Computers in Human Behavior 36 (2014) 76–81

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Research Report

Social categorization and right-wing authoritarianism in reporting potential terrorist threats in cyberspace

Marek Palasinski *, Jacek Granat, Kyoung Ok Seol, Lorraine Bowman-Grieve

University of Derby, UK
University of Gdansk, Poland
Ewha Womans University, South Korea
Waterford Institute of Technology, Republic of Ireland

ARTICLE INFO

Article history:
Available online 14 April 2014

Keywords:
Internet
Self-categorization
Terrorist threat

ABSTRACT

Two studies, which took social categorization and right-wing authoritarianism into account two factors unexamined jointly in previous research, explored reporting of potential terrorist threats in cyberspace in a generally Muslim-intolerant 'Eastern European' setting. In *Study 1*, 92 white men observed a simulated online encounter between an anti-Muslim extremist and two of his apparent followers '*planning to do something big and violent*.' The results show that participants took less time to respond to the terrorist threat if Muslims were referred to in terms of a broad European identity rather than a narrow national identity, but only when participants were primed with the broad identity. In *Study 2*, where a separate group of 100 white men observed the same encounter, the focus was put on the mono-cultural and multicultural primes of their national identity. The response time was shorter when participants were primed with the multicultural contents, but only when the Muslim outgroup was described in terms of national rather than European inclusion. Providing theoretical guidelines for facilitating the reporting of potential terrorist threats in cyberspace, this work complements the classical social identity model of helping by revealing new layers of complex interactive categorization and their potential application to mobilizing counter-terrorist community responses.

1. Introduction

Given far-right extremist Anders Breivik's open expression of his views online, which included his calls for the violent annihilation of 'Eurabia' and multiculturalism, as well as the deportation of all Muslims from Europe, one may wonder at the ease with which he carried out the 2011 Oslo and Utøya attacks that cost 77 lives. According to the UK's first research centre into contemporary fascism, in the recent years right-wing groups radicalised thousands of people online, encouraging them to seek alternative and violent ways to express their opposition to Islam, immigration and economic stagnation (Brown, 2012). Accounting for the importance of prejudice reduction by redrawing social category boundaries (Sapountzis, Figgou, Bozatzis, Gardikiotis, & Pantazis, 2012) leads to a question about how cyberbystanders (i.e., Internet users spotting interactions indicative of impending abuse and violence), can be motivated to hamper extremists. Some of such extremists, in particular the independently acting 'lone wolf' (Spaaij, 2012, p.2) type, who appear to be less traceable and more unpredictable than terrorist cell members, are unlikely to be stopped by surveillance alone (Brown & Korff, 2009). This leaves scope for the online community to step in and intervene.

Although the idea that group size is inversely related to the likelihood of intervention was consolidated by two meta-analyses (Fischer et al., 2011; Latané & Nida, 1981), finding confirmation in research on social rule violation (Chekroun & Brauer, 2002), computer chat groups (Markey, 2000; Palasinski, 2012) and online Internet forums (Voelpel, Eckhoff & Förster, 2008), the dimension of social category relations also appears to be important (Cherry, 1995; Levine, Cassidy, & Brazier, 2002; Levine, Prosser, Evans, & Reicher, 2005). Self-categorization theory (Turner, Hogg, Oakes, Reicher, & Wetherell, 1987) suggests that intervention-conducive bystander cohesion is created by a perceived similarity of needs, goals and interchangeable interests, making people feel a sense of connectedness with others (Dovidio, Piliavin, Gaertnel, Schroeder, & Clark, 1991; Sassenberg & Boos, 2003; Spears, Lea, & Lee, 1990). The other pole of the spectrum is taken by extreme acts of inhumanity, including terrorism, which an integrative five-step

* Corresponding author. Address: University of Derby, Department of Psychology, Kedleston Road, Derby DE22 1GB, UK. Tel.: +44 770959100.
E-mail address: marekpalasinski@hotmail.com (M. Palasinski).

http://dx.doi.org/10.1016/j.chb.2014.03.049
0747-5632/

social identity model (Reicher, Haslam, & Rath, 2008) explains in terms of celebrating them as acts of virtue. Specifically, the model clarifies how such celebration is possible through (a) the creation of a cohesive ingroup through shared social identification; (b) the exclusion of specific populations from the ingroup; (c) the constituting of the outgroup as a danger to the existence of the ingroup; (d) the representation of the ingroup as uniquely virtuous; and (e) the celebration of outgroup annihilation as the defence of (ingroup) virtue.

Given the strategic role of identities in cyberspace (Chia-Ping & Mei-Lein, 2008; Talamo & Ligorio, 2001), as well as the finding that anonymous group discussions lead to more influence under the salience of a shared social identity (Postmes, Spears, Sakhel, & de Groot, 2001), it is worth exploring how the manipulation of identities might be used to facilitate the reporting of potential terrorist threats in generally anonymous chatrooms. Although there are studies exploring terrorism in cyberspace (Ginges, Atran, Sachdeva, & Medlin, 2011; Jacobson, 2010; Levin, 2002; Soriano, 2012) and those examining bystander responses to violent incidents in immersive virtual environments (Slater et al., 2013), ours are the first ones that tackle the issue of real-time threat reporting, paving the way for the following three key questions: Q1 how can social identities be used to mobilize chatroom users to report potential terrorist threats? Q2 how could social identity contents serve such mobilization? Q3 what are its theoretical and practical implications? As one's identity often depends on the perceived salience of a given place (Dixon & Durrheim, 2001), this process might allow for recategorizing a former outgroup as part of the ingroup (Levine & Thompson, 2004). Drawing on the finding that the role of closely-knit social networks appears to be far greater in instigating terrorism than individual factors (Ginges et al., 2011), and in responding to the call for exploring the systems of categorization and psychological boundaries (Chryssochoou's, 2000), we ran two related cybersecurity studies.

2. Study 1

Building on a study that manipulated group boundaries of 'place identities' in a Western setting (UK) (Levine & Thompson, 2004), we took into account factors that 'place identities' are subtly, but frequently intertwined with, such as religious affiliations. In this study, we used a European setting where the national identity is closely tied in with Christianity and where Islam is generally not tolerated (Day, 2009; Hetnal, 1999) – 38 million-strong Poland. Specifically, we used a Polish national identity and a European 'pan-national' identity as primes for Polish participants in this study. Whereas, the former is narrowly defined and connotes national borders, the latter is more loosely defined and has a supranational character.

Drawing on the social identity literature on helping, which suggests that primes of broad social identity can extend the boundaries of social inclusiveness to the outgroup and lower its perceived outgroupness (Levine & Thompson, 2004; Reicher, Cassidy, Wolpert, Hopkins, & Levine, 2006; Reicher, Hopkins, & Harrison, 2006), we formulated two hypotheses. Firstly, we anticipated that participants exposed to the salience of the European identity would take less time to respond to a terrorist threat aimed at the Muslim outgroup than participants primed with the Polish identity. Secondly, we also anticipated that this would particularly be the case if the Muslim outgroup was referred to as European rather than as Polish. In other words, the salience of European and national identities were expected to respectively recategorize the Muslim outgroup as less and more of an outgroup. Thus, we anticipated that when the Muslim outgroup was referred to as European, participants would take less time to respond to a terrorist threat aimed at the Muslim outgroup than when the Muslim outgroup was referred to as Polish.

2.1. Method

2.1.1. Design, participants and procedure

The study was a 2 (Level of Muslim Belongingness: European/Polish) × 2 (Participant Identity Prime: European/Polish) design. We placed online adverts inviting participants to an exploration of responses to extremism in cyberspace. A total of 92 non-psychology university student volunteers who answered our adverts took part in this study. Their mean age was 20. Given that political chatrooms are more likely to be visited by men than by women (Harcourt, 2000), in the two studies all participants were Polish male and participated only once. When they arrived for the study, one of the authors introduced himself by name, thanked them for coming and informed them that he was interested in Internet chatrooms. He also advised them of the sensitive nature of the pre-programmed simulation[1] and asked for signed informed consent that allowed them to leave the study anytime they wished. All participants completed the experiment, were given an educational debriefing form and any additional questions pertaining to the experiment were addressed.

Participants were randomly divided into 46 pairs of two, and each pair participated in the study separately. Using such paired groups and measures in sensitive virtual reality simulations has been shown to be relatively easy, methodologically sound and ethically acceptable, enhancing the sense of chatroom co-user presence that could be seen as authentically human rather than computer-generated (Palasinski, 2012). By limiting the intervention types and increasing experimental control, this approach also allowed for a more exclusive focus on social identity processes. The first set of 23 pairs was assigned to Subgroup A and *'invited to an exploration of the Polish identity,'* and the remaining second set of 23 pairs was assigned to Subgroup B and *'invited to an exploration of the European identity'* (2 Participant Identity Primes). The focus of the Polish media and the educational system on these two identity types make them readily salient in Polish minds, lending support to their use in this research. All the pairs came from five different departments and their members reported not knowing each other.

Using number-coded slips of paper and drawing lots, participants were randomly assigned to the two sub-groups. Each pair then sat individually at different computers in opposite cubicles and their members could no longer see and communicate with each other.

When requested to click on the central Start Button, a program written in Java guided participants automatically. The computer informed participants that although they could not make any comments or see each other's input, they would see the symbolical presence of each other as *'chatroom users'* and that they would have up to 100 s (the exchange duration) to simultaneously engage in both of two actions: *'alerting the Internet administrator and the police.'*

Drawing on the proven usefulness of these two channels of intervention in online sexual abuse emergencies (Palasinski, 2012), participants could thus be provided with some of the most practical, available and easiest opportunities to intervene. On the one hand, alerting the administrator might be seen as signalling some major breach of cyber rules and regulations on a civilian level, on the other hand, alerting the police might be seen as signalling a more serious danger on a criminal level. Given a range of technological and ethical challenges, it was clarified that the

[1] Leading participants to believe that they would observe genuine real-time chatter featuring an authentic terrorist threat would be more difficult to control and carry the risk of serious ethical and legal problems.