested model assumes application of several methods, which computational complexity has not been evaluated yet. This sets prerequisites for the future work.

Acknowledgement

I express a gratitude to Professor Władysław Homenda from Warsaw University of Technology for his opinion and remarks on the topic presented in this paper.

References

1. Mosby's Medical Dictionary, http://medical-dictionary.thefreedictionary.com/
2. Slater, M. D.: Alienation, aggression, and sensation seeking as predictors of adolescent use of violent film, computer, and website content. Journal of Communication, 53(1), 105-121 (2003)
3. Slater, M. D., Henry, K. L., Swaim, R. C., Anderson, L. L.: Violent media content and aggressiveness in adolescents a downward spiral model. Communication Research, 30(6), 713-736 (2003)
4. Anderson, C. A., Sakamoto, A., Gentile, D. A., Ihori, N., Shibuya, A., Yukawa, S., Kobayashi, K.: Longitudinal effects of violent video games on aggression in Japan and the United States. Pediatrics, 122(5), e1067-e1072 (2008)
5. Willoughby, T., Adachi, P. J., Good, M.: A longitudinal study of the association between violent video game play and aggression among adolescents. Developmental psychology, 48(4), 1044 (2012)
6. Coyne, S. M., Padilla-Walker, L. M.: Sex, violence, & rock n'roll: Longitudinal effects of music on aggression, sex, and prosocial behavior during adolescence. Journal of adolescence, 41, 96-104 (2015)
7. Mast, J. F., McAndrew, F. T.: Violent lyrics in heavy metal music can increase aggression in males. North American Journal of Psychology, (13), 63-64 (2011)
8. Lennings, H. I. B., Warburton, W. A.: The effect of auditory versus visual violent media exposure on aggressive behaviour: the role of song lyrics, video clips and musical tone. Journal of Experimental Social Psychology, 47(4), 794-799 (2011)
9. Moore, M. J., Nakano, T., Enomoto, A., Suda, T.: Anonymity and roles associated with aggressive posts in an online forum. Computers in Human Behavior, 28(3), 861-867 (2012)
10. Buelga, S., Cava, M. J., Musitu, G.: Cyberbullying: adolescent victimization through mobile phone and internet. Psicothema, 22(4), 784-789 (2010)
11. Gutschmidt, A.: Classification of User Tasks by the User Behavior: Empirical Studies on the Usage of On-Line Newspapers. Berlin GmbH: Logos Verlag (2013)

12. Xian, X., Chen, F., Wang, J.: An Insight into Campus Network User Behavior Analysis Decision System. In Computer, Consumer and Control (IS3C), IEEE, 537-540 (2014)
13. Canali, D., Bilge, L., Balzarotti, D.: On the effectiveness of risk prediction based on users browsing behavior. Proceedings of the 9th ACM symposium on Information, computer and communications security. ACM New York, 171-182 (2014)
14. Ho, S. M., Timmarajus, S. S., Burmester, M., Liu, X.: Dyadic Attribution: A Theoretical Model for Interpreting Online Words and Actions. In Social Computing, Behavioral-Cultural Modeling and Prediction, Springer International Publishing, 277-284 (2014)
15. Vachirapanang, K., Sinthupinyo, S., Tuisima, S., Sirivunnabood, P.: The Classification of the Real-Time Interaction-Based Behavior of Online Game Addiction in Children and Early Adolescents in Thailand. International Journal of Advanced Research in Artificial Intelligence 1 (7): 7-13 (2012)
16. Defence Advanced Research Projects Agency: Detection and computational analysis of psychological signals (DCAPS). NY. Information Innovation Office (2014).
17. Bosse, T., Provoost, S.: Towards Aggression De-escalation Training with Virtual Agents: A Computational Model. In Learning and Collaboration Technologies. Technology-Rich Environments for Learning and Collaboration, Springer International Publishing, 375-387 (2014)
18. Klein, M., Mogles, N., van Wissen, A.: Intelligent mobile support for therapy adherence and behavior change. Journal of biomedical informatics, 51, 137-151 (2014)
19. Sajewicz-Radtke, U., Radtke, B. M., Kalka, D.: Kwestionariusz agresywności młodzieży-reaktywność emocjonalna: normy dla młodzieży ponadgimnazjalnej. Pracownia Testów Psychologicznych i Pedagogicznych SEBG (2014)
20. Gaś, Z. B.: Zrewidowana wersja Inwentarza psychologicznego syndromu agresji–IPSA-II. Przegląd Psychologiczny, 30 (4), 1003-1016 (1987)
21. Buss, A. H., Perry, M. P.: The aggression questionnaire. Journal of Personality and Social Psychology, 63, 452-459 (1992)
22. Choynowski, M.: Agresywność: pomiar i analiza psychometryczna. Warszawa: Polskie Towarzystwo Psychologiczne (1998)
23. Gabryel, M., Woźniak, M., Nowicki, R. K.: Creating learning sets for control systems using an evolutionary method. In Swarm and Evolutionary Computation, Springer Berlin Heidelberg, 206-213 (2012)
24. Budnikas, G.: Research on user online behavior. Statistics in Transition (2015) (in press)
25. Gabrilovich, E., Markovitch, S.: Text categorization with many redundant features: Using aggressive feature selection to make SVMs competitive with C4.5. In Proceedings of the twenty-first international conference on Machine learning, ACM, 41-50 (2004)
26. Perperis, T., Giannakopoulos, T., Makris, A., Kosmopoulos, D. I., Tsekeridou, S., Perantonis, S. J., Theodoridis, S.: Multimodal and ontology-based fusion approaches of audio and visual processing for violence detection in movies. Expert Systems with Applications, 38(11), 14102-14116 (2011)
27. Sakellaropoulos, A., Pires, J., Estes, D., Jasinski, D.: Workplace aggression: assessment of prevalence in the field of nurse anesthesia. AANA journal, 79 (4 Suppl), S51-7 (2011)
28. Lemmens, J. S., Valkenburg, P. M., Peter, J. The effects of pathological gaming on aggressive behavior. Journal of youth and adolescence, 40(1), 38-47 (2011)
29. Homenda, W., Luckner, M., Pedrycz, W.: Classification with rejection based on various SVM techniques. In Proceedings of the 2014 International Joint Conference on Neural Networks (IJCNN), IEEE, 3480-3487 (2014)
30. Homenda, W., Jastrzebska, A., Pedrycz, W., Piliszek, R.: Classification with a limited space of features: Improving quality by rejecting misclassifications. In Proceedings of the 2014

Fourth World Congress on Information and Communication Technologies (WICT), IEEE, 164-169 (2014)
31. Hu, J., Zeng, H. J., Li, H., Niu, C., Chen, Z.: Demographic prediction based on user's browsing behavior. In Proceedings of the 16th international conference on World Wide Web, ACM, 151-160 (2007)
32. Law, D. M., Shapka, J. D., Domene, J. F., Gagné, M. H.: Are cyberbullies really bullies? An investigation of reactive and proactive online aggression. Computers in Human Behavior, 28(2), 664-672 (2012)
33. France, K., Danesh, A., Jirard, S.: Informing aggression–prevention efforts by comparing perpetrators of brief vs. extended cyber aggression. Computers in Human Behavior, 29(6), 2143-2149 (2013)
34. Bidel, S., Lemoine, L., Piat, F., Artieres, T., Gallinari, P.: Statistical machine learning for tracking hypermedia user behavior. In Proceeding of the 2nd Workshop on Machine Learning, Information Retrieval and User Modeling (2003)